

FATF



# Anti-money laundering and counter-terrorist financing measures

## Germany

### Mutual Evaluation Report

August 2022





The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard.

For more information about the FATF, please visit the website: [www.fatf-gafi.org](http://www.fatf-gafi.org).

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

**This assessment was adopted by the FATF at its June 2022 Plenary meeting.**

Citing reference:

FATF (2022), *Anti-money laundering and counter-terrorist financing measures –Germany*,  
Fourth Round Mutual Evaluation Report, FATF, Paris  
<http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-germany-2022.html>

©2022 FATF/OECD - All rights reserved.

No reproduction or translation of this publication may be made without prior written permission.

Applications for such permission, for all or part of this publication, should be made to

the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France

(fax: +33 1 44 30 61 37 or e-mail: [contact@fatf-gafi.org](mailto:contact@fatf-gafi.org)).

Photo Credit - Cover: © Gettyimages

## Table of Contents

<b>Executive Summary .....</b>	<b>3</b>
Key Findings.....	3
Risks and General Situation .....	7
Overall Level of Compliance and Effectiveness .....	8
Priority Actions.....	14
<b>MUTUAL EVALUATION REPORT.....</b>	<b>17</b>
Preface .....	17
<b>Chapter 1. ML/TF RISKS AND CONTEXT.....</b>	<b>19</b>
ML/TF Risks and Scoping of Higher Risk Issues.....	21
Materiality.....	25
Structural Elements .....	26
Background and Other Contextual Factors .....	26
<b>Chapter 2. NATIONAL AML/CFT POLICIES AND CO-ORDINATION.....</b>	<b>39</b>
Key Findings and Recommended Actions.....	39
Immediate Outcome 1 (Risk, Policy and Co-ordination).....	42
<b>Chapter 3. LEGAL SYSTEM AND OPERATIONAL ISSUES.....</b>	<b>55</b>
Key Findings and Recommended Actions.....	55
Immediate Outcome 6 (Financial Intelligence ML/TF) .....	59
Immediate Outcome 7 (ML Investigation and Prosecution) .....	73
Immediate Outcome 8 (Confiscation).....	88
<b>Chapter 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION.....</b>	<b>101</b>
Key Findings and Recommended Actions.....	101
Immediate Outcome 9 (TF investigation and prosecution).....	104
Immediate Outcome 10 (TF preventive measures and financial sanctions) .....	120
Immediate Outcome 11 (PF financial sanctions) .....	133
<b>Chapter 5. PREVENTIVE MEASURES .....</b>	<b>139</b>
Key Findings and Recommended Actions.....	139
Immediate Outcome 4 (Preventive Measures).....	141
<b>Chapter 6. SUPERVISION .....</b>	<b>161</b>
Key Findings and Recommended Actions.....	161
Immediate Outcome 3 (Supervision).....	164
<b>Chapter 7. LEGAL PERSONS AND ARRANGEMENTS.....</b>	<b>197</b>
Key Findings and Recommended Actions.....	197
Immediate Outcome 5 (Legal Persons and Arrangements).....	200
<b>Chapter 8. INTERNATIONAL COOPERATION .....</b>	<b>213</b>
Key Findings and Recommended Actions.....	213
Immediate Outcome 2 (International Cooperation) .....	214

<b>TECHNICAL COMPLIANCE</b> .....	<b>231</b>
Recommendation 1 – Assessing risks and applying a risk-based approach .....	231
Recommendation 2 - National Cooperation and Co-ordination .....	233
Recommendation 3 - Money laundering offence.....	237
Recommendation 4 - Confiscation and provisional measures .....	238
Recommendation 5 - Terrorist financing offence .....	240
Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing .....	242
Recommendation 7 – Targeted financial sanctions related to proliferation .....	249
Recommendation 8 – Non-profit organisations.....	253
Recommendation 9 – Financial institution secrecy laws.....	257
Recommendation 10 – Customer due diligence.....	257
Recommendation 11 – Record-keeping .....	262
Recommendation 12 – Politically exposed persons.....	263
Recommendation 13 – Correspondent banking .....	264
Recommendation 14 – Money or value transfer services .....	265
Recommendation 15 – New technologies.....	266
Recommendation 16 – Wire transfers .....	269
Recommendation 17 – Reliance on third parties .....	271
Recommendation 18 – Internal controls and foreign branches and subsidiaries.....	272
Recommendation 19 – Higher-risk countries.....	273
Recommendation 20 – Reporting of suspicious transaction.....	274
Recommendation 21 – Tipping-off and confidentiality.....	274
Recommendation 22 – DNFBPs: Customer due diligence .....	275
Recommendation 23 – DNFBPs: Other measures .....	276
Recommendation 24 – Transparency and beneficial ownership of legal persons .....	277
Recommendation 25 – Transparency and beneficial ownership of legal arrangements .....	286
Recommendation 26 – Regulation and supervision of financial institutions .....	288
Recommendation 27 – Powers of supervisors .....	290
Recommendation 28 – Regulation and supervision of DNFBPs .....	291
Recommendation 29 - Financial intelligence units .....	294
Recommendation 30 – Responsibilities of law enforcement and investigative authorities.....	295
Recommendation 31 - Powers of law enforcement and investigative authorities .....	297
Recommendation 32 – Cash Couriers.....	299
Recommendation 33 – Statistics.....	301
Recommendation 34 – Guidance and feedback .....	301
Recommendation 35 – Sanctions .....	302
Recommendation 36 – International instruments .....	305
Recommendation 37 - Mutual legal assistance .....	305
Recommendation 38 – Mutual legal assistance: freezing and confiscation.....	307
Recommendation 39 – Extradition .....	309
Recommendation 40 – Other forms of international co-operation.....	310
<b>Annex A. Länder supervisors of DNFBPs</b> .....	<b>313</b>
<b>Annex B. Overview of Germany’s obliged non-financial sector</b> .....	<b>319</b>
<b>Summary of Technical Compliance – Key Deficiencies</b> .....	<b>320</b>
<b>Glossary of Acronyms</b> .....	<b>324</b>

## Executive Summary

1. This report summarises the anti-money laundering and counter-terrorist financing (AML/CFT) measures in place in Germany as at the date of the on-site visit from 1 to 19 November 2021. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Germany's AML/CFT system, and provides recommendations on how the system could be strengthened.

### Key Findings

- a) Germany has made significant improvements to its AML/CFT framework over the past five years, including using the National Risk Assessment (NRA) process to develop a stronger national understanding of money laundering/terrorist financing (ML/TF) risks, establishing mechanisms to improve co-operation and co-ordination between Federal and state (*Länder*) governments, significantly boosting human resources to the main financial sector supervisor (BaFin) and the Financial Intelligence Unit (FIU) to increase their capabilities, removing limitations in asset recovery and the ML offence and putting in place the Transparency Register to improve access to information on beneficial ownership. While technical compliance with the FATF Standards is generally strong, some of the recent reforms are not yet fully effective.
- b) Based largely on its first NRA (2019), Germany has a good understanding of the risks related to real estate and the banking sector, and emerging risks from the COVID-19 pandemic and virtual assets. Risks related to cash and cross-border risks are well-understood (with the exception of risks related to unaccompanied cash). ML risk understanding is still developing in some areas, particularly relating to complex ML, professional enablers and the use of legal entities, partly as a result of information gaps, previous issues in the ML offence, and limited involvement of some sectors in the NRA. Germany has taken steps to mitigate identified risks in the real estate sector. Additional measures are required to more effectively mitigate the risks in relation to cash and *hawala* services.

- c) Germany has taken important recent steps to improve co-operation and co-ordination issues identified in its 2010 FATF mutual evaluation report (MER). Germany's new public-private partnership, the Anti-Financial Crime Alliance (AFCA), is a positive step and should be developed further. While co-operation has improved, ensuring co-ordination between and across the *Länder*, particularly with the over 300 DNFBP supervisors, remains challenging.
- d) Germany has taken a number of positive steps to strengthen the role of the FIU and improve the quality of financial intelligence. However, there is scope to further improve access and use of financial intelligence held by the FIU and better align FIU analysis with the operational needs of law enforcement authorities (LEAs). While the FIU and LEAs have access to, and use, a broad range of financial intelligence sources; processes could be improved and made more efficient by continuing to equip the FIU with tools to process and analyse available data, including through the use of artificial intelligence or other advanced analytics.
- e) Germany has demonstrated a commitment to investigating and prosecuting ML at the policy level. However, it is not clear that this commitment has fully translated into results at the operational level. The overall number of ML cases that progress to prosecution is lower than expected and is not fully aligned with Germany's risk profile.
- f) Germany introduced non-conviction based asset confiscation laws in 2017 and also made asset confiscation a mandatory consideration for prosecutors in every case. These legal and policy changes have been supported by an increase in resourcing that has led Germany to achieve impressive asset confiscation outcomes over the last five years. However, cross-border cash smuggling risks (particularly through mail and cargo) are not well recognised.
- g) TF activity is effectively investigated, prosecuted and disrupted in Germany using a range of offence provisions. Germany is proactive in pursuing the investigation of TF activity alongside terrorism-related investigations and has demonstrated capacity and willingness to use all available measures to disrupt TF activity including banning organisations and other measures to combat violent extremism.
- h) Understanding and mitigation of TF risks in Germany's non-profit organisation (NPO) sector is strong and proportionate. While Germany has sponsored United Nations (UN) designations, it does not proactively designate individuals and entities in line with its risks and context or use targeted financial sanctions (TFS) to support its broader TF and counter-terrorism strategy. Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) are generally aware of their TFS obligations, although monitoring of TFS compliance is complex and not fully effective (particularly in the DNFBP sectors). There are a range of domestic measures available to deprive terrorists and financers of assets, although these have limitations and some measures could be better exploited. The overall

amounts frozen are low compared to the total amounts raised in Germany.

- i) Germany requires all FI and DNFBP sectors (and many additional non-financial sectors) to implement preventive measures. Larger FIs and virtual asset service providers (VASPs), particularly major banks, MVTS, insurance providers, and VASPs, generally have a good understanding of their ML/TF risks and apply adequate preventive measures. Risk understanding among DNFBPs is still developing, and DNFBPs, including some entities in higher risk sectors (such as legal professionals, notaries, REAs, DPMS), face challenges implementing preventive measures. There are major shortcomings in suspicious transaction reporting (STR), which is particularly low for non-bank FIs and DNFBPs. Poor reporting by DNFBPs is likely due to a range of factors including lack of awareness, misunderstandings of the reporting threshold, poor implementation of preventive measures, and confusion around professional secrecy obligations.
- j) All FIs, DNFBPs and VASPs (which are considered FIs in Germany) are subject to AML/CFT supervision. BaFin largely implements a satisfactory risk-based framework for supervising FIs (including VASPs) based on a strong understanding of risks. However, there is a low level of independent BaFin supervisory activity in some higher risk non-bank sectors. A range of remedial measures are applied, some of which are used to positive effect. However, in particular cases, measures have not ensured prompt remediation of non-compliance or the prevention of repeated breaches. Market entry requirements are sufficient, but the low number of rejections and a lack of data makes it difficult to form a definitive conclusion on the robustness of controls and BaFin could take a more proactive approach to identifying unlicensed MVTS providers, especially *hawala* operators.
- k) DNFBP and other financial supervisors have begun moving towards a risk-based approach to AML/CFT supervision. However, this is hampered by challenges co-ordinating the large number of supervisors, the vast scope of the supervised non-financial sector population (approximately 1 million entities), and a critical lack of resources. Remedial measures are used to a limited extent and not always in a proportionate manner. Measures to prevent and detect criminals and associates entering the market are stronger for licensed sectors, while the dealers in precious metals and stones (DPMS) sector has more limited measures and there are no market entry checks for the trust and company service provider (TCSP) sector. Measures to identify unauthorised DNFBP providers are largely reactive outside the casino sector.
- l) Germany has taken important steps towards implementing a regime to allow competent authorities and the general public access to beneficial ownership (BO) information on legal persons and arrangements through a Transparency Register. However, accurate and up-to-date BO information was not yet consistently available at the time of the on-site and there will be a substantial transition period before all entities, particularly civil law partnerships, will be covered by the regime. There

are challenges relating to bearer shares and nominee shareholders that are not yet fully addressed.

- m) International co-operation is prioritised by Germany and there is effective co-operation with Germany's most important international crime co-operation partners. Mutual legal assistance (MLA) and extradition under the European schemes are particularly effective and timely. However, statistics, centralised case management and case tracking is a challenge in Germany's federal system and is an area for improvement.
- n) The lack of available data across the Federal and *Länder* governments to measure effectiveness, the need to apply new technologies to enhance the use of data to combat AML/CFT and the need to work with Data Protection and Privacy authorities arose in multiple areas.

## Risks and General Situation

2. Germany is the largest economy in the EU and the fourth largest in the world after the US, China, and Japan. Frankfurt is the most important financial centre in continental Europe and, since 2016, Germany has the highest number of credit institutions and foreign branches in the European Union (EU).<sup>1</sup> Within its large financial sector, there are 6 high-risk major banks and co-operatives that were subject to over 20 sanctions by BaFin in 2019-2020. The large German commercial banks offer a variety of financial services, some with substantial presence abroad. Two major German banks account for the majority of Germany's correspondent banking relationships, including those with high-risk countries and one of those banks has been subject to enforcement actions from overseas regulators, as well as BaFin.<sup>2</sup> Germany is also home to the sixth largest stock exchange in the world, the Frankfurt Stock Exchange. It has the largest banking sector in the euro area, with total assets of about EUR 7.85 trillion at the end of 2014.<sup>3</sup> A key component of Germany's economic strength stems from their many small and medium sized enterprises, and thus Germany has a significant number of obligated entities in the non-financial sector. One study suggests that 20-30% of proceeds of crime in Germany are laundered in the non-financial sector.<sup>4</sup> Seventy-five percent of transactions in Germany happen in cash and Germans have a strong social and historical attachment to cash. Unlike some other EU countries, Germany does not have cash transaction limits. Germany is strategically located in the centre of the Schengen zone and it has the third-largest number of international migrants worldwide (11 million). The German economy is globally networked and export-oriented, including an advanced technology industry.
3. The main money laundering/terrorist financing (ML/TF) risks faced by Germany arise from its well-performing economy, its cash-intensive nature and international interconnectedness: international ML/TF risks (including from foreign predicates), cash-based ML/TF, laundering through the real estate sector, misuse of legal persons/arrangements, emerging risks (including virtual assets) and a range of legally or illegally obtained sources of funds for TF.

---

<sup>1</sup> International Monetary Fund (IMF), [Financial Sector Assessment Program \(FSAP\), Technical Note on Anti-Money Laundering and Combating the Financing of Terrorism](#), IMF Country Report No. 16/190, June 2016

<sup>2</sup> [www.dfs.ny.gov/reports\\_and\\_publications/press\\_releases/pr1701301](http://www.dfs.ny.gov/reports_and_publications/press_releases/pr1701301);  
[www.federalreserve.gov/newsevents/pressreleases/files/enf20170530a1.pdf](http://www.federalreserve.gov/newsevents/pressreleases/files/enf20170530a1.pdf)

<sup>3</sup> International Monetary Fund (IMF), [Financial Sector Assessment Program \(FSAP\), Technical Note on Anti-Money Laundering and Combating the Financing of Terrorism](#), IMF Country Report No. 16/190, June 2016

<sup>4</sup> Bussmann, K.-D. and M. Vockrodt, '*Geldwäsche-Compliance im Nicht-Finanzsektor: Ergebnisse aus einer Dunkelfeldstudie*', 2016, *Compliance-Berater* 5: p.138-143 referenced in the EU Supranational Risk Assessment (2019).

## Overall Level of Compliance and Effectiveness

4. On technical compliance with the FATF Standards, Germany has strong results. On effectiveness, many of these changes have occurred in the three to five years before the on-site visit, or less, and while some initiatives are beginning to show results, other reforms have been too recent or are structural and require an appropriate period of time to be operational and lead to changes in the effectiveness of the overall system. Changes that were implemented earlier (e.g., asset recovery reform) have led to a material increase in effectiveness, whereas more recent changes (e.g., efforts to improve DNFBP supervision, co-ordination with and across the *Länder*, changes to the ML law, and the introduction of the Transparency Register) are not fully effective. Areas that have enjoyed a sustained focus since the last evaluation (counter-terrorism and related CFT measures and international co-operation) continue to demonstrate results.

### *Assessment of risk, coordination and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)*

5. Germany has taken a range of steps since its last MER to increase its national ML/TF risk understanding. Germany's first NRA (2019) provides a good basis for assessing ML/TF risks based on input from a range of national and *Länder* agencies and representatives from the private sector. The NRA has triggered additional initiatives, including NPO and legal person risk assessments, which will feed into the national risk understanding and AML/CFT policies going forward. Individual agencies (including BaFin and the FIU) and all *Länder* have also developed risk assessments or products. Germany's public-private partnership, the Anti Financial Crime Alliance (AFCA), is a positive development in bringing together public and private sector stakeholders to ensure an ongoing assessment and understanding of risks, including emerging risks. These initiatives have given Germany a good understanding of the ML/TF risks related to cash, real estate and the banking sector, as well as cross-border risks and emerging risks from the COVID19 pandemic and virtual assets. TF risk understanding is good, based on regular TF situation reports and other risk assessment products including, to a lesser extent, the NRA. Further work is required to consider risks in other areas, particularly in the non-financial sector (outside of cash and real estate) and in relation to complex ML (including professional enablers and the use of legal entities).
6. National AML/CFT policies and activities (including the 2020 National AML/CFT Strategy) are aimed at mitigating identified ML/TF risks, enhancing co-operation, addressing persistent technical compliance issues and implementing EU requirements and recommendations of the previous FATF evaluation. Positive measures have been taken to respond to identified risks in the real estate sector. While some action has been taken, additional and more comprehensive measures are required to mitigate the identified ML/TF risks of cash and *hawala* services.
7. Germany has taken recent steps to address co-ordination issues identified in the 2010 MER, including establishing an informal national Steering Committee and a network of co-ordinating offices in the *Länder*. While co-operation has improved, co-ordination remains a challenge due to the scale and complexity of the system. The newly-established mechanisms need formal mandates, additional resources, and other support to ensure their effectiveness moving forward. The lack of available data across the Federal and *Länder* governments hampers Germany's ability to measure its own effectiveness in a number of areas of the system.

*Financial intelligence, ML investigations, prosecutions and confiscation  
(Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)*

8. Competent authorities have access to a broad range of information to use in financial investigations and case studies demonstrated that LEAs, prosecutors and intelligence agencies have the skills and capacity to conduct complex financial investigations using multiple information sources. However, financial intelligence is only accessed and used to some extent.
9. Germany implemented fundamental reforms to its financial intelligence framework in 2017 when it transitioned from a law enforcement FIU to an administrative FIU. Overall, this has been a positive move with increases in resourcing and the FIU taking on a more active role in financial intelligence analysis than it was under the previous decentralised FIU model. The transition has been challenging with particular issues around co-operation and buy-in from LEAs, access to data and use of advanced analytics leading to inefficiencies with a significant amount of cross-checking of data done manually by FIU staff. There is also room for improvement with FIU prioritisation to support LEA needs. The number of requests for FIU intelligence from LEAs is low and while there is a high number of intelligence disseminations, only a small proportion are used in support of criminal proceedings. Germany is taking a number of positive steps to address these issues but were not fully in place or effective at the time of the evaluation.
10. Germany was able to demonstrate ML investigations and prosecutions across a wide range of cases. However, the overall number of ML cases investigated and prosecuted in Germany is low considering the size of the country and the economy. Germany takes a reactive rather than a proactive approach to the identification of ML and it is not clear that ML involving professional ML networks, cash smuggling, foreign predicates, complex ML and cases involving legal persons are being detected. In practice, there is a focus on prosecuting for the predicate offence and barriers to pursuing ML in cases where there is no clear link to a predicate offence. Alternative measures, particularly asset confiscation, are used extensively by Germany however these measures are pursued regardless of whether or not it is possible to secure an ML conviction. There is no clear policy or strategy for disrupting and sanctioning ML in a consistent and comprehensive manner.
11. Asset confiscation is consistently pursued as a policy and operational objective. The introduction of non-conviction based asset confiscation laws in 2017 and the direction that it is mandatory for prosecutors to consider asset recovery in all cases involving proceeds of crime has led to significant outcomes and large amounts of assets being confiscated. LEAs have the tools and skills to trace, freeze and confiscate assets including assets of equivalent value. However, Germany's understanding and approach to cash smuggling (via mail and cargo and beyond cash couriers) is limited considering the significant risks of cash-based ML.

*Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)*

12. Authorities proactively pursue terrorism and TF and actively investigate TF activity alongside terrorism-related investigations in line with their risk profile. A robust array of tools, data sets and capabilities are available and used to analyse and investigate TF-related activity. Domestic co-ordination and co-operation is strong between authorities at both the federal and *Länder*-levels via standing taskforces and shared databases. Data and statistics on TF are not kept in a comprehensive manner in Germany which makes it challenging for authorities to differentiate between TF and terrorism cases and monitor the ongoing effectiveness of their system. The use of alternative measures are a strong feature of Germany's system with active use of association bans, programs to address violent extremism and effective use of the TFS offence to prosecute TF activity.
13. Germany has a good understanding of the TF risks associated with NPOs and applies a targeted risk-based approach to mitigating those risks. TFS mechanisms are not used effectively, or to support Germany's broader TF and counter-terrorism strategy. Agencies prefer to rely on domestic disruption mechanisms (which are limited in scope) and are not aware of or do not see the value in TFS. This is a major shortcoming in light of Germany's risks and context. There is some outreach to FIs, but generally limited guidance and support for other entities and insufficient proactive communication with DNFBPs and non-bank FIs, including higher-risk sectors such as MVTS and DPMS. DNFBPs are not effectively monitored for compliance with TFS implementation. Beyond TFS, Germany has access to a range of domestic measures to deprive terrorists and financiers of assets, however, these are limited in scope and cannot provide an effective alternative to TFS designations, given Germany's risk and context. Authorities demonstrated that they can use association bans (with accompanying asset recovery) and criminal confiscation effectively and proportionately. Other tools, such as BaFin and FIU freezes, could be better exploited. Overall, the amounts frozen under the various mechanisms are relatively low in relation to Germany's risk and context and its estimates of the total amounts raised within Germany.

### *Preventive measures (Chapter 5; IO.4; R.9-23)*

14. Germany has extremely large and diverse financial and DNFBP sectors. All FIs, DNFBPs (as defined by the FATF) and VASPs (which are licensed FIs in Germany) are required to apply AML/CFT preventive measures. AFCA has been a positive development in making available a wider range of risk information to obliged entities. In general, FIs, including VASPs, apply a range of preventative measures. Larger FIs particularly major banks (including online banks), MVTS institutions, insurance providers, and VASPs, have a good level of understanding of ML/TF risks and obligations. Smaller FIs, including some regional/niche banks and money service businesses, showed a less sophisticated awareness of risks and mitigation measures. The risk understanding among DNFBP sectors is mixed. Larger and better supervised DNFBPs (particularly major legal or REA firms or large-scale DPMS) take a risk-based approach to the preventative measures they employed. Smaller DNFBPs, including in higher risk sectors (such as notaries and legal professionals), face challenges applying preventive measures, including in relation to customer due diligence (CDD), politically exposed persons (PEPs) and TFS. The combination of a range of factors inhibits the effective implementation of preventive measures by all DNFBPs (including the lack of supervisory resources, the large number of obliged entities in the financial sector, and the changing status of certain obliged entities year-to-year).
15. There are major shortcomings in STR reporting. The number of STRs received from non-bank FIs and DNFBPs is low and, until recently, the number received by banks was also lower than expected given Germany's risks and context. Almost all STRs (97% in 2020) come from the financial sector, with banks filing 90% of STRs. Reports from FIs, particularly banks, have seen a recent exponential increase but started from a modest base. The increase reflects FIs' improved awareness and recent changes to the STR regime, but may also be in part as a result of defensive reporting. A range of factors contribute to the low level of STR reporting in DNFBP sectors: lower awareness, uncertainty regarding reporting thresholds, issues implementing preventative measures, and confusion surrounding professional secrecy obligations. Sectors covered by legal professional privilege have a very broad understanding of the concept, which prevents STR reporting in the absence of 'positive knowledge' that ML or TF has occurred through the entity. Germany has adopted mandatory rules-based reporting in real estate transactions to address a lack of reporting by these sectors. This has had a positive effect on reporting from notaries, but is limited to real estate transactions and there is insufficient understanding and ongoing confusion among the obliged entities to which it applies.

### *Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)*

16. All FIs and DNFBP sectors (as defined by the FATF) are supervised for AML/CFT compliance in Germany. BaFin, the main supervisor of FIs (including VASPs), has seen an evolution in its approach to AML/CFT supervision and has implemented regular reforms in response to changing risks and instances of non-compliance (including structural reforms resulting from a recent major scandal). Measures to prevent criminals and associates from entering the market are satisfactory, although a lack of data makes it difficult to form a definitive conclusion. BaFin is actively targeting unlicensed VASPs, but could take a more proactive approach to unlicensed money value transfer service (MVTs) providers, especially *hawala* operators. BaFin has a strong understanding of risk at a national, sectoral and firm-specific level. It largely applies supervisory measures in line with this risk understanding, significantly supported (but not replaced) by annual external audits of FIs. However, there is a low level of independent BaFin supervisory activity in some higher risk non-bank sectors. BaFin applies a range of remedial measures and sanctions and undertakes outreach efforts. Measures in particular cases (including involving major banks) do not always ensure the prompt remediation of non-compliance or prevent repeated breaches, and it is difficult to conclude on the extent to which supervisory efforts (as opposed to the annual audit process, legislative reforms and growing global awareness) have had a positive impact on compliance. BaFin could consider all options from its range of sanctions to address repeated breaches and to ensure prompt remediation.
17. There are a large number of supervisors (approximately 337) at the *Länder* or district-level to supervise DNFBPs and other FIs (i.e., certain insurance entities). Since Germany's last MER and starting in 2017, there has been a positive shift towards a risk-based approach by many of these supervisors informed by *Länder* risk assessments. However, the number of supervisors, the critical lack of resources, and the vast size of the supervised population (approximately 1 million obliged entities in the non-financial sectors), create major difficulties in ensuring all supervisors have a consistent risk understanding and take an effective risk-based approach to supervision. Risk-based supervision varies considerably; while risk is a consideration for DNFBP supervisors, they generally do not consider all relevant risk factors and variables in fully actualising a risk-based approach and supervisory strategy. Co-ordinating the large number of DNFBP and other FI supervisors also poses challenges and results in an overlap in supervisory responsibilities and activities. Licensed DNFBP sectors and insurance entities have stronger market entry measures in place, while DPMS and TCSP sectors are subject to more limited checks. Outside the casino sector, measures to identify unlicensed providers are largely reactive. While there are some very recent positive indications, sanctions in the DNFBP sectors remain infrequent and are not always applied in a proportionate manner. Guidance for obliged DNFBP entities has been developed and some supervisors engage in outreach, although feedback indicates that this could be more practical and consistent. The impact of supervisory engagement in DNFBP sectors is unclear.

### *Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)*

18. Germany has a complex system of registers in place to capture information on legal persons and arrangements in Germany, particularly through the Commercial Register and the Transparency Register. Whilst Germany has conducted a risk assessment on legal persons and arrangements this assessment does not suitably incorporate data from all relevant authorities on how legal persons may be abused in Germany. Germany is taking steps to collect and centralise beneficial ownership (BO) information on the Transparency Register (initially launched in 2017) with reforms on track to turn the Transparency Register from a supplementary register into a full register by the end of 2022. While the Transparency Register will improve the accessibility and accuracy of BO information (which still present issues), there remain issues with the scope of the Register as it will not include civil law partnerships. While the Register has been in place since 2017, it is not actively and systematically used by competent authorities to obtain BO information as the information held on the register is not reliably verified and there are issues with the accuracy and timeliness currently held. The Electronic Account Retrieval System has been in place since 2003 and has been the main source of BO information for competent authorities up to now. This system allows authorities to have direct access to account and deposit information held by German credit institutions. It is used extensively but relies on the entity having a bank account in Germany. The continued use of bearer shares and the use of nominee shareholders in Germany is a source of risk that Germany is also yet to fully mitigate.

### *International co-operation (Chapter 8; IO.2; R.36–40)*

19. Germany has an effective legal and operational framework in place for mutual legal assistance (MLA), extradition and asset recovery (including asset repatriation). Assistance is provided promptly and requests and responses are generally good quality. A particular feature of Germany's system is that assistance can be provided under German law to any country without the need for a treaty arrangement. The types of assistance that can be provided is broad and includes all the tools that LEAs can use for domestic investigations. Most of Germany's most important international crime co-operation partners are other EU member states and the use of streamlined mechanisms for international co-operation through European Investigation Order (EIO) and the European Arrest Warrant (EAW) mean that Germany can provide prompt and streamlined assistance.
20. Germany's system for receiving, processing and tracking requests for international co-operation is decentralised and requests are often sent directly to officials in the different *Länder* for consideration and response. Statistics and records are not kept at the national level which makes it more challenging for Germany to identify new and emerging risks and trends and proactively prioritise resources. It also makes it difficult for Germany to track the timeliness of responses to requests and raises challenges in cases where there are requests for assistance that require co-ordination between multiple *Länder*.

## Priority Actions

- a) Ensure that Federal and *Länder* Governments consistently prioritise ML/TF/PF issues:
  - a. at the political-level, secure high-level commitment and ongoing accountability by Federal and *Länder* governments for co-ordination in risk understanding, mitigation and allocation of resources;
  - b. at the official-level, give the RÜST-GW a formal and binding mandate and ensure all relevant authorities are adequately represented, including adding tax authorities and strengthening procedures for appropriate participation of the *Länder*; and,
  - c. formalise the *Länder* Co-ordinating Offices and give them the mandate and resources to ensure adequate and regular co-operation and co-ordination of the national and regional framework at both policy-making and operational levels (including on supervision and law enforcement functions).
- b) Substantially strengthen the detection, investigation and prosecution of ML by: prioritising ML as an offence distinct from predicate offences; and, enhancing understanding and prioritisation of cases in high-risk areas for Germany including cases involving legal persons, professional third party ML and foreign predicate offences.
- c) Improve the availability and use of financial intelligence by: increasing FIU access to bulk data and analytical tools to enhance the efficiency and effectiveness of FIU analysis; and, enhancing co-ordination and co-operation between the FIU and LEAs so that FIU intelligence prioritisation models and products more fully align with LEA operational needs.
- d) Enhance DNFBP supervision by adopting measures to ensure a harmonised, risk-based approach; considering a mechanism for oversight of DNFBP supervision across Germany; substantially increasing DNFBP supervisory resources (human and technical); and enhancing information available to DNFBP supervisors.
- e) Implement the planned reforms to the Transparency Register and registration requirements for civil law partnerships; enhance and deepen understanding of risks arising from legal persons in Germany; and, consider additional mitigation measures to address the risks arising from bearer shares and nominee shareholders.
- f) Considering the risks associated with cash-based ML, develop comprehensive policies to address these risks and consider all available measures. Improve understanding of risks arising from cross-border cash movements (particularly bulk cash movements); actively monitor and target high-risk movements of cash through mail and cargo. Ensure the risks from informal MVTs (such as *hawala*) are addressed holistically and there is continued focus on the investigation, prosecution and disruption of these illicit finance through these channels.

- g) Improve the effectiveness of the TFS system by proactively proposing designations and considering the development of a domestic listing process (in addition to the EU list). Address technical deficiencies to ensure that UN listings that occur on Friday afternoon or on a national holiday are implemented without delay.
- h) Improve STR reporting by: reviewing whether legal professional privilege requirements are impeding reporting in practice and ensure that there are adequate measures (such as guidance) to encourage higher-risk sectors to fulfil their legal reporting obligations; having the FIU routinely analyse the quality of STRs and provide substantive feedback; understanding the root causes of STR increases from the banking sector to ensure there is no defensive reporting and, if so, provide clarity on when STRs should be filed; and enhancing guidance to obliged entities including by continuing to support the work of Germany's public-private partnership AFCA.
- i) Improve FI supervision and compliance by assessing the level of inspections BaFin carries out itself each year of higher risk non-bank FIs to ensure entities are subject to regular supervisory activity as necessary; adopting a more proactive approach by BaFin to the prevention and detection of unlicensed MVTs providers, including informal value transfer services such as *hawala* operators; and increasing BaFin's use of sanctions, including business restrictions and personal accountability as appropriate in light of the level of dissuasiveness of these measures.
- j) Improve Germany's collection and use of data across its system to increase its ability to measure and monitor its performance on AML/CFT on an ongoing basis (particularly ML/TF investigations and prosecutions, international co-operation and areas of shared or decentralised responsibilities). Make better use of data and utilise advanced analytics to improve effectiveness in several areas of the AML/CFT system.

## Effectiveness & Technical Compliance Ratings

**Table 1. Effectiveness Ratings**

<b>IO.1</b> - Risk, policy and co-ordination	<b>IO.2</b> International co-operation	<b>IO.3</b> - Supervision	<b>IO.4</b> - Preventive measures	<b>IO.5</b> - Legal persons and arrangements	<b>IO.6</b> - Financial intelligence
<b>Substantial</b>	<b>Substantial</b>	<b>Moderate</b>	<b>Moderate</b>	<b>Moderate</b>	<b>Moderate</b>
<b>IO.7</b> - ML investigation & prosecution	<b>IO.8</b> - Confiscation	<b>IO.9</b> - TF investigation & prosecution	<b>IO.10</b> - TF preventive measures & financial sanctions	<b>IO.11</b> - PF financial sanctions	
<b>Moderate</b>	<b>Substantial</b>	<b>Substantial</b>	<b>Moderate</b>	<b>Moderate</b>	

Note: Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.

**Table 2. Technical Compliance Ratings**

<b>R.1</b> - assessing risk & applying risk-based approach	<b>R.2</b> - national co-operation and co-ordination	<b>R.3</b> - money laundering offence	<b>R.4</b> - confiscation & provisional measures	<b>R.5</b> - terrorist financing offence	<b>R.6</b> - targeted financial sanctions – terrorism & terrorist financing
<b>LC</b>	<b>LC</b>	<b>C</b>	<b>C</b>	<b>LC</b>	<b>PC</b>
<b>R.7</b> - targeted financial sanctions - proliferation	<b>R.8</b> - non-profit organisations	<b>R.9</b> – financial institution secrecy laws	<b>R.10</b> – Customer due diligence	<b>R.11</b> – Record keeping	<b>R.12</b> – Politically exposed persons
<b>PC</b>	<b>LC</b>	<b>C</b>	<b>LC</b>	<b>C</b>	<b>LC</b>
<b>R.13</b> – Correspondent banking	<b>R.14</b> – Money or value transfer services	<b>R.15</b> –New technologies	<b>R.16</b> –Wire transfers	<b>R.17</b> – Reliance on third parties	<b>R.18</b> – Internal controls and foreign branches and subsidiaries
<b>PC</b>	<b>LC</b>	<b>LC</b>	<b>C</b>	<b>LC</b>	<b>LC</b>
<b>R.19</b> – Higher-risk countries	<b>R.20</b> – Reporting of suspicious transactions	<b>R.21</b> – Tipping-off and confidentiality	<b>R.22</b> – DNFBPs: Customer due diligence	<b>R.23</b> – DNFBPs: Other measures	<b>R.24</b> – Transparency & BO of legal persons
<b>C</b>	<b>C</b>	<b>C</b>	<b>LC</b>	<b>C</b>	<b>PC</b>
<b>R.25</b> - Transparency & BO of legal arrangements	<b>R.26</b> – Regulation and supervision of financial institutions	<b>R.27</b> – Powers of supervision	<b>R.28</b> – Regulation and supervision of DNFBPs	<b>R.29</b> – Financial intelligence units	<b>R.30</b> – Responsibilities of law enforcement and investigative authorities
<b>LC</b>	<b>LC</b>	<b>C</b>	<b>LC</b>	<b>C</b>	<b>C</b>
<b>R.31</b> – Powers of law enforcement and investigative authorities	<b>R.32</b> – Cash couriers	<b>R.33</b> – Statistics	<b>R.34</b> – Guidance and feedback	<b>R.35</b> – Sanctions	<b>R.36</b> – International instruments
<b>C</b>	<b>C</b>	<b>PC</b>	<b>LC</b>	<b>LC</b>	<b>LC</b>
<b>R.37</b> – Mutual legal assistance	<b>R.38</b> – Mutual legal assistance: freezing and confiscation	<b>R.39</b> – Extradition	<b>R.40</b> – Other forms of international co-operation		
<b>C</b>	<b>C</b>	<b>C</b>	<b>LC</b>		

Note: Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non compliant.

## MUTUAL EVALUATION REPORT OF GERMANY

### Preface

This report summarises the AML/CFT measures in place as at the date of the e visit to Germany (1-19 November 2021). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system, and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by Germany, feedback from other countries, open-source reports and information obtained by the evaluation team during its on-site visit.

The evaluation was conducted by an assessment team consisting of financial, legal and law enforcement experts:

- Damian Brennan, Central Bank of Ireland (financial expert)
- Katrina Feitt, United States Department of the Treasury (financial expert)
- Kodai Hashimoto, Ministry of Foreign Affairs, Japan (targeted financial sanctions expert)
- Ole Bo Ketelsen, Financial Intelligence Unit Denmark (law enforcement expert)
- George Pearmain, Department for the Economy, Jersey (beneficial ownership expert)
- Bernhard Romstorfer, Financial Market Authority Austria (financial expert)
- Lida Tsagkaraki, representing the Ministry of Finance, Greece<sup>5</sup> (risk & international co-operation expert)
- Anne Mette Wadman, ØKOKRIM, Financial Intelligence Unit Norway (legal & law enforcement expert)

with the support from the FATF Secretariat of Shana Krishnan, Liz Owen and Mei-Lin Wang. The report was reviewed by: Alvin Koh, Monetary Authority of Singapore; Sveinn Magnusson, Icelandic Prosecution Service; and Daria Kudryashova, Eurasian Group Secretariat.

Germany previously underwent a FATF Mutual Evaluation in 2010, conducted according to the 2004 FATF Methodology. The 2010 evaluation and 2014 third follow-

---

<sup>5</sup> On secondment to the National Centre of Audiovisual Media and Communication, EKOME S.A. at the time of the on-site visit.

up report has been published and is available at: [www.fatf-gafi.org/countries/#Germany](http://www.fatf-gafi.org/countries/#Germany).

The 2010 Mutual Evaluation concluded that Germany was compliant with five Recommendations; largely compliant with 24 Recommendations; partially compliant with 15 Recommendations; and non-compliant with five Recommendations. Germany was compliant or largely compliant with nine of the 16 Core and Key Recommendations.

Germany was placed under regular follow-up after the adoption of its 2010 Mutual Evaluation and reported back to the FATF in January 2012, January 2013 and June 2014 and provided a supplementary update in February 2015. Germany exited the follow-up process in June 2014 as it had addressed deficiencies in all Core Recommendations and the overall progress achieved by Germany was considered sufficient to be removed from the regular follow-up process although remaining deficiencies existed in relation to two Key Recommendations on the terrorist financing targeted financial sanctions regime SR.I (now R.36) and SR.III (now R.6).<sup>6</sup>

---

<sup>6</sup> FATF, [Third Follow-up Report of Germany](#), June 2014

## Chapter 1. ML/TF RISKS AND CONTEXT

21. Size and territorial makeup: Germany, officially the Federal Republic of Germany (in German: *Bundesrepublik Deutschland*), is in the centre of Europe and covers 357 092 square kilometres. Germany shares borders with Poland, the Czech Republic, Austria, Switzerland, France, Luxembourg, Belgium, the Netherlands and Denmark.
22. Constitutional Structure: Germany is a democratic, federal, parliamentary republic of 16 states (*Bundesländer* or *Länder*, singular *Land*) that have political autonomy in certain policy areas. The German political system operates under a framework laid out in the 1949 constitutional document known as the Basic Law, *Grundgesetz* (GG), which in practice serves as Germany's constitution (therefore hereafter referred to as the Constitution). An important element of the German legal landscape is that power is divided between the federation and the *Länder*. The Constitution presumes that all power remains at the *Länder*-level unless otherwise stated in the Constitution itself. This rule applies to all *Länder* competencies. However, while the execution of laws remains largely with the *Länder*, the Constitution allocates vast legislative powers to the federation and, as a general rule, any federal law overrides *Länder* law if the legislative power lies at the federal level.
23. The federal system and distribution of responsibilities for AML/CFT activities is a central feature of Germany's system and is relevant for all 11 Immediate Outcomes. In particular, the 16 *Länder* governments are critical for law enforcement, DNFBP supervision and NPO monitoring and many of the legal person and arrangement registries. Only policy areas for which exclusive legislative and administrative powers are allocated at the federal level by the Constitution can be governed and controlled centrally. Policy areas that fall within the remit of the *Länder* or that qualify as shared (concurrent) powers are governed and controlled regionally at the *Länder* level or in co-operation with the federal government.

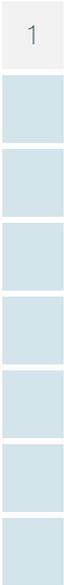
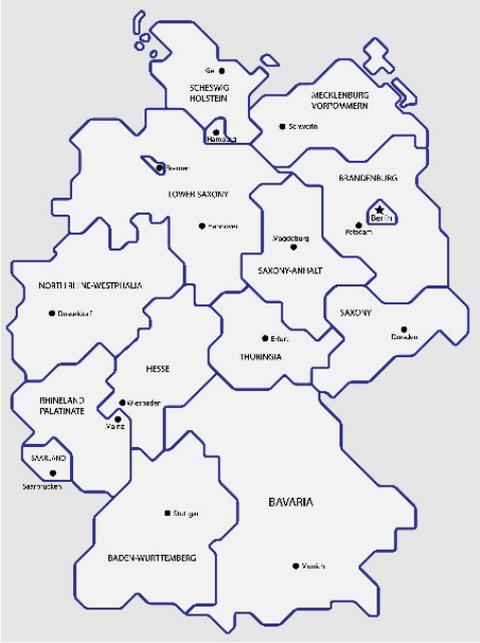


Figure 1.1. Map of German Länder



Source: GettyImages

Figure 1.2. German constitutional structure and governance

	Legislature	Executive	Judiciary	
Federation	German Parliament <i>(Bundestag)</i>	Federal President  Federal Government  Federal Administration	Federal Constitutional Courts  Federal Courts	Federal Prosecutor General
Länder	Land Parliament <i>(Landtag)</i>	Land Government  Land Administration	Higher Regional Courts  Regional Courts  Local Courts	Public Prosecutor General's Office  Public Prosecution Offices
District	District Council	District Administration		
Local Authority	Local Council	Local/City Administration		

Source: German Authorities

24. **Economy:** Germany is the largest economy in the EU and the fourth largest in the world after the US, China, and Japan, with a gross domestic product (GDP) of EUR 3.85 trillion.<sup>7</sup> Frankfurt is the most important financial centre in continental Europe. Accounting for 99.7% of all companies in Germany, small and medium-sized enterprises (SMEs) – the German *Mittelstand* – generate 35% of revenue and provide more than 70% of jobs in Germany. Publicly listed companies are found on the DAX index<sup>8</sup> at the Frankfurt Stock Exchange. Twenty-nine of the world’s 500 largest stock market listed companies measured by revenue are headquartered in Germany.
25. **Population:** With over 83 million inhabitants, Germany has the largest population of any member state of the European Union (EU) and the country is home to the third-largest number of international migrants worldwide (nearly 11 million). Germany’s population is distributed fairly evenly throughout most of the country with a high proportion of the population living in urban areas (74%).
26. **Role in the EU:** Germany is a founding member of the EU, a part of its single market and strategically located in the centre of the Schengen zone (a group of European countries with a combined population of approximately 400 million people, covering more than 4 million square kilometres). There is a free movement of people in the Schengen zone by road, rail and air. Germany uses the euro, and, as part of the euro area, its monetary policy is set by the European Central Bank in Frankfurt.

## ML/TF Risks and Scoping of Higher Risk Issues

### Overview of ML/TF Risks

27. Germany faces significant ML and TF risks. It faces higher than average ML risks as a large economy and financial centre strategically located in the middle of Europe, with strong international linkages and exposure to cross-border illicit flows. Germany has a large and sophisticated economy and financial sector, plays a significant role in world trade, and is involved in high volumes of cross-border trade and financial flows. Germany also has a significant informal sector and the use of cash is high. The euro is one of the most widely used currencies in the world.
28. Germany also faces higher than average TF risks due to the size of its economy; geographical situation (and developments in states bordering Europe); the presence of foreign terrorist organisations and structures, sympathisers, and FTFs; and the prominence of cash. Germany faces threats from international terrorist organisations, including domestic risks (jihadist groups without organisational structures operating in Germany, self-funding lone wolves, organised right-wing terrorist groups) and cross-border risks (domestic support for foreign terrorist groups). The highest-risk TF channels are MVTs (including informal *hawala* services) and cross-border cash transfers.

<sup>7</sup> World Bank, “World Bank Open Data” (2020). Available at: [www.data.worldbank.org](http://www.data.worldbank.org).

<sup>8</sup> Consisting of the 40 major German blue chip companies trading on the Frankfurt Stock Exchange.

### Country's Risk Assessment & Scoping of Higher Risk Issues

29. Germany's first National Risk Assessment (NRA), published in October 2019, rates the overall ML threat as medium-high with fraud, drug-related crime, human trafficking, and related organised crime, generating the most proceeds. TF threat is also rated medium-high. The Federal Ministry of Finance, *Bundesministerium der Finanzen* (BMF) is the national AML/CFT co-ordinator and led the NRA process with input from 35 agencies and private sector stakeholders. The NRA primarily draws upon the work of four interagency working groups, including law enforcement and supervisory bodies from both federal and *Länder* authorities, meeting over a period of 14 months (from December 2017). The NRA builds on and is informed by other risk assessments and sources, including the supra-national EU risk assessment (SNRA), sector-specific or issue-specific assessments by federal and *Länder* authorities and input from the private sector and academics. The NRA identifies high-risk proceeds-generating offences and assesses the residual risks of ML and TF at the sectoral level using the World Bank NRA Tool (adapted for national circumstances). The NRA methodology and process appears sound and the conclusions reasonable, although there are information gaps that hamper the risk assessment in certain areas (see IO.1).
30. In deciding what issues to prioritise for increased focus, the assessors reviewed material provided by Germany on their national ML/TF risks (as outlined above), and information from reliable third party sources (e.g. reports of other international organisations and NPOs). The assessment team focused on the following priority issues which are broadly consistent with those identified in the NRA:
- International ML/TF risk, including foreign predicates: Germany's key ML/TF risks arise from its well-performing economy, its international interconnectedness and its cash-intensive nature. The NRA identifies ML of foreign predicate crime as high and highlights high risks of ML from specific foreign jurisdictions. Recent events also suggest that proceeds of crime from these countries can enter Germany or its financial institutions via branches in other EU member states. The assessment team focused on measures applied to the banking sector (including group-wide implementation of AML/CFT measures and correspondent banking risks), cross-border movement of cash, trade-based money laundering, investigations and prosecutions of complex ML schemes and proactive and responsive international co-operation, including with countries deemed to pose a higher risk.
  - Cash-based ML and TF: Access to the Euro in a cash-intensive economy makes Germany an attractive destination to launder foreign proceeds. Illicit cash may also be converted into tangible high value assets increasing risks in the DNFBP sectors<sup>9</sup> (particularly real estate and dealers in precious metals and stones (DPMS)). The vast circulation of cash also has implications for ML/TF through the banking sector and the MVTS sector (including agents) where payments are generally made in cash, often outside an existing business relationship as

<sup>9</sup> Germany's AML/CFT obligations apply to a broad range of non-financial institutions, beyond those covered by the FATF Recommendations. For the purposes of this report, references to "DNFBPs" refer only to those sectors defined as DNFBPs under the FATF standards (casinos; real estate agents; DPMS; lawyers, notaries and other independent legal professionals and accountants; and TCSPs). References to the "non-financial sector" refer to Germany's broader population of non-FI obliged entities.

well as through unlicensed MVTs (e.g., *hawala* dealers). The assessment team focused on the measures put in place to mitigate cash-based ML and TF by FIs and DNFBPs, as well as controls on cross-border cash movements (in and out of Germany and including bulk-cash movements) and any other risk-based measures to curb cash-based ML and encourage the use of other, more transparent means of payment.

- **Laundering through the real estate sector:** The German real estate market is attractive to both international and domestic investors due to its high and stable value. Transparency International estimated that EUR 30 billion was laundered through German real estate in 2017. The NRA cites foreign ownership of real estate and real estate investments through complex structures of legal persons and arrangements as a large ML/TF threat, particularly in some geographic regions (therefore closely linked to the point below on the misuse of legal persons and arrangements). The assessment team focused on the role of real estate agents, notaries and lawyers, and financial institutions in undertaking adequate due diligence on higher-risk transactions, the ability of law enforcement to obtain property ownership information across all the *Länder* and explore the role of complex corporate structures and cash in property purchases.
- **Misuse of legal persons or arrangements:** Germany has introduced additional measures (the Transparency Register) to augment a decentralised system of existing beneficial ownership reporting requirements in other existing registries. The assessors explored the effectiveness of this system, the inclusion of all beneficial owners therein and sought additional information on Germany's understanding of risks related to legal persons. Highlighted as issues in the previous MER, the assessment team explored the impact of professional privilege on the ability of authorities to obtain required information from lawyers, notaries and accountants and whether these sectors are effectively supervised.
- **Emerging risks:** Beyond the NRA, the assessment team explored how entities and authorities assess and manage emerging ML/TF risks from virtual assets, the adoption of other new technologies, the impact of COVID-19 and the potential impact of the withdrawal of the United Kingdom from the European Union.
- **Terrorist financing (TF):** Germany faces the threat of religiously-motivated terrorism, and is sensitive to potential threats from right-wing and left-wing extremists. Sources of TF risk include: personal funds, investment in real estate and business, sham NPOs to generate donations under false pretences or foreign funding for radicalisation that leads to the recruitment of terrorists, illegal activities such as theft, trafficking and fraud. Cash and unlicensed MVTs activity are likely involved in TF activities. The assessors sought further information on the TF risks, Germany's assessment and understanding of those risks, and the activities of authorities in identifying, investigating and prosecuting TF, as well as mitigation and prevention measures.
- **More granular risk understanding:** The assessment team sought further information on whether the ML/TF risks and materiality vary regionally and to what extent authorities across the federal government and *Länder* governments understood their risks.

31. Through the scoping note exercise, a few areas were identified for lesser focus:
- Offences under the Weapons Act, handling stolen goods (small value items) as low risk predicate crimes for ML, unless linked to organised crime activities.
  - While the German insurance sector is sizeable, and the bank-insurance linkages are significant, many of the services/products provided by insurance companies are considered medium-low or low risk. Insurance undertakings supervised at the regional level are considered of less economic importance and limited to operating within a state (*Land*). However, some insurance companies and products supervised by BaFin do present greater risks.
  - Ship-based casinos are only permitted in two of Germany's *Länder* and can operate only as branches of a land-based operation. At present, no permits for ship-based casinos branches have been granted in either *Land*.
32. In addition to the higher risk areas for ML/TF, the assessment team highlighted areas in the institutional response to ML/TF/PF that were of greater focus:
- Co-operation and co-ordination between Federal and *Länder* governments and between agencies at the *Länder*-level: The constitutional framework adds significant complexity to the German AML/CFT system and the assessment team focused on how information sharing and co-ordination mechanisms allow for effective mitigation of ML/TF risks. Particular areas of focus include supervision of DNFBPs, co-ordination of investigations and prosecutions for ML and asset confiscation, the provision of international co-operation and availability and access to beneficial ownership information. Lastly, the team considered whether adequate mechanisms are in place for co-ordination between *Länder*-level authorities.
  - FIU: In 2017, Germany reorganised and transferred the FIU from the Federal Criminal Police Office (BKA) to the Central Customs Authority to address some of the issues identified in previous evaluations.<sup>10</sup> Media reports and other sources suggest issues (most of which are historic, but some are ongoing), such as significant backlogs in the analysis of suspicious transaction reporting and dissemination of information to law enforcement agencies, insufficient resources and capacity with the FIU and challenges in co-operation between the FIU and investigators and prosecutors.<sup>11</sup> The Assessment Team reviewed the progress of the FIU in addressing some of these challenges, particularly the co-operation with investigative and prosecution authorities and the use of Joint Financial Investigation Groups.
  - Supervision: BaFin restructured its AML directorate in 2017, and again in 2020, and assessors reviewed the outcomes of the move towards a more vigorous risk-based approach to supervision of FIs. Germany has a

<sup>10</sup> Reuters (9 August 2016), "Schäuble leads the fight against money laundering".

<sup>11</sup> Handelsblatt (24 November 2020), "Streitfall Vortatenkatalog: Banken hadern mit neuer Geldwäsche-Richtlinie", available at: <https://de.finance.yahoo.com/nachrichten/streitfall-vortatenkatalog-banken-hadern-neuer-183741556.html>. Spiegel Politik (27 August 2021), "Deutschland, ein Paradies für Geldwäscher", available at: [www.spiegel.de/politik/deutschland/geldwaesche-deutschland-ein-paradies-fuer-geldwaescher-a-739b7eaa-0002-0001-0000-000178959711](http://www.spiegel.de/politik/deutschland/geldwaesche-deutschland-ein-paradies-fuer-geldwaescher-a-739b7eaa-0002-0001-0000-000178959711). Tageschau (15 September 2020), "Rechnungshof fordert mehr Rechte", available at: [www.tagesschau.de/inland/fiu-geldwaesche-101.html](http://www.tagesschau.de/inland/fiu-geldwaesche-101.html).

decentralised model for the supervision of DNFBPs and the previous MER highlighted inconsistencies in the supervisory regime stemming from the fact that there are large numbers of DNFBP supervisors (over 300) and there was little exchange of information between supervisors. Assessors reviewed efforts to improve effectiveness and co-ordination of DNFBP supervision as well as FI supervision.

- **Proliferation financing and targeted financial sanctions (TFS) implementation:** Considering Germany's financial and diplomatic ties with Iran and diplomatic ties to DPRK and previous reports of sanctions evasion and its large internationally connected economy, the assessment team focused on Germany's implementation of TFS measures.

### Materiality

33. Germany is the largest economy in the EU and the fourth largest in the world with an annual gross domestic product (GDP) of USD 3.85 trillion in 2020 (equivalent to EUR 3.41 trillion).<sup>12</sup>
34. The German economy is globally-networked and export-oriented. The use of cash is high in Germany relative to other countries and Germany has a large informal sector; cash accounts for 48% of all turnover and 74% of all transactions.<sup>13</sup> Germany is a major host country for refugees; it had the 5<sup>th</sup> largest refugee population in 2020 and the largest in the EU.<sup>14</sup> Germany is one of the largest exporter of financial services globally along with the United States, United Kingdom and Luxembourg. Frankfurt is an international financial centre and the largest in the EU. Germany has the largest banking sector in the euro area,<sup>15</sup> with total assets of about EUR 7.66 trillion at the end of 2020. The large German commercial banks offer a variety of financial services, some with substantial presence abroad. Germany's five largest banks represent more than one third of the overall banking sector (in terms of total balance sheet).<sup>16</sup> However, Germany also has a high bank density with around 1 575 independent banks in 2020.

<sup>12</sup> GDP sourced from World Bank Data. Conversion from USD to EUR at a rate of 0.89 as at 4 January 2022.

<sup>13</sup> Federal Ministry of Finance (2019), First National AML/CFT Risk Assessment 2018/2019, pg.26.

<sup>14</sup> UNHCR (2020), "Global Trends in Forced Displacement - 2020", available at: [www.unhcr.org/statistics/unhcrstats/60b638e37/global-trends-forced-displacement-2020.html](http://www.unhcr.org/statistics/unhcrstats/60b638e37/global-trends-forced-displacement-2020.html)

<sup>15</sup> IMF (2016), Germany: Financial Sector Assessment Program.

<sup>16</sup> BaFin (2019), Subnational Risk Assessment for the Financial Sector 2019-2020, pg.12.

35. The DNFBP sectors are material in Germany. Notaries have a state-mandated role in property transactions and in establishing certain legal persons and arrangements. Real estate agents, the legal profession (including lawyers and tax advisors<sup>17</sup>), and TCSPs also play a prominent role in real estate transactions and/or company formation. Germany's legal sector is the second largest in Europe.<sup>18</sup> While many TCSPs in Germany operate solely as office space providers, this sector can also provide company formation, shelf and shell company, and *Treuhänder* services.<sup>19</sup> Data is not available on the number of TCSPs (in total or those providing these higher-risk services). Other DNFBP sectors, particularly DPMS, are considered material due to the prevalence/use of cash in the economy. In addition to DNFBPs (as defined by the FATF), Germany's AML/CFT obligations also apply to a range of other non-financial sectors, such as motor vehicle traders, antiques dealers and all trader in goods. This broader scope is partly as a result of the prevalence of cash in its economy and Germany's evaluation of risk in these sectors. For the purpose of this report, references to DNFBPs refer only to the DNFBP sectors as defined in the FATF methodology. References to the "non-financial sector" refer to Germany's broader population of non-FI obliged entities. One study suggests that 20-30% of proceeds of crime in Germany are laundered in the non-financial sector.<sup>20</sup>

### Structural Elements

36. Germany has all of the key structural elements required for an effective AML/CFT system including political and institutional stability, governmental accountability, rule of law, and a professional and independent legal profession and judiciary.

### Background and Other Contextual Factors

37. Germany has a long-standing legislative AML regime. Its first Money Laundering Act, *Geldwäschegesetz* (GwG) was introduced in 1993. Since this time, the GwG has been regularly amended and was replaced entirely in 2008. Recent amendments have been made in 2017, 2019 and 2020 to implement the EU AML Directives and in preparation for this evaluation. The first GwG applied only to FIs, but most DNFBPs (including notaries, lawyers, real estate agents and DPMS) have been captured since 2002, with Germany's implementation of the second EU AML Directive (2001/97/EG).

<sup>17</sup> Tax advisors are only captured in the FATF requirements (and covered in this report) to the extent that they fall within the definition of lawyers, other legal professionals or accountants undertaking the functions set out in R.22. In practice, tax advisors in Germany may be involved in the creation, operation or management of companies, legal persons or arrangements.

<sup>18</sup> CCBE (2016), "CCBE LAWYERS' STATISTICS 2020", available at: [www.ccbe.eu/fileadmin/speciality\\_distribution/public/documents/Statistics/EN\\_STAT\\_2020\\_Number-of-lawyers-in-European-countries.pdf](http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/Statistics/EN_STAT_2020_Number-of-lawyers-in-European-countries.pdf).

<sup>19</sup> The FATF definition of TCSPs covers entities providing a range of services, including office providers and company formation. Federal Ministry of Finance (2019), *First National AML/CFT Risk Assessment 2018/2019*, pg.105.

<sup>20</sup> Bussmann, K.-D. and M. Vockrodt (2016), "Geldwäsche-Compliance im Nicht-Finanzsektor: Ergebnisse aus einer Dunkelfeldstudie", in *Compliance-Berater* 5, pg.138-143; referenced in the EU Supranational Risk Assessment (2019).

38. Germany has also amended its criminal AML/CFT framework since its last FATF evaluation. The offence of ML was expanded to include self-laundering in 2015 and amended again in 2020 to include all offences as predicate offences. Germany does not face significant issues from corruption. Germany was ranked 9<sup>th</sup> on Transparency International's global Corruption Perception Index 2020 (where a higher ranking reflects a lower perception of corruption).<sup>21</sup>
39. Germany has a high degree of financial inclusion, in part due to the large number and high branch penetration of local savings and co-operative banks, including in less wealthy and less populated regions.<sup>22</sup> Nonetheless, Germany's large refugee population face challenges in terms of financial inclusion and are likely to rely to a large extent on cash-based channels for conducting financial transactions, including savings, payments and remittance.<sup>23</sup>
40. In terms of the PF context, Germany has a financial relationship with Iran, including through several Iranian banks branches in Germany. Following the conclusion of Joint Comprehensive Plan of Action (JCPOA) in 2015, trade and financial transactions between the two countries increased temporarily, but dropped again considerably following the withdrawal of the US from the JCPOA in 2018 and the subsequent re-introduction of US extraterritorial sanctions. Trade relations have since focused on humanitarian goods. Germany's relationship with DPRK is less significant, although Germany is a destination of choice for procurement of technology by both Iran and North Korea.

### AML/CFT strategy

41. Germany published its first formal National AML/CFT Strategy in January 2020, following the NRA. The Strategy identifies 11 broad areas to improve Germany's AML/CFT system, with specific actions identified within each area. There is a mix of measures to respond to regional and international standards (including EU and FATF requirements) and to respond to regional and national risks (see IO.1, Section 2.2.2). Implementation of the Strategy is monitored by the interagency Steering Committee for Combating ML/TF (RÜST GW/TF), which was also established in 2019 (see R.2). Prior to the 2020 Strategy and RÜST GW/TF, AML/CFT policies and objectives were co-ordinated on an *ad hoc* and informal basis, led primarily by the Federal Ministry of Finance (BMF).

### Legal & institutional framework

42. The legal framework of AML/CFT measures applies across Germany and is set out in the GwG which contains the requirements for preventative measures. Criminal offences for ML and TF also apply across Germany and are set out in the German Criminal Code, *Strafgesetzbuch* (StGB). The main AML/CFT authorities include:
  - **Policy-setting authorities:** Overall, the **Federal Ministry of Finance (BMF)** is the key agency for ML/TF prevention. BMF undertakes co-ordinating tasks and is responsible for the GwG. The BMF also exercises legal and supervisory

<sup>21</sup> Transparency International (2020), "Corruption Perceptions Index", available at: [www.transparency.org/en/cpi/2020/index/deu](http://www.transparency.org/en/cpi/2020/index/deu).

<sup>22</sup> Neuberger, Doris (2015), *Financial Inclusion, Regulation, and Education in Germany*, Asian Development Bank Institute Working Paper Series, pg.9.

<sup>23</sup> Dhawan, Swati Mehta (2018), *Financial Inclusion of Germany's Refugees: Current Situation and Road Ahead*, European Microfinance Network, pg.11.

control over Federal Financial Supervisory Authority (BaFin), the FIU (to the extent permissible), the Central Office of the German Customs Investigation Service (ZKA) and the General Customs Authority (GZD) in general. The **Federal Ministry of Justice (BMJ)** is responsible for criminal law issues and the **Federal Ministry of the Interior and Community (BMI)** is responsible for internal security, including related to ML/TF. The BMI exercises legal and supervisory control over the Federal Criminal Police Office (BKA) and the Federal Office for the Protection of the Constitution (BfV). The **Chancellery** exercises legal and supervisory control over the Federal Intelligence Service (BND). *Länder* authorities also play a role in setting policies in their areas of responsibility (law enforcement policy, DNFBP supervision, corporate registries).

- **International co-operation:** MLA and extradition are federal matters and the primary responsibility of the BMJ. Functionally, decision making powers have been delegated to the **Federal Office of Justice (BfJ)** in Bonn and *Länder* governments which have further delegated responsibilities to different courts and public prosecution offices. The BfJ acts as the central authority for receiving and making requests and takes the lead in cases involving federal jurisdiction. All other cases are decided on and actioned by the relevant *Länder* authorities.
- **FI supervision** (including VASPs) is mostly centralised at the federal level and undertaken by **BaFin**. **DNFBP supervision** (as well as some aspects of insurance supervision) is regulated at the Federal level, but implementation is decentralised and is the responsibility of the 16 *Länder* governments, which have different institutional arrangements for supervising different sectors (see section 1.4.6 below and Annex B).
- **FIU:** In 2017, the **FIU** was established as a functionally independent authority housed within the **General Customs Authority (GZD)** which falls under the portfolio of the Federal Ministry of Finance (BMF). The FIU is the exclusive recipient of STRs from obliged entities (FIs, DNFBPs and tax authorities). The FIU analyses these reports and disseminates information to competent authorities (including international counterparts) spontaneously or upon request. Prior to 2017, there was a decentralised model in place where the Federal Criminal Police Office (BKA) and *Länder*-level authorities (predominantly Joint Financial Investigation Groups (GFGs)) performed FIU functions.
- **Money laundering investigations/prosecutions and asset confiscation:** the investigation and prosecution of ML is primarily a responsibility of ***Länder* criminal police offices (LKAs)**, local police offices and the relevant ***Länder* public prosecution offices**. In addition to being the national central agency for criminal policing, the **Federal Criminal Police Office (BKA)** is a law enforcement agency in its own right and has jurisdiction in cases of ML involving organised crime or international ML. The Federal Intelligence Service (BND) also supports investigations by these institutions. **Customs** investigates ML cases involving cross-border cash movements and predicate offences falling within its investigative competence. Asset confiscation is a mandatory consideration for public prosecutors in all criminal cases involving proceeds-generating crimes. Specialised **asset recovery offices** have been set

up at police offices at all levels (federal, *Länder* and local) to support asset recovery efforts.

- Terrorist financing investigations/prosecutions: responsibility for the investigation and prosecution of TF is shared between federal and *Länder* authorities. Compared with ML, federal agencies play a much greater role in TF with the **Federal Prosecutor General (GBA)** taking on a significant number of cases. On investigations, Germany's domestic intelligence agency the **Federal Office for the Protection of the Constitution (BfV)** and the foreign intelligence agency, the **Federal Intelligence Service (BND)** as well as the **BKA** play a key role. Domestic coordination mechanisms like the **Joint Terrorism Centre (GTAZ)** in Berlin and the **Joint Centre for Extremism and Terrorism (GETZ)** in Cologne focus on terrorism but consider TF as part of their intelligence function. The main *Länder* authorities are the **LKAs, public prosecution offices and *Länder*-level intelligence agencies (LfVs)**. The important exchange between the federal and *Länder* authorities during the investigations takes place within the framework of the above-mentioned centres as well as in the context of regular bilateral co-operation.
- Targeted financial sanctions implementation: Germany's **Federal Foreign Office (AA)** is responsible for proposing designations and de-listings to the EU and UN. The **Federal Ministry for Economic Affairs and Climate Action (BMWK)** is responsible for issuing domestic freezing orders under the Foreign Trade and Payments Act, *Außenwirtschaftsgesetz* (AWG). The central bank, **Deutsche Bundesbank** receives reports of funds freezes, authorises releases of funds, and supervises FIs' TFS compliance (jointly with BaFin for terrorism-related TFS). DNFBP TFS supervision differs depending on the sector, with a gap in supervision for some DNFBPs (see IO.3, 10 and 11 for further detail). Criminal enforcement of TFS breaches is undertaken by federal or *Länder* police, while any administrative offence proceedings are handled by the Main Customs Offices.
- NPO supervision: NPOs are registered in line with their status as a legal person (i.e., as associations, foundations or limited liability companies; there is no separate registration as a NPO) and are supervised by *Länder* tax authorities for compliance with their non-profit status.

### *Financial sector, DNFBPs and VASPs*

43. Germany has a materially significant financial sector. BaFin's AML/CFT supervisory population comprises 6 498 FIs (1 575 FIs within the banking sector and 4 923 FIs in the non-banking sector of which 2 723 are agents providing payment services). These entities undertake a wide range of activities including banking, investment services, insurance, leasing, factoring, foreign currency dealing, payment services and virtual assets service providers (VASPs). In addition, Germany has three economically insignificant insurance companies and 81 061 insurance intermediaries that are FIs under the FATF Standards, but that are supervised at the *Länder*-level and therefore not captured in the table below.

**Table 1.1. Overview of Germany's financial sector (2020)**

	Number of obliged entities	Assets held (EUR millions)	Percentage of assets
<b>TOTAL FINANCIAL SECTOR</b>	<b>6 498</b>	<b>11 656 457</b>	<b>100</b>
<b>Banking sector</b>	<b>1 575</b>	<b>7 663 995</b>	<b>65.75</b>
Major banks, co-operative central institutions and central institutions under public law	10	2 501 795	21.46
Branches and branch offices of foreign banks	107	430 420	3.69
Regional banks and other commercial banks	152	999 092	8.57
Co-operative banking group institutions	1 188	2 269 300	19.47
Other credit institutions	118	1 463 388	12.55
<b>Non-bank financial sector</b>	<b>4 923</b>	<b>3 992 462</b>	<b>34.25</b>
Investment firms	750	3 600	0.03
Securities trading	38	33 000	0.28
Crypto custodians*	34	-	-
AMCs	608	2 391 400	20.52
Foreign currency dealing	8	62	Close to 0
Leasing	434	115 500	0.99
Factoring			
Payment service providers	83	6 900	0.06
Agents	2 723	-	-
Insurance undertakings	245	1 442 000	12.37

\* Other VASPs are covered as payment service providers.

Source: German Authorities

44. Germany has a large and diverse DNFBP population. All DNFBPs (as defined by the FATF) are obliged entities under Germany's AML/CFT framework, in addition to a broad range of other non-financial sector institutions, including gambling providers, property leasing agents and traders in goods.<sup>24</sup> This broad approach, particularly regarding traders, results in an estimated 800 000 obliged entities in the merchandise trade sector alone. The NRA estimates that 60 000 of these are higher-risk high-value dealers (i.e., DPMS or traders in jewellery, watches; works of art and antiques; motor vehicles, ships, and motorboats). More than 700 000 traders in goods are subject to AML/CFT obligations without any specific risk information on them. Together with DNFBPs outside the merchandise trade sector, the population of obliged entities across the non-financial sector is estimated at 1 million (see Annex C).

<sup>24</sup> Germany's AML/CFT obligations apply to a broad range of non-financial institutions, beyond those covered by the FATF Recommendations. For the purposes of this report, references to "DNFBPs" refer only to those sectors defined as DNFBPs under the FATF standards (casinos; real estate agents; DPMS; lawyers, notaries and other independent legal professionals and accountants; and TCSPs). References to the "non-financial sector" refer to Germany's broader population of non-FI obliged entities.

**Table 1.2. Overview of Germany's DNFBP sectors**

Type of DNFBP	Number of obliged entities
Legal professionals (2020):	
Lawyers	Approx. 36 791*
Tax advisors	86 625
Notaries (2020)	6 912
Accountants (2020)	14 758
Real estate agents (2017)	30 324
Casinos (2020)	28 land-based casinos
DPMS (2017)	Approx. 7 993
TCSPs	Unknown

Note: \* Lawyers are obliged entities only where conducting certain transactions and the number changes in any given year. The number of obliged entity lawyers for 2020 is based on an estimate by legal supervisors that 22% of all lawyers conduct such transactions.

A full breakdown of obliged entities in Germany's non-financial sectors is included in Annex C.

Source: German Authorities

45. The ranking of regulated sectors is based on their relative importance in Germany's context. These rankings inform the conclusions throughout the report, with positive and negative findings weighted more heavily for important sectors. This approach applies throughout the report, but is most evident in IO.3 and IO.4.
- The **banking sector** is weighted most heavily in Germany's context, based on its materiality and risks. The banking sector is materially significant, holding 66% of Germany's total financial sector assets, and is the largest in the euro area. Major German banks service a broad client base, including high net-worth individuals, and are internationally connected. Two major German banks account for the majority of Germany's correspondent banking relationships, including those with high-risk countries. The NRA identified the banking sector as high risk for ML and medium-high for TF due to its diverse product range, large business volumes and international interconnectedness.
46. MVTS and money services businesses, VASPs, real estate agents, notaries, lawyers and accountants are weighted heavily based on their materiality and risk:
- **MVTS and money service businesses** are weighted heavily based on the nature of their business. The sector in Germany is dominated by a small number of relatively large foreign payment institutions, which operate through agents. It is high risk because of the agent structure and the high use of cash (which is particularly important in Germany's context), generally outside an existing business relationship. The NRA rated the ML/TF threat of the sector as high. The risks associated with unregulated activities, including unlicensed *hawala* service providers, also fall under this category.
  - **VASPs** are also weighted heavily. This sector forms a small part of Germany's financial sector, in part as they have historically been more highly regulated in Germany than in neighbouring jurisdictions. In 2020, Germany had 20 independently licensed VASPs (i.e., not otherwise licensed as a financial institution). Nonetheless, as an emerging and growing sector, with clear inherent risks due to the level of anonymity and limited global regulation, this sector has more weight. The NRA rated the ML threat as medium-low and the TF risk as low, although authorities noted that the risk understanding has

evolved since this time and the sector is now considered to present a higher level of risk.

- While **real estate agents** are not involved in all real estate transactions, they are weighted heavily based on their involvement in higher-risk real estate transactions, including real estate share deals and other transactions where ownership may be obscured. Transparency International estimates that EUR 30 billion with unclear origins entered the Germany real estate market in 2017.<sup>25</sup> The NRA rated the ML risk as high and TF risk as medium.
  - **Notaries, the legal profession (including lawyers and tax advisors) and accountants** are also weighted heavily due to their higher-risk services (particularly real estate transactions and company formation), the relatively large size of the sectors, and recent changes in the legislative framework clarifying their reporting requirements and affording their supervisors greater authority. The NRA rated notaries and lawyers as a high ML risk and accountants and tax advisors as medium risk. All liberal professions were rated as medium-low TF risk.
47. The securities sectors, e-money and payment service providers (other than MVTs), foreign currency dealers, DPMS and TCSPs are weighted as moderately important based on their materiality and risk:
- The **securities** sector is considered moderately important based on the size of the sector, exposure to cross-border risks (through foreign investment) and the nature of the transactions. The securities industry expanded rapidly in the late 20<sup>th</sup> century and asset management companies (AMCs) held over 20% of Germany's total financial sector assets in 2020. Transactions tend to be complex and involve high volumes. The NRA rated the ML/TF threat in the securities sector as medium and the vulnerabilities as medium-high.
  - **E-money and payment service providers (other than MVTs)** are considered moderately important. The sector is relatively small and regulated, but exposed to risks due to the use of cash and opportunities for anonymity. The NRA rated the ML threats in this sector as low, and the vulnerability as medium-high.
  - **Foreign currency dealers** are moderately important. The sector is small, with only 10 bureaux de change licensed by BaFin to specialise exclusively in foreign currency dealing, all of which have long been under BaFin supervision. Nonetheless, the exposure to cash and international transactions creates ML vulnerabilities. The NRA rated the threat in this sector as high, and the vulnerability as medium-high.
  - **DPMS** are considered moderately important on the basis of their exposure to cash transactions and foreign clients, and the relatively limited supervisory engagement and oversight. The sector comprises around 7 000 entities and forms part of Germany's expansive traders in goods sector (totalling over 800 000 obliged entities). The NRA, rates high-value dealers (including DPMS) as medium-high risk for ML and medium risk for TF.

<sup>25</sup> Transparency International (2019), "Three ways to stop money laundering through real estate", available at: [www.transparency.org/en/news/three-ways-to-stop-money-laundering-through-real-estate](http://www.transparency.org/en/news/three-ways-to-stop-money-laundering-through-real-estate).

- **TCSPs** are weighted moderately heavily. While Germany considered that most such providers engage in relatively lower risk services (e.g., office providers), there are instances of companies performing the functions of TCSPs providing large volumes of higher risk company formation and shelf services and there are information gaps in relation to this sector (including the number of entities). In addition, while the NRA rates the ML risks in this sector as medium-low and the TF risk as low, it recognises that criminals often rely on complex legal arrangements and that the use of TCSPs is “an alternative to the heavily monitored financial sector”.<sup>26</sup>
48. Casinos and the insurance sector are weighted as being of relatively less importance:
- **Casinos** are considered less important due to their limited number and the strong and long-standing supervisory engagement, which mitigate the inherent risks posed by the sector’s exposure to cash. Assessors were more sensitive to the risks posed by online casinos, due to the nature of transactions, although these remain highly regulated and limited in number. The NRA rated the overall gambling sector as a high ML threat and low TF threat.
  - The **insurance sector** is given less weight based on its limited product range, regional/national focus, and lack of exposure to cash (most insurance undertakings in Germany do not accept or pay out cash). The NRA rated the ML risk of the insurance sector as medium low. Nonetheless, the assessment team noted that the size of the sector (12% of total financial sector assets) and persistent low interest rates led to some risk in the sector.

### *Preventive measures*

49. Preventative measures for all obliged entities are set out in the German Anti-Money Laundering Act (GwG). The GwG covers all the FIs and DNFBPs required by the FATF Standards. The GwG also covers some entities that are not required under the FATF Standards including all traders in goods when they transact in cash over EUR 10 000. This is a requirement in the EU 4<sup>th</sup> AML Directive (4AMLD). Non-binding guidance on the GwG has been issued for all FI and DNFBP sectors. This elaborates on supervisors’ expectations of obliged entities when implementing their GwG obligations.

### *Legal persons and arrangements*

50. There are numerous types of legal person which can be established under German law. Broadly, they can be broken down into two categories: corporations and partnerships. Partnerships are not considered to be part of the German definition of legal person but are considered to be legal persons as defined by the FATF. Foundations, co-operatives and associations with separate legal personality are considered a sub-set of corporations but are subject to different legal, regulatory and reporting requirements than other commercial corporations.

---

<sup>26</sup> NRA, pg.105.

51. There are two types of trust-like structures that can be established under German law, *Treuhand* and foundations.<sup>27</sup> There are trust-like structures that can be established under German law, like foundations, without legal capacity or other *Treuhand* (fiduciary relationships). Express trusts cannot be created under German law but trusts created under foreign law are recognised and can operate in Germany.

**Table 1.3. Types of Legal Persons and Arrangements in Germany**

Type of legal person/arrangement	Number	Basic characteristics and significance
<b>Corporations</b>		
Limited liability companies ( <i>Gesellschaft mit beschränkter Haftung</i> (GmbH)) and entrepreneurial company ( <i>Unternehmergeellschaft haftungsbeschränkt</i> (UG))	1 419 590	GmbH are formed by one or more founding shareholder(s) adopting the articles of association and appointing one or more managing directors in a notarial deed. GmbH acquire legal personality upon registration on the Commercial Register. UGs are a special form of limited liability company which is not required to meet the legally mandated EUR 25 000 share capital required of a GmbH. It is primarily used for small businesses. They are otherwise the same as GmbH. Together, GmbH and UG are the most common type of legal person in Germany
Stock corporations ( <i>Aktiengesellschaft</i> (AG))	13 689	Corporations that may be traded on the German stock exchange: AGs are subject to increased regulatory oversight compared to GmbH and UGs
Foundations under private law with legal capacity ( <i>Stiftung</i> )	23 876	Foundations are used for non-profit enterprises and do not generally engage in commercial activities.
Registered associations ( <i>eingetragener Verein</i> )	614 628	Associations are established by groups of people to accomplish a common purpose (e.g. a sports club). Associations acquire separate legal personality when they are registered on the Register of Associations. Unregistered associations exist but do not have separate legal personality.
Societas Europaea (SE)	765	Public companies created and registered under European law. SEs are used by commercial bodies with operations in more than one EU country.
Partnerships limited by shares ( <i>Kommanditgesellschaft auf Aktien</i> (KGaA))	380	The KGaA is a stock corporation that has partners instead of a board of directors. KGaA's have legal personality and are used for commercial enterprises.
European cooperative	22	Cooperatives founded under European law for cooperatives operating in multiple EU countries.
Registered cooperative (eG)	8 960	Registered cooperatives are similar to registered associations but may carry out commercial activities.
Public law corporations	781	Legal persons that are created under public law e.g. owner-operated municipal enterprises and public utility companies.
Foreign associations that own property in Germany	340	This applies to associations whose registered office is located outside of Germany when they acquire immovable property located in Germany.
Foreign companies	7 371	Companies created under foreign law and registered on the Commercial Register

<sup>27</sup> A *Treuhand* is created when the *Treuhänder* (trustee) is authorised to exercise rights over property in his or her own name, on the basis of and in accordance with a binding agreement with another person, the *Treugeber* (settlor). The *Treuhand* can exist without any written record and property can be managed for the benefit of the original trustee or for the benefit of a third party.

<b>Partnerships</b>		
Civil law partnerships ( <i>Gesellschaft bürgerlichen Rechts</i> (GbR))	572 139 engaged in commercial activity	GbRs are made up of at least two members who can be natural or legal persons. There are currently no mandatory registration requirements for GbR in Germany and so the total number of GbRs in Germany is unknown but it is estimated that approximately 572 139 were engaged in commercial activity in 2017. GbRs are not registered on the Commercial Register but once turnover exceeds EUR 250 000 or employs more than 5 staff, the GbR must be registered and converted into an oHG although there is no strict threshold for conversion.
General partnership ( <i>Offene Handelsgesellschaft</i> (oHG))	22 730	The oHG is a partnership engaged in commercial activity registered on the Commercial Register.
Limited partnership ( <i>Kommanditgesellschaft</i> (KG))	288 960	KGs are partnerships made up of one or more general partner(s) and other shareholders (limited partners). KGs must be registered on the Commercial Register.
Partnership company ( <i>Partnerschaftsgesellschaft</i> (PartG))	15 104	An exclusive legal form of partnerships for freelance professionals such as lawyers or tax advisers
Foreign partnerships and partnership companies	195	Partnerships and partnership companies created under foreign law and registered on the Commercial Register
<b>Legal arrangements</b>		
Foundations without legal capacity	1 775	Foundations without legal capacity are created under general contract law and are not required to be registered. They are similar to a common law trust in that funds are provided for a specific purpose with the general contract operating as a trust agreement between the settlor and the trustee.
Trusts established under foreign law	343	These are express trusts established under foreign law, operating in Germany and registered on the Transparency Register.
<i>Treuhand</i>	Unknown	" <i>Treuhand</i> " refers to a large variety of different contractual relationships which can have characteristics similar to common law trusts.

Note: This information was current as of 1 August 2021.

Source: German Authorities

52. Germany collects and records basic information through a complex system of registers which collect and record basic and beneficial ownership information with various requirements depending on the legal form and arrangement. These registers are decentralised and operated by *Land* district courts. The obligation to enter and update information primarily lies with the entity and verification and registration of information entered into the registers has largely been delegated to notaries. Germany has taken steps to make this information available in a centralised *Land* register portal (*Registerportal*) which allows users to access all registers using a single platform. The main register for legal persons engaged in commercial activity is the “Commercial Register” (*Handelregister*). Associations, cooperatives, some forms of partnerships and foundations are required to register on specific registers. Some limited BO information was captured on these existing registers but not in a comprehensive manner. In 2017, Germany introduced the Transparency Register to capture BO information that wasn’t captured on other registers and also basic and BO information on legal arrangements. From 2021, Germany will begin to transition the Transparency Register into a full register meaning that entities with filing obligations (excluding associations) will have to separately register and update information on the Transparency Register and it will no longer rely on drawing information from existing registers.

**Table 1.4. Registers for basic and BO information of legal persons and arrangements in Germany**

Register	Registration requirements	Entities captured on the register
Transparency Register	Basic and BO information not captured on other registers (2018-2021) and from 2021, all basic and BO information to be filed separately except for associations.	All entities registered on the <i>Handelsregister</i> , and specified legal arrangements. From 2021, associations will have information automatically transposed into the Transparency Register and will not be subject to filing obligations with respect to the Transparency Register.
Commercial Register ( <i>Handelsregister</i> )	Basic information	Corporations and partnerships engaged in commercial trading activity (GmbH, UG, AG, SE, oHG, KG, KGaA)
Register of Cooperatives	Basic information	Cooperatives and European cooperatives
Partnerships Register	Basic information	PartG but not GbRs
Register of Associations	Basic information	All associations with separate legal personality

### Supervisory arrangements

53. There are over 300 AML/CFT supervisors in Germany that supervise obliged entities under the GwG. Supervisory powers are largely set out in the GwG and, for the financial sector, in a range of other sectoral legislation (see R.27 and R.28). Financial sector supervision is largely centralised with **BaFin**. BaFin is an integrated supervisory authority, undertaking prudential, conduct and AML/CFT supervision. BaFin has also taken on the role of licensing and supervising VASPs. Supervision of the insurance sector is split between BaFin and the *Länder*, with BaFin supervising insurers of material economic and financial significance and those operating across borders and the relevant *Länder* ministry supervising smaller or localised entities. In 2014, the European Central Bank assumed responsibility for licensing, acquisition of qualifying holdings and licence revocations for certain credit

institutions according to the common procedures and its mandate under the euro zone's Single Supervisory Mechanism.<sup>28</sup>

54. DNFBP (and broader non-financial sector) supervision is decentralised in Germany and is the responsibility of the 16 *Länder* governments. Each *Land* government decides its DNFBP supervisory framework independently and there is a broad range of authorities or self-regulatory bodies (SRBs) responsible for supervision at the *Länder*-level. The exact total number of DNFBP supervisors could not be provided due to the level of decentralisation, but it is estimated to be over 300 different bodies. Except for accountants, which are supervised by the Federal Chamber of Accountants, all DNFBP sectors are supervised at the *Land* level. Lawyers, accountants and tax advisors are supervised by self-regulatory bodies (bar associations, chambers of tax advisors, Chamber of Accountants). Casinos are generally regulated and supervised by the *Land* Ministry of Interior, although there are exceptions. Notaries are supervised by the President of their regional courts (in most cases multiple regional courts in a *Land*). DPMS (which come under the heading of 'traders in goods'), real estate agents and TCSPs are supervised at the local/district government-level, generally by *Land* Ministries of Economy or Interior or State Offices.
55. Whereas "city-state" *Länder* such as Berlin, Hamburg and Bremen tend to concentrate their supervisory framework in a single source, geographically large and economically significant *Länder* such as Bavaria, Baden-Württemberg and North Rhine-Westphalia involve a number of existing structures/authorities to perform DNFBP supervision.

---

<sup>28</sup> See EU Council Regulation 1024/2013, art.4(1). Common procedures cover the assessment of the mentioned applications for both 'significant institutions' and 'less significant institutions'. While the European Central Bank has direct responsibility for the supervision of 'significant institutions', the direct responsibility for the supervision of 'less significant institutions' except common procedures remains by the national competent authorities. See: [www.bankingsupervision.europa.eu/banking/list/criteria/html/index.en.html](http://www.bankingsupervision.europa.eu/banking/list/criteria/html/index.en.html)

**Table 1.5. Supervisors of DNFBPs across the *Länder***

DNFBP Sector	Organisation/Legal basis for AML/CFT supervision	Type of supervisor
Real estate agents	Decentralised and varies according to the <i>Land</i> , <i>Land</i> -level legislative basis	District governments within the <i>Land</i> , <i>Land</i> Ministries of Economy, various County/city authorities or State offices. (Over 26 supervisors for each sector – some common supervisors in a <i>Land</i> for multiple sectors)
Dealers in goods (including precious metals and stones)		
TCSPs (not covered as lawyers, tax advisors, or accountants)		
Legal profession (lawyers and tax advisors)	Decentralised and varies according to the <i>Land</i> , legislative basis in GwG	Various <i>Land</i> bar associations and chambers of tax advisors (27 bar associations and 21 chambers of tax advisors)
Notaries	Decentralised and uniformly performed by regional courts in each <i>Land</i> , legislative basis in GwG	Regional courts in each <i>Land</i> (115 regional courts)
Accountants	Centralised, legislative basis in GwG	Federal Chamber of Accountants
Casinos	Decentralised and varies according to the <i>Land</i> , <i>Land</i> -level legislative basis	<i>Land</i> Ministries of interior, State Officers, District or regional governments (20 supervisors)

Note: A full summary of all *Land* DNFBP supervisors and relevant legislation can be found at Annex B.  
Source: German Authorities

### *International co-operation*

56. As set out above, Germany faces significant cross-border ML and TF risks due to its globally networked and export oriented economy and international interconnectedness of its obliged entities. The NRA identifies ML related to foreign predicate crime as high and highlights high risks of ML from Eastern Europe (in particular Russia), Türkiye, China, Cyprus,<sup>29</sup> Malta, British Virgin Islands, Cayman Islands, Bermuda, Guernsey, Jersey and Isle of Man. In relation to TF, Germany faces significant cross-border risks arising from domestic support for foreign terrorist groups based in the Middle East or in Türkiye.
57. Germany has a decentralised model for decision making on international co-operation requests. The Federal Ministry of Justice (BMJ) has delegated its decision-making authority to the Federal Office of Justice in Bonn (BfJ) and to the *Länder* authorities, including regional courts and public prosecution offices. The delegation means that in practice, decisions are mostly made by the *Länder* authorities that are responsible for executing the request according to the location of the assistance sought.

<sup>29</sup> Note by Türkiye: The information in this document with reference to “Cyprus” relates to the southern part of the Island. There is no single authority representing both Turkish and Greek Cypriot people on the Island. Türkiye recognises the Turkish Republic of Northern Cyprus (TRNC). Until a lasting and equitable solution is found within the context of the United Nations, Türkiye shall preserve its position concerning the “Cyprus issue”.

Note by all the European Union Member States of the OECD and the European Union: The Republic of Cyprus is recognised by all members of the United Nations with the exception of Türkiye. The information in this document relates to the area under the effective control of the Government of the Republic of Cyprus.

## Chapter 2. NATIONAL AML/CFT POLICIES AND CO-ORDINATION

### Key Findings and Recommended Actions

#### Key findings

- a) Germany has a good understanding of the national ML/TF risks related to cash, real estate and the banking sector, as well as cross-border risks and emerging risks from the COVID-19 pandemic and virtual assets. This understanding is shared by most federal and *Länder* authorities, and is reflected in the 2019 NRA, subsequent *Länder* risk assessments, and other risk products. TF risk understanding is generally strong, although authorities did not have a comprehensive national, inter-agency approach to the risks posed by *hawala* services.
- b) The national understanding of risk in some areas is still developing, particularly in relation to complex ML (including professional enablers and the use of legal entities), certain parts of the non-financial sector (outside of real estate and cash-related risks), and ML risks related to tax crime. This may be due to information gaps, a lack of statistics, previous limitations in the ML offence (until August 2021), and the more limited involvement of certain authorities and non-financial sectors in the NRA process.
- c) Germany has national policies that respond to certain identified risk areas, including through a National AML/CFT Strategy that was developed based on the NRA. More recent risk assessment products (including the *Länder* risk assessments, a NPO risk assessment, and a legal persons and arrangements risk assessment) are still being brought together to feed into national AML/CFT policies and/or the National AML/CFT Strategy.
- d) Germany has taken a range of measures to mitigate identified risks in the real estate sector. It has also taken some steps to mitigate the high risk of cash-based ML. However, additional measures need to be considered to more effectively mitigate the identified risks in this area, as well as in relation to informal *hawala* services. Germany covers all FIs and DNFBPs under the AML/CFT requirements (no wholesale exemptions apply) and extends the requirements to a broader range of entities in line with risks and requirements at the EU-level. FIs and DNFBPs must apply enhanced and simplified measures in line with ML/TF risks and, in certain cases, Germany has put in place enhanced measures that go beyond the FATF and EU requirements to respond to identified risk areas (e.g., extending AML/CFT obligations to public auctions).
- e) Objectives and activities of competent authorities are largely in line with ML/TF risks. BaFin (the financial supervisor) and the FIU have

implemented structural and resourcing changes in response to identified ML/TF risks. TF authorities' take a risk-based approach to their activities, and specialised law enforcement resources are available in certain *Länder* that face higher ML risks. Other agencies, particularly some LEAs and DNFBP supervisors, are still aligning their objectives and activities with ML/TF risks.

- f) Germany has made progress to address co-operation and co-ordination issues identified in the 2010 MER, although this remains a challenge considering the scale and complexity of the system. The establishment of the Steering Committee on AML/CFT (RÜST-GW) and the 16 *Länder* co-ordinating offices are positive steps, although these mechanisms need strengthening through a formal mandate and additional resources. The Anti-Financial Crime Alliance (AFCA) is another recent step that promotes public-private sector co-operation. While co-operation has improved, ensuring co-ordination between and across the *Länder*, particularly with the over 300 DNFBP supervisors, remains difficult.
- g) The Federal Government has made political commitments to prioritise AML/CFT initiatives. It is not clear if there are mechanisms to prioritise AML/CFT at the political level within *Länder* Governments, which play a vital important role in understanding and mitigating risk, supervision, law enforcement and resource allocation.

## Recommended Actions

- a) Ensure that Federal and *Länder* governments consistently prioritise ML/TF/PF issues, including by securing high-level commitment and ongoing accountability by Federal and *Länder* governments for co-ordination in risk understanding, mitigation and allocation of resources at the Federal and *Länder*-level.
- b) Strengthen and formalise newly-established structures by:
  - a. Formalising the *Länder* Co-ordinating Offices and giving them the mandate and resources to ensure proper and regular co-operation and co-ordination of the national and regional framework and development and implementation of any additional policies to combat ML/TF, at both policymaking and operational levels (including on supervision and law enforcement functions).
  - b. Give the RÜST-GW a formal and binding mandate and ensure all relevant authorities are represented by *inter alia* including tax authorities and formalising the representation and rotation principle for *Länder* Co-ordinating Offices.
- c) Develop a more granular understanding of risks under the second NRA process, with formalised input from all *Länder* governments and authorities (including tax authorities), with a focus on understanding the DNFBP sectors and regional specificities, exposure to abuse by complex corporate structures and professional money launderers, cash-based and trade-based money laundering and emerging risks such as virtual assets.
- d) Considering the risks associated with cash-based money laundering, develop comprehensive policies to address these risks and consider all available measures (for example: a cash-limit for transactions; mandatory reporting on cash transactions; extending reductions of thresholds for conducting CDD to other non-financial sectors; measures to control risks of cash-intensive businesses; a co-ordinated framework for addressing illegal MVTs activities; enhanced customs controls; operational co-operation between the FIU, LEAs and tax authorities; and incentives to encourage people to move from cash to electronic forms of payment and storage).
- e) Engage in proactive co-operation and co-ordination with Data Protection and Privacy authorities to provide regulatory clarity on enhanced information sharing and intelligence functions through advancements in technology and use of advanced analytics to improve effectiveness in several areas of the AML/CFT system.

58. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34, and elements of R.15.

## Immediate Outcome 1 (Risk, Policy and Co-ordination)

### Country's understanding of its ML/TF risks

59. Germany has a good understanding of the ML/TF risks related to cash, real estate and the banking sector. Authorities also demonstrated a good understanding of the emerging risks related to virtual assets. The national understanding of risk in other areas, particularly in relation to certain parts of the non-financial sector (outside of real estate and cash-related risks) and complex ML is still developing. The assessment team's findings are based on: a review of Germany's National Risk Assessment (NRA), the EU Supranational Risk Assessment (SNRA), *Länder* risk assessments, sectoral risk assessments (including of the financial sector, legal persons, and NPOs), and other risk assessment products (e.g., BaFin's Subnational Risk Assessment, FIU annual reports, AFCA papers, TF Situation Reports); as well as discussions with individuals and agencies who participated in developing the NRA and other risk assessment products, policy making agencies, LEAs, intelligence services, supervisors, and the private sector (including FIs, DNFBPs, and NPOs).
60. While Germany produces a range of risk assessment products, many authorities identified the NRA as the foundational document summarising their risk understanding. Germany completed its first NRA in 2019. The Federal Ministry of Finance (BMF) led the NRA process, with the participation of 35 federal and *Länder* agencies.<sup>30</sup> The NRA provides a good basis for risk understanding, although the analysis of certain DNFBP sectors could be more detailed (particularly TCSPs, lawyers and accountants). The NRA was developed drawing on statistics, academic analyses and research, the SNRA, existing risk-assessment products, and discussions between relevant authorities and the private sector. The financial sector fed into the process via working group consultations, a questionnaire, and follow-up consultations. Both industry groups and individual FIs provided input, with entities selected to represent a cross-section of the sector. Involvement of the non-financial sector was more limited, and primarily through industry associations and questionnaires.
61. In addition to the NRA, Germany produces other risk assessment products in particular areas. These include reports and analyses by BaFin (the financial sector supervisor), the FIU and the Federal Criminal Police (BKA). These assessments vary in depth and quality. BaFin's Subnational Risk Assessment (of the financial sector) demonstrates that it has a granular understanding of risk in the financial sector (see IO.3). This assessment is not published, although the findings were communicated to FIs through BaFin outreach. While BaFin contributed to the NRA, the public NRA is much less detailed in its assessment of certain financial sectors (e.g., securities). The FIU's typologies and annual report provide information on certain risk areas. These products largely reflect the risks identified in the NRA, although they do not always include red flags specific to Germany's risk and context.

<sup>30</sup> Agencies and organisations participated through four operational working groups: ML national threat situation/national vulnerability; ML in the financial sector; ML in the non-financial sector; and TF.

62. Following the NRA, all 16 *Länder* were required to produce their own independent risk assessments. These identified regional differences that, in some cases, lead to different, more specific conclusions from the NRA on the risk of certain sectors or products in a particular *Land*. For example, traders in goods (including art and antiquities) are rated medium-high risk for ML in the NRA, whereas the Bavaria risk assessment concludes that the risk in the region is low, given the size of the market, the nature of the customer base, and the type of transactions observed in the region. Some *Länder* risk assessments provide a more nuanced assessment of risk in some DNFBP sectors than that in the NRA. Professional body DNFBP supervisors (for accountants and the legal profession) have also completed risk assessments which vary significantly in the sophistication of their analysis (see IO.3). As these assessments remain recent, their findings have not yet been brought together to provide a national-level understanding of the relative risks between sectors and across regions. Supplementary risk assessments on NPOs and legal persons and arrangements were also developed after the NRA (these are assessed in IO.10 and IO.5 respectively).
63. Germany identifies external threats posed by different jurisdictions. The NRA assessed the ML threat posed by 33 countries/territories, including those with close geographical, economic or immigration links to Germany. Eleven jurisdictions are assessed as posing a high ML risk, including several EU member states. Law enforcement (including those involved in international co-operation) and supervisory authorities demonstrated a good awareness of this assessment. The NRA also shows a good understanding of how geographical risks interact with other risks, e.g., identifying the typologies and predicate offences particular to identified higher-risk jurisdictions.
64. Germany also demonstrated its ability to assess certain national risks on an ongoing basis. The processes established in bringing together stakeholders in the context of the NRA helped authorities to monitor the evolving risks posed by the COVID-19 pandemic and virtual assets. Germany's public private partnership, the Anti-Financial Crime Alliance (AFCA) is a good practice in this respect and provides a forum for relevant government agencies and the private sector to share information to stay on top of changing risks.

### Box 2.1. Germany's understanding of and response to emerging risks posed by the COVID-19 pandemic

The COVID-19 pandemic emerged in early 2020. Germany maintained an awareness of the emerging and evolving risks in this area through regular discussions in the AML/CFT Steering Committee (RÜST GW/TF). In particular, Germany noted the increased ML threat from fraud and cybercrime, compounded by the risk of misappropriation of financial assistance and increased financial volatility.

In response to these risks, in October 2020, Germany released an independent analysis of the impact of the pandemic on Germany's AML/CFT systems, with corresponding recommendations for further work.

In addition, individual authorities took response actions:

- BaFin acknowledged the constraints on on-site inspections and supervisory visits and implemented alternative digital measures, including remote inspections. Through guidance, BaFin encouraged entities to make use of simplified due diligence options where risk permitted, e.g., in the provision of government assistance loans.
- The FIU identified an increase in STRs related to COVID-19 and took steps to prioritise these. Analysis of these showed a concentration of online criminality, including an increase in fraud (e.g., attempts to obtain government assistance and fraudulent offers of protective equipment). Based on this analysis, in May 2020, the FIU released a typology report on fraud and ML related to COVID.
- Intelligence authorities and LEAs established separate units/working groups to address COVID-19 challenges, including exchanging information with foreign counterparts on emerging risks.
- AFCA developed a COVID-19 white paper based on its internal, cross-agency discussions on risks. The paper, which has been updated three times, provided typologies and red flags for fraud and cybercrimes cases related to COVID-19. At the time of the on-site visit, it was made available to approximately 15 700 registered reporting entities.

65. Despite these strengths, Germany still has a developing risk understanding in certain areas. The heavy focus on real estate and cash overlooks other important risks considering Germany is an international financial centre. In particular, the risks of complex corporate structures (including foreign companies) and professional enablers are not as well understood. Issues relating to corporate structures were not comprehensively covered in the NRA, as Germany instead conducted a separate risk assessment of legal persons and arrangements. However, this assessment focused on inherent vulnerabilities rather than materialised threats/risks and was limited in using practical information from supervisors, the FIU, LEAs or other stakeholders to inform risk understanding (see IO.5). In relation to professional enablers, this risk is not analysed in detail in the NRA and authorities and institutions often had a relatively limited appreciation of these risks.

66. Germany's understanding of risk in these areas is hampered by several factors. There are information gaps on the number of professionals engaging in higher-risk activities (e.g., lawyers providing company formation services) and the number of TCSPs operating in Germany. Limitations in Germany's ML offence meant that, until mid-2021, authorities focused more on predicate offences and organised crime than on ML. Law enforcement authorities also tend to focus on natural persons (see IO.7) limiting the information available for assessing risks. Some law enforcement and supervisory bodies demonstrated an understanding of risks in these areas; however, in general, there is a limited appreciation of how complex corporate structures or professional enablers could be used for ML outside of the real estate sector.
67. Similarly, ML risks related to tax crime remains an area of developing risk understanding. The NRA acknowledges the risk of tax evasion in cash-intensive sectors, but the NRA and the assessment team noted some lack of awareness among relevant authorities, including tax authorities, law enforcement and DNFBP supervisors. This may be as tax authorities were not involved in the NRA and because most tax offences were not predicate offences for ML until 2021. Information gaps and with a lack of statistics may also impede Germany's national risk understanding and its ability to monitor implementation of AML/CFT measures. For example, Germany does not routinely collect nor is able to isolate statistics on: all ML prosecutions or convictions (as cases are registered based on the 'main' offence and kept in 141 independent prosecution offices) or MLA requests which prevents a complete understanding of the extent to which these mitigation measures are being pursued and the residual risk in the jurisdiction.

### *Money laundering*

68. Germany rates its ML threat as medium-high, due to its high economic attractiveness, high use of cash, and the diversity of its economy. Authorities, including *Länder* representatives met at the on-site, share a good, consistent understanding of the crimes identified in the NRA as the most significant proceeds-generating offences at the national level: fraud, drug-related crime and human trafficking. Authorities demonstrated a strong understanding of ML related to organised crime. The NRA shows an understanding of the different methodologies and sectors that might be used for the identified higher-risk predicates (e.g., proceeds of drug crime are often laundered through real estate, urban businesses, and gambling and betting establishments). This understanding was echoed by federal and *Länder* LEAs. However, the understanding of risks related to tax crime, complex ML, and legal persons and arrangements was less consistently understood.

*Terrorist financing*

- 2
69. Germany's NRA rates its overall TF threat as medium-high. This is distinguished from the risk of terrorism itself, which is identified as a high abstract threat on the basis of risks posed by individual radicalised actors. The NRA focuses on the threat from international terrorist organisations, although it distinguishes between domestic risks (jihadist groups without organisational structures operating in Germany, self-funding lone wolves, organised right-wing terrorist groups) and cross-border risks (domestic support for foreign terrorist groups). The NRA identifies the highest-risk TF channels as MVTs (including informal *hawala* services) and cross-border cash transfers. In addition to the NRA, federal law enforcement and intelligence agencies<sup>31</sup> regularly develop confidential TF situation reports. These provide a high level of detail and nuance on Germany's specific TF threats and vulnerabilities. Based on the NRA and these reports, federal and *Länder* authorities demonstrated a good understanding of TF funding streams, including legal sources (e.g., donations, sale of goods) and illegal sources (e.g., improper receipt of government transfers). TF authorities also demonstrated an awareness of how the different TF risks interact with available funding channels.

*National policies to address identified ML/TF risks*

70. Germany has taken policy action to respond to certain identified risk areas. However, policies lag behind in other high-risk areas and certain issues have persisted since the last evaluation in 2010. The assessment teams' findings are based on: risk assessment products (including the NRA); AML/CFT strategies; and discussions with policy-makers, law enforcement, supervisors, and the private sector.
71. Following the completion of the NRA, Germany published its first documented National AML/CFT Strategy in January 2020. The Strategy identifies concrete actions in 11 areas to respond to regional and international standards (including EU and FATF requirements) as well as national risks. The Strategy draws on the NRA, and is therefore consistent with the NRA's findings. However, certain higher risks identified in the NRA or other risk assessments (such as informal *hawala* services) are not addressed in the Strategy (or through other national policies; see below). Positively, a large number of the Strategy's actions have already been completed, including amending the ML offence to include all offences as predicate offences (see IO.7).
72. Prior to the Strategy, Germany took steps to address risks identified during the NRA process. For example, a number of concrete measures were implemented in response to identified risks in the real estate sector (see Box 2.2 below). However, other risks in this sector (such as the existence of bearer deeds or the request from law enforcement to bring together data in 532 different property registers in each *Land*) remain unaddressed or are at an early stage. Germany's response to the COVID-19 pandemic (see Box 2.1 above) is another good example of a multi-agency response to emerging risks.

---

<sup>31</sup> The Federal Office for the Protection of the Constitution (BfV), Federal Intelligence Service (BND) and Federal Criminal Police Office (BKA).

**Box 2.2. Actions to address risk in the real estate sector**

Germany has implemented a broad range of national, cross-agency measures to address the risks identified in the real estate sector:

- **Application of AML/CFT measures to leasing agents:** In recognition of the risks related to luxury leasing, Germany extended AML/CFT measures (risk management and due diligence obligations) to estate agents acting in high-value rental or lease agreements.
- **Rules-based STR requirement for real estate transactions:** Because of a strict interpretation of legal professional privilege, notaries and the legal profession in Germany stated that in practice they will only report STRs where they have positive knowledge of ML/TF. To overcome this in respect of the identified higher-risk area of real estate transactions, in mid-2020, Germany issued an ordinance mandating reporting by these professions where a specific red flag is identified in the context of a real estate transaction.
- **Beneficial ownership requirements for companies acquiring real estate:** At the end of 2019, Germany expanded its Transparency Register requirements to oblige foreign companies acquiring real estate in Germany to enter their beneficial owners in the Transparency Register.
- **AFCA working group on real estate:** One of AFCA's five working groups focuses on ML in the real estate sector. The group includes representatives from real estate financing entities and real estate agents, as well as public sector agencies. The group has developed papers on ML risks and typologies in the real estate sector, which are available to all reporting entities.
- **FIU focus on real estate:** Following an increase in STRs related to real estate (due in part to the new rules-based reporting requirement), the FIU is undertaking work to analyse these STRs to identify trends. The FIU conducts workshops with industry groups (including real estate agents, notaries and lawyers) on the risks in the sector and relevant red flags.
- **Berlin notary supervision task force:** In the beginning of 2020, following the NRA, the Berlin notary supervision unit (at the Berlin Regional Court) established a special task force for supervising notaries involved in real estate transactions.

- 
- 2
73. Germany identifies cash as a high risk for both ML and TF, particularly in the German context. The risks in this area are well understood and some action has been taken, including lowering the threshold for enhanced due diligence for cash transactions in high-cash sectors, including casinos and DPMS (see R.22). BaFin has also issued guidance for FIs encouraging enhanced measures for cash payments. Certain reporting entities also implement their own enhanced measures in this area, such as refusing to accept cash or undertake cash transactions (see IO.4). Nonetheless, there is a cultural and traditional attachment to cash, which may have prevented Germany from considering a wider range of measures that could better mitigate the risks in this area, such as cash transaction limits or mandatory cash reporting. Authorities have only recently taken steps to target and mitigate the risks posed by cross-border unaccompanied cash movements (see IO.8).
  74. Germany identifies informal MVTs services like *hawala* as one of the highest risk TF channels. Certain agencies (particularly intelligence services and BaFin) undertake some activity in recognition of these risks. However, this remains a challenging area and there is no co-ordinated strategy or inter-agency response to combating or collecting intelligence on informal *hawala* services. This gap may contribute to overlooked risk areas; for example, several major MVTs providers spoke about the identification of challenges they face in relation to providing services to refugees/asylum-seekers. BaFin has produced guidance on this issue, but could consider whether further flexibility could be encouraged in the application of CDD processes to ensure this group can access services and does not resort to unlicensed channels, perpetuating the market for *hawala* services.

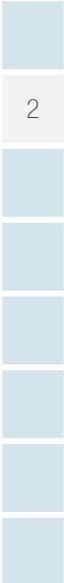
### *Exemptions, enhanced and simplified measures*

75. All relevant FIs and DNFBPs are required to implement AML/CFT measures and Germany has not granted any wholesale exemptions from AML/CFT requirements. FIs and DNFBPs must apply enhanced and simplified measures in line with ML/TF risks (see R.1). The assessment team's findings are based on: Germany's AML/CFT regulatory framework; risk assessment products; and discussions with authorities and the private sector.
76. Based on the risks identified in the NRA, Germany has applied enhanced measures that go beyond the FATF and EU requirements. For example, AML/CFT obligations have been applied to public sector auctions in recognition of the high use of cash and resulting risks in this area. The threshold for applying AML/CFT measures for the sale of precious metals and stones was reduced from cash transactions of EUR 10 000 to EUR 2 000. Online gambling providers are subject to stricter CDD requirements than land-based providers in line with the high risks identified in the gambling sector, which are compounded online by the variety of available payment methods and room for anonymity. Germany also requires enhanced measures in line with the FATF Recommendations (see R.12 and R.19).

77. Germany allows reporting entities to apply simplified due diligence to low risk situations, although the list of low risk factors that FIs and DNFBPs can consider includes factors that are not based on an assessment of risk (see R.1) Beyond this, Germany has not adopted general simplified measures on the basis of its risk assessment. During the COVID-19 pandemic, in light of the difficulties with face-to-face identification, BaFin reminded financial institutions of their ability to conduct simplified due diligence (e.g., by accepting a copy of an identification document) where risk permitted. BaFin has also produced guidance for CDD for refugees and others without standard identification documents but could consider further flexibility to enable refugees to send and receive funds from abroad as appropriate (see IO.4).

### *Objectives and activities of competent authorities*

78. The objectives and activities of Germany's competent authorities are largely in line with its identified risks. The assessment teams' findings are based on: discussions with policy-makers, law enforcement and supervisory authorities; risk assessment products, including analyses, typologies, and horizontal reviews; and information on staffing levels and organisational structures of relevant agencies.
79. Federal policy bodies have been successful in incorporating the results of Germany's risk assessments into recent legislative and regulatory changes. The BMF has also established new units to improve co-ordination between Federal and *Länder* governments, in recognition of the vulnerabilities in this area. It is not clear that all *Länder* governments have taken similar steps to align their objectives and activities to identified regional risks, including in terms of the prioritisation and risk-based allocation of resources.
80. Certain Federal ministries or agencies have also adjusted their resources and structures in line with the identified risks (see R.1). The FIU's work processes were restructured in 2019 so that the key analytical teams are arranged according to risk areas. The risks identified by the FIU as key risk areas are largely consistent with those identified in the NRA. This enables the FIU to focus on these risks and prioritise STRs accordingly. As a result, the typologies produced by the FIU align with the major risk areas identified in the NRA. However, the development of the FIU's risk priorities was undertaken with limited input from LEAs and they do not wholly align with LEA's operational priorities.

- 
- 2
81. Law enforcement authorities at the federal and *Länder* level have shown their ability to form dedicated teams around large-scale cases and in asset recovery, but in general, resources are not allocated to specific risk areas or focused on ML (separate to a focus on predicate offending). Agencies are able to establish joint taskforces to deal with specific ML cases where necessary. The BKA and certain *Länder* police authorities and public prosecution offices have set up units responsible for economic crime and asset recovery (including ML); however, there is limited evidence that they have amended their broader objectives or activities to focus on specific ML risks. The BKA while taking an important role in combating TF, primarily pursues ML in the context of organised crime. The developing risk understanding in relation to legal persons and arrangements, complex ML, and professional enablers means efforts in these areas remain relatively limited, and LEAs in particular remain focused on natural persons. In contrast, law enforcement and intelligence agencies demonstrated their ability to respond to specific TF risks. Two separate bodies have been established in line with the identified risk areas. The Joint Counter-Terrorism Centre (GTAZ) focuses on religious extremism and religiously-motivated terrorism risks, while the Joint Centre for Combating Extremism and Terrorism (GETZ) considers right-wing and left-wing extremism and terrorism, foreign (non-religious) extremism, and other risks as they arise. In addition, the BKA has established a specific division on religiously-motivated terrorism, and the Federal Office for the Protection of the Constitution (BfV) has clear policies and strategies for responding to religiously-motivated domestic and foreign extremism and terrorism, high-risk NPOs, and the risks of right-wing and left-wing extremism.
  82. The risk-based approach is well-cemented within BaFin. BaFin has demonstrated its ability to align its resources to identified risk areas; for example, additional staff have been added in in response to emerging risks from VASPs (see IO.3). BaFin's structure allows it to focus on the highest risk areas and institutions, with sufficient flexibility to respond to changes in its risk landscape. Horizontal reviews by BaFin have focused on identified higher-risk areas, e.g., correspondent banking. There is a mixed approach among DNFBP supervisors, most of which operate at the *Länder* level. DNFBP supervisors take certain risk factors into account in their supervisory activity, but generally are not considering all relevant ML/TF risk factors and variables in fully actualising a risk-based approach and supervisory strategy. Nonetheless, there are some good examples of supervisors responding to identified risks, for example, the Berlin Task Force for notary supervision was established in response to specific risks identified in Berlin's real estate sector. In most cases, however, DNFBP supervisors face challenges due to the size of their supervised population and the acute lack of resources available, which severely impairs their ability to implement an effective risk based approach to supervision (see IO.3). As a result, they are still working to establish a risk-based approach.

*National co-ordination and co-operation*

83. Key AML/CFT functions are highly decentralised in Germany and many of the core AML/CFT activities are conducted at the *Land*-level. Poor co-ordination was identified as an issue in Germany's last mutual evaluation in 2010. Germany has made efforts to improve co-operation and co-ordination between the Federal and *Land* governments and across *Länder* since this time. However, many of these efforts are recent (commencing in 2017). While these efforts are positive, they are yet to reach their full potential and it is difficult to judge their effectiveness. While the Federal Government has made political commitments to prioritise AML/CFT initiatives, it is not clear if there are mechanisms to prioritise AML/CFT at the political level with *Länder* Governments. The findings are based on: discussions with Federal and *Land* authorities; and information on and documents from relevant bodies and committees.
84. High-level co-ordination on ML/TF issues happens through the Steering Committee on ML (RÜST-GW). RÜST-GW is an informal committee that Germany established in 2019 in advance of the FATF evaluation. It exchanges information to identify new risks, monitor existing risks, and develop and implement policy responses. The Committee has played a positive role in monitoring emerging risks (especially in the COVID-19 context) and was responsible for producing the National AML/CFT Strategy. The Committee brings together relevant federal authorities, although tax authorities are not represented, and includes two *Länder* representatives on a rotating basis (see R.2). The *Länder* representatives are responsible for channelling information to and from other *Länder*. It is positive that the *Länder* representatives themselves have a role in sharing information across the 16 *Länder* governments, however, this alone does not assure the buy-in or prioritisation of AML/CFT by *Länder* governments. RÜST-GW does not have a fixed mandate, and operates based on inter-agency agreement. As it lacks a formal structure and clear political support from all 17 governments, the committee currently has a limited ability to ensure the continued prioritisation of AML/CFT issues and monitoring of recent reforms.
85. Germany has made other recent, positive efforts to promote co-ordination across the *Länder* and between the Federal and *Länder* governments. From early 2021, all *Länder* have established permanent Co-ordinating Offices. These are responsible for engaging with the Federal government and other *Länder* on AML/CFT issues, co-ordinating and contributing to risk assessments, and sharing information to/from relevant *Länder* authorities. This is a positive measure new development, which is still evolving. Co-ordination is more advanced in some *Länder* than in others. In most cases, the Co-ordinating Office is currently a single person contact point, with FTEs ranging from 0.5 to 2.8 persons. This level of resources limits the Offices' ability to proactively co-ordinate and engage with relevant authorities in their *Land*. Co-ordination is further complicated in some *Länder* where supervisory responsibilities are delegated to district governments (see IO.3), meaning the Co-ordinating Office must co-ordinate an even wider range of authorities within the *Land*. Likely due to the recency of this mechanism, it is not yet clear that these Offices have the resources and capacity necessary to co-ordinate and liaise with the many relevant *Länder* authorities (both law enforcement and supervisory), identify important information (e.g., on emerging risks or policy concerns), and feed this to other *Länder* and the Federal government as necessary, in addition to communicating important messages from Federal authorities.

86. In practice, operational co-operation between agencies works well through established mechanisms for co-operation and on an *ad hoc* basis when required. On the law enforcement side, Joint Financial Investigation Groups (JFIGs) have been established in all *Länder* and bring together customs and police authorities to conduct joint investigations on ML. *Ad hoc* cooperation is also used when needed and LEAs make good use of task forces to investigate large multi-jurisdictional cases. For TF, the GTAZ and GETZ bring together 40 Federal and *Länder* police, prosecution and intelligence agencies to co-ordinate and co-operate on terrorism issues and individual cases, including TF, through daily briefings. The FIU is also able to participate in these groups on an as-needed basis and Germany is working addressing operational co-operation issues between the FIU and *Länder* LEAs.
87. On the supervisory side, co-operation and co-ordination across the over 300 *Land* supervisors remains an ongoing challenge. There are mechanisms that exist to promote co-operation, such as a national symposium, the Darmstadt Working Group on ML Prevention, which brings together supervisors to share experiences. These efforts have had positive outputs, including developing consistent, national guidance for the different DNFBP sectors. However, ensuring a consistent and strategic approach to supervision remains a major challenge, particularly for DNFBP entities that operate across multiple *Länder* and are therefore subject to different supervisory processes and regimes (see IO.3).
88. Co-operation between the public and private sector is developing well, particularly due to AFCA, which provides a formal forum for this co-operation. Private sector membership is predominantly from the banking sector but has also expanded to include real estate agents, casinos and the Federal Chamber of Notaries. While it is a new body (established in 2019), AFCA has proved effective in drawing on a range of expertise to produce typologies and working papers on identified risks. As trust and confidence in the body grows, it could be further enhanced through increased practical and operational use, e.g., in specific cases.
89. An area for further development is co-operation between AML/CFT authorities and data protection authorities. Germany has 17 data protection authorities (see R.2). Several operational agencies as well as members of the AFCA mentioned the need for greater co-operation with data protection authorities to enable more effective data integration, information sharing and advanced analytics which is critical for effective AML/CFT mitigation in the context of the German federal system where information can be fragmented.
90. Fora exist for co-operation on PF sanctions, including an inter-ministerial co-ordination group, a Ministerial Working Group for Export Control, and a Prohibition Discussion Group (see R.2). These are largely focused on the implementation of targeted financial sanctions, rather than on broader PF issues. Germany could benefit from a more established forum for PF co-operation to monitor risks and trends and ensure consistent implementation of PF measures given Germany's context (see IO.11).

### *Private sector's awareness of risks*

91. Germany has taken steps to inform relevant stakeholders of the NRA's findings and many obliged entities demonstrated a good awareness of risks. The assessment team's findings are based on: discussions with the private sector; discussions with public authorities; and websites and other publications by government authorities.

92. The private sector was involved in the NRA, with particularly strong engagement from the financial sector. This engagement helped to promote the NRA findings within FIs. DNFBPs were involved through industry associations, with limited direct engagement. Nonetheless, both financial and non-financial supervisors and other government authorities at the federal and *Länder* level have endeavoured to publicise the findings of the NRA. Information is shared with the supervised population, both through supervisors' websites, targeted outreach and in the course of supervisory activity. In addition, obliged entities are required to incorporate the NRA into their risk assessment. AFCA provides another positive platform for increasing the private sector's awareness of risks. The FIU makes typologies, AFCA papers, and other risk information available to registered reporting entities.

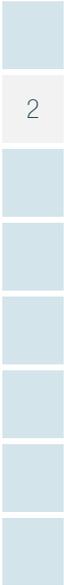
## Overall Conclusion on IO.1

Germany has taken steps to increase its national understanding of ML/TF risks, including through its first NRA, a range of other risk assessment products, activities by individual agencies at the *Land*-level, and the creation of a public-private partnership, AFCA. These steps have given Germany a better national understanding of the risks related to cash, real estate and the banking sector, as well as cross-border risks and emerging risks from the COVID-19 pandemic and virtual assets. Risk understanding in other areas is still developing, particularly in relation to complex ML, certain areas of the non-financial sector, and ML risks related to tax crime.

Mitigation measures for risks related to real estate are particularly strong and steps have been taken to respond to risks in other areas (e.g., extending or strengthening AML/CFT requirements for public auctions and online gambling providers). Measures to address the high risk of cash-based ML have not been comprehensively considered in light of the risks Germany has identified in this area. Limited resources in some areas also hampers prioritisation, resource allocation and effectiveness in implementing risk-based mitigation measures, particularly for DNFBP supervision and pursuing ML investigations and prosecutions. Information gaps and a lack of statistics may impede Germany's national risk understanding and its ability to monitor implementation of AML/CFT measures.

There are moderate shortcomings in co-operation and co-ordination mechanisms, which are given weight given the complexity of Germany's system, and the *Länder* responsibility for policy-making and implementation of substantial elements of the AML/CFT regime (both preventive and law enforcement). Germany has taken positive steps in this area since 2017, although many of these efforts remain recent and their full effectiveness is yet to be seen.

**Germany is rated as having a substantial level of effectiveness for IO.1.**



## Chapter 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

### Key Findings and Recommended Actions

#### Key Findings

##### 10.6

- a) Competent authorities have access to a broad range of information to use in financial investigations of predicate offences, ML, TF and to identify proceeds of crime. Case studies demonstrated that LEAs, prosecutors and intelligence agencies have the skills and capacity to conduct complex financial investigations using multiple information sources.
- b) LEAs access and use financial intelligence to some extent. STRs and reports on cross-border cash movements are under-utilised and there is scope for improving use of FIU disseminations. There is a low number of requests to the FIU for financial intelligence. While a large number of STRs are disseminated to LEAs, only a small proportion are used in criminal proceedings despite the German mandatory prosecution principle that requires all leads must be investigated. This indicates that disseminations are not being made fully in line with LEA operational needs.
- c) The transition to a new FIU in 2017 has been a positive change to address challenges arising from the old decentralised FIU model. However, there have been challenges in the transition including with co-operation and buy-in from LEAs. The FIU has increasing access to data but technical limitations impact its effectiveness and efficiency. FIU analysts manually search and cross-check information which is a highly resource intensive process. This remains an impediment to the FIU's ability to efficiently filter and focus on complex and advanced analytical work with enhanced analytical tools.
- d) The FIU receives, to some extent, STRs that contain relevant and accurate information. STR quality is variable and underreporting from high-risk DNFBP sectors (particularly real estate) limits the financial intelligence available in relation to high-risk sectors. While efforts to address the low-reporting by notaries has been addressed, the changes had not resulted in intelligence or operational outcomes. There is access to information on cross-border cash reports on a hit/no-hit basis but the data is not fully integrated into the FIU database.
- e) In active investigations, competent authorities co-operate and exchange information and financial intelligence well, particularly in TF cases (although the FIU could be better integrated in a more timely or direct manner into formal TF co-ordination and co-operation frameworks). Task

forces and joint investigation teams are particularly effective at bringing together information and investigating leads.

#### 10.7

- a) Amendments to the ML offence demonstrate that Germany is committed to the active pursuit of ML at the policy level; however, these reforms have not yet fully translated into operational results. In practice, there is a focus on prosecuting for the predicate offence and barriers to pursuing ML in cases where there is no clear link to a predicate offence.
- b) ML is identified and pursued in line with risks to some extent. Overall, Germany takes a reactive rather than proactive approach to the identification of ML cases. ML related to fraud, drug trafficking and the real estate sector are well understood and pursued. However, ML related to professional ML networks, cash smuggling, human trafficking, foreign predicates and complex ML is more difficult for Germany to identify and investigate. The overall number of prosecutions pursued by Germany is also low indicating that ML cases are not being proactively pursued and prioritised.
- c) Germany has demonstrated the capacity to prosecute and obtain convictions for different types of ML but, due to gaps in the statistics, it was not demonstrated that different types of cases are systematically pursued. It is also not clear that Germany prioritises the pursuit of ML investigations involving legal persons (particularly in complex cases where a natural person or a predicate offence cannot be immediately identified).
- d) A wide range of sanctions are available but they are not imposed in a manner that is fully effective and dissuasive. Sentences tend to be in the lower end of the scale with the majority of cases ending with a fine even for more complex ML cases.
- e) There is a lack of comprehensive statistics on all convictions of ML with more detailed statistics only available in cases where ML was the most serious offence, whereas statistics in cases where ML was not the most serious offence do not offer the same degree of details and are only available from 2017 onwards. Case tracking and monitoring is carried out at the *Land*-level and this creates challenges for Germany in detecting trends and formulating responses at a national level.
- f) Germany has tools to pursue alternative measures through prosecutions for predicate offences and asset recovery measures. However, these measures are pursued regardless of whether or not it is possible to secure an ML conviction and there is no clear policy or strategy for disrupting and sanctioning ML in a consistent and comprehensive manner.

#### 10.8

- a) Germany recognises the importance of asset recovery and law enforcement agencies consistently pursue confiscation as a policy objective. The introduction of non-conviction based asset recovery in 2017 accompanied by instructions to police and prosecution agencies and the provision of

additional resources have resulted in an increase in the amount of criminal proceeds confiscated.

- b) The overall figures on assets frozen and confiscated are large (approximately EUR 920 million annually including corporate fines) and broadly in line with Germany's risk profile. Asset confiscation is a mandatory consideration for prosecutors when handling cases involving proceeds of crime. LEAs have the tools and skills to trace, freeze and confiscate assets including instrumentalities of crime and assets of equivalent value.
- c) There is a framework in place to detect cross-border cash movements and some understanding of risks related to cash smuggling. However, sanctions related to declarations and disclosures are low and asset confiscation of seized cash could be improved. Customs agencies were able to evidence operational activity focused on the confiscation of cross-border cash movements, particularly cash couriers, but there was limited information of the risks arising from bulk cash and cash movements through mail and cargo considering Germany's risk profile.
- d) While asset confiscation statistics are impressive, there are issues with the way data and statistics are collected and while there are relatively comprehensive statistics kept on asset freezing, equivalent data is not available for asset confiscation and cross-border cash disclosures and declarations.

## Recommended Actions

### 10.6

- a) Review the financial intelligence development process and clearly outline roles and responsibilities between the FIU and the GFGs and ensure that relevant parties are adequately mandated and resourced to perform these functions and understand each other's roles.
- b) Continue to resource and support the development of the FIU by: improving the tools available to the FIU to automatically assess different data sets in the prioritisation process and substantially improving the tools available to bring together and analyse information efficiently including artificial intelligence or other advanced analytics; promoting the FIU's role and services; hiring staff with a LEA or financial services background and forensic accountants.
- c) Reconsider the FIU's prioritisation mechanisms in line with detailed feedback from law enforcement agencies and ensure that disseminations are in line with operational needs, and that professional and third-party money laundering is captured under this risk framework.
- d) Implement measures to improve access to information and exploit synergies between the FIU and LEAs, such as a real time or automatic

mechanism for LEAs to identify and retrieve information from the FIU on a hit/no-hit basis in relation to ongoing investigations, such that the FIU can concentrate on proactive disseminations and increase its role in providing financial analysis (based on STRs and other consolidated information sources) for LEAs.

- e) Enhance the FIU's engagement in terrorist financing cases and formalise the FIU's role in TF coordination mechanisms to ensure that financial intelligence is meeting operational needs and financial intelligences features prominently in interagency mechanisms.

#### 10.7

- f) Increase the detection, investigation and prosecution of complex and professional ML with dedicated, co-ordinated and focused resources for investigating and prosecuting ML across Germany. The FIU and GFGs should further prioritise and improve the quality of cases to increase the capacity of prosecutors to focus on high-risk ML activities.
- g) Utilise the revised ML offence to pursue prosecutions of different types of ML in line with Germany's risk profile (e.g., foreign predicate offence, third-party laundering, stand-alone offence).
- h) Prioritise the planned reforms to liability of legal persons for criminal offences including ML and enhance the investigation of legal persons in ML schemes (particularly in complex ML cases where a natural person cannot be identified).
- i) Increase *Länder*-level resources for financial investigators and prosecutors dedicated to ML investigations (similar to the increase that accompanied changes to the asset recovery legislation).
- j) Enhance the availability of comparable, detailed and up-to-date data on ML investigations, prosecutions and convictions across Germany to enable a better understanding of the number and type of cases of ML pursued to inform resource allocation and risk mitigation efforts.

#### 10.8

- a) Further develop ML/TF risk understanding and detection of bulk-cash movements, particularly through mail and cargo and address required mitigation measures.
- b) Consider whether it would be beneficial to establish additional units or to increase staffing for existing units to pursue parallel investigations into proceeds of crime or investigations into proceeds of crime where there is no link to a predicate offence.
- c) Consider whether the current confiscation regime with respect to cross-border cash movements is adequate and whether it would be beneficial to introduce the concept of objective factual circumstances to the regime; and, whether sanctions are sufficient in all cases.
- d) Pursue actions at early stages of investigation to trace and freeze assets to reduce the discrepancy between confiscation orders granted and those that are ultimately satisfied. Also actively pursue the retrieval of assets from

other jurisdictions and the proceeds of foreign predicate offences located in Germany.

- e) Improve data collection to enable corporate fines to be distinguished from asset recovery amounts.

93. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32 and elements of R.2, 8, 9, 15, 30, 31, 34, 37, 38, 39 and 40.

### Immediate Outcome 6 (Financial Intelligence ML/TF)

#### *Use of financial intelligence and other information*

94. Federal and *Länder* authorities have access to, and use, a broad range of financial information from different sources that helps them investigate predicate offences, money laundering (ML) and terrorist financing (TF) and trace related criminal proceeds. There is active use of a wide range of information and intelligence sources including disseminations from the FIU, bank account information retrieved through the Electronic Account Retrieval System, corporate registers, real estate registers, cash declaration and disclosure reports, tax information, telecommunications intercepts, surveillance and undercover operations. However, while FIU disseminations are used to some extent, the low number of requests for information to the FIU from LEAs and the relatively low proportion of disseminations used in criminal proceedings suggests that STR information is not fully exploited to detect and investigate ML and related predicate offending and FIU analysis could be better aligned with LEA needs.
95. The assessment team's findings are based on: statistics on STR reports and disseminations; some limited statistics on enquiries made to various databases; and interviews and case studies involving Federal and *Länder* investigation and prosecution authorities.
96. Germany has a de-centralised structure for investigations and prosecutions with responsibility for criminal investigations primarily falling to the *Länder* but has put in place the necessary frameworks and co-ordination mechanisms to support financial investigations. Case studies demonstrated that there is significant competence in conducting financial investigations within specialist offices. At the investigative level, Germany has established Joint Financial Investigation Groups (JFIGs) bringing together investigators from the relevant police agency and Customs to review disseminations from the FIU and conduct preliminary financial investigations. Twenty-nine specialised financial crime offices operate in *Länder* prosecution offices with higher exposure to financial flows. These are staffed with dedicated prosecutors, economic consultants and accountants whose expertise can be drawn upon in investigations. In addition, ten *Länder* have specialised asset recovery units (either at a central office or specialised departments at local public prosecution offices) and ten specialised TF units have been established at *Länder* and federal-level to pool expertise and are available to support investigations. Complex cases involving multiple *Land* or cases with an international dimension can be referred to, or co-ordinated, by the BKA or co-ordinated through a task force model.

97. The mandatory prosecution principle<sup>32</sup> and a legal requirement to pursue asset recovery in proceeds generating offences means that LEAs routinely access and use financial information and investigations if a case requires it. The case studies below demonstrate that LEAs use financial and other information as part of these investigations.
98. Information on cash declarations and disclosures is held by Customs on a separate database that can be accessed directly by the FIU and by police and prosecutors upon request. Customs is the primary user of this information for Customs-related investigations. The FIU cross-checks incoming STRs against the cross-border cash declaration database on a hit/no-hit basis. Further cross-checks must be done manually; both sets of data are not automatically cross-checked on an ongoing basis. Other investigative agencies can access the information by request but no statistics are available on the extent to which this database is used by these authorities.
99. As demonstrated by the case studies below, investigation agencies and prosecutors have broad access to financial information through various databases and registers to progress ML, TF and predicate offence investigations. In the course of a criminal investigation, prosecutors, intelligence agencies and police have the power to access information without going through a court process which ensures that they have access to information from obliged entities when needed. Prosecutors and LEAs indicated that they would often use this option rather than going through the FIU for information as they have the relevant powers and were accustomed to doing so before the centralised FIU was put in place.

### Box 3.1. Use of financial intelligence and information in an ML case - MV-GW-4/NW-GW-115

The accused offered ML services to criminal groups by opening and running numerous money collection accounts through which they could receive and launder funds. In this case, the accounts were used to launder proceeds of online fraud. Victims from Germany and abroad were asked to deposit money into these collection accounts which were used by the criminal group to obscure their identity.

The case originally started as a fraud investigation. The ML component came to light when a website was identified which listed accounts that could be used for ML purposes. In order to identify the natural person behind these accounts, investigators obtained information from banks that identified three telephone numbers linked to the accounts that were then subject to monitoring using telecommunications intercept powers. Searches of the Commercial Register and requests for information from the FIU to foreign FIUs uncovered information on 17 foreign bank accounts, beneficial owners of these bank accounts, information on account transactions and information on foreign legal persons which helped investigators assess the extent to which financial transactions abroad were related to the investigations in Germany. This information helped investigators to uncover the fraud and ML scheme whereby foreign nationals were brought to Germany to

<sup>32</sup> According to ss.152(2), 160 and 163 of the Code of Criminal Procedure (*Strafprozessordnung*, ("StPO")), authorities must investigate and prosecute where they have a suspicion that a crime has been committed.

be made nominee directors of companies and open company accounts which could be used for ML purposes.

The investigations uncovered the use of ten accounts through which EUR 50 million had been laundered over the course of a year. The accused was convicted of 136 counts of ML and was sentenced to four years in prison. The fee he received for his services (EUR 190 299) was also subject to asset confiscation measures and EUR 50 000 was ultimately confiscated.

Source: German Authorities

### Box 3.2. TF/TFS Case Study: Use of financial intelligence to identify and pursue a middleman in an international TF fundraising network - GBA-TF-4

The accused was suspected to have supported a foreign terrorist organisation (the so-called Islamic State of Iraq and the Levant (ISIL)). The accused allegedly worked as a middleman in an international fund-raising network and was suspected of having supported ISIL by channelling EUR 15 000 through the hawala system to ISIL fighters in Syria.

The investigation was triggered via an MLA request from Belgium in December 2016. From December 2017, the *Land* Criminal Police Office (LKA) Schleswig-Holstein acting on behalf of the Federal Prosecutor General (GBA) surveilled the accused and family members using telecommunications intercepts to determine their connection with ISIL. Authorities also seized and evaluated financial documents from a search warrant of a house, determined the accused's bank details via enquiries to BaFin's Electronic Account Retrieval System, obtained consolidated account statements from banks and made enquiries to large MVTs providers. Based on these enquiries one of the large MVTs providers filed an STR in February 2018 which was disseminated by the FIU to the public prosecutor. Authorities also queried the pension insurance (social security) system and land registries. Prosecutors also received further analysis by one of the large MVTs providers on the broader financial network via US authorities.

The investigations revealed that the accused received money transfers from Kosovo, Belgium, Germany and Norway (mostly via two large MVTs providers) and then withdrew the money in cash. Based on the telecommunications surveillance and the evaluated chat communications, it was established that, immediately after the cash withdrawals, the accused met with a *hawala* dealer in Germany and communicated with the money recipient in Syria about the collection of the money from a *hawala* office.

The intercepts and financial investigations allowed investigators to trace 15 money transfers from countries including Kosovo, Belgium and Norway via the accused to the hawala dealer and onto the recipient in Syria. Donors in Germany were also identified.

Investigations were launched in Germany against two suspected *hawala* dealers and investigations were also launched into two donors located in Germany which were ultimately terminated as intent to finance terrorist activity could not be established.

Following further covert measures and MLA requests to Kosovo, the US, Norway, Italy and Belgium, an arrest warrant was issued against the accused in June 2018. Search warrants were also issued against the donors in Germany. The warrants were executed at the same time as measures were taken in Norway against the persons suspected of financing terrorism there. In March 2020, the accused was sentenced to a prison term of three years and nine months for supporting a foreign terrorist organisation in breach of targeted financial sanctions under section 18 of the *Foreign Trade and Payments Act (AWG)*.

Note: More details of the case are outlined in box 4.2.  
Source: German Authorities

100. A significant amount of information is available to investigators through registers like the Transparency Register, Commercial Register, registers of associations and real estate Registers but the multiplicity of registers across the different *Länder* and missing, incomplete or unverified information on them can limit the usefulness of these registers for investigators (see IO.5). Some investigators also noted it could be challenging to search the registers as many were not centralised and required separate queries with each *Land*. The most commonly used source of information is bank account information retrieved through the Electronic Account Retrieval System run by BaFin that allows access to information on accounts collected and held by obliged entities (including information on the owner and beneficial owner). The FIU and investigative agencies made 304 240 enquiries in 2020 which is over double the number of enquiries made in 2017 and reflects an overall increasing trend in the use of this tool.

**Table 3.1. Bank account enquiries through the Electronic Account Retrieval System**

Requesting agency	2017	2018	2019	2020	2021 (up to June)
FIU	2 049	10 318	18 113	15 387	8 409
Police Authorities	84 092	87 931	130 770	219 754	141 225
Public Prosecution Office	27 812	30 671	29 818	39 375	21 418
Customs Authorities	10 173	9 645	10 624	14 057	6 206
Tax Investigation Service	13 690	13 249	12 626	15 667	9 654
<b>Total</b>	<b>137 816</b>	<b>151 814</b>	<b>201 951</b>	<b>304 240</b>	<b>186 912</b>

Source: German Authorities

101. While authorities use a wide range of sources, information from the FIU and from STRs is only used to some extent. Statistics on requests for FIU information show that there is a low number of requests compared to the number of spontaneous disseminations and the number of enquiries made to other information sources such as through the Electronic Account Retrieval System. For example, in 2020 there were 3 798 requests for FIU information compared to 304 240 requests for information through the Electronic Account Retrieval System (see Table 3.1 above). Feedback reports from public prosecution authorities indicates that while the FIU also makes a large number of disseminations (24 700 in 2020), the majority of these disseminations do not result in an investigation or prosecution and are closed after a preliminary assessment by the relevant Joint Financial Investigation Group (GFG) or public prosecution office. In 2018 and 2019, prosecutors reported that only 2% of disseminations were used in a case where there was an indictment, conviction or

penalty order. Even given that this feedback may relate only to ML proceedings and that there are time lags in investigations, these figures are low. In 2020, this percentage increased to 6.2% due to an increase in COVID-19 related emergency aid fraud. This suggests that FIU prioritization and analysis products are only aligned with LEA operational needs to some extent. While there is a positive upwards trend in the number of requests being made and the number of cases where FIU information is being used, FIU information is only being proactively sought and used to some extent. The restructuring of the FIU from a law enforcement to an administrative FIU in 2017 has required significant changes to the way that the FIU and LEAs work together and changes in LEA understanding of FIU analysis and intelligence outputs which had previously been directly accessible by LEAs.

**Table 3.2. STRs leading to indictments, convictions and penalty orders**

	2018	2019	2020
Indictments	73	113	234
Convictions	72	54	79
Penalty orders	130	156	468
Total number of feedback reports from prosecutors <sup>33</sup>	14 065	17 565	12 618
Percentage of reports of FIU dissemination leading to indictment, conviction or penalty order	2%	2%	6.2%

Note: The total number of feedback reports is different from the number of STRs disseminated in any given year as cases can span several years. Statistics start in 2018 as the FIU was restructured in 2017 and figures from the previous FIU are not available.

Source: German Authorities

**Table 3.3. Spontaneous and reactive FIU disseminations**

	2018	2019	2020
Total number of STRs filed with the FIU	77 252	114 914	144 005
Number of spontaneous disseminations made by the FIU to other domestic authorities	Not available	33 800	24 700
Number of disseminations in response to requests by other domestic authorities	1 850	3 260	3 798

Note: This table includes requests by all government agencies (police, prosecutors, tax authorities, supervisory authorities, customs, and intelligence services).

Source: German Authorities

### *STRs and other reports received and requested by competent authorities<sup>34</sup>*

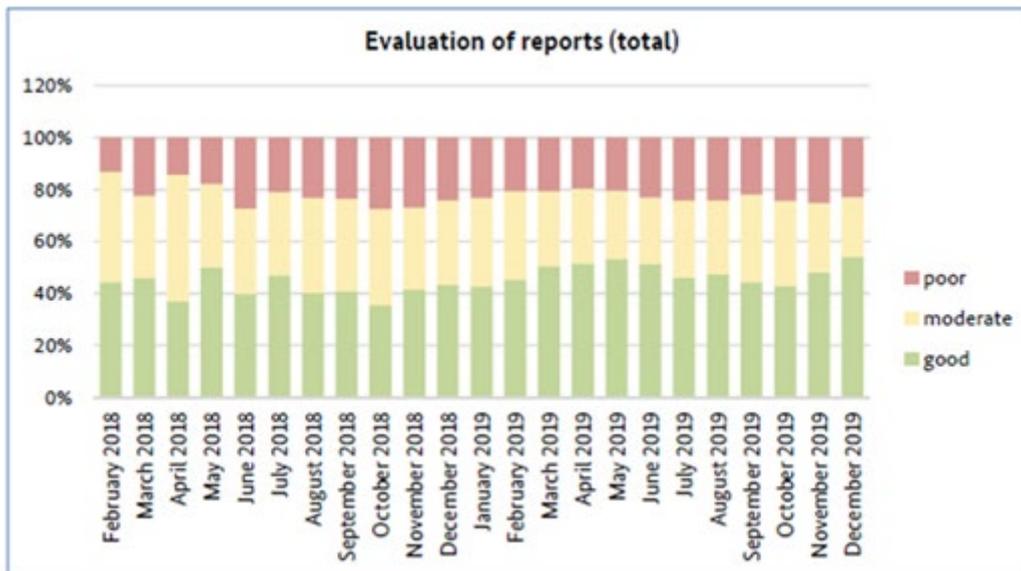
102. The FIU receives STRs that, to some extent, contain relevant information that advances investigations. The assessment team's findings are based on: data and statistics and interviews with the FIU, investigators, prosecutors and the private sector.

<sup>33</sup> Feedback reports are notifications made to the FIU under s.42 of the Money Laundering Act (GwG) which provide information on how FIU disseminations have been used.

<sup>34</sup> This section focuses on the quality of STRs received and requested by competent authorities as well as cross-border cash reporting. Analysis of the FIU disseminations are covered in the next section and requests by LEAs are included in the previous section.

103. It should be noted that up until February 2018 when a digital FIU reporting database was established, the FIU was receiving STRs by fax and processing them manually. A concurrent increase in the number of STR filings led to a considerable backlog of STRs and delays in analysis and dissemination. This impacted on the availability of STR information for a significant period of time between 2017 and 2018.
104. The number of STRs received has significantly increased over the past six years from 32 008 reports in 2016 to 144 005 reports in 2020. The FIU assesses that 43% of STRs filed are of good quality, which leaves room for further improvement. Obligated entities are not receiving adequate feedback on the quality and usefulness of their STR filings. In interviews, obliged entities and the FIU noted that current feedback on STRs focuses on giving feedback to the obliged entity on whether the report was filled in according to the required form and there is a lack of feedback on how STRs are used and the usefulness of the information provided.
105. As set out in section 5.2.5 on preventative measures, while there has been an exponential increase in STRs in the past few years, the number of reports from DNFBPs and non-bank FIs is low and, until recently, reports from the banking sector were also lower than expected taking into account Germany's risk and context. As set out in IO.4, very low levels of reporting from notaries (prior to 2020) and real estate agents reduced the financial intelligence available to the FIU and other authorities in higher risk areas. Overall, the issues with the rate of reporting and the quality of STRs limited the amount of relevant and accurate information available to competent authorities through the FIU data pool and the amount of information available to the FIU for analysis.

**Figure 3.1. FIU evaluation of quality of STRs**



Note: This table reflects the completeness of the form of STRs, rather than their substantive quality.  
Source: German Authorities

106. Reports on cash declarations and cash controls are recorded on the Customs database (INZOLL) and is available to LEAs on request and directly to the FIU (see Table 3.18). The number of cash declarations received has been relatively stable between 2017 and 2019. There was a significant decline in 2020 due to COVID-19 related travel restrictions reducing the amount of cross-border travel. Information on declarations is recorded in the Customs database (INZOLL) and is now kept for at least five years. Prior to 2021, information was only kept for 12 months limiting the usefulness of this database. Comprehensive statistics on the number of (intra-EU) cash disclosures received by Customs are not kept although authorities advise that there is some informal information sharing on cash controls with the FIU but it is not clear how the FIU uses this information. As set out in section 3.2.1, Customs are the primary users of the material and it is not clear to what extent other competent authorities access or use this information and how useful it is for intelligence or investigative purposes or to inform a national understanding of risks arising from the use of cash.

### *Operational needs supported by FIU analysis and dissemination*

107. In 2017, the FIU restructured and moved from the BKA to the Federal Customs Agency. The change centralised the FIU function into one independent agency was a move away from the decentralised model that existed prior to 2017. The reform process has been significant and Germany has implemented, and plans to implement, a large number of changes that will lead to increased effectiveness over time. However, there have been significant and ongoing challenges and at the time of the onsite, the FIU's financial analysis and disseminations only support operational needs to some extent. The assessment team's findings are based on: statistics, case studies, reviews of sample disseminations and interviews with the FIU, LEAs (BKA, LKAs, Customs, Tax) and prosecutors.
108. Prior to the creation of a new FIU in 2017, the FIU's role in financial intelligence and analysis was limited to the detection of trends and typologies and did not include operational analysis work. In practice, STRs were filed with the relevant *Land* police or prosecution office (with a copy sent to the BKA FIU) who then processed and analysed the STRs through a "clearing" process to substantiate whether to initiate a criminal investigation or not. Joint Financial Investigation Groups (GFGs), comprising officers from police and Customs, were established to carry out these preliminary investigation or "clearing" functions and carried out FIU analysis functions prior to the creation of the new FIU in 2017. The GFGs have continued to operate since the transition of the FIU to Customs and continue to undertake a preliminary review of disseminations and pass them on to prosecutors if they require further investigation. GFGs also work to support ML investigations.
109. In interviews, some LEAs expressed dissatisfaction with the time it took for STRs to be disseminated compared with the direct access to STRs LEAs had under the old FIU model. At the time of the on-site it was reported that these issues have largely been resolved but the availability of STR information up until very recently has been a significant impediment to the effective use of STR information.

110. The FIU has historically disseminated a large proportion of STRs to LEAs but the proportion of these disseminations made in response to requests from LEAs is low (see Table 3.3 above). Germany is taking steps to improve this through feedback processes, ongoing outreach to LEAs on the new FIU model, seconding FIU liaison officers to LKAs and also implementing plans for LEAs in future to have direct automatic access to the FIU database to conduct basic hit/no hit searches to verify whether the FIU has information relevant to a case or not.

#### *FIU staffing and IT*

111. FIU staffing has increased significantly over the last five years and it has sufficient human resources to carry out its function, although it could include further law enforcement and financial expertise. In 2017, the FIU had 165 staff and at the time of the onsite, this had increased to 572 staff with a plan to further increase staffing to 720 by 2026. The FIU is divided into seven different divisions with its own head of division who is responsible for day-to-day decision-making as set out in the table below. The rapid expansion coupled with the transition to Customs led to challenges in attracting staff with relevant experience, knowledge and skills. Breakdowns show that only three staff in the FIU have a police background suggesting very few staff from the previous FIU structure moved with the FIU to Customs in 2017.

**Table 3.4. FIU staffing breakdown**

Staff Division/Function	Allocated positions	Filled positions
Risk, management, compliance	10	10
Policy matters, international co-operation	25	27
National co-operation and co-ordination	68	66
Strategic analysis	39	41
Operational analysis (ML)	142	142
Requests in individual cases and state security	54	53
IT	15	15
Business support staff from Customs	219	228
Total number of FIU analysts	235	236
Total number of FIU Staff	572	582

Note: Staff numbers were current as of 11 November 2021. Business support staff from Customs are staff that are both engaged in operational analysis which includes assessing STRs and cross-checking data in different databases.

Source: German Authorities

112. In the transition, the FIU has faced significant IT issues that have impeded the FIU's access to information and has negatively affected the FIU's capacity to undertake complex operational and strategic analysis. When the new FIU was established in 2017, plans were put in place to implement a new electronic FIU database (GoAML) for the receipt and processing of STRs. The database became fully operational in February 2018. Up until February 2018, STRs were sent by fax and processing them manually leading to a significant backlog of STRs. The FIU is also still in the process of gaining automated access to a number of important databases. For example, the FIU has the right to direct access to bank and securities account information through the Electronic Account Retrieval System. However, IT interface problems mean the FIU cannot directly access the information and must make requests for the information through the Federal Central Tax Office (BZSt). Other databases like the

Transparency Register and the Customs database also require FIU analysts to make manual queries even though they have the right to direct access to the data. Germany is taking steps to improve automated direct data access for example, by giving the FIU automatic data access to the Electronic Account Retrieval System in 2022 but these efforts are still ongoing and the results of these measures were not yet in full effect at the time of the on-site visit.

113. The FIU's current analytical tools also require improvement to enhance the FIU's capacity to conduct complex operational or strategic analysis. The FIU does not have adequate access to tools necessary for automatic analysis of multiple sources of data and prioritisation of STRs for further analysis or undertaking complex network analysis. As a result, analysts may need to spend much of their time cross-checking databases or miss complex connections. To handle the increasing number of STRs, the FIU is planning to improve the automatic filtering and analysis of STRs through the implementation of an artificial intelligence software called "FIU Analytics". Field tests of the software started in November 2020. The planned upgrades to Germany's suite of IT tools are a positive development but were not in place at the time of the on-site.

#### *Operational analysis*

114. The FIU has a comprehensive process in place for reviewing and prioritizing STRs however the risk-based model could be further enhanced with greater co-operation and input from LEAs. The FIU has developed two documents, "Standards for Operational Analysis" and "Instructions for Operational Analysis" which set out the steps and basic framework for the conduct of operational analyses.
115. Priority is given to STRs marked urgent which involve transactions in motion but not yet executed, cases involving TF, and cases involving PEPs.<sup>35</sup> These STRs must be processed by the end of the business day in which they are received and there is a dedicated unit in the FIU handling these reports staffed by 142 employees dedicated for ML operational analysis and 28 employees dedicated to TF operational analysis. STRs related to TF are immediately transmitted to the relevant national security division of the relevant Land Criminal Police Office (LKA) and the Federal Office for the Protection of the Constitution (BfV). The number of STRs marked urgent has significantly increased since 2018 and in 2020 made up 4% of all STRs filed. In 2020, approximately 95% of urgent STRs that were disseminated were processed within the specified timeframe of one working day.

---

<sup>35</sup> In motion transactions are ones that are held by the obliged entity for a three day period after an STR filed and needs to be reviewed by the FIU within this period to allow the transaction to be executed or use FIU powers to freeze the assets for 30 days to conduct further enquiries if there are indications the transaction is related to ML, TF or PF (s.40, GwG).

**Table 3.5. Urgent STRs**

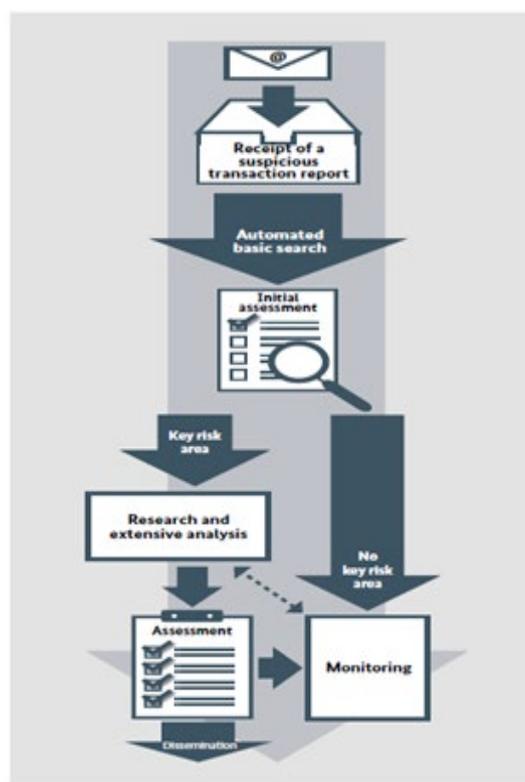
Year	Number of received STRs marked as "urgent"	Total number of disseminated urgent cases	Number of disseminated urgent cases, processed no later than the next working day	Number of disseminated urgent cases, processed within 3 working days (Section 46 (1) no. 2 GwG)	Not disseminated as "urgent case"	Immediate measures due to urgent cases
Quarter 4/2018	632	535	530	534	97	0
2019	3 416	2 652	2 623	2 647	764	12
2020	5 432	4 312	4 210	4 301	1 120	4

Note: Urgent STRs includes STRs identified as related to TF and PEPs.

Source: German Authorities (FIU)

116. All STRs are subject to an automated basic search against the federal police database (INPOL) on a fully automatic basis and the customs (INZOLL) database on a semi-automatic basis.
117. Information on cash declarations and disclosures are currently only hit/no hit and the FIU analyst will need to separately access the relevant database for access to information. A preliminary assessment by an analyst determines if the STR is urgent or relates to a key risk area using a key word search. STRs classified as urgent or related to a key risk area are then subject to a full analysis (25% of disseminations) or summarised analysis (75% of disseminations). A summarised analysis is more basic and cursory and may not add significant value to the STR. In a full analysis, information from different databases not currently part of the automatic basic search are searched manually and requests for additional information can be made to obliged entities and other national authorities. The analysis is then disseminated or held in the FIU data pool for monitoring.

Figure 3.2. FIU STR processing flow chart



Source: FIU Annual Report 2020, pg.14

118. The current risk prioritisation model requires further understanding and input from LEAs. The FIU prioritises STRs according to ten identified risk areas which are based on the findings of the NRA. Statistics show that 14% of disseminations made in 2020 related to these key risk areas which seems somewhat low. The process for developing and updating the key risk areas would be improved with greater consultation with LEAs. It is not clear if this prioritisation tool (which relies on a key word search) is adequately sophisticated to harness the full potential of the STRs reported as 75% of STRs are filtered out at this stage. STRs filtered out remain in the data pool, there appeared to be very limited use of the data pool for more sophisticated analysis of patterns and structures and the pool is only checked if there is a specific target identified.

Table 3.6. Disseminations against key risk areas in 2020

Key risk area	Number of disseminations 2020
Real estate	377
Use of cash (to purchase high-value goods)	346
Trade-based money laundering	223
Gambling/betting	407
Organised crime in the form of "clan crime"	302
Severe tax crimes	365
Commercial fraud	414
Abuse of non-governmental organisations and non-profit organisations	306

Key risk area	Number of disseminations 2020
Abuse of money or value transfer services (MVTs)	70
Use of new payment methods	766
<b>Total disseminations against key risk areas:</b>	3 576 (14% out of 24 700 disseminations made in 2020)

Note: The number of disseminations does not correlate with the number of STRs filed in all cases as a single dissemination can include multiple STRs.

Source: German Authorities (FIU)

- 3
119. While the FIU's tools and resources are increasing and there are indications that their output is more in line with LEA needs, the statistics show relatively low use of disseminations. While an increasing number of disseminations are made to LEAs in line with the FIU's prioritisation model, a significant number of these are closed after initial inquiries by the GFGs in the *Länder* (94% of disseminations were closed in 2020). This also brings into question the quality and relevance of the proactive dissemination and operational analysis. The number of proactive (spontaneous) disseminations from the FIU has been consistently high but since 2017 has been declining despite the rising number of STRs filed. The sample of FIU disseminations reviewed by the assessment team provided a range of facts and information from various databases but did not necessarily provide actionable intelligence assessments for LEAs and a clear actionable line of investigation.
  120. Issues with access to information also hinders the FIU's capacity to produce actionable intelligence. For example, suspicious cash flows are not reported to the FIU for analysis. Instead, reports are sent directly to Customs officers at GFGs for preliminary investigation "clearance". The FIU does not have direct access to bulk data on cash declarations/disclosures and checks STRs manually against the data on declarations in the Customs database. Up until 3 June 2021 when new Regulations entered into force, data held on the Customs database is retained only for one year which limited its availability and utility. From this date, records will be retained for a period of five years starting from the date on which the data was obtained with the possibility of a further three year extension but this had limited application on the period under assessment.<sup>36</sup> The GFG structure operates to mitigate some of the issues at the investigation level with a Customs officer placed in every GFG to share information and collaborate with other law enforcement agencies.

### *Strategic analysis*

121. The FIU undertakes strategic analysis but it is not always clear to what extent it is supporting operational outcomes. At the time of the on-site visit, there was a team of 41 analysts working on strategic analysis. Since 2017, the FIU has produced 17 typologies reports and participated in or led 14 ad hoc and ongoing strategic analysis projects including two projects with the Egmont Group on laundromats and professional money laundering. Analysis on typologies and trends related to key risk areas is also published in the FIU Annual Report. From the examples provided, the assessment team considered that the strategic analysis varied in quality with some earlier reports relying heavily on international typologies reports with little domestic contextual information. There was extensive use of the STR database to

<sup>36</sup> Article 13, REGULATION (EU) 2018/1672 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 23 October 2018.

draw conclusions based on numbers and types of reports but limited use of additional information sources. In one case, the FIU produced a typologies report on *hawala* dealers based on information it held in the STR database but did not demonstrate its ability to identify other sources of information to add-value to its strategic analysis. Overall, LEAs, policymakers and obliged entities could benefit from deeper and more frequent strategic analysis that is enriched by joining together different financial data sources and enhanced with input from LEAs and other operational level agencies.

### *Co-operation and exchange of information/financial intelligence*

122. Co-operation and co-ordination on financial intelligence is essential in Germany as the FIU operates at federal level but *Länder* authorities are primarily responsible for law enforcement. Adequate measures are in place to protect the confidentiality of information exchanged and used and co-operation and information exchange between LEAs and other operational agencies is good. However, while Germany has some mechanisms in place to support co-operation and information exchange between the FIU and operational agencies, many of these measures are new and while the assessment team found that these would lead to increased effectiveness in the future, they were yet to deliver tangible outcomes at the time of the onsite visit. The assessment team's findings are based on: interviews with the FIU, police (BKA and some LKAs), prosecutors, Customs, and tax investigation officers.

### *Money laundering and predicate offences*

123. In operational casework matters for ML and predicate offences, there is good formal and informal co-operation and co-ordination between different federal and *Länder* police, prosecutors, customs and tax authorities. The multi-agency and multi-jurisdiction approach is formally supported by Guidelines on multi- *Länder* co-operation that have been agreed by all *Länder* Ministries of Justice and Ministries of Interior.
124. Germany's use of multi-agency task forces and joint investigation teams to facilitate the sharing of information and intelligence is a strong feature of the system. Task forces are set up on both an ad hoc basis to deal with specific cases and on a permanent basis. The permanent GFG taskforce structure ensures cooperation and information exchange between police and customs at the individual *Länder*-level. Joint investigation teams are also commonly used to tackle individual cases.

### **Box 3.3. Multi-agency investigation unit: OLET (HE-GW-50; HE-GW-S3)**

In 2017, the Federal Criminal Police Office (BKA) came into possession of a large amount of data (approximately 2.78 terabytes) which would become known as the "Panama Papers" which included confidential documents and records from the offshore service provider Mossack Fonseca.

A special investigation team "OLET", comprising 35 employees from the Federal Criminal Police Office (BKA) and the tax authority of the Land of Hesse, was established in order to examine and analyse the data to identify transactions involving German nationals that may be relevant to criminal police agencies or of tax law relevance. The main focus was on identifying ML activities and the associated predicate offences, as well as tax offences detrimental to the German

tax authorities. Due to the diverse content falling within the remit of other authorities, the FIU, intelligence agencies and supervisory authorities were also involved in the evaluation of the data.

As a result of the investigation, 270 000 names of companies administered by Mossack Fonseca were entered into the joint police INPOL database in September-October 2017. Information on INPOL is available to the FIU and other LEAs for further analysis and cross-matching with information held on other databases including the FIU database.

Investigation of the data led to investigations into ML, TF, predicate offences and sanctions evasion activity both in Germany and abroad, including international arrest warrants for managers of the Mossack Fonseca law firm. In Germany, a number of investigations related to ML have been started and remain ongoing. In two cases triggered by information from the “Panama Papers”, the Public Prosecution Office in Frankfurt imposed a regulatory fine of EUR 15 million for Bank A and a fine of EUR 30 million for AML/CFT compliance failures.

Source: German Authorities

### *Terrorist financing*

125. Cooperation and information exchange in TF is robust with strong informal networks in operation between intelligence agencies (BfV, BND), police (BKA, LKAs), prosecutors and Customs. Two national centres for information exchange on terrorism and terrorist financing have been established at the federal level to facilitate cooperation and information exchange: the Joint Counter-Terrorism Centre (GTAZ) and the Joint Centre for Countering-Extremism and Terrorism (GETZ). Similar TF centres also exist in the *Länder*. However, the FIU is not involved as a regular member of the GTAZ and GETZ and only attends meetings on an ad hoc basis. At meetings the FIU does not attend, Customs authorities keep the FIU informed. The FIU could be better integrated in a more timely or direct manner into formal TF co-ordination and co-operation frameworks to increase the profile of financial intelligence in interagency mechanisms.

#### **Box 3.4. Co-operation and co-ordination in TF: GTAZ**

The GTAZ in Berlin brings together 40 authorities from federal and *Länder* agencies to work together on a day-to-day basis to review and compare information from LEAs and intelligence sources. The Centre is focused on terrorism broadly but this includes consideration of financial information and intelligence and TF investigations in every case where there is TF activity

The Centre holds daily situation reviews and regular case conferences and discussions of threats. The Centre allows for the prompt pooling, analysis and evaluation of all relevant information to prevent terrorist attacks, align criminal investigations and co-ordinate disruption activities.

Source: German Authorities

*FIU co-operation and information exchange*

126. Co-operation between the FIU and LEAs is developing but requires further attention. The transition of the FIU out of the BKA fundamentally changed the relationship between LEAs and the FIU from a self-service model to a client (LEAs) and service provider (FIU) model. Formal and informal co-operation and information exchange mechanisms between the LEAs and the FIUs needed to be formed under this new model. While there appears to be a positive trend in the relationship between some LEAs and the FIU, there are a significant number of regional police and prosecutions units in Germany and outreach efforts are ongoing. The FIU noted that there was a cultural shift that needed to happen with some LEAs in their understanding of the role of the FIU. Many did not fully appreciate the process for screening analysing STRs and still preferred direct access to STRs in line with their local investigations and priorities. The recent media reports of the ‘raids’ on the FIU (where prosecutors were investigating FIU staff for obstruction of justice offences for allegedly withholding STR information) may reflect a lack of understanding of some LEAs on the role of the FIU, but it is difficult to draw conclusions as it was an ongoing investigation at the time of the on-site visit.<sup>37</sup> A number of measures are in place to strengthen these frameworks including outreach and training to LEAs on the new FIU-model and functions and the secondment of FIU liaison officers to LKAs and GFGs. The FIU has set up a feedback mailbox to receive targeted criticism and feedback from LEAs but receives limited feedback through this mechanism (95 responses received in 2019) which is primarily related to the handling of specific cases. Further recruitment or secondment of LEA staff to the FIU and planned direct access for LEAs to STRs (on a hit/no hit basis) could further build the relationship.

*Confidentiality*

127. Information exchanged between the FIU and other competent authorities is protected. Authorities did not report any breaches of security in information exchange. The FIU office is securely located in a facility also housing customs and police with restricted access. The FIU offices are subject to secondary security measures. Access to the FIU database is restricted to FIU employees and then further restrictions are applied to classified data held on the database with only analysts cleared to “top secret” allowed to access the most sensitive data related to national security and terrorism. As set out above, the media reports of ‘raids’ on the FIU were in fact undertaken via warrant and the FIU cooperated with the authorities and do not represent a breach of STR confidentiality or security.
128. Disseminations of STRs to police and intelligence services are through encrypted email on secure networks or in-person for particularly sensitive matters. Disseminated STR data that is received by LEAs is also held in secure LEA databases. Recipients of STR information are bound by law to protect the confidentiality of information they receive and breaches of official secrecy are a criminal offence.

<sup>37</sup> DW (9 September 2021), “German Finance, Justice ministries searched in fraud probe”, available at: [www.dw.com/en/german-finance-justice-ministries-searched-in-fraud-probe/a-59133201](https://www.dw.com/en/german-finance-justice-ministries-searched-in-fraud-probe/a-59133201). ACAMS (14 July 2020), “In Unprecedented Move, German Police Raid Financial Intelligence Unit”, available at: [www.moneylaundering.com/news/in-unprecedented-move-german-police-raid-financial-intelligence-unit/](https://www.moneylaundering.com/news/in-unprecedented-move-german-police-raid-financial-intelligence-unit/).

## Overall conclusion on IO.6

Both Federal and *Länder* authorities have demonstrated through case studies that they access and use a broad range of financial information sources in investigations and prosecutions and co-operation and information exchange between LEAs and intelligence agencies is generally good. However, financial intelligence from STRs and from cross-border cash movements is only used to some extent.

Access to FIU intelligence is impeded by a number of different factors including: limitations in direct access to crucial sets of data, limited technical capacity to undertake complex operational or strategic analysis (particularly automatic bulk data analysis and advanced analytics), challenges around knowledge transfer from the previous FIU and limited feedback from LEAs. It is not clear if the prioritisation model always delivers results in line with LEA's operational needs. While there is an increasing number of disseminations made, LEAs and prosecutors do not pursue a high number of proactive (spontaneous) disseminations from the FIU and it is not clear yet if recent improvements have materialised into results at the LEA level.

The FIU has acknowledged these issues and is making considerable efforts to address them with many initiatives completed or underway to strengthen the role of the FIU and improve the quality of financial intelligence. The transition to the new FIU model has overall been a positive change. However not all of these measures were in place at the time of the on-site and these challenges affected the quality and availability of actionable financial intelligence suggesting that some major improvements are required.

**Germany is rated as having a moderate level of effectiveness for IO.6.**

### Immediate Outcome 7 (ML investigation and prosecution)

129. Changes to the ML offence were enacted and came into effect on 18 March 2021 to improve the capacity of LEAs to “follow the money” in ML cases reflecting Germany's commitment to reform in this area. The assessment period covers activities that took place before these amendments as there had been no prosecutions under the amended law at the time of the on-site.
130. The main change amended the law to move away from a list-based approach to an “all crimes” approach. The changes responded to identified barriers to effective investigation and prosecution. Under the old offence, prosecutors needed to identify the predicate offence to establish that it was a listed offence even though proof of the predicate offence was not an explicit element. Certain offences were also threshold based which added additional challenges. For example, tax offences were only predicate offences for ML when committed on a commercial basis or as part of an organised criminal group. The old offence limited the pursuit of cases where it is not possible to identify a predicate offence. This includes cases of third-party money laundering or complex money laundering involving the use of legal structures.

131. Investigating and prosecuting money laundering is a *Länder* responsibility and primarily undertaken by *Land* police and prosecutorial authorities. Where there is an international dimension to the investigation, or a complex case involving organised crime, the BKA also plays a role in co-ordinating investigative efforts but cases will always be led by a *Land* prosecution office. The BKA has jurisdiction for investigations in cases of ML involving organised crime or international ML. The Federal Prosecutor General (GBA) does not play a role in the investigation or prosecution of ML cases. Customs authorities investigate ML if the offences fall within the investigative competence of Customs or it relates to the cross-border movement of cash. Tax investigation authorities will be involved in the investigation of cases involving tax predicate-offences.
132. Germany makes a distinction between financial investigations “inside” a criminal investigation and preliminary investigations or queries made by LEAs “outside” a criminal investigation prior to a formal criminal investigation being opened by a public prosecutor (see also IO.6). While both of these processes are called investigations, activities prior to the opening of a formal criminal investigation process are carried out by the FIU and GFGs. These investigators prior to the formal process or “outside” of the official criminal investigation process is the same as an intelligence assessment that would be conducted by an FIU in other jurisdictions. GFGs have been established in all of the *Länder*. In 14 out of the 16 *Länder*, GFGs receive disseminations directly from the FIU and conduct these investigations outside of criminal proceedings and make a recommendation to the public prosecutor.<sup>38</sup> The principle of mandatory prosecution also applies in Germany. This means that all reports of potential crime must be investigated and prosecuted and prosecutors are the only ones with the power to decide to close a case. In practice, this means that all case decisions come to the prosecutor including decisions to not take forward an investigation for legitimate reasons such as insufficient evidence of a crime.

### *ML identification and investigation*

133. While Germany has demonstrated its ability to pursue ML when connected with a predicate offence (particularly fraud or drug trafficking), standalone or complex cases of ML are only identified and investigated to some extent. Challenges in relation to development of financial intelligence (see IO.6) and the still developing understanding of, and focus on, some of the highest ML threats impacts the downstream ability of prosecutors to pursue complex ML cases. Due to these issues and restrictions in the ML offence and principles in German law around aggregate sentencing (which often leads prosecutors to decide to pursue prosecution for the predicate offence only if it carries a higher penalty), prosecutors and police acknowledge they did not have the incentives to prioritise ML (particularly cases of standalone and third party ML) and instead focused on predicate offending or asset recovery tools as an alternative measure. Germany has taken steps to address these issues with the enactment of amendments to the ML offence and significant reforms to the FIU and the approach to financial intelligence, these measures are still in an early stage of implementation. The assessment team based its conclusions on: case studies; statistics on investigations and prosecutions; policy documents; interviews

---

<sup>38</sup> In two Land (North-Rhine-Westphalia and Schleswig-Holstein) FIU disseminations go directly to the public prosecutor.

with LEAs and prosecutors from federal agencies and a representative sample of different *Länder*.

134. ML cases are identified primarily through: (1) investigations of predicate offences; (2) FIU disseminations; (3) information received through international co-operation (both formal and informal). Challenges around the availability of actionable financial intelligence have had a cascading impact on Germany's capacity to identify and investigate cases of complex ML using corporate structures which rely heavily on FIU information to detect. ML related to cross-border cash movements can be investigated by all LEAs but Customs is the sole agency responsible for the supervision of cross-border cash movements. In interviews, prosecutors confirmed that it was difficult to initiate a successful investigation and prosecution for ML due to the construction of the offence and ML was mainly investigated as an aggravating factor in cases of commercial or gang-based fraud. In most cases, it would be easier to get a case outcome by prosecuting for the predicate offence and then targeting proceeds of crime using asset recovery measures.
135. There appears to be adequate resourcing for financial investigations however, these resources are focused more broadly on financial crime or organised crime and not specifically focused on ML. While authorities have the skills and knowledge to identify and investigate complex financial crimes it not clear that there is adequate prioritization and application of these resources to pursuing ML cases.
136. Resourcing and specialisation varies between the different *Länder*. Some *Länder* have established specialised units to bring together expertise and increase specialisation (see box 3.5 below). As can be expected, LEAs and prosecution offices in financial centres like Frankfurt having greater resource allocations to ML and financial crime. Unlike the increase in resources that accompanied the changes to asset recovery laws in 2017 (see IO.8), there has not been a comparable increase in relation to prioritising ML in response to the recent changes to the ML offence. Similarly, the restructure of the FIU also requires an increase in staff to handle an expected increase in disseminations and cases. However, resourcing for some GFGs in the *Länder* exposed to greater risks have decreased recently and does not appear to be in line with the policy/legislative change to facilitate more ML investigations/prosecutions. At the Federal level, the BKA has a small team pursuing ML related to organised crime and international ML cases. BKA outlined plans to increase its staff but many of the positions remained unfilled at the time of the onsite.

**Box 3.5. Specialised public prosecution offices and task forces****North-Rhine-Westphalia: Task force to combat ML, TF and Organised Crime**

In North Rhine-Westphalia, 40 investigators from the Land Criminal Police Office of North Rhine-Westphalia (LKA NRW) and the Tax Investigation Service (Steufa) have combined with two prosecutors to form a Task Force to Combat Terrorist Financing, Money Laundering and Organised Crime. The key function of this Task Force is to trace and recover the proceeds of crime, increase co-operation, enable the detection of illicit payment flows and uncover and counter criminal schemes. The Task Force is currently working on investigations into cum/ex trading, suspected nursing care insurance fraud, corruption, embezzlement, tax evasion and identifying proceeds of crime connected to senior members of “criminal clans”. The Task Force has been involved in two large-scale proceedings in connection with *hawala* banking, which also involve the issue of money laundering. In another case, there is suspicion that a family is conducting a large number of predominantly illegal transactions and has accumulated considerable assets as a result. In addition, there is the suspicion that the family received social benefits amounting to approximately EUR 4500 00 through fraud in the period from 2014 to 2017. The issue of money laundering is also being investigated. Another case that involves allegations of money laundering cannot be presented at this time in order to prevent the investigations from being jeopardised.

**Bavaria: Specialised Prosecution Offices**

Bavaria has tasked 17 out of 22 public prosecution offices in the Land with investigating and prosecuting ML offences and 8 offices who can take cases on referral from other offices. This means that they take ML cases alongside their other casework. These 17 offices are staffed with 60 public prosecutors and specialised investigators, consultants and accountants.

Source: German Authorities

***Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies***

137. Germany has investigated and prosecuted ML in line with its main predicate crime risks but has not adequately pursued ML in with its risk profile as an international financial centre. Limitations in the ML offence and issues with availability of financial intelligence information have prevented Germany from fully and proactively pursuing ML cases to the extent that would be expected considering the size of the German economy. The assessment team based its findings on: some rather limited statistics, a review of case studies and interviews with prosecutors and LEAs.

138. Germany identified fraud, drug trafficking, human trafficking and associated organised crime as the three highest risk, proceeds-generating predicate offences.<sup>39</sup> Foreign predicate offences, the use of cash (cross-border cash movements and purchase of high-value goods using cash) and the real estate sector were also rated high risk in the NRA.
139. **Number of ML investigations and prosecutions:** Only a small proportion of cases move from investigation to prosecution (see table 3.7 and 3.8 below). The number of ML proceedings initiated and closed by prosecutors without further action in 2020 (36 371) is much larger than the number of proceedings completed by filing an indictment (629) or an application for a written summary penalty order (773) (i.e. only 3.7% of ML cases proceed to an indictment or an application for a written summary penalty order). Other statistics support the conclusion that the overall number of ML prosecutions appears low considering Germany is a major financial and economic centre. Based on the potential number of proceeds-generating crimes in the jurisdiction (12 680 individuals were sentenced for theft and fraud committed on a commercial or organised basis in 2020, while only 788 were sentenced for ML) and the attractiveness of the economy for international trade and transactions, it was not established that Germany is pursuing ML investigations and prosecutions fully in line with its risk profile. Interviews and case studies do suggest that regions facing higher risks are generally prosecuting more complex ML cases although this could not be confirmed as Germany does not keep statistics on the type of ML cases prosecuted and other statistics could not be broken down by *Land*.

**Table 3.7. ML Prosecution Statistics**

	2015	2016	2017	2018	2019	2020	Total
Persons adjudicated	868	1 006	889	887	895	1 005	5 550
- Convictions	713	833	727	696	678	788	4 435 (81%)
- Acquittals	19	37	22	32	47	41	169 (3%)
- Proceedings terminated	135	135	140	159	167	173	909 (16%)
- Court dispensed with penalty	1	1	0	0	3	3	8 (>1%)

Note: These statistics on prosecution relate to cases where ML was the offence carrying the highest penalty for statistical purposes and includes both standalone cases and cases where ML was prosecuted alongside another offence. The numbers do not relate to cases or proceedings, but to the number of persons adjudicated for ML offences. These figures also do not include 317 minors who had cases related to ML adjudicated (resulting in 184 convictions) between 2015 and 2020.

Source: German Authorities

**Table 3.8. ML prosecutions where ML did not carry the highest penalty**

	2017	2018	2019	2020	Total
Persons adjudicated	304	373	327	417	1 421
- Convictions	265	319	282	350	1 216 (86%)

Source: German Authorities

<sup>39</sup> The NRA also identified six predicate offences as medium risk: corruption, human smuggling, illegal employment, tax offences, weapons offences and product piracy.

140. It should be noted that Germany does not maintain consistent or comprehensive statistics on ML investigations. The investigation statistics recorded by the police and prosecutors vary drastically. Authorities explained that in the police statistics a case in which several offences were committed either through a single action or several actions which are linked with each other is recorded just once under the offence which carries the most severe penalty. Therefore, ML cases are not recorded in the police statistics if they are investigated alongside a predicate offence which carries a higher penalty by law. In addition, financial investigations conducted independently can lead to the identification of a predicate offence which carries a higher penalty and under which the case is then counted in the police statistics. Prosecutors will record the number of proceedings and one proceeding may include several cases and several different offences. In the public prosecution statistics, a proceeding is recorded under the offence which is the focus (*Schwerpunkt*) of the proceeding. The prosecutor's decision on which offence constitutes the focus of the proceeding may lead to the proceeding being recorded under a different offence than the police statistics. The statistics would also record all possible proceedings even if the case does not go forward to prosecution. For example, a self-laundering case could be recorded as two proceedings (one for the predicate offence and one for the ML) even if the ML offence is not pursued later.
141. While Germany has a high number of ML investigations recorded it is not possible to determine the number of full formal criminal investigations (compared to the number of 'investigations' dismissed summarily soon after receipt due to a lack of prima-facie evidence). The police report an average of 9 782 ML investigations per year and the prosecutors report an average of 41 500 ML investigations opened. However, the number of investigations that move forward to prosecution and conviction are very small. As mentioned above, there must be a decision by a public prosecutor to close any case where a crime has been alleged to have occurred. This approach greatly inflates the number of cases officially opened and then closed by the public prosecutor. It is not clear from the statistics what proportion of the investigations refers to full formal criminal investigations and which are decisions on FIU disseminations or other reports of crime. Based on the high numbers of investigations and the low number of prosecutions, it is assumed that most of the investigations are only preliminary and that a large proportion are possibly related to investigations of predicate offences which do not get taken forward as separate ML prosecutions or which get converted into asset confiscation cases.

**Table 3.9. ML Case Investigation Statistics: Police**

	2016	2017	2018	2019	2020	Total
Number of money laundering investigations (including preliminary inquiries outside a formal criminal investigation)	11 541	10 015	8 652	9 764	8 942	48 914
Number of persons investigated	10 715	9 914	8 173	9 170	8 751	46 723

Note: These statistics include all cases reported to police (federal and *Land*) and would mainly arise from FIU disseminations but can also include cases that are detected through other means (e.g. investigation of a predicate offence or tip-off from the public) (i.e., this includes both instances when police undertake initial queries outside a criminal investigation as well as actual ML investigations that are approved by the prosecutors). The ML cases recorded here include offences of accessory after the fact and receiving stolen property.

Source: German Authorities

**Table 3.10. ML Investigation and Prosecution Statistics: Public Prosecutors**

	2015	2016	2017	2018	2019	2020	Total
Number of criminal proceedings initiated by prosecutors (total)	5 016 541	5 207 583	4 884 497	4 914 931	4 966 760	4 976 469	29 966 781
Number of ML proceedings initiated by prosecutors	40 777	45 790	40 304	39 873	40 760	37 462	244 966
Number of proceedings completed by prosecutors (total)	4 989 559	5 181 670	4 858 212	4 939 174	4 938 651	4 996 494	29 903 760
Number of ML proceedings completed by prosecutors	39 386	45 504	41 049	37 584	40 612	37 773	241 908
Number of ML investigations completed by filing an indictment or an application for a written summary penalty order	989	1 117	1 078	962	1 085	1 402	8 035
Persons adjudicated for ML*	868	1006	889	887	895	1 005	5 550

Note: Unlike the previous table, this table captures the number of proceedings opened by prosecutors rather than the number of cases/investigations (apart from the last row). Each proceeding may include several cases (e.g. a series of fraud cases committed by one or more accused). The number of proceedings is usually lower than the number of cases. \*Unlike the rest of the table, the last row does not reflect the number of proceedings (which may involve more than one accused), but the number of persons adjudicated for ML. If a proceeding involved two accused, it would be counted as one proceeding, but if the case went to trial for both of the accused, it would be counted as two persons adjudicated.

Source: German Authorities

142. **ML associated with high-risk predicate offences:** As statistics were not available on the predicate offences for ML cases, Germany shared a sample of representative case studies. The assessment team reviewed 72 ML cases that were representative of ML cases pursued in Germany and found that the most common predicate offences were fraud (25 cases), drug offences (22 cases) and tax evasion (10 cases). While human trafficking was classified as one of the highest-risk predicates in the NRA, no cases involving human trafficking were presented. A research study commissioned by the BMF to look at ML cases between 2014 and 2016 found that fraud was the underlying predicate offence in 92.5% of prosecuted cases. With respect to organised crime related to these high-risk predicates, Germany has a strong focus on organised crime investigations and prosecutions and a strong orientation towards identifying ML related to organised crime. The BKA in particular, place a priority on combatting international organised crime (and associated ML) and overall is well equipped to pursue these cases. Based on shared case examples Germany appears to be pursuing cases in line with the identified risks in the NRA. There is likely an underrepresentation of ML associated with tax evasion due to issues with the ML offence prior to recent changes.
143. **Cash-based ML:** Cash smuggling was a feature of 14 of the 84 sample case studies. Customs is primarily responsible for the detection and investigation of these cases and while many cases of money mules are detected at the border and asset confiscation action pursued, a number of investigations into the ML activity were closed when a link to a predicate offence could not be established. Authorities did present case studies on some intensive investigations into complex ML networks and demonstrated that there was capacity to pursue these types of cases. However, it was not clear that these types of investigations were being regularly and proactively pursued and there were also limited cases involving unaccompanied cash (cash transported through mail or cargo).

144. **ML through the real estate sector:** Case studies and discussions with LEAs confirmed that authorities had a good understanding that the real estate sector was high-risk for ML, particularly in terms of ownership by natural persons and were taking steps to prioritise these cases. It was not clear to what extent these cases were being pursued when complex company or other arrangements are in place.
145. **Trade-based ML:** Case studies and discussions with LEAs confirmed that there was an awareness of trade-based ML as a growing risk in Germany. Several case studies were presented to demonstrate that it was being actively pursued (see case example below).

### Box 3.6. ML Cases involving High Risk Sectors

#### **Drug trafficking and ML in the real estate sector: HE-GW-10**

The Specialised Economic Crime Prosecution Unit of the Public Prosecution Office in Frankfurt am Main investigated an organised crime group involved in the trafficking of cocaine. Investigations established that proceeds from the drug trafficking were being laundered through a professional money launderer who used proceeds of crime to purchase real estate (86 properties valued at EUR 250 million). The properties were then leased for profit. Members of the organised crime group were charged with drug offences, tax offences and ML. The professional money launderer Was prosecuted, convicted and sentenced to 3 years and 10 months imprisonment for tax evasion and a fine of 230 daily rates of EUR 500 each. The proceedings for money laundering were discontinued pursuant to section 153a of the Code of Criminal Procedure (StPO) in return for a payment of EUR 1 800 000 (effected from non-arrested funds) to the state treasury.

Asset confiscation proceedings were also initiated. With the opening of the main proceedings, an order for asset seizure had been issued for around EUR 10 000 000 against the money launderer related to tax evasion and money laundering. On 20 August 2021, the defendant's apartment was searched and EUR 856 000 in cash, 1.5kg of gold and other valuables were seized. Debt securing mortgages on real estate of the defendant were registered in the amount of EUR 10 000 000. Most of the seized assets have been released as it could be proven that they were obtained legally but EUR 856 000 remains seized and separate money laundering proceedings have been initiated with respect to the cash.

#### **Tax evasion and trade-based ML case with complex ML and foreign predicate offences: NW-GW-113**

The Specialised Economic Crime Prosecution Unit of the Public Prosecution Office in Dusseldorf is investigating an organised crime group involved in trade-based money laundering to evade tax and launder funds. It is suspected that a large number of clothing companies are procuring goods from overseas and then using false invoices generated using domestic shell companies to evade import duties and also claim tax deductions. These shell companies were also used to transfer funds derived from fraud offences committed in France and Belgium.

Investigations in this case are still ongoing.

**Cash smuggling case involving foreign predicate offences and complex third-party ML: BW-GW-3**

In this case, a group of four people entered into a scheme to transfer significant sums of cash derived from drug offences from the Netherlands to UAE via Germany. The plan was for the cash to be transported by cash couriers and discussed as payments for gold trades. To conceal the origins of the cash, companies were set up in UAE, Germany, Romania and the UK to show that there was a purchase of gold from UAE that was then sold by the German company to Romania. A UK company was used as another intermediary company for gold to be sent back and forth between UAE and Germany via the UK without any real trading activity occurring. Proceeds from drug sales were collected in Netherlands, transported the cash to Germany by car and then handed over the cash to several couriers who would travel to UAE with the cash and declare that the cash was related to the gold trade business the group had set up. It is estimated that EUR 45 007 116 was laundered through this scheme between January 2017 and January 2018. Proceedings were launched against six couriers for money laundering but preliminary proceedings were ultimately discontinued because there was no evidence of knowledge of the illicit origin of the transported funds or gold. The case was detected through the inspection of a car by Federal Police in Kleve who stopped and searched the car transporting the cash from the Netherlands to Germany on 11 January 2018 and found EUR 1.5 million in cash hidden in the car.

All four involved in the scheme have been prosecuted and convicted of ML offences. Sentences ranged from three years and nine months to nine years and six months. Asset confiscation action has been taken in relation to EUR 1.3 million in proceeds of crime and 66kg of seized gold.

**Cash smuggling case where predicate offence could not be established: NW-GW-6**

The Federal Police discovered EUR 1.5 million in cash concealed in a vehicle belonging to a cash transportation company travelling across the German border with the Netherlands. The driver claimed that the cash originated from the sale of gold in the Netherlands.

The GFG started investigations on the basis that the driver was a cash courier but could not establish a specific predicate offence. The ML investigation was closed but asset confiscation proceedings were pursued to deprive the suspect of the proceeds.

Source: German Authorities

146. Overall, Germany is making efforts to pursue ML in line with its predicate-crime risks and in line with identified high-risk sectors. However, the limitations in the old ML offence were a barrier to the pursuit of cases where it was difficult to prove the predicate offence, including cases involving third-party money laundering, cross-border cash smuggling and cases involving foreign predicate offences. The overall number of cases that Germany prosecutes and secures convictions for is also low and not fully in line with Germany's overall size and profile as an international financial centre.

### *Types of ML cases pursued*

147. Germany was able to demonstrate through case studies that it has the ability to prosecute and secure convictions for cases of self-laundering, standalone ML and third party ML. However, different types of ML are not being pursued and prosecuted consistently due to issues in detecting and investigating third-party and standalone ML and limitations in the ML offence. The assessment team based its findings on: case studies presented by Germany and interviews with LEAs. Germany was not able to provide detailed statistics on the types of ML cases being pursued.
148. **Standalone and third party ML prosecutions:** the absence of statistics and issues in identifying these cases (section 3.2.2 above) suggest that they are not being pursued actively. Based on the case studies, the assessment team found that many ML cases start as investigations into other predicate offences like fraud or embezzlement and are investigated as aggravating circumstances to the predicate offence rather than as standalone cases. There is also a tendency to be reactive rather than proactive in pursuing these cases with many cases depending on tip-offs or notifications from foreign countries rather than being proactively detected through financial intelligence (see core issue 7.1 and IO.6).
149. **Complex ML cases** (for example, involving the use of legal persons to obscure ownership) are not actively pursued. Legal persons in Germany are not subject to criminal liability and so cannot be prosecuted for ML under the criminal law although they are liable for punishment under administrative law. In practice, this appears to dissuade prosecutors from pursuing cases where a natural person cannot be identified as the perpetrator. Germany did not provide any statistics or case studies to demonstrate that investigations and prosecutions into legal persons are actively pursued. In interviews, LEAs explained that when investigating cases one of the first steps would be to identify a natural person and if this was not possible, the case would likely not be pursued as an ML case although asset confiscation and supervisory measures would be considered as alternative measures. The statistics provided on sentences imposed for ML (see Table 3.11 below) indicates that most ML cases that proceed to prosecution are lower-level ML cases as 92% of convictions result in a fine or a sentence of less than 1 year imprisonment.
150. **Foreign predicate offences:** Germany shared a number of cases of investigations into cases of ML involving foreign predicate offences (primarily fraud, drug trafficking and tax evasion cases) and demonstrated their capacity to investigate and prosecute where a foreign authority alerted authorities of potential ML and there was good level international co-operation. However, there are no statistics to demonstrate that Germany consistently pursues foreign predicate offences in line with its risk profile or that it actively targets ML where there is no established link to the foreign predicate offence. In addition, authorities noted that it was difficult to pursue these cases as evidence of the foreign predicate offence was often hard to obtain and this was a practical requirement of the old ML offence.
151. **Self-laundering:** Germany only recently criminalised self-laundering in 2015. The first case considering the new provision in court was in 2018. Germany shared one additional case study where self-laundering was being investigated. Overall, this appears to be a type of ML that is rarely pursued which is line with the general tendency to pursue prosecution of the predicate offence.

**Box 3.7. Investigation and Prosecution of Professional ML****Investigation and prosecution of professional ML: MV-GW-4/NW-GW-115**

The Criminal Police Inspectorate Rostock, the Land Criminal Police Office Mecklenburg-Vorpommern, the Specialised Prosecution Office Information and Communication Technology Rostock, The Public Prosecution Office Dusseldorf, BaFin, the BKA and the FIU worked together in a multi-agency investigation and prosecution of an individual suspected of providing professional ML services to criminal groups. The suspect opened and operated a number of accounts in Germany into which proceeds of other offences (primarily fraud offences) could be deposited and laundered through a number of shelf companies in Germany. In the course of the investigation, it was discovered that these bank account services were being offered online. Extensive investigations which also involved international co-operation with Europol and authorities in Germany, Poland, Italy, the Czech Republic and Bulgaria linked the bank accounts to the accused.

In February 2020, the accused was convicted of 136 counts of ML and sentenced to four years imprisonment and a fine of EUR 50 000.

Note: more information on this case is in IO.6 box 3.1.

**ML using a professional intermediary: NW-GW-112**

In June 2016, the Public Prosecution Office Duisburg and the BKA have been jointly investigating into members of the 'Ndrangheta organised crime group and their associates for drug trafficking, money laundering and organised crime offences.

To launder funds, a system was set up whereby "investors" in Germany acted as loan providers for drug transactions through a series of false or fraudulent contracts and through property purchases in Italy.

Investigations have revealed the involvement of a lawyer and a notary, amongst other associates, in Germany who have been involved in the setting up of front companies and contractual arrangements to facilitate the ML activity. While proceedings against the notary did not proceed as the person has passed away, separate criminal proceedings have been initiated against a lawyer who facilitated the scheme and 13 other defendants linked to the case. These proceedings remain ongoing.

Source: German Authorities

***Effectiveness, proportionality and dissuasiveness of sanctions***

152. Germany does impose a broad range of sanctions against natural persons but it could not be fully demonstrated that the sanctions imposed for ML are effective proportionate and dissuasive and there are no cases of sanctions being applied against a legal person for ML. The assessment team based its findings on: statistics on convictions and penalties, case studies and interviews with prosecutors.

153. The sentencing range for ML offences in Germany ranges from a fine to a term of imprisonment ranging from 3 months to 15 years for serious offending. However, the majority of sentences in ML cases are quite low. Most cases end in a fine or a term of imprisonment of less than 1 year. While a maximum fine of up to EUR 10.8 million is possible (360 daily rates at EUR 30 000 each), in practice, the maximum fine imposed for natural persons in the last 5 years (2016-2020) has been EUR 40 500 (150 daily rates at EUR 270 each) with a median fine of between EUR 620 to EUR 1 800).<sup>40</sup> In 2020, 78% of cases ended with a fine and 13% with a term of imprisonment of less than 1 year. Only three people were sentenced to a term of imprisonment of between 5 and 10 years (the highest sentence imposed in 2015-2020). The breakdown of sentences is broadly consistent with lower-level theft and fraud but not consistent with sentencing for organised or commercial fraud/theft and narcotics offences, particularly organised narcotics activity where higher sentences are common.
154. Overall, the sentences at the higher-end of sentences available are rarely used. This could be reflective of upstream issues with difficulties in identifying and investigating complex ML cases, third party launderers and ML activity occurring on a commercial scale.

**Table 3.11. Sanctions in ML cases**

	Total number of persons sentenced	<1 year	1-2 years	2-5 years	5-10 years	Fine
2015	713	106	43	3	0	561
2016	833	113	30	13	0	677
2017	727	100	42	12	3	570
2018	696	115	45	16	0	520
2019	678	108	46	7	1	516
2020	788	104	43	20	3	618
<b>Total number</b>	<b>4 435</b>	<b>646</b>	<b>249</b>	<b>71</b>	<b>7</b>	<b>3 462</b>
<b>Total percentage</b>		<b>14.6%</b>	<b>5.6%</b>	<b>1.6%</b>	<b>0.1%</b>	<b>78%</b>

Source: German Authorities

<sup>40</sup> Fines in Germany are calculated on the basis of “daily rates”. When determining the severity of a fine only the number of daily rates is to be considered as the amount of the daily rate varies depending on the personal and financial circumstances of the person to be sentenced. The number of daily rates can vary from 5 to 360 and the amount of the daily rates can vary from EUR 1 to EUR 30 000.

**Table 3.12. Sanctions imposed for ML compared with other crimes in 2020**

	Total number of persons sentenced	<1 year	1-2 years	2-5 years	5-10 years	10-15 years	Fine
Fraud	70 890	6 508 (9.2%)	3 054 (4.3%)	839 (1.2%)	54 (0.1%)	1 (0.01%)	60 434 (84%)
Theft	86 903	15 390 (18%)	3 684 (4.2%)	1 321 (1.5%)	82 (0.1%)	0	66 425 (76%)
Fraud and theft offences committed as a member of an organised criminal group	582	90 (15.5%)	236 (40.5%)	207 (35.6%)	32 (5.5%)	0	17 (2.9%)
Narcotics offences	59 239	6 280 (10.6%)	5 020 (8.5%)	2 279 (3.8%)	479 (0.8%)	16 (0.03%)	45 164 (76.2%)
Narcotics offences committed as part of an organised criminal group	377	16 (4.2%)	98 (26%)	148 (39.3%)	107 (28%)	7 (1.9%)	1 (0.3%)
Money laundering	788	104 (13.2%)	43 (5.5%)	20 (2.5%)	3 (0.4%)	0	618 (78.4%)

Note: Germany only record statistics for the offence that attracted the highest penalty so cases where ML was the subordinate offence are not captured here.

Source: German Authorities

### *Use of alternative measures*

155. Germany pursues alternative measures to some extent. Where it is not possible to secure a conviction for ML, Germany has alternative criminal justice measures that could be taken. The main measures taken would be pursuit of the predicate offence or pursuing asset recovery. Authorities explained that in all cases, other actions (e.g. the pursuit of predicate offence charges or asset recovery) will be followed through regardless of whether or not it is possible to secure an ML conviction indicating that these measures are not always being pursued as a strict alternative to ML.
156. Indicting and prosecuting for ML is a prosecutorial decision and the prosecutor has the discretion to choose to focus on the predicate offence. Where there are different criminal acts that constitute a violation of more than one criminal provision, prosecutors will prosecute the crime which will attract the harsher sentencing. This means that prosecutors often indict the offender with the predicate offence before the ML offence where the former leads to a higher sanction (e.g. drugs or tax offences). This also means that these offences will not show up in the ML statistics as crime statistics in Germany only capture the offence that attracted the highest sentence.
157. The most commonly used and effective alternative measure employed is asset recovery. In 2017, Germany changed the asset recovery laws to enable for the pursuit of asset recovery when it is not possible to prosecute or convict the person for the underlying offence. Authorities presented case studies of this being used (see IO.8).

158. In addition to criminal justice measures, there are non-criminal justice measures that could be taken under the Order Relating to Notifications in Criminal Matters. Authorities explained that depending on the case, supervisory authorities must be notified of the criminal proceedings. It would then be open to the supervisor to initiate supervisory action to sanction obliged entities for regulatory offences. Notifications can also be sent to obliged entities to action. For example, it is common for a bank to block an account by exercising a special contractual or statutory right of termination if it is notified that there is an account being misused for ML. Overall however, it is not clear how these measures are used in a consistent and comprehensive manner to disrupt and sanction ML.

## Overall conclusion on IO.7

Germany has prioritised the pursuit of ML to some extent and has demonstrated commitment at the policy level to reforms to improve the effectiveness of the regime. However, challenges with the previous version of the ML offence have contributed to an ongoing focus on pursuing predicate offences over ML.

There are a large number of investigations initiated but only a very small proportion of cases proceed to prosecution. The identification of ML cases is a challenge and upstream issues with the availability of actionable financial intelligence hampers the identification and investigation of some types of ML (particularly complex ML) and a significant amount of resources goes into examining cases with little likelihood of successful prosecution.

ML cases investigated and prosecuted show some alignment with Germany's risk profile with case studies showing many cases related to fraud and drug trafficking pursued. However, there is a lack of proactive investigations into professional third party ML and ML without a proved predicate crime or link to Germany and a focus on natural persons rather than ML involving legal persons. Overall, Germany is only identifying, investigating and prosecuting ML in line with risks, to some extent. While there is a broad spectrum of cases being pursued, the overall number of cases that proceed to prosecution is low considering Germany's size. This indicates that ML cases are not fully prioritized and proactively pursued in line with Germany's risk profile. Issues with statistics also hampered the ability to evidence Germany's effectiveness in this area.

The available sanctions for ML appear to be appropriate but there are a limited number of cases in which higher penalties are applied, indicating that the cases may be in relation to lower-end ML.

Germany can use alternative measures in cases when an ML prosecution is not possible but there does not appear to be a clear strategy or policy on how to use these tools to disrupt and sanction ML.

**Germany is rated as having a moderate level of effectiveness for IO.7.**

### Immediate Outcome 8 (Confiscation)

#### *Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective*

3

159. Federal and Länder authorities actively pursue asset confiscation as a policy objective. Asset confiscation is a legal, mandatory consideration for prosecutors when they are investigating and prosecuting cases and asset confiscation action must be initiated if there are proceeds of crime identified. Assets are normally identified and traced as part of the investigative process into the proceeds generating offence or as part of an ML investigation. The assessment team based its findings on: statistics, case studies and interviews with LEAs and prosecutors working on asset confiscation cases.
160. Germany enacted legislative reforms in 2017 to make confiscation of proceeds of crime and confiscation of a sum of money equal to the value of the proceeds of crime a mandatory consideration for prosecutors in criminal investigations.<sup>41</sup> The law was also simplified to concentrate responsibility for asset confiscation with public prosecutors and extend non-conviction based asset confiscation to all offences. Policies and Guidelines are in place to support these efforts to pursue asset confiscation in all cases. It is a priority in the National Strategy and the Federal Ministry of Justice (BMJ) and the Ministries of Justice of the *Länder* have agreed Guidelines for Criminal and Regulatory Offences Proceedings to increase co-ordination and consistency in asset confiscation approaches across the Federal and *Länder* jurisdictions.
161. In practice, public prosecution offices have received additional resourcing since the 2017 reforms and 8 out of the 16 *Länder* LKAs have increased their staffing levels. Specialised units have been established in all of the LKAs and public prosecution offices to focus resources to pursue proceeds of crime. Regular training is available and authorities have also taken the initiative to build an archive of information to share practical information between LEAs and prosecutors working on asset recovery.
162. Public prosecutors manage the investigations to detect, freeze and recover assets. Police support investigations at the direction of the prosecutor. The prosecutor is also responsible for applying for court decisions relating to asset freezing and confiscation. In exigent circumstances, the prosecutor and police officers (as investigators for the public prosecutor) may make asset freezing decisions themselves in which case (except for the seizure of movable property) the prosecutor must apply to the court for confirmation of the order within a week of the freeze. Authorities explained that asset confiscation investigations are pursued from the outset of a case as part of the overall investigation. If assets are found and there is a risk of dissipation before assets can be confiscated, steps will be taken to freeze or seize the assets.

---

<sup>41</sup> Asset confiscation is mandatory for proceeds of crime but this would not include instrumentalities of crime. However, in practice, instrumentalities are also regularly frozen and confiscated.

### Box 3.8. Specialised asset recovery units

#### **Criminal Police Office of Bavaria**

In Bavaria, 49 case handlers are specifically trained in the field of asset recovery and they work centrally at the Land Criminal Police Office of Bavaria as well as in each of the ten Bavarian regional police headquarters. This shared resource assists in knowledge sharing particularly in complex investigations. Other authorities, such as the Tax Investigation Service, the BKA, public prosecution offices and the German pension insurance provider, are also involved training courses which take place twice a year.

#### **Criminal Police Office of Berlin**

The LKA in Berlin has three criminal police inspectorates employing a total of 24 police officers who specialise in financial investigations. These units undertake asset recovery and also have a dedicate hotline to provide advice on asset recovery to other investigators, the regional police headquarters, the judiciary and other authorities and units of the Land of Berlin.

Source: German Authorities

### Box 3.9. Asset recovery archive

Four LKAs (North Rhine-Westphalia, Baden-Wuerttemberg, Bavaria and Lower Saxony) work together to jointly publish the “recovery archive”. This is a MediaWiki application with 150 forms regarding asset recovery as well as comprehensive information on: forms, basics, international asset recovery, contacts in Federal and *Länder* authorities, case law, criminal police tactics, training dates and regulations. It also includes guidelines on cross-border asset recovery and on the freezing of virtual currencies (including model orders and forms).

This archive is used to exchange best practice tools across public prosecution offices, police and tax authorities throughout Germany (and is not limited to the four LKAs that maintain the tool). The recovery archive has a volume of over 1900 websites and 8600 users.

Source: German Authorities

**Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad**

163. Germany actively confiscates the proceeds of domestic and foreign predicates and pursues proceeds moved offshore. Using these tools, Germany is able to deprive criminals of a large amount of proceeds of crime and property of equivalent value. The new legal regime is robust and the legal, policy and structural changes enacted in recent years have been effective in increasing the amount of assets confiscated. The assessment team based its findings on: statistics, case studies and interviews with police and prosecutors.
164. Since 2017 when the law was changed, there has been a significant increase in the amount of assets confiscated from EUR 198.6 million in 2017 up to EUR 821 million in 2020. However, it should be noted that this total figure from 2017 and 2018 includes corporate fines that were issued together with the asset confiscation order and Germany was not able to provide more detailed statistics on the quantum of corporate fines separated from the total amount of proceeds of crime confiscated. Since 2018, the BMJ has issued guidelines to public prosecution offices to only record asset confiscation figures and not corporate fines and figures from 2019 and 2020 do not include corporate fines in the totals.
165. Overall, the statistics kept on asset confiscation are not detailed or comprehensive (see table 3.13 below), however better statistics are kept on asset freezing (see table 3.14, 3.15 and 3.20).

**Table 3.13. Assets Confiscated 2017-2020**

	2017	2018	2019	2020	Average
Confiscated assets (including corporate fines)	EUR 198 646 000	EUR 1 866 580 000	EUR 796 255 000	EUR 821 078 000	EUR 920 639 000
Number of cases	19 484	49 910	61 681	64 576	48 912

Note: The total figures provided for 2017 and 2018 include the asset confiscation part of at least some corporate fines. The abnormally large figure in 2018 arose from one particularly large asset confiscation case that was resolved in 2018 where the corporate fine was EUR 5 million and the asset confiscation was EUR 995 million. The figures for 2019 and 2020 do not include, at least not to a significant extent, the asset confiscation part of corporate fines as this is against the guidelines issued to the public prosecution offices and, after some initial mistakes in reporting, the guidelines are now mostly being followed.

Source: German Authorities

166. Between 2017 and 2020, on average, approximately EUR 1.95 billion in assets were authorised to be frozen and EUR 500 million of assets were actually frozen. There is a large discrepancy between the amount of assets frozen compared to assets authorised to be frozen because authorities can seek an order for the total estimated proceeds generated and not just the assets that are available at the time (property of equivalent value). While there is an expectation that some of the assets would not be available or already be spent or dissipated, authorities acknowledged there is room for improvement in reducing the discrepancy between the amount of assets authorised for freezing and the assets actually frozen through earlier interventions or the active pursuit of assets located abroad. Further the statistics of overall numbers of cases suggest that asset freezing only occurs in one out five cases meaning that authorities not be preventing the dissipation of funds in the majority of cases.

167. Case studies provided by Germany demonstrate the authorities' ability to seize and confiscate a wide range of proceeds, instrumentalities, and assets of equivalent value including real estate, cash, bank accounts, virtual assets, cars, jewellery and precious metals and interests in assets like mortgages or accounts receivable. Over the last three years there has also been a significant growth in the amount of virtual assets frozen from 5.5 million in 2018 to 40 million in 2020. Frozen assets are actively managed to preserve their value. Asset management is well supported by internal police policies although different *Länder* take different approaches to this with some creating dedicated asset management units within the LKA. Assets are first and foremost used to compensate victims of crime. Assets that remain are in general returned to consolidated revenue. Remaining assets can – under certain conditions – also be used to further the administration of justice (e.g. funding for rehabilitation programs, or to fund public prosecution and police positions).

Table 3.14. Assets Frozen

	2017 EUR	2018 EUR	2019 EUR	2020 EUR	Average EUR
Proceeds and instrumentalities of crime authorised to be frozen	1 170 996 142	1 083 549 650	1 408 210 754	1 120 504 492	1 195 815 259
Actual proceeds and instrumentalities of crime frozen	497 912 545	468 405 371	505 978 658	529 008 112	500 326 171
Number of cases	11 977	11 746	10 855	11 120	11 424

Source: German Authorities

Table 3.15. Types of Assets Frozen

	2018	2019	2020
<b>Cash</b>	EUR 75 839 382 (16.2%)	EUR 104 512 072 (20.7%)	EUR 111 558 202 (21.1%)
<b>Movables</b>	EUR 64 697 399 (13.8%)	EUR 87 236 859 (17.2%)	EUR 90 930 985 (17.2%)
<b>Real estate</b>	EUR 106 479 479 (22.7%)	EUR 120 209 237 (23.8%)	EUR 135 973 985 (25.7%)
<b>Receivables</b>	EUR 215 843 795 (46.1%)	EUR 215 843 795 (35.9%)	EUR 150 428 903 (28.4%)
<b>Virtual assets</b>	EUR 5 545 317 (1.2%)	EUR 12 429 287 (2.4%)	EUR 40 036 529 (7.6%)
<b>Total</b>	EUR 468 405 371	EUR 505 978 658	EUR 529 008 112

Note: Movables includes non-fixed assets such as cars, jewellery, electronic goods. Receivable refers to claims to assets including securities and money held in bank accounts.

Source: German Authorities

### Box 3.10. Case study: asset tracing and confiscation of different types of assets (NW-GW-83)

In June 2016, the Public Prosecution Office of Cologne commenced an investigation into a large family who appeared to be in possession of large amounts of unexplained wealth following a tip-off. Information provided was verified through checks of information on previous investigations and data on land registries, vehicle registers, foreclosure proceedings and STRs filed by a German and Austrian bank in 2013. On the one hand, records showed they were receiving social security benefits but were also in possession of large amounts of high-value assets including real estate, luxury vehicles, jewellery and cash. The suspected predicate offence was fraud.

Investigators used long-term undercover operations (confidential informants, surveillance, telecommunications intercepts) to gather evidence of the predicate offences (thought to be fraud) and attribute beneficial ownership of the assets to members of the family. Financial investigations were also carried out looking into the account data of more than 100 account holders at 67 banks, loan documents were consulted and evaluated and land register searches were conducted for around 100 properties.

Three members of the family and one associate were charged with money laundering. Asset confiscation action has also been started against the following assets:

- EUR 912 724 in assets
- Four properties in North-Rhine-Westphalia worth EUR 1 571 000

Source: German Authorities

#### *Foreign predicate offences*

168. Germany could not provide detailed statistics across multiple years on whether underlying predicate offences were domestic or foreign in asset confiscation cases. However, based on some limited international cooperation statistics from 2019, case studies and interviews, the assessment team was satisfied that authorities are capable of freezing and confiscating the proceeds of foreign predicate offences both on its own initiative and in the context of an international cooperation request (see IO.2).
169. Germany does not keep detailed statistics on asset recovery and repatriation but was able to demonstrate that there was a framework in place to allow for international asset repatriation and that it had been used in some cases to share assets with both EU and non-EU countries. In one case example various assets (gold and silver bars and frozen accounts) worth EUR 350 000 were frozen on behalf of US authorities pursuant to a MLA request alleging that the assets were the proceeds of fraud and then repatriated on the basis of a mutual confiscation order agreed with the offender. In another case example, EUR 4.2 million of assets held in bank accounts and securities accounts was frozen in March 2020 at the request of Swiss authorities (proceedings were ongoing at the end of the onsite visit).

**Box 3.11. Case example: foreign proceeds of crime****Foreign proceeds of crime from fraud (BY-GW-15)**

In this case, the Public Prosecution Office in Munich opened a case in 2018 following an STR filed by a bank where the offender held an account. Investigations revealed, that the offender was running an ML scheme through various bank accounts in Germany. Victims of fraud committed in Switzerland and the Netherlands were directed to deposit funds into bank accounts run by the accused in Germany where they were then transferred to a company domiciled in Austria to conceal the origin of the funds. The offender was paid a commission of 5% of the funds deposited in each case.

The offender was sentenced to a term of imprisonment for three years and three months for ML on a commercial basis and an order was made for the confiscation of EUR 558 710.52 in criminal proceeds.

**Foreign proceeds of crime from tax evasion (HH-GW-19)**

In this case, the offenders were part of an extensive tax evasion scheme committed in Belgium and Denmark and obtained unjustified tax advantages of EUR 1.3 billion. A proportion of these proceeds were laundered in Germany and several other countries.

The Hamburg Public Prosecution Office started an investigation in September 2015 following a tip-off from Danish authorities and an international Joint Investigation Team was established. In parallel, German authorities conducted an investigation into the ML activity in Germany. The investigations in Germany focused on identifying assets linked to the main offender and a large number of other persons involved in the tax evasion scheme.

Searches were carried at three banks in Germany and 10 terabytes of financial data was analysed. German authorities also requested account documents and turnover lists from other banking institutions.

Searches also took place in Denmark, the United Kingdom, Luxembourg, the United Arab Emirates and Malaysia. Account data was obtained and asset recovery measures were also instituted in Luxembourg, Switzerland, Monaco, France, Finland, the United States, the United Arab Emirates, the United Kingdom, Singapore, Malaysia and Jersey.

Following receipt of a request for mutual legal assistance from Denmark, EUR 230 million of assets held in bank accounts were frozen.

In March 2021, the Public Prosecution Office Hamburg filed charges against 7 defendants and 16 other participants and initiated confiscation proceedings. The main defendant has been charged with money laundering on a commercial basis while the six other defendants have been charged with money laundering. The prosecution has applied for confiscation of EUR 230 122 186, GBP 15 641 903 and USD 99 985. In addition, the prosecution has applied for confiscation of contingent convertible bonds in the value of EUR 5 million and shares in the value of EUR 4 million. All of these assets have been secured in the investigation. Furthermore, the

prosecution has applied for the confiscation of assets of equivalent value from the main defendant in an amount of EUR 125 300 000.

Source: German Authorities

3

### *Proceeds located abroad*

170. With respect to the pursuit of assets derived from domestic predicate offences, Germany demonstrated that cases were actively pursued but the statistics for cases pursued overseas do not appear to be in line with Germany's risk profile and the overall number of cases of confiscation. Statistics from 2019 show that Germany had requested the freezing of EUR 11.9 million in funds in 47 different operations. In 2020, this amount grew to EUR 54.4 million frozen in 63 different operations with one particularly large case involving EUR 41 million in Ukraine. However, considering the total amount of assets frozen domestically, there is room for improvement to further the proactive pursuit of proceeds located abroad.

**Table 3.16. Assets frozen outside of Germany in 2020**

Requesting authority	Number of cases	Amount frozen (EUR)
Baden-Württemberg	20	3 452 977
Bavaria	10	43 508 191
Illicit Employment Monitoring Authority	2	634 695
Lower Saxony	7	1 367 231
North Rhine-Westphalia	2	38 909
Saarland	6	2 222 093
Schleswig-Holstein	4	182 225
Thuringia	5	302 309
Customs Investigation Service	3	229 650
Federal Border Police (BPol)	1	128 525
Federal Criminal Police Office (BKA)	3	2 374 741
<b>Total</b>	<b>63</b>	<b>54 441 546</b>

Note: Statistics were not provided for other *Länder* or agencies.

Source: German Authorities

**Table 3.17. Assets frozen outside of Germany by receiving country 2020**

Respondent country	Number of operations	Amount frozen (EUR)
Ukraine	1	41 000 000
Australia	1	2 193 478
Switzerland	5	1 874 408
Ireland	1	1 499 216
Poland	5	1 392 282
Hungary	6	1 032 883
Türkiye	2	882 667
Romania	3	840 102
Netherlands	6	775 055

Respondent country	Number of operations	Amount frozen (EUR)
Serbia	4	442 000
Bulgaria	4	425 618
Luxembourg	3	255 338
Austria	5	242 309
Croatia	2	206 000
Czech Republic	1	197 154
Lithuania	1	195 609
France	2	165 000
Spain	1	136 500
Lebanon	1	128 525
Italy	2	116 434
Gibraltar	1	110 000
Cyprus	1	107 485
United Kingdom	2	99 678
Lichtenstein	1	93 000
Finland	1	26 799
Slovakia	1	4 006
<b>Total</b>	<b>63</b>	<b>54 441 456</b>

Source: German Authorities

### *Confiscation of falsely or undeclared cross-border transaction of currency/BNI*

171. Germany has measures in place to detect and prevent cross-border movements of currency and BNIs and confiscates assets to some extent. There is a written declaration system in place for all persons entering or leaving the EU with currency or BNIs above a EUR 10 000 threshold. To supplement this, Germany has also implemented a disclosure system which requires movements within the EU to be disclosed to Customs officials. However, the powers available to seize and confiscate falsely or undeclared or disclosed funds are underutilised and the overall amount of assets seized is low. Sanctions imposed are also low considering the high-risk associated with cash in Germany. There has been limited action taken with respect to cash movements through mail and cargo which is an area of heightened risk for Germany. The assessment team based its findings on: statistics, case studies and interviews with Customs, the FIU and other LEAs.
172. Cash is acknowledged by all agencies as high-risk and the risks around the physical transport of cash by travellers were well understood. In Germany, declarations and disclosures extend to precious metals and gems as equivalent means of payment but does not extend to jewellery (nor is this currently required under the FATF Standards). Customs develops intelligence products to highlight risks associated with cash couriers. However, there was limited awareness about the risks of cash transportation through mail and cargo. While Germany put measures in place to monitor the transport of cash through mail and cargo in June 2017, Germany only carried out its first active inspection of cash transported through the postal system in 2020 and at the time of the on-site it was not clear that there was regular, active monitoring and inspection of cash transported through postal services and no active monitoring of bulk cash movements through cargo. Germany has only required disclosures for cash transportations through mail and cargo since June 2021.

173. Sanctions for intentional or negligent failure to declare/disclose and false declarations/disclosures are subject to an administrative fine but the penalties applied in practice are low. Less than 1% of cases result in a fine of over EUR 10 000 with the vast majority of fines falling in the EUR 1 000 to EUR 10 000 range although a maximum fine of EUR 1 million is possible and asset confiscation action can be taken if there is a suspicion that the cash is the proceeds of crime (please see table 3.19). Authorities explained that internal Guidelines specified that in cases of negligence, the prescribed fine should be 12% of the amount carried increasing to 25-50% in cases with clear intent or with aggravating circumstances. Separate asset confiscation action may also be taken with respect to the full amount of the cash seized. The low range of fines applied also reflects the type of cases commonly referenced (predominantly cash courier activity). Overall, sanctions applied in practice for failures to declare or disclose cash may be proportionate but are not sufficiently dissuasive in all cases.

**Table 3.18. Total number of cash declarations and disclosures and fines 2017-2020**

	2017	2018	2019	2020
Total number of cash declarations and disclosures	24 529	24 236	24 376	<b>13 355</b>
Total amount of fines imposed (declarations and disclosures) (EUR)	5.8 million	5.3 million	5.6 million	2.5 million
Number of fines	2 997	2 606	<b>2 453</b>	1 907
<b>Declarations</b>				
Number of cash seizures	132	155	206	283
Total amount of cash frozen (EUR)	6 753 240	8 668 292	7 428 465	15 143 609
<b>Disclosures</b>				
Number of cash seizures	26	26	26	83
Total amount of cash frozen (EUR)	1 376 216	1 155 426	1 104 728	6 267 940

Note: Seizures refers to the amounts of cash detained. Figures on the total amount of cash that is confiscated was not available. Germany also reports that approximately 20% of all declarations are related to commercial activity. For example: credit institutions or supermarkets in German towns close to the Swiss border depositing their daily revenue (often a high amount of cash) in bank accounts in Switzerland.

Source: German Authorities

**Table 3.19. Breakdown of fines**

Amount of fine in EUR	Number of fines 2019	Number of fines 2020
0-500	134	155
501-1 000	561	345
1 000-10 000	1 735	1 381
10 000-20 000	16	18
20 000-50 000	5	5
50 000-100 000	1	2
Over 100 000	1	1
	Total no. of fines: 2 453	Total no of fines: 1 907

Source: German Authorities

174. Customs officers have the power to seize assets if there is a suspicion of ML or TF and can hold the assets for a period of five days (which can be extended up to three months) while further enquiries are made. This power is used with relative frequency but from the case examples shared with the assessment team it seems that most cases are discontinued after a preliminary investigation by the GFGs and do not result in an ML investigation or asset confiscation action. It is expected that changes to the ML offence will make it easier to pursue investigations for ML when the predicate offence cannot be established but the objective factual circumstances indicate ML activity as is often the case with cash interceptions. In particular, the assessment team found that there were a large number of cases involving the use of money mules but most of these ended with an administrative fine and without an investigation being pursued into the organisers of the ML network. Customs seems sufficiently resourced to take on this increased work load but the GFGs may benefit from additional staff to support the increased case load.

### Box 3.12. Case example: seizure of cash and assets

In June 2019, the person concerned travelled by car from Switzerland to Germany and underwent a customs inspection. Customs officers asked him about any cash carried. When asked to declare the cash carried by him, the person concerned did not comply and expressly denied the questions asked in that regard. During the subsequent control search, officers found EUR 517 000 and 400 Krugerrand gold bullion coins with a total value of EUR 1 002 748 in the car of the person concerned. The person had not submitted the required written declaration of cash above the reportable threshold of EUR 10 000.

Due to the overall circumstances of the control, the cash and assets were seized and a clearing procedure was initiated at the GFG Police/Customs Baden-Württemberg. These preliminary investigations could not find evidence to found a suspicion of ML or that the assets were derived from criminal offending and the seizure was revoked and an administrative fine of EUR 250 687 was imposed for failing to declare the cash and gold coins.

Source: German Authorities

### *Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities*

175. Germany's confiscation results are largely in line with its ML/TF risks and national AML/CFT policies and priorities. While statistics were not available on the top proceeds generating offences for asset confiscation, available statistics on asset freezes show that most cases relate to money laundering and other high-risk predicate offences, namely: fraud, narcotics, corruption and tax offences. However, there were no human trafficking cases identified even though it was identified as one of the top three high-risk predicate offences in the NRA. The assessment team based its findings on: statistics, case studies and interviews with relevant competent authorities.

176. Germany has also identified ML through the real estate sector and ML using cash as high-risk. Overall, case studies and interviews with prosecutors supported the conclusion that assets laundered through real estate are targeted for asset confiscation and approximately 24% of frozen assets relate to real property (see table 3.15). With respect to cash, 19% of the assets frozen in Germany relate to cash. This is in line with cash being a high-risk area but based on case studies and interviews, the assessment team concluded that this figure should be higher in Germany considering the intensive use of cash and the large number of cross-border cash cases which end with an administrative fine rather than asset confiscation. With respect to Germany's status as an international financial centre, the assessment team was able to review some cases where Germany had taken action to pursue assets in situations where the predicate offence had occurred overseas and Germany was the transit or destination country for the proceeds. However, it seems that these cases are triggered by an international request for assistance and it was not clear if these types of cases were proactively initiated by Germany on the basis of domestic ML.
177. There is a difference in risk across the different *Länder* and variation in the amounts of assets confiscated with lower amounts confiscated in smaller *Länder* and higher amounts in *Länder* with higher population sizes and increased economic activity. The assessment team reviewed a sample of asset confiscation figures across the *Länder* and found that it was broadly consistent with variation in risk profile across the *Länder*.

**Table 3.20. Total assets frozen: Top proceeds generating offences (EUR)**

Predicate offence	2017	2018	2019	2020
Money laundering	39 726 473	48 770 999	114 597 754	80 747 156
Fraud	105 646 135	235 503 593	110 268 042	151 127 392
Narcotics offences	29 159 218	39 244 957	30 646 069	49 491 002
Theft	30 890 974	36 689 236	29 158 319	26 284 993
Corruption	197 695 595	3 334 240	25 117 306	14 182 504
Tax offences	24 640 492	11 701 757	25 058 924	12 746 640
Intellectual property offences	9 736 769	1 764 263	24 687 961	41 222 507

Source: German Authorities

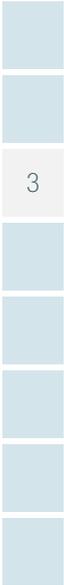
## Overall conclusion on IO.8

178. The mandatory requirement for prosecutors to pursue asset confiscation in all cases involving proceeds of crime has a positive impact on Germany's effectiveness and overall, the amount of assets frozen and confiscated and the number of cases in which asset confiscation is pursued is high. Legislative and policy changes implemented in 2017 and increases in resources have supported these efforts.
179. LEAs have the capacity to trace proceeds of crime and have demonstrated significant financial investigation capacity. Asset freezing and confiscation is also mostly in line with risk. However, efforts to trace and recover proceeds related to foreign predicate offences and assets located abroad leaves minor room for

improvement.

180. Cash controls are in place and Customs is active in pursuing cross-border cash movements, particularly in relation to cash couriers. However, the low quantum of assets recovered from these efforts and the low penalties for disclosure/declaration offences leaves room for some improvement. Actions to improve risk understanding and target bulk cash movements and general cash movements through mail and cargo are also an area for improvement considering Germany's risk and context.
181. Overall, there is scope for major improvements in relation to cross-border cash movements and minor improvements that could be made with respect to the pursuit of assets located abroad and foreign predicate offence. Considering the positive aspects of the rest of the regime, overall moderate improvements are required.

**Germany is rated as having a substantial level of effectiveness for IO.8.**



## Chapter 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

### Key Findings and Recommended Actions

#### Key Findings

##### 10.9

- a) Germany proactively investigates TF activity alongside terrorism-related investigations and consider financing as a form of support for terrorist organisations. TF case studies are broadly in line with identified risks around: low-level funding for religiously-motivated terrorist groups; more complex fundraising for Turkish-based terrorist groups; and, TF involving foreign terrorist fighters (FTFs), at-risk NPOs, *hawala* dealers and right-wing extremism.
- b) Authorities have a robust array of tools, data sets and capabilities they can employ to investigate and analyse TF-related activity. Authorities have developed a Joint Situation Report on TF and case studies demonstrate that a range of TF activity is pursued, and that TF is prosecuted under a variety of offences. However, statistics do not differentiate between TF activity and other forms of terrorist support and further efforts could be taken to proactively and systematically investigate TF activity independent of terrorism investigations and in cases where a natural person cannot be identified.
- c) TF investigations are well-integrated into broader counter-terrorism strategies, and the imperative of combating terrorism ensures that agencies co-ordinate and co-operate well across the federal and *Länder*-levels via standing taskforces and shared databases. As set out in 10.6, further integration of the FIU in these mechanisms would increase the prominence of financial intelligence in cross-government initiatives.
- d) Convictions and sentencing for natural persons appear to be in line with other serious crimes and is supplemented with counter-radicalisation and reintegration programs.
- e) Germany has demonstrated its ability and willingness to use all available measures to disrupt TF, including banning of organisations and proactive measures to address violent right-wing extremism and using the TFS offence to prosecute TF activity.

##### 10.10

- a) Germany relies primarily on the EU framework for implementing TFS; it does not have a separate domestic list for implementing UNSCR 1373. In 2020, Germany enacted a domestic framework which has mitigated

designation delays at the EU-level to-date. While Germany has sponsored UN designations under UNSCR 1267, it does not proactively designate individuals and entities under UNSCR 1373 in line with its risks and context. Law enforcement authorities prefer to use other measures (which are limited in scope) to respond to TF risks and are not aware of or do not see the value in designation as part of Germany's broader counter-terrorism and CFT strategy.

- b) Measures are in place to publicise lists, and to proactively and immediately communicate new listings and de-listings to banks. Proactive communication with other sectors, including higher-risk sectors such as MVTS and DPMS, is insufficient.
- c) Germany has a good understanding of the TF risk in its NPO sector and the typologies used by different terrorist and extremist groups. Mitigation measures are adequate and proportionate, and authorities have demonstrated their ability to respond quickly to new risks. Engagement with NPOs is largely through umbrella organisations. This ensures NPO involvement and ownership, but risks missing smaller NPOs and results in limited direct, ongoing exchange between NPOs and the government.
- d) Germany has access to domestic measures to deprive terrorists, terrorist organisations, and terrorist financiers of their assets. Authorities demonstrated that they can use association bans (with accompanying asset confiscation) and criminal confiscation tools effectively and proportionately. However, these measures have limitations in the context of IO.10. Other tools, namely freezing powers of BaFin and the FIU, are used to a lesser extent. Alternative domestic measures are limited in scope and cannot provide an effective alternative to TFS designations, given Germany's risk and context. The overall amounts frozen under the various mechanisms are relatively low when compared to Germany's estimates of the total amounts raised within Germany for various terrorist organisations.

#### IO.11

- a) Germany implements UNSCRs 1718 (DPRK) and 2231 (Iran) through the same mechanism as terrorism-related TFS. Funds have been frozen under both regimes, in line with Germany's context.
- b) FIs compliance with proliferation-related TFS is monitored by the Deutsche Bundesbank. DPMS, REAs, casinos, TCSPs and insurance intermediaries do not have a statutory supervisor for TFS compliance and supervision of DNFBPs in general is limited, including in higher-risk sectors (such as DPMS).
- c) While most FIs and larger DNFBPs (particularly larger legal and accounting firms, and major DPMS entities) perform sanctions screening, there are screening gaps, in practice, in some higher-risk sectors (such as DPMS) that impact the effectiveness of TFS implementation. Smaller FIs and DNFBPs have a weaker understanding and implementation of their proliferation-related TFS obligations, in line with the limited supervision and outreach to these sectors.

## Recommended Actions

### 10.9

- a) Improve and formalise feedback from intelligence agencies and LEAs to the FIU on the use of financial intelligence to enable enhanced and targeted detection capabilities, tactical and operational analysis from the FIU in TF matters.
- b) Take a more systematic approach to investigating TF (distinct from terrorism investigations) to ensure the risks from informal money value transfer systems are addressed holistically (detection, investigation, prosecution and disruption) and to ensure that TF networks using legal persons or complex structures are fully investigated through 'structural proceedings' and appropriate civil or administrative measures taken. Consider whether additional measures are required to facilitate TF investigations and prosecutions in situations where it is difficult to establish and prove a link to a specific terrorist act or terrorist organisation (including, if necessary, amendments to the TF offences or the introduction of other criminal justice measures).
- c) Improve the collection of statistics on TF disruption, investigations, prosecutions and convictions in order to better assess the effectiveness of the system in light of the relevant TF risks.

### 10.10 and 11

- a) Improve the effectiveness of the TFS system by:
  - a. raising awareness of TFS as a tool for TF disruption, proactively proposing UNSCR 1373 designations as appropriate and considering the development of a domestic listing process;
  - b. address technical deficiencies to ensure that UN listings that occur on Friday afternoon or on a national holiday are implemented without delay;
  - c. ensuring DNFBPs are supervised for compliance with TFS in line with risk and that supervisors of higher-risk sectors actively raise awareness of TFS obligations and proactively alert entities to new listings; and
  - d. ensuring all relevant government authorities (including legal person and arrangement registries and the transparency register) scan sanctions lists to proactively identify and freeze assets.
- b) Continue and increase support for NPO-led efforts to raise awareness of TF risks and preventive measures, including among smaller NPOs, and establish mechanisms for ongoing communication between a broad range of NPOs, the government and the financial sector to tackle de-risking and maintain awareness of emerging risks.

182. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5-8, 30, 31 and 39, and elements of R.2, 14, 15, 16, 32, 37, 38 and 40.

### Immediate Outcome 9 (TF investigation and prosecution)

183. In Germany's federal system, responsibility for the investigation and prosecution of TF is shared between federal and *Länder* authorities. Compared with ML, federal agencies play a much greater role in TF as it is considered a matter of state security subject to federal jurisdiction. Complex, international and otherwise significant TF cases are normally investigated by the Federal Prosecutor General (GBA) and the Federal Criminal Police Office (BKA). On investigations, Germany's domestic intelligence agency the Federal Office for the Protection of the Constitution (BfV) and the foreign intelligence agency, the Federal Intelligence Service (BND) are actively involved in the detection and investigation of terrorism and TF cases.

### Prosecution/conviction of types of TF activity consistent with the country's risk-profile

184. Germany prosecutes and secures TF convictions in line with the country's risk profile to a large extent. The assessment team's findings are based on: an academic study as part of the NRA process that looked in-depth at TF-related cases in Germany from 2015-17, updated statistics from the GBA and FIU; case studies; interviews; and confidential operational reports.
185. Overall, authorities demonstrated a good understanding of their TF risks. Germany assess its overall terrorism risk as high and its TF risk as medium-high. TF risk varies across the different *Länder* with 95% of TF cases taking place in eight *Länder* (North Rhine-Westphalia, Baden-Wurttemberg, Hesse, Berlin, Bavaria, Rhineland Palatinate, Hamburg and Lower Saxony) who have higher exposure and risk for terrorism and TF. A shared understanding of risk is enhanced by strong formal and informal relationships between agencies and the co-ordination mechanisms already put in place for countering terrorism. Religiously-motivated terrorist groups, primarily ISIL and its associates are a beneficiary of TF in Germany. Germany has identified the use of self-funding, small scale-fundraising through social media and relatives, use of *hawala* dealers and at-risk NPOs as common methods for raising or moving funds. Fundraising for terrorist groups targeting Türkiye like the Kurdistan Workers' Party (PKK) has been a persistent issue since the 1980s with over half of all fundraising for this group in Europe raised in Germany. In 2020, the PKK raised around EUR 16.5 million in Germany. This is the second largest source of cases in Germany although the number of cases is significantly lower than cases related to religiously-motivated terrorist groups. Fundraising for right-wing violent extremist groups is viewed as a growing area of concern.

186. Germany presented 30 case studies from 2012 to 2021 which demonstrate that a broad range of TF is prosecuted, including financing of different types of terrorism and via various means.<sup>42</sup> Out of the 30 cases, 23 related to religiously-motivated terrorist groups, six related to Türkiye-based terror groups and one case related to a right-wing extremist group. With respect to the methods of financing, four cases identified the use of *hawala* dealers and two cases involved the misuse of NPOs. Eight cases involved FTFs and either self-funded activity or funding by friends and associates of the FTFs (see box 4.1 - GBA-TF-30). For the most part, fundraising involved small amounts of funds and the methods used to transfer funds were simple. However, Germany has also demonstrated capacity to pursue cases of complex financing (e.g. cases involving sophisticated fundraising networks and international movement of funds (see box 4.1 - GBA-TF-14). Two cases were presented that investigated the facilitators of two large-scale, organised fundraising networks for ISIL in Europe (see box 4.1 - GBA-TF-23).

#### Box 4.1. TF case examples: prosecution of different TF cases

##### Case example: prosecution of organised ISIL fundraising (collection of funds - GBA-TF-23)

The suspect operated a “media office” in Germany distributing ISIL propaganda through social media and messenger service and ask users to make donations to ISIL. By January 2018, the accused had collected EUR 3 770 in donations. Together with his own funds, the suspect had collected a total of EUR 4 000 which he intended to transfer to ISIL in Syria through *hawala* dealers. Through extensive investigations including telecommunications intercepts, surveillance and mail seizures carried out by police and intelligence services the suspect was connected to the funds and also to ISIL members.

The suspect was convicted on 2 August 2019 of supporting a terrorist organisation and soliciting support for a terrorist organisation (ss.129a(1) and 129b, StGB) and sentenced to four years imprisonment. While it not possible to breakdown the TF component of the final sentence, feedback from prosecutors notes that the other elements of this case (transfer of data to members of ISIL) attracted much lower penalties and that the TF was the most significant aspect of the offence.<sup>43</sup> Investigations into the suspect’s donors are ongoing.

<sup>42</sup> Germany considers that the case studies are representative of TF investigations and prosecutions across Germany and notes that cases that started in 2012 are still current as they relate to ongoing structural investigations are still ongoing or were only concluded within the last five years.

<sup>43</sup> In forming the penalty, the German Criminal Code uses the system of a total penalty, according to which the penalties imposed for the individual offences are not schematically added up, but in the context of the formation of the total penalty, the highest penalty imposed is merely increased by the court, taking into account the circumstances of the individual case due to further penalties imposed. This means it cannot be referred from the reasons of the judgement which share of the total penalty is attributable to the financing component.

**Case example: Prosecution of self-funded foreign terrorist fighter travel (use of funds - GBA-TF-30)**

In 2014, two suspects travelled from Germany to Syria to join ISIL and participate in terrorist activity. Prior to leaving Germany, one of the suspects took out a EUR 5 000 overdraft loan and gave most of the cash to the other suspect to fund their travel to Syria and finance their living expenses.

After three months, both suspects returned to Germany. They were prosecuted for membership and involvement in a foreign terrorist organisation (StGB, s.129a(1) and 129b(1)). They were sentenced to prison terms of four years and three months and three years for these offences. While a range of activity was involved, the handing over of the money was assessed as one of several acts of membership activity.

**Case example: Prosecution of organised fund-raising activity (collection and provision of funds - GBA-TF-14)**

In this case, the suspect was the active member and head of European Operations for the Devrimci Halk Kurtulus Partisi-Cephesi – the Revolutionary People’s Liberation Party/Front (DHKP-C). They are a designated terrorist group in the EU.

Search operations in the Netherlands and Germany indicated that the suspect was a ringleader of DHKP-C and seized computer records proved the receipt and forwarding of funds from the organisation’s annual fundraising campaign. There was evidence to prove that the suspect had received numerous sums of money between EUR 3 000 and EUR 10 000 between 2009 and 2010 that represented the proceeds of the group’s annual fundraising campaign. There was also evidence to support the suspect being actively involved in fundraising activity in 2016-17 and instructing other members of the group.

The suspect was prosecuted for membership of and involvement in a foreign terrorist organisation (StGB, ss.129a(1) and 129b(1)) and violations of the Foreign Trade and Payments Act. The suspect was convicted and given a prison sentence of six years and nine months.

**Case example: Investigation and prosecution for fundraising although no funds ultimately received (attempted funding - BW-TF-1)**

In this case, the suspect was planning a terrorist attack in Germany. He sought to procure firearms and ammunition for the attack and appealed online for financial and material support from donors sympathetic to ISIL. This included seeking support for travel to Romania to acquire a firearm.

The suspect was detained at the airport and although no funds had been received, the fundraising activity was sufficient to sustain a TF charge.

The suspect was convicted under s.89c of the Criminal Code (StGB) and given a two-year suspended sentence for terrorist financing in February 2017.

Source: German Authorities

187. The case studies and interviews with authorities supplement the limited available data on TF investigations and prosecutions to demonstrate that Germany is prosecuting TF cases in line with its risk profile to a large extent. Germany only has partial statistics on TF cases as TF is predominantly prosecuted under broader terrorism support offences<sup>44</sup> and authorities cannot readily identify which cases were TF cases and which cases did not relate to financing. To address this gap, Germany commissioned an academic study as part of the NRA process that looked in-depth at TF-related cases across Germany from 2015-17. Available statistics from 2015-2017 show that there were 681 TF investigations and 44 convictions by federal and *Länder* prosecutors (see Table 4.1). More recent statistics are only available at the federal level (see Table 4.2) and show that from 2018 to 2020, there were 156 investigations and 12 TF prosecutions by the GBA at the federal level. Compared to the statistics for terrorism investigations/prosecutions, a higher percentage of TF investigations result in a TF prosecution. More cases have been investigated and prosecuted by *Länder* authorities in 2018-2020 but statistics on cases prosecuted by *Länder* prosecutors are not available.

**Table 4.1. TF case outcomes by Federal and *Länder* public prosecutors 2015-2017**

Case outcome	Number of cases
Convictions	44 (6%)
Referral to another authority for alternative action	107 (16%)
Cases closed*	530 (78%)
<b>Total number of cases investigated</b>	<b>681</b>

Note: This includes all cases prosecuted by the GBA and *Länder*-level public prosecutions. \*The category “case closed” refers to cases that do not proceed to prosecution for a variety of reasons including lack of evidence, innocence of the accused, there is no public interest in pursuing the prosecution or because the offence is already being prosecuted in another country.

Source: Ludwig-Maximilian-Universität München (LMU)/KPMG Research Project: National Risk Assessment: Combating Money Laundering and Terrorist Financing – Criminal and preliminary proceedings concerning terrorist financing in Germany from 2015 to 2017 (27 April 2020).

<sup>44</sup> See R.5. Germany relies on a range of offences to criminalise and prosecute TF activity broadly in line with the FATF standards. The offences considered to be TF offences for the purposes of R.5 are the offence of funding specific terrorist acts (German Criminal Code (StGB), s.89c) and support for terrorist organisations (s.129a(1), (2) and (5)). Prosecutors explained that s.89c has a lower threshold for initial suspicion and is a useful basis for starting an investigation. The offence also carries a high penalty and triggers access to coercive investigative techniques like telecommunications intercepts and surveillance. Where investigations reveal connections to a terrorist organisation, prosecutors prefer to prosecute TF activity under offences for forming or supporting a terrorist organisation (StGB, ss.129a (1), (2) and (5), 129b(1)). Prosecutors noted that s.89c may not be the most appropriate for prosecution as it requires proof of a link between the financing and a specific terrorist act to satisfy the physical/conduct elements. The TF offences (ss. 89c, 129a and 129b) carry similar penalties.

**Table 4.2. Terrorism and TF investigations and prosecutions by the Federal Prosecutor General (GBA)**

	2016	2017	2018	2019	2020	Total
Terrorism investigations	238	1210	1196	662	551	3 857
TF investigations	Not available	Not available	57	58	41	156
Terrorism prosecutions	21	18	12	13	10	74
TF prosecutions	Not available	Not available	3	5	4	12

Note: These statistics only include cases investigated and prosecuted by the GBA. Prior to 2018, specific data on terrorist financing investigations and prosecutions were not recorded separately at the time.

Source: German Authorities

188. There are no convictions of legal persons for TF as Germany's legal framework does not extend criminal liability to legal persons. However, apart from association bans (see Box 4.4 – case example on association ban) there was also little evidence of action taken using civil and administrative law provisions. The case studies also did not show targeting of TF facilitators (for example, *hawala* dealers or professionals involved in developing complex TF schemes via legal persons).

### *TF identification and investigation*

189. Germany identifies and investigates TF activities as part of broader terrorism investigations and the specific role of the terrorist financier is generally identified. While the statistics presented by Germany were not comprehensive, the assessment team was able to base its conclusions on these limited statistics; case studies and interviews with relevant law enforcement, intelligence and prosecution agencies.
190. TF activity is identified as part of a holistic approach to combating terrorism. Cases are primarily detected and investigated as part of a broader terrorism case, through a tip-off or notification from a foreign LEA, through information from the intelligence services or through an FIU dissemination. Domestic co-ordination mechanisms like the GTAZ in Berlin and the Joint Centre for Extremism and Terrorism (GETZ) in Cologne focus on terrorism but consider TF also as part of their intelligence function. Financial investigations are an important tool used to identify, investigate and disrupt terrorism. When TF investigations are commenced, investigators have a wide range of powers and information sources to draw upon (see IO.6 and IO.7).
191. STRs with a TF link are immediately disseminated to the BfV, which is a strong feature of the German system as it means that there is a rapid fusion of financial intelligence and other intelligence sources. In parallel, the FIU analyses the STR and disseminate the findings of this operational analysis to relevant LEAs, the BND (if it falls in an area of responsibility) and the BfV if the STR has previously been sent to it. Intelligence agencies send staff to the FIU to better understand the role of the FIU and of financial intelligence in terrorism and TF investigations. There has been a rise in the number of TF-related STRs since 2017. Comparing the numbers from 2017 (3 210) with 2019 (6 253), there are almost double the number of STRs being linked to TF and automatically disseminated. This is in part due to an overall rise in the number of STRs being filed by obliged entities (see IO.4 and IO.6) and the introduction of specific TF risk-indicators related to NPO activity and the abuse of

MVTS, that the FIU implemented in 2019 to prioritise STRs for analysis and dissemination.

**Table 4.3. Number of TF-related STRs received and disseminated**

	2017	2018	2019	2020
TF-related STRs received and disseminated	3 210	4 516	6 253	3 595*

Note: As all TF-related STRs are disseminated immediately, the number of STRs on TF received and disseminated to BfV and LEAs is the same. As a result of a change in the way statistics are maintained, the figures in 2020 are lower and only refer to the number of reports disseminated (including multiple STRs).

Source: German Authorities (FIU)

### Box 4.2. Case studies: identification and investigation of different forms of TF activity

#### Case example: Detecting TF through an STR (BW-TF-4)

In January 2018, a money transfer provider filed an STR about a man suspected of collecting and transferring money to the organisation Hai'at Tahrir asch-Sham via an aid association in Germany. The money was collected through the bank account of the association and was made up of donations from members of the diaspora community. Funds were then transferred to an individual in Türkiye and the onward to the destination country.

There were extensive investigations into two accused for using an independent aid organisation as a cover to support the foreign terrorist organisation. This included financial investigations to search various property and police registers and the databases of the FIU and BaFin. Investigations were also conducted into donors. The case was ultimately terminated but is a good example of how TF activity can be detected through an STR.

#### Case example: TF case involving right-wing terrorist group identified through intelligence sources (GBA-TF-27)

In September 2019, a group of five individuals formed a right-wing terrorist organisation. The organisation's aim was to disrupt and destroy the political and social order of Germany and planned attacks on politicians, asylum seekers and minority ethnic groups to trigger a civil war. The group met and organised their activities through the internet, messenger services, chat rooms and by telephone. Seven supporters were also identified who had agreed to provide financial support or procure weapons for the group. The case came to the attention of LEAs through information provided by a whistle-blower who reported on the content of various group chats. Surveillance was started and investigations launched. Financial investigations were also commenced into financial flows related to the group. Several members of the group were found to have pledged financial support to the organisation.

Twelve individuals were arrested and are being prosecuted for forming a, membership and support of a terrorist organisation (StGB, s.129a). Five

defendants are charged with having agreed in September 2019, one of them as ringleader, to join together as members for an indefinite period in order to shake and overcome the existing state and social order of the Federal Republic of Germany by committing attacks against politicians, asylum seekers and persons of Muslim faith. Seven (originally eight) defendants are suspected of supporting the terrorist organisation by promising financial contributions to purchase weapons or participating in armed attacks against mosques and worshippers. Proceedings are ongoing.

**Case example: Investigation into a TF middle-man identified through STRs (BE-TF-2)**

In 2015, two MVTs providers filed STRs in relation to several payments involving EUR 7 100 and EUR 1 400 flagging a TF concern. Police investigating the case found a link to a French jihadist couple who had travelled to Syria.

The suspect received money into his account from many people and then withdrew the funds and forwarded it to a recipient in Türkiye via an MVTs provider who then forwarded the funds to ISIL. There is no connection between the people depositing funds and the suspect. It is suspected that the person is acting as a middle-man to facilitate funds transfer to ISIL.

Investigations are still ongoing as the suspect left the country and only returned to Germany in 2020. He was arrested at that point and is currently serving a two-year prison sentence for smuggling-related offences.

**Case example: Investigation into ISIL international financing networks identified through MLA requests (collection and provision of funds) (GBA-TF-4)**

In this case, Germany authorities worked with international counterparts in Norway, Switzerland, the US, Kosovo, Italy and Belgium to investigate a middleman in an international fund-raising network for ISIL.

The case came to light in December 2016 following the receipt of an MLA request from Belgium. The MLA request revealed that the accused had arranged for several money transfers to Kosovo and had received money from Belgium which was then intended to be transferred to Syria via MVTs and *hawala* networks. In December 2017, the accused was stopped at the German-Swiss border and traces of explosive were found upon inspection of the vehicle. Taken together, the information in the MLA request and the findings of the vehicle check were sufficient for the Public Prosecution Office Flensburg to initiate a preliminary investigation on the basis of TF (StGB, s.89c(1)) and preparing a serious act of violence endangering the state (StGB, s.89a(2)(3)).

Extensive investigations were conducted in Germany including telecommunications intercepts, online chat monitoring, and seizures of electronic data and financial documents. Enquiries were made into the accused financial transactions including information on his bank accounts obtained via BaFin, examination of account statements and queries with financial service providers including Western Union, MoneyGram, Ria Money Transfer, pension insurance systems and searches of land registers.

Enquiries were also made with foreign counterparts including co-operation with Swiss authorities to search the accused's house, seized electronic data and financial documents and co-operation with US authorities to obtain information on

financial transactions made via Western Union. An FIU dissemination based on STR information from Western Union Payment Services Ireland in February 2018 further supported the case.

Put together, the information obtained allowed police to trace the path of 15 money transfers from Kosovo, Belgium, Norway and other countries that were transferred via legitimate MVTs providers to the accused who would withdraw the funds in Germany and then transfer the funds to a *hawaladar* who would then transfer the funds to FTFs in Syria.

At this stage, the GBA took over the proceedings and submitted MLA requests to a number of countries and issued an arrest warrant for the accused in June 2018. Search warrants were also issued and simultaneously executed in Germany and Norway (against persons suspected of related TF activity there).

In March 2020, the accused was sentenced to a prison term of three years and nine months for supporting a foreign terrorist organisation in breach of targeted financial sanctions under section 18 of the AWG.

Note: More details of the case are outlined in box 3.2.

Source: German Authorities

192. German authorities noted that there were currently 40 structural proceedings ongoing targeting terrorist groups operating in Germany. These proceedings are complex, longstanding and ongoing investigations into the activities and support networks of these groups. This includes investigations into financing activity both as part of broader structural investigations into terrorist groups operating in Germany and specific structural investigations into specific financing support networks operating in Germany to support terrorists and terrorist groups operating overseas. Individual criminal cases are identified through these broader structural proceedings and then referred to prosecution. Two examples of structural proceedings that generated TF investigations, prosecutions and convictions against individuals are set out in box 4.3. Authorities noted that the ongoing structural investigation into PKK led to five TF-related convictions in 2020-2021 alone.

### Box 4.3. “Structural proceedings”: investigations to establish the TF activity and the role of the terrorist financier

#### Case example: Syrian wallet case - investigation into ISIL financing (collection and movement of funds - GBA-TF-3)

In this case, structural proceedings were opened in co-ordination with Eurojust and other EU member states to look at activity related to remittances made to a known ISIL money mule based abroad. This money mule functioned as a middleman to transfer funds to ISIL members in Syria. Information provided by foreign countries led to the identification and investigation of 49 German money remitters, 450 individuals with a link to Germany and transactions made between 2013 and 2020 involving 670 transactions, with a value of EUR 450 000.

Preliminary proceedings have been initiated by the GBA and relevant *Länder* prosecution offences against the money remitters and individuals involved in sending funds on suspicion of supporting a foreign terrorist organisation, terrorist financing, violation of targeted financial sanctions and other related offences. One-third of the proceedings have been discontinued for various reasons and the remaining investigations remain ongoing.

#### Case example: investigation into foreign terrorist group (collection, movement and use of funds - GBA-TF-11)

In 2006, Germany launched investigations, in conjunction with a number of other European countries, into the activities of the Communist Party of Türkiye /Marxist-Leninist (TKP/ML) both inside Türkiye and in Western Europe. TKP/ML is outlawed in Germany and designated as a terrorist group by Türkiye. The proceedings spanned 10 years during which there was active monitoring of open source information, MLA requests to a number of countries, the establishment of joint investigation teams with other countries, monitoring of communications and collection of intelligence information. The investigation identified a number of persons who were involved in the TKP/ML’s “Foreign Section” in Germany and involved in organising annual fundraising campaigns and events to support the group financially. Through these activities, they were able to generate between EUR 360 000 and EUR 510 000 annually to support TKP/ML.

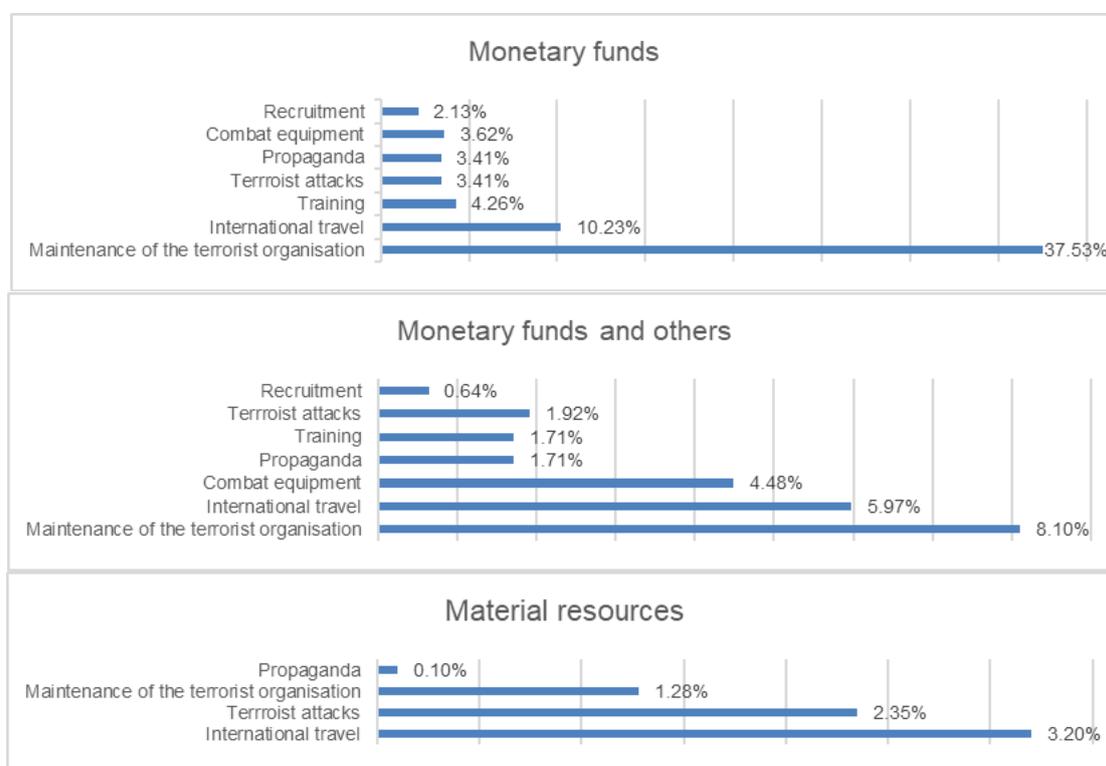
Ten people were arrested and charged with terrorism and TF offences. The main accused and ringleader was convicted and sentenced to six years and six months imprisonment for leading a terrorist organisation as a form of criminal financing of terrorism. The other nine accused were sentenced to prison terms between two years and nine months and five years for membership of a foreign terrorist organisation and their involvement in TF activity.

This is an ongoing structural investigation which continues to lead to a convictions for TF. The latest conviction was in Munich on 28 June 2020.

Source: German Authorities

193. It is difficult to assess trends in the number of TF cases investigated due to a lack of comprehensive statistics. Germany provided total numbers of TF investigations and prosecutions from 2015-17 (covering cases from both the Federal and *Länder* prosecutors) and cases initiated in 2019-20 by the Federal Prosecutor General (GBA). In total, across five years (but not including 2018), there were at least 780 investigations involving TF activity in Germany.
194. Investigations suggest that funds are primarily raised in Germany to fund international terrorist groups, travel, training and purchasing equipment (see figure 4.1). The focus on religiously-motivated terrorist groups could explain the relatively low level of sanctions applied for TF offences as many of these cases involve small-scale, simple financing activity or self-funding of activity like travel).

**Figure 4.1. Breakdown of TF activity in Germany 2015-17**



Note: This refers to analysis of 427 proceedings where it was possible to identify the purpose intended by the financier for the assets.

The definition of the terms can be described as follows:

**Monetary funds:** Financial assets, including cash, bank credit, traveller's cheques, bank cheques, money orders, cryptocurrencies, etc.

**Monetary funds and other:** Monetary funds combined with other assets such as material re-sources or legal documents or instruments in any form, including shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.

**Material resources:** Economic resources, material goods and property of any kind as well as legal instruments evidencing title entitlements to a services, such as airline tickets, military equipment, explosives, weapons, clothing, food, medicine, prepaid cards for cell phones, oil cans or vehicles.

Source: Ludwig-Maximilian-Universität München (LMU)/KPMG Research Project: National Risk Assessment: Combating Money Laundering and Terrorist Financing – Criminal and preliminary proceedings concerning terrorist financing in Germany from 2015 to 2017 (27 April 2020).

195. Based on the case studies, Germany is detecting and investigating TF to a large extent and the use of structural proceedings to maintain ongoing investigations into complex terrorist support networks was a positive aspect of the system. While Germany had difficulty presenting detailed data on TF cases distinct from terrorism cases, information about the structural proceedings demonstrate that Germany is taking a proactive approach to following financial leads and was investigating TF activity as part of a holistic approach to combating terrorism. For example, the PKK's main terrorist activities are in a foreign country and the main activity it carries out in Germany is fundraising. Germany has a proactive approach to monitoring, investigating and prosecuting and disrupting TF activity related to PKK (see box 4.4).

#### **Box 4.4. TF case examples: identification, investigation and prosecution of financiers of PKK**

##### **Case example: Prosecution of fundraiser related to PKK (collection of funds - GBA-TF-32)**

Based on structural investigations, authorities identified a terrorist financier who held a full-time leadership position in the PKK between June 2017 and June 2019. In this position, he acted as an “area officer” and “regional officer” and coordinated activities in his local area of responsibility reporting directly to a “European leadership team”. He was active in organising propaganda and fundraising events. He accused was charged with membership of a terrorist organisation for the fundraising activity and sentenced to three years and five months imprisonment.

##### **Case example: Prosecution of financier related to PKK (collection and transfer of funds & kidnapping for ransom - GBA-TF-33)**

A terrorist financier worked for the PKK from 2014 to 2018 as a local organiser and fundraiser in Hamburg, then Berlin and then Baden-Wurtemberg, especially in the Stuttgart region. His main duties were to collect donations in his locality or area and pass them on to the PKK. In April 2018, he organised the kidnapping of a person to raise funds for the PKK. The GBA laid charges under s.129a and 129b of the StGB and convicted and sentenced to 4 years and three months in prison.

##### **Case example: Identification of financier from PKK structural investigation**

Between June 2020 and April 2021, the accused raised EUR 940 000 and transferred them to the PKK. Based on a range of information from the structural proceeding on PKK which identified the accused's role, the GBA laid charges on 12 November 2021 in Higher Regional Court Frankfurt am Main under sections 129a and 129b of the StGB.

##### **Case example: identification and investigation of legal persons associated with TF**

In 2019, the Federal Ministry of the Interior, Building and Community (BMI) exercised the power to ban two companies that were associated with the PKK which has been a designated terrorist group in Germany since 1993.

Investigations and a search of the business premises had shown that the two companies were operating as publishing companies to benefit the PKK. All of the

business activities of the two companies were conducted exclusively for the benefit of the PKK. Their earning capacity gave a sustained boost to PKK's capacity to operate in Germany and Europe. It was not possible to prosecute the companies for TF activity so German authorities banned the association and seized the assets of the two companies, effectively winding them up. In line with due process protections, both organisations appealed the ban but this appeal was dismissed on 26 January 2022 by the Federal Administrative Court. Asset confiscation action targeting approximately EUR 300 000 of real estate is also being pursued.

Source: German Authorities

### *TF investigation integrated with and supportive of national strategies*

196. TF investigations are generally well-integrated with and supportive of Germany's national strategy on countering terrorism. The assessment team's findings are based TF and counterterrorism strategy documents and operational reports, interviews with prosecutors, LEAs, intelligence agencies, Customs and the FIU.
197. In the *Strategy to Counter Money Laundering and Terrorist Financing* (National AML/CFT Strategy), Germany has committed to intensify efforts to combat TF by enhancing the role of the GETZ and GTAZ models to other areas in Germany to promote enhanced domestic cooperation and intelligence sharing. There is also a commitment to increasing resources to enhance international cooperation to combat TF.
198. One positive feature of the German system is the confidential *Joint Situation Report on TF* which is regularly updated by a working group made up of the intelligence agencies (BfV and BND) and the BKA. This assessment is useful tool for authorities and takes into account recent TF activity detected.
199. However, the role of the FIU in TF investigations could be improved by a formal integration into the overall TF framework. While there is a strong focus in the National AML/CFT Strategy on enhancing domestic co-ordination and cooperation and also enhancing the use of financial intelligence through the FIU, the FIU itself is only involved in an ad hoc basis in the various task forces on TF (see IO.6).

### *Effectiveness, proportionality and dissuasiveness of sanctions*

200. Germany generally applies proportionate and dissuasive sanctions for TF for natural persons in line with sentencing standards for serious crimes in the jurisdiction. Again, limited statistics are available so the assessment team based its conclusions on the statistics that were available, case studies and interviews with prosecutors.
201. TF is considered a serious offence under German law and the various offences that cover TF activity carry a penalty of up to ten years imprisonment with the highest sentence actually imposed being seven years imprisonment at the federal level. Higher sentences may have been imposed in *Länder* proceedings but German authorities were not able to confirm this.

202. Rules on sentencing require the consideration of various factors that allow for proportionate sentencing including: including the culpability of the offender, the nature of the crime and assorted factors like the criminal history of the person, their rehabilitation prospects and their likelihood of reoffending. For sentencing, the following specific factors are considered: whether the suspect is a major actor in the TF system; complexity of the TF activity; the number of proactive measures by the suspect (e.g., number of transfers involved); value of assets; whether assets were actually used for terrorist purposes; the threat posed by the terrorist organisation being supported; whether the person testified or confessed; previous criminal convictions; time and length of proceedings, and admission of guilt at the time of sentencing.
203. The average sentence imposed based on statistics from 2015-17 was two years and eleven months. Sentences are suspended in 43% of cases while another 46% of cases receive a sentence of less than two years' imprisonment. However, a substantial number of cases (33%) receive a sentence of more than four years imprisonment. Longer sentences are imposed in cases where the suspect was involved in larger scale financing activity or was working more actively as a financier. The cases where lower sentences were imposed were cases involving lower amounts of funds or less sophisticated financing methods. Overall, the sentences imposed are proportionate to the seriousness of the conduct. For example, a more serious sentence of three to four years imprisonment was imposed in a case of a foreign terrorist fighter using a bank overdraft to fund travel to ISIL territory to engage directly in terrorist acts. In this case, the financing was unsophisticated and did not involve a large amount of funding but the direct connection between the funds and an intention to commit a terrorist act triggered a large sentence.
204. Comprehensive national level data and statistics on sentences in cases completed after 2017 were not available. The GBA was able to provide data on federal prosecutions from 2018 to 2020 and sentences imposed in these cases. In total, there were sentences imposed in nine cases. A sentence of one to three years was imposed in three cases; three to five years in four cases; and five to ten years in two cases. The highest sentence imposed for TF activity during this period was a sentence of seven years and imprisonment for supporting a foreign terrorist organisation, violations of targeted financial sanctions and terrorism related offences. Overall, sentences imposed in federal TF cases tend to be higher than the national average as the Federal Prosecutor General has primary responsibility for the prosecution of terrorist crimes and usually only refers cases of lesser importance to the public prosecution offices of the *Länder*. When compared with sentences imposed for terrorism offences, sentencing for TF is broadly comparable (although justifiably higher in some terrorism offences).

**Table 4.4. Sentences imposed for TF offences: 2015-17**

	2015-17
Suspended sentences	27 (43%)
0-1 year	5 (8%)
1-2 years	24 (38%)
2-3 years	13 (21%)
4-6 years	18 (29%)
More than 6 years	3 (5%)
Average	2 years and 11 months

Note: Suspended sentences refer to cases where a person has been convicted and has received a sentence that includes a term of imprisonment but under German law, there is an option for this sentence to be served under probation instead.

Source: German Authorities

**Table 4.5. Sentences imposed for terrorism offences**

	2016	2017	2018	2019	Total (by sentence of length)
0-1 year	1 (4%)	4 (10%)	3 (9%)	2 (5%)	10 (7%)
1-2 years	9 (32%)	14 (34%)	10 (29%)	13 (32%)	46 (32%)
2-3 years	7 (25%)	12 (29%)	12 (34%)	11 (27%)	42 (29%)
3-5 years	7 (25%)	8 (20%)	6 (17%)	11 (27%)	32 (22%)
5-10 years	4 (14%)	3 (7%)	4 (11%)	3 (8%)	14 (10%)
Total (by year)	28	41	35	40	144

Note: These are convictions may be duplicative of the table above as the same offences are used to prosecute TF and terrorism.

Source: German Authorities

205. It was not possible to assess the sanctions imposed on legal persons. While German law does not allow for criminal liability of legal persons, there are administrative penalties that can be applied where there is a legal person involved in ML/TF activity. The maximum administrative penalty that can be applied is EUR 10 million but authorities explained that this could be augmented and supplemented by proceeds of crime provisions that enable the penalty to be increased by an asset confiscation amount that reflects the gain the legal person attained from the criminal act. Germany did not submit any case studies, statistics or other information to demonstrate the effectiveness of this part of the system apart from association bans levied on legal persons associated with PKK which led to confiscation of assets but no fines (see Box 4.4).

*Alternative measures used where TF conviction is not possible (e.g. disruption)*

206. German authorities make good use of alternative measures when it is not practicable to secure a TF conviction. The most effective measures are association bans, asset recovery and temporary asset freezes (and are further covered in core issue 10.3). Further where it is not possible to achieve a TF conviction or in addition to a TF conviction, other offences are pursued particularly the offence of breaching TFS (see Box 4.5 and case studies earlier in this section). Additionally, authorities also noted that they could use powers to prevent travel either at the border through Customs or by cancelling a person's passport to prevent FTFs from travelling. The assessment team based its findings on: discussions with the public prosecutors and the Ministry of Justice (BMJ).
207. In time sensitive cases, authorities can use the FIU's power to take immediate measures and freeze accounts for 30 days where there is a suspicion of TF activity. In 2019, the FIU used this power in two TF related cases (see section in IO.10).
208. German authorities can ban associations under certain circumstances (if the association pursued aims or activities contravening criminal laws or is directed against the constitutional order or against the concept of international understanding). A ban is an effective tool to disrupt the activities of a terrorist group or an association that financially supports terrorist organisations if the prerequisites mentioned above are fulfilled. In these cases, there will ordinarily also be an order to seize the assets of the association. This is a significant tool that has the effect of dissolving an association under an administrative process (see section in IO.10). Association bans are regulated according to the requirements and provisions of the Association Act. A ban is an administrative procedure. Legal action may be taken against a ban as well as against individual confiscations. German authorities noted that this was a particularly effective tool they used to disrupt the fundraising activities of the PKK. As this is a well-established organisation, fundraising activity is well-concealed and spread between different people. It was noted that when one functionary was subject to investigation and prosecution, they would see new people emerging to take on the role so it is difficult to address the issue solely through investigations and prosecutions after the fact. Overall, association bans have proven to be an effective tool in disrupting the fundraising activity which are being applied proportionately to address TF risks. However, it is not always clear that persons associated with these associations are also pursued to prevent further fundraising activities.
209. Authorities have taken a variety of approaches to preventing fundraising activity by terrorist organisations. In interviews, agencies described how they would work together with regulatory authorities to block groups and individuals from hosting public events to raise funds. For example, they could revoke or not issue licenses to sell food or drink at an event, taking into account the applicable administrative laws, in order to disrupt the fundraising activity. Based on case examples during the on-site, this is an effective tool to prevent and disrupt fundraising activity.

**Box 4.5. Case examples: use of alternative measures****Case example: Prosecution using alternative charges (BY-TF-3)**

Following a tip-off from international counterparts, a cash courier was identified crossing the border into Germany and travelling to Munich with suspicions that the cash movements were related to TF. While TF activity could not be established, the investigation uncovered a *hawala* network and the suspect was charged with providing authorised payment services in 131 cases in conjunction with serious fraud.

**Case example: Prosecution of family members for general support of a terrorist and use of *hawala* networks using TFS offence (GBA-TF-28/HH-TF-2)**

In 2017, the Public Prosecutor General's Office in Hamburg investigated and prosecuted four relatives of a member of ISIL for sending funds to her while she was residing in Syria. The case was triggered by telecommunications intercepts and internet chat surveillance which revealed the intention to send funds through *hawala* transfers. In total, approximately EUR 27 000 was sent in 2017 from Hamburg to ISIL controlled territory using *hawala* networks. There was extensive evidence that the recipient of the funds was an enthusiastic member of ISIL and had communicated this to the relatives via instant messenger. The funds were allegedly to be used to fund her day-to-day living expenses and provide general support to ISIL.

The four relatives were prosecuted for supporting a foreign terrorist organisation and violating targeted financial sanctions under s.18 of the AWG. Sentences handed down ranged from nine months to one year and 6 months.

Source: German Authorities

## Overall conclusions on IO.9

Germany authorities proactively pursue TF investigations as part of broader counter terrorism efforts. Prosecutions, investigations and convictions are broadly pursued in line with TF-risk. Germany prosecutes and has achieved convictions for TF under various offences. Co-ordination between agencies is good and supported by both formal frameworks and informal relationships. Authorities also make good use of alternative criminal justice measures such as the TFS offence and other alternative measures to disrupt TF activity, including with the ban on associations and asset freezes. These measures are applied proportionately and are effective tools to disrupt the activity of companies and associations when they cannot be prosecuted for TF. However, statistics on TF cases are not captured in a systematic and comprehensive manner so as to establish a full picture of Germany's effectiveness. Statistics provided were mainly from 2015-2017 and are outdated.

TF activity is identified and investigated using a wide variety of information sources and investigative agencies have very broad powers to access different information. However, some areas of co-ordination with the FIU in TF matters could be improved to make better use of FIU data and increase the prominence of financial intelligence in interagency efforts.

Sanctions for natural persons appear to be proportionate and dissuasive considering Germany's context. While there have been some administrative actions targeted at entities involved in TF for the PKK, further evidence was not available on the pursuit of legal persons involved in TF.

**Germany is rated as having a substantial level of effectiveness for IO.9.**

### Immediate Outcome 10 (TF preventive measures and financial sanctions)

#### *Implementation of targeted financial sanctions for TF without delay*

210. Germany relies primarily on the EU framework for implementing targeted financial sanctions (TFS) under UNSCRs 1267/1989/2253 and the 1988 regime (collectively referred to as UNSCR 1267) and UNSCR 1373 (see R.6). A domestic framework is in place to mitigate designation delays at the EU-level. While Germany has proposed designations under UNSCR 1267, it does not pursue designations under UNSCR 1373 in line with its risks and context. Germany does not have a separate domestic financial sanctions list; while there are other measures that allow national freezing of terrorist assets, these are limited in scope.
211. The assessment team's conclusions are based on: a review of the German and EU legal framework; statistics on designations and assets frozen; case studies showing asset freezing and actions for non-compliance; interviews with relevant government agencies; and discussions with FIs and DNFBPs.

*Designation*

212. Germany has a process in place for proposing designations of individuals or entities under UNSCR 1267 or 1373, although this process is not documented (see R.6). This leads to some lack of clarity over responsibilities and accountability throughout the process and reflects the lack of proactive use of the TFS regime. The same process is followed for designations under UNSCRs 1267 and 1373. While targets for designation can be identified by a range of agencies, the case studies provided show that targets are generally initially identified by the Federal Foreign Office (AA) (see box below). Law enforcement authorities are best-placed to identify targets, but prefer to use other tools to address TF risks. Discussions with LEAs indicated that they were not aware of or did not see additional value in TFS designations. Following identification, an inter-ministerial committee (*Ressortkreis*) reviews available evidence (including information from law enforcement, open source evidence, etc.) to assess the target against the UN or EU criteria. Agencies co-operate well in this process, with good input from law enforcement when requested. If the criteria is met, the AA will confirm the *Ressortkreis* decision and propose the designation to the relevant UN or EU committee. This process generally takes several months but can be lengthier as demonstrated by the case study below (see box below).
213. While Germany has demonstrated its ability to make designations, the number of proposals under UNSCR 1373 (one) is very low, particularly in light of Germany's risks and context. In total, Germany has proposed 22 listings and co-sponsored an additional 25 listings to the UN under UNSCR 1267. Since 2018, Germany has not proposed any listings and has co-sponsored 10 listings. Germany has proposed only one listing in total to the EU under its UNSCR 1373 regime. Since 2018, Germany has proposed no listings and co-sponsored three designations under this regime; in one of these cases, the target was arrested and remanded in custody in Germany, but the designation was initiated by another EU member. In general, Germany does not use UNSCR 1373 listings as a tool for mitigating its TF risks.

**Table 4.6. Designations proposed/co-sponsored by Germany (2018-2020)**

		2018	2019	2020
UNSCR 1267	<i>Proposals</i>	0	0	0
	<i>Co-sponsors</i>	0	2 individuals	3 individuals 5 entities
UNSCR 1373	<i>Proposals</i>	0	0	0
	<i>Co-sponsors</i>	2 individuals	1 individual	0

Source: German Authorities

214. Germany's process for de-listing is similar to the listing process, with the AA submitting de-listing requests to the UN or EU. The EU also regularly reviews listings, at least every six months. Since 2016, Germany has supported de-listing requests for six persons or entities under UNSCR 1267. These were either directly addressed to the ombudsperson by the listed individuals or proposed by third countries. Germany has not submitted any additional de-listing proposals under UNSCR 1267 since 2016. Germany has co-sponsored the de-listing of 3 entities and 1 individual since 2016 under the EU's UNSCR 1373 regime.

215. While Germany has a process for national designations, this is not used for unilateral/autonomous designations and is used only as a stopgap measure to reduce designation delays at the EU level. The underutilisation of TFS is mitigated only to some extent by Germany's access to other measures, including association bans and freezes of specific accounts, as these measures are subject to limitations
216. BaFin is able to issue freezing orders to freeze accounts where there is a link to TF. In theory, these orders could be used to freeze assets at the national level where an individual or entity has not been listed by the EU but Germany considers that the criteria are met, or where EU regulations do not require freezing (e.g., for listed EU nationals and residents; indeed, this was the purpose behind the initial creation of this freezing power). However, BaFin orders are not used like this in practice; for example, BaFin does not have a system to regularly screen its Electronic Account Retrieval System (a central bank account database) to detect any new accounts related to listed EU internals. In addition, BaFin orders are limited in application as they apply only to accounts held by credit institutions. Requests for designation to Germany from third countries would be considered under the EU mechanisms; Germany does not have a national list or other domestic process to give effect to foreign requests for designation where such requests are not implemented at the EU level.

#### Box 4.6. Examples of designation proposals/cosponsors by Germany

##### Designation proposal under UNSCR 1267

At the start of 2013, the UN Monitoring Teams notified the AA of a potential target in Germany. The AA referred the matter to the *Ressortkreis* in March 2013. The target had been under surveillance by the German security authorities and was in the Syrian-Turkish border region. Due to an ongoing undercover investigation, the *Ressortkreis* refrained from pursuing a designation. On 14 May 2014, Germany issued a European arrest warrant against the target.

The *Ressortkreis* therefore reconsidered designation and reached consensus to propose designation. The BKA prepared a draft of the submission form and provided the necessary information on the target. The submission form was submitted to the *Ressortkreis* for consideration at the end of July 2014. The *Ressortkreis* concluded its assessment of the proposal in September 2014 and decided to reach out to like-minded states (via the AA) for support on the proposal. Following consultation with other states, the AA submitted the proposal to the UN on 12 January 2015 and the target was listed on 10 February 2015.

##### Co-sponsored designation under EU UNSCR 1373 regime

In July 2018, Germany arrested an Iranian national wanted for his involvement in a thwarted terrorist attack in France. The individual was subject to a European Arrest Warrant issued by Belgium, as well as a domestic arrest warrant that had been issued by Germany. [Following his arrest], France contacted Germany asking Germany to co-sponsor the designation. The AA examined the proposal and referred the matter to the *Ressortkreis*, which approved the proposal in October/November 2018. The designation was formally proposed to the EU in November 2018, approved thereafter, and entered into force in January 2019.

Source: German Authorities

*Implementation*

217. Germany has established a system to bridge the delay between UN and EU designations under UNSCR 1267. Where the UN makes a new designation, Germany issues a national freezing order under the Foreign Trade and Payments Act (AWG) which applies to all natural and legal persons (including FIs and DNFBPs). The AWG order comes into force upon publication in the Federal Gazette. Since developing this procedure in January 2020, Germany has implemented all UNSCR 1267 designations within 24 hours of the UN communication (see table below). Technical limitations (see R.6) have not impacted effectiveness since the AWG framework came into effect.<sup>45</sup> The AWG order is temporary and remains in place until the EU listing which has direct effect in Germany; if no EU listing is made, the order expires after one month. This process has been used a total of seven times between January 2020 and November 2021 to implement UNSCR 1267 designations. TFS under UNSCR 1373 are implemented through the EU system; once a designation is made at the EU level, the freezing obligation automatically applies in Germany.

**Table 4.7. German implementation of UN 1267 designations (2020-2021)**

Date listed by UN	Date of UN communication	Date AWG entered into force via Federal Gazette	Hours between UN communication and German implementation
4 February 2020	Wednesday 5 February 2020, 07h30	5 February 2020, 15h00	7.5 hours
23 February 2020	Tuesday 24 February 2020, 18h54	25 February 2020, 15h00	20 hours
4 March 2020	Thursday 5 March 2020, 07h30	5 March 2020, 15h00	7.5 hours
21 May 2020	Friday 22 May 2020, 07h30	22 May 2020, 15h00	7.5 hours
16 July 2020	Thursday 16 July 2020, 23h44	17 July 2020, 15h00	15 hours
8 October 2020	Thursday 8 October 2020, 22h58	9 October 2020, 15h00	16 hours
17 June 2021	Thursday 17 June 2021, 23h58	18 June 2021, 15h00	15 hours
23 Nov. 2021	Wednesday 24 Nov. 2021, 21h29	25. Nov. 2021, 15h00	17.5 hours
End of on-site			

Note: All times are shown in Central European Time.

Source: German Authorities

<sup>45</sup> See R.6: As the gazette is not published on weekends or holidays, there will be a delay in implementation of UN designations issued immediately prior to weekends or holidays (and a delay has been seen in the implementation of another sanctions regime).

218. Germany has a system in place to immediately and proactively communicate new listings to certain FIs. The Deutsche Bundesbank (Germany's central bank) issues a circular to approximately 1 800 FIs (including all banks and VASPs) within 24 hours of a new listing or de-listing by the UN, EU or under the AWG. The Bundesbank has a computer-monitoring system that ensures all credit institutions respond with either a positive or negative report to track frozen funds. The EU also provides a TFS newsletter service to which entities or individuals can subscribe. There are also mechanisms to publicise listings. The Ministry of Justice of North-Rhine Westphalia maintains an online financial sanctions database, *FiSaLis*, which provides an easily searchable, consolidated sanctions list.<sup>46</sup> Relevant agencies (including the Bundesbank and Customs) also provide up-to-date information on TFS on their websites, including links to *FiSaLis* and EU sanctions lists. While these measures are positive, they rely on non-banks, DNFBPs and the general public (including institutions in higher risk sectors such as certain MVTs, agents and DPMS) regularly checking relevant sites. Given the issues in applying TFS measures, particularly within smaller non-bank FIs and DNFBPs (see IO.4, Chapter 5.2.4), more proactive communication mechanisms are required to make sure all institutions, particularly higher risk institutions, are aware of new listings and de-listings to ensure effective TFS implementation. While many DNFBPs undertake screening, shortcomings in controls create a gap in TFS implementation.
219. Sanctions breaches may be detected during TFS monitoring or supervision. A lack of supervision in many DNFBP sectors (see IO.3) means breaches are less likely to be detected in these sectors (some of which, like DPMS, are higher risk for sanctions evasion). In addition to TFS monitoring, sanctions breaches may be detected by the FIU, whose database systematically screens incoming STRs against the UN sanctions lists. If FIU analysis identified a possible TFS breach, this analysis would be disseminated to the relevant law enforcement agency. The FIU does not maintain statistics on how often this occurs, but was able to provide case studies where analysis relating to potential sanctions breaches was disseminated to customs. The *Länder* land registers also screen new registrations against sanctions lists. There is no regular screening of other government sources (e.g., the Commercial Register, the Transparency Register, or BaFin's Account Retrieval System/bank account database) to proactively identify if newly-listed persons or entities hold assets in Germany; authorities note that this is, in part, for data protection reasons.
220. Germany has frozen funds pursuant to TFS. As at 30 June 2020, Germany had a total of EUR 7 150.55 frozen under UNSCRs 1267 and 1373 (see Table 4.8). The majority of these funds are held by three prisons where designated persons are detained. The remainder is divided among 20 accounts at various banks. Gaps in screening in practice and issues in the supervision of DNFBPs create vulnerabilities in these sectors' compliance with freezing obligations (see IO.3 and IO.4). The Bundesbank is responsible for authorising access to frozen funds. From 2016 to 2019, Germany issued 23 approval notices permitting access to frozen funds in response to 31 requests. For authorisations related to UNSCR 1267, approval is sought from the UN Committee in accordance with UN procedures.<sup>47</sup> The Bundesbank requires proof that released funds are used for the specified purpose (e.g., receipts).

<sup>46</sup> Available at: [www.finanz-sanktionsliste.de/fisalis/](http://www.finanz-sanktionsliste.de/fisalis/)

<sup>47</sup> For funds released for basic expenses, the Bundesbank notifies the UN Committee and of its intention to grant access to frozen funds and will grant approval if no negative decision is received from the Committee after 48 hours.

*Targeted approach, outreach and oversight of at-risk non-profit organisations*

221. Germany has a good understanding of the TF risks in its NPO sector and has identified the NPO sub-sectors at highest risk. The general framework for regulating and monitoring NPOs largely mitigates the TF risk, without significantly disrupting legitimate activities. De-risking of NPOs by the financial sector is an issue, and Germany has started work to address this. The assessors' conclusions were based on: discussions with government authorities, NPOs and NPO associations; the 2020 NPO risk assessment; and NPO guidance and outreach material.
222. Germany has a good understanding of the risks of TF abuse of its NPOs, drawing largely on its 2020NPO risk assessment. The risk assessment drew on a wide range of qualitative and quantitative information.<sup>48</sup> The assessment distinguished the risks of abuse of legitimate NPOs (medium-low) and sham NPOs (medium-high). The funds involved can be significant where used for establishing and maintaining terrorist organisations (logistics, propaganda, living expenses). This is the case for the few cases where German NPOs have been linked to TF. In practice, authorities have a good understanding of the likely typologies, as well as how typologies intersect with risks (e.g., the differences in how religiously-motivated terrorist organisations misuse NPOs compared to right-wing terrorist groups). Agencies demonstrated a good understanding of evolving and emerging risks, although NPOs noted that this could be strengthened by ongoing communication beyond the scope of the formal risk assessment process.
223. Law enforcement authorities, including at the *Land* level, make efforts to engage with at-risk NPO communities and directly with particular NPOs (see box below). Nation-wide outreach to the NPO sector is often conducted via government support for efforts by NPO umbrella organisations (see R.8). This approach has been positive in ensuring NPO involvement and ownership, although risks not reaching NPOs outside such networks. NPOs considered that increased support for industry efforts and an ongoing exchange with the government would be a positive development to ensure government awareness of ongoing risks and challenges. NPOs generally have a good understanding of their risks and implement mitigation measures. This is particularly the case for organisations working in high risk jurisdictions or receiving government funding. Smaller organisations tend to have a lower awareness and may need additional support in light of the identified risks.

---

<sup>48</sup> Including: statistics on the NPO population; STRs; data and case studies on criminal and administrative proceedings involving TF through NPOs; information from law enforcement and intelligence services; FIU analysis; self-assessments by NPOs; practical experience from NPOs; hypothetical risk scenarios; FATF risk assessments; and other countries' experience.

224. Mitigation measures and monitoring for NPOs are generally sufficient to prevent and detect abuse, proportionate to the risk in the NPO sector. Authorities have also demonstrated active intervention where specific risks are identified (see box below). NPOs are subject to general registration requirements, although requirements for NPOs formed as associations (which pose a higher risk) are less stringent. NPOs distributing government aid are subject to rigorous checks, including the involvement of on-site liaison officers. All NPOs are subject to annual tax monitoring to confirm their non-profit status. This has proven effective in identifying approximately ten NPOs per year that are suspected of operating as extremist or terrorist organisations or engaging in TF. In such cases, non-profit status is withdrawn (with consequential retroactive tax liabilities) and tax authorities report the case to the relevant *Land* Office for the Protection of the Constitution, which will impose sanctions (see below). Civil society itself also engages in its own monitoring, which is a positive element of Germany's system. The German Central Institute for Social Issues, *Deutsches Zentralinstitut für soziale Fragen* (DZI), a civil society institution, publishes reports and warnings on organisations it has identified as engaging in risky behaviour. In several cases, these have led to investigations or sanctions in connection with TF. A public register of NPOs in Germany is planned for 2024, and both government authorities and NPOs noted that this would add an additional safeguard, particularly to ensure responsible donations.

**Box 4.7. Proactive measures to respond to identified risks of misuse of NPOs**

**Example 1:** Western areas of Germany suffered devastating flooding in mid-2021. As part of regular monitoring, the Federal Office for the Protection of the Constitution (BfV) identified right-wing extremists taking advantage of the disaster to collect funds, raising concerns about potential TF. The fundraising was generally through individual actors, but small groups were also involved, including to collect donations on-the-ground. In response, BfV liaised with *Land* authorities in order to analyse the presence and work of extremists in the disaster region and assess potential TF risk.

**Example 2:** An LKA in one *Land* noted the risk of terrorist infiltration of a certain community of NPOs in the region. In response, the LKA developed an action plan for early detection and established police officers as contact officers within the NPO community. These officers build trust within the NPO community through intensive contact with communities, clubs and associations. The officers regularly share information with the competent police investigative teams. The LKA oversees and co-ordinates this work, ensure experience-sharing, and provides officers with intelligence and situation reports.

Source: German Authorities

225. A range of sanctions are available for NPOs that violate their obligations (see R.8). These range from publication through to a complete ban on operation. In most cases, issues related to transparency and good governance are addressed by withdrawing of an organisations non-profit status (with corresponding orders to repay tax benefits) or, for NPOs receiving government funding, the termination of any contract and an order to repay any funds awarded. In more serious cases, certain *Land* and federal authorities can impose measures on “extremist” organisations to prevent extremism evolving into terrorism. The definition of ‘extremist organisations’ is not limited to violent extremism and applies to organisations that violate criminal law, systematically undermine the constitutional order, or use financial or material means to create or support conflicts in other countries. This is a broad definition, but authorities explained that there are additional safeguards and procedures (set out in the following paragraph) to protect from potential misuse.<sup>49</sup> Authorities stressed, and demonstrated in case studies, that this is a high bar that does not capture all radical or extreme organisations. NPOs interviewed in the course of the evaluation did not express concerns on the scope of these powers.

<sup>49</sup> For general information, see UNHRC (2020) “Human rights impact of policies and practices aimed at preventing and countering violent extremism”.

226. Severe measures can be imposed on extremist organisations, including publicly identifying the organisation (resulting in the withdrawal of non-profit status), limiting gatherings or activities, disrupting income streams, and banning NPOs (and successor organisations) entirely. A range of checks and balances exist to prevent these measures being misused and disrupting legitimate NPO activities, including judicial review and active monitoring by a Parliamentary Oversight Panel and a parliamentary-appointed Commission. Importantly, feedback from NPOs during the course of the evaluation and reports from civil society and human rights organisations do not point to concerns in Germany's use of these powers. These measures can have a strong disruptive impact and NPOs unanimously highlighted the dissuasive nature of these measures. Due to the seriousness of certain measures, they are implemented prudently, following an investigation and (for an association ban) also an administrative proceeding. Bans are nonetheless used relatively regularly (just under 100 over the course of ten years). While bans are focused on extremist organisations (not only terrorist organisations), in practice many of the bans imposed relate to organisations with links to terrorist groups.

#### Box 4.8. Detection and sanctioning of NPO used for TF

In 2015, the BfV and relevant LfV had intelligence that a NPO in Baden-Württemberg had propagated terrorism, recruited ISIL fighters for the conflict in Syria, and raised funds for terrorism by holding benefit events for supposed humanitarian aid. This information was shared with the relevant *Land* banning authority and in December 2015 the NPO was banned and its assets and premises were confiscated. A criminal prosecution was pursued for terrorist financing and formation of a terrorist organisation, but was ultimately discontinued due to the death of some suspects and a lack of sufficient evidence relating to others.

Source: German Authorities

227. NPOs largely rely on regulated financial channels for money transfers. However, NPOs have suffered from de-risking in the banking sector, despite the relatively low risk of misuse. NPOs confirmed that this is increasingly leading NPOs to turn to lesser or non-regulated channels (such as *hawala*) to transfer funds abroad, thereby creating new vulnerabilities. Germany was made aware of this issue in the course of the NPO risk assessment, and has commenced work to develop a formal tripartite dialogue between NPOs, the government, and the financial sector. Work so far has included sending questionnaires to NPO and FI associations and conducting bilateral discussions to fill information gaps, identify and analyse practical issues, and develop a clear path forward.

### *Deprivation of TF assets and instrumentalities*

228. Germany has access to a range of measures to deprive terrorists, terrorist organisations, and terrorist financiers of their assets. These include administrative freezes by BaFin and the FIU; association bans and resulting asset recovery; criminal confiscation; and terrorist designations. Authorities demonstrated that they can use association bans and criminal confiscation tools effectively and proportionately. However, these measures are subject to limitations for the purposes of IO.10. Germany could be more proactive in using BaFin freezes and TFS and could better exploit the FIU's freezing power in line with its TF risk profile. Agencies co-ordinate, including through GETZ and GTAZ, to determine whether to implement measures in any given case, based on the specific scenario. Authorities demonstrated a high degree of co-operation and co-ordination, although earlier collaboration could improve the use of FIU freezes. These findings are based on: discussions with BaFin, the BMI, the BfV and LfV; case studies and statistics on freezes and confiscation; and relevant legislation.
229. BaFin is able to order a freeze of specific accounts, securities deposits, and safe deposit boxes where there is a link to TF. This power is used rarely; two account relationships were frozen between 2017 and 2020. BaFin acts at the request of a law enforcement body like the BKA and based on information from law enforcement. In addition to its other uses (see IO.6), BaFin's Account Retrieval System (central bank account database) allows it to identify bank accounts, securities deposits or safe deposit boxes in the name of specific persons or groups, which facilitates its freezing power. In practice, BaFin's freezing power has been used in a small number of instances to respond to state-sponsored terrorism threats or threats from specific individuals (see box below). Unlike general TFS designations, a BaFin freezing order is limited in scope as it applies only to accounts/funds held by FIs. To date, BaFin freezing orders have not been accompanied by a proposal for designation (either to the UN or the EU), meaning other assets of the account holders were not subject to freezing. Germany does not routinely use this power to freeze accounts where an individual or entity has not been listed by the EU but Germany considers that the criteria are met. Nor does BaFin regularly screen its Bank Account Retrieval System to detect any new accounts or deposits related to EU nationals and residents where EU TFS regulations do not require freezing. As a result, this power is not being used to its full potential to support Germany's broader CFT strategy or ensure robust implementation of TFS.

#### Box 4.9. Use of BaFin’s account freezing powers to deal with urgent TF threats

In 2019, BKA intelligence regarding an extremist group in Frankfurt indicated the group was planning an attack. The BKA conducted a raid and seized a range of instruments that provided further evidence of a planned attack. The BKA asked BaFin to identify accounts related to the individual involved and to issue a freezing order (Banking Act, *Gesetz über das Kreditwesen (KWG)*, s.6a) to prevent other terrorist uses of the funds. BaFin identified one account with a small amount of money and issued a freezing order, resulting in the account being frozen within two days. After completion of the investigation it was concluded that the funds were not intended for terrorist purposes, at which point BaFin lifted the freeze at the request of the Frankfurt Public Prosecutor’s Office.

Source: German Authorities (BaFin)

230. As noted in the section above, federal and *Land* authorities have a range of measures available to disrupt the funding streams of extremist and terrorist associations, from restrictions of activities through to complete association bans. These measures are used (and should continue to be used) cautiously and in line with due process to avoid disrupting legitimate activities. A banned association is dissolved and typically, its assets are seized and donated for charitable purposes. In the past ten years, there have been less than 100 association bans, half of which have targeted organisations with links to the PKK. From 2017 to 2020, approximately EUR 1.2 million has been seized at the federal level, including real estate and other valuables, following 7 extremist association bans.
231. Association bans entitle authorities to dissolve the organisation and any successor associations. Authorities noted that in this respect, they preferred these measures to TFS designations. However, bans are limited as they cannot apply to individuals and they are an internal, domestic measure, whereas a designation helps foreign counterparts track and identify international networks and reduces global TF flows. Authorities have also used other administrative measures to prevent TF (see Box 4.10 below).

#### Box 4.10. Creative measures to disrupt TF

Since 2013, the LfV in Lower Saxony has been monitoring “cake-day events” in Hanover. At these events, a special permit allows various aid organisations to create pedestrian zones on roads to fundraise by selling cakes. The LfV identified that some of the organisations involved in these events had links to terrorist organisations. These risks contributed to a law change in June 2018 allowing the use of public roads to be restricted where the “special use serves to pursue or support activities which are directed against ... the existence or security of the Federation or of a *Land* or which endanger the foreign interests of the Federal Republic of Germany.” In 2019, at least two special use permits were denied on the grounds that donations collected at the event were linked to TF.

Source: German Authorities

232. The FIU has an immediate freezing power that allows it to freeze transactions for up to one month where it has reason to believe that the transaction is connected to ML or TF. The FIU uses this power where additional time is required to analyse a suspicious transaction prior to dissemination to law enforcement, at which point the transaction is released. FIU freezes are therefore not a deprivation measure in and of themselves. From 2017 to 2020, the FIU requested 19 freezes relating to TF. The amounts frozen are significant. Often orders relate to single transactions of over EUR 100 000 and in one case, a single transaction of EUR 500 million (see table below). In about half these cases, the FIU's analysis did not identify a concrete suspicion and the funds were accordingly released. In the remaining cases (9 of 19), the FIU identified grounds for suspecting a criminal offence and disseminated its analysis to law enforcement. The freeze is generally lifted upon dissemination or shortly thereafter, which creates a risk that funds are dissipated before a criminal asset freeze can be pursued. Asset recovery has not yet resulted from any of these cases.
233. As noted under IO.8, Germany has an effective system for criminal confiscation, particularly following the introduction of expanded (non-conviction based) confiscation in 2017. Federal TF confiscation statistics are not maintained, but data is available from certain *Länder*.<sup>50</sup> Available statistics show that the amounts confiscated in individual cases are often relatively low. This is largely in line with Germany's risk profile, particularly funding for lone wolf attacks and foreign terrorist fighters, but is not consistent with the identified risk of larger scale funding support for certain terrorist groups (such as the PKK). Total amounts confiscated are relatively low; depending on the *Land*, amounts varied from EUR 20 000 to EUR 100 000 annually. Case studies demonstrated Germany's ability to confiscate cash and instrumentalities related to TF, such as vehicles and electronic devices.

**Table 4.8. Amounts frozen annually under TF freezing and deprivation mechanisms**

	2017	2018	2019	2020
UNSCR 1267 freezes*	7 251.37	14 998.35	7 328.59	6 970.44
UNSCR 1373 freezes*	0	40.44	45.08	45.93
Federal association bans	2 bans Approx. 40 000 recovered	10 bans Approx. 6 000	2 bans Approx. 6 000	2 bans Approx. 1 100.000 recovered(plus real estate properties)
BaFin freezes*	1 freeze 230 million frozen	0 freezes	1 freeze 150 million frozen	0 freezes [
FIU temporary freezes	12 orders 1.1 million frozen	4 orders 500 million frozen	2 orders 21 300 frozen	1 order 39 000 frozen

Note: \*BaFin and UNSCR freezes apply over multiple years, so these figures capture the total amount frozen in a given year, rather than the amount of *new* funds frozen (as is the case for the other mechanisms displayed in the table).

National criminal confiscation figures are not available.

Source: German Authorities

<sup>50</sup> There are differences in record-keeping between *Länder*, e.g., some figures capture TF-specific confiscations, while other can only isolate confiscation related to national security violations.

*Consistency of measures with overall TF risk profile*

234. The measures undertaken by Germany are consistent with its overall TF risk profile to some extent. However, Germany does not designate terrorist persons and groups in line with its risk and context. Its engagement with UNSCR 1373 designations is particularly low given its exposure to certain TF networks, the materiality of its financial sector, and its leadership role in the EU. While authorities have access to other freezing measures, these are not always used actively and are limited in scope compared to TFS; for example, association bans apply only to organisations, not individuals, while account freezes apply only to accounts, securities deposits, and safe deposit boxes held by FIs, not all assets.
235. Measures taken to prevent and detect the abuse of NPOs are in line with risks in the sector. Authorities have demonstrated that they target their outreach activities in line with identified risks.
236. Germany's use of deprivation mechanisms is aligned with risk to some extent. Association bans have largely focused on Germany's highest risk areas for TF. For example, Germany has banned 52 associations with links to the PKK (approximately half of issued association bans). This focus is in line with Germany's risk profile, noting that roughly half of the funds raised for the PKK in Europe are raised in Germany. However, in light of these estimates, the overall amounts deprived are relatively low and not fully consistent with Germany's TF risks. BaFin freezing orders could be used more effectively in line with risks, including to target individuals (where association bans cannot apply) and to freeze funds in cases where EU designations have not been made or do not require freezing.

**Overall conclusions on IO.10**

While Germany has a system for implementing UNSCRs 1267 and 1373, major improvements are needed. In particular, the number of designations proposed to the EU under its UNSCR 1373 regime (one) is very low given Germany's risks and context. Law enforcement authorities are not aware of or do not see the additional value in TFS designations as a CFT tool, and instead prefer alternative national mechanisms which are subject to limitations for the purposes of IO.10. More proactive communication mechanisms are required to immediately notify non-bank FIs, DNFBPs and the general public (particularly institutions in higher risk sectors) of new listings or de-listings.

Germany's framework for preventing and detecting abuse of NPOs for TF is strong and proportionate to the risks in this sector. National mechanisms exist for the deprivation of TF assets, although, these have scope limitations and are not always used proactively or effectively in line with Germany's risks and context. Germany has had success in depriving terrorists of assets via association bans, however, BaFin freezes and TFS are under-utilised and the potential of FIU freezes is not fully exploited. Overall, the amounts frozen are relatively low given Germany's risks and context and compared to its estimates of the total amounts raised within Germany for various terrorist organisations.

**Germany is rated as having a moderate level of effectiveness for IO.10.**

**Immediate Outcome 11 (PF financial sanctions)**

237. In terms of context, Germany has financial ties with Iran through several Iranian banks branches in Germany. Germany prioritises broader counter-proliferation efforts, particularly through diplomatic action, and was a key driver of the Joint Comprehensive Plan of Action (JCPOA). Following JCPOA implementation in 2016, trade and financial transactions between the two countries increased, but dropped again considerably following the withdrawal of the US from the JCPOA in 2018 and the subsequent re-introduction of US extraterritorial sanctions. Germany's relationship with DPRK is less significant, although Germany is a destination of choice for procurement of technology by both Iran and North Korea. In terms of the potential for breaches of proliferation-related TFS, particularly relevant sectors include banks, MVTS, insurance, and DPMS.
238. Germany's framework for proliferation-related TFS pursuant to UNSCR 1718 (and its successor resolutions on DPRK) and UNSCR 2231 (on Iran) is largely the same as for implementing terrorism-related TFS (see IO.10), subject to some important differences in supervisory responsibilities. To the extent possible, the text cross-references to IO.10 rather than repeat information.
239. The assessors' conclusions on this IO are based on: a review of the German and EU legal framework; statistics on designations and assets frozen; case studies showing asset freezing and actions for non-compliance; interviews with relevant government agencies; and discussions with FIs and DNFBPs.

***Implementation of targeted financial sanctions related to proliferation financing without delay***

240. As with terrorism-related TFS, Germany relies primarily on EU Regulations that have direct effect in Germany to implement UNSCRs 1718 and 2231. National freezing orders under the AWG are used to mitigate delays in the EU implementation of UN designations. The process for proliferation-related TFS is undocumented, but appears to operate in the same way as for terrorism-related TFS. Following a *Ressortkreis* decision, the AA is responsible for confirming the decision and proposing the designation to the EU or the UN.
241. Germany proactively makes proposals to the EU for proliferation-related TFS. Between 2015 and 2020, Germany proposed 24 designations under the DPRK regime and 139 under the Iran regime for addition to the EU's autonomous lists. Germany has made fewer designation proposals to the UN largely due to a range of political factors, including a focus on EU sanctions and the process leading to the adoption of the JCPOA. The UN listed one of the DPRK-related targets Germany had proposed to the EU, although this was not on the basis of a proposal from Germany.

242. Once a designation occurs at the EU-level, the freezing obligations under the EU Regulations become directly applicable in Germany (see R.7). In some cases, there may be a delay between a UN listing and a corresponding EU listing. As with terrorism-related TFS, in such cases, Germany would issue a national freezing/prohibition order under the AWG immediately after the UN listing. This would stay in force until the EU listing, thereby bridging the gap in implementation. In practice, there have been no new UN listings under the UNSCR 1718 or UNSCR 2231 regimes since the entry into force of this interim AWG regime. As the process is the same as for terrorism-related TFS, the assessment team concluded that this process would generally be effective (see Chpt.4.3.1) despite technical shortcomings (see R.7).
243. Germany communicates proliferation-related designations in the same manner as for terrorism-related TFS). The Bundesbank proactively informs 1 800 FIs (including all banks and VASPs) of new listings and de-listings via a circular and information is publicised on other government and EU websites. The EU also provides a TFS newsletter service. More proactive, targeted communication is required to make sure all institutions are aware of new listings and de-listings, particularly smaller, higher-risk FIs (such as MVTS and insurance entities) and DNFBPs (such as cash-intensive sectors like the gold sector) that may not use sanctions screening software.

**Box 4.11. Communication and outreach in advance of JCPOA implementation day**

The JCPOA resulted in multiple delistings under the EU's UNSCR 2231 (Iran) list. Germany took steps to raise awareness of these delistings:

- The Federal Ministry for Economic Affairs and Climate Action (BMWK), in co-operation with the AA and the Federal Ministry of Finance (BMF), held four events in 2015 and two events in 2016 to provide for information on major changes and the lifting of sanctions in connection with the JCPOA. Events were focused on the financial sector; four out of these six meetings were specifically dedicated to German banks and banking associations, with the participation of major Iranian banks in two of these meetings. Other meetings included associations and representatives of the business community.
- The Bundesbank engaged directly with Iranian FIs in Germany, which had to fulfil legal and technical requirements for reconnection to the EU electronic payment systems.
- The Bundesbank issued a proactive circular in late 2015 informing credit institutions of the EU's decision to delist multiple entities, but noting that the delisting would not come into effect until implementation day. A subsequent circular was sent on 18 January 2016 (two days after implementation day) advising institutions that the delistings had entered into force and informing entities of their obligation to lift freezes.
- On 26 January 2016, the Bundesbank contacted FIs in Germany that had previously reported funds frozen pursuant to UNSCR 2231. The FIs were required to report any funds still frozen.
- Information on the JCPOA and delisting was made available on the websites of Customs and the Federal Office for Economic Affairs and Export Control.

Source: German Authorities

***Identification of assets and funds held by designated persons/entities and prohibitions***

244. Under EU Regulations, all persons and entities are required to report any frozen funds to the Bundesbank. As of November 2020, Germany has EUR 1.3 million frozen as a result of sanctions against Iran. This amount has decreased from a high of EUR 2.2 billion (in 2011) because of de-listings and subsequent releases of funds, including under the JCPOA. For TFS relating to DPRK, Germany has EUR 410 872 frozen. The amount is much lower than that for Iran-related sanctions due to Germany's weaker economic ties with DPRK.

**Table 4.9. Assets frozen in Germany related to UNSCRs 1718 (DPRK) and 2231 (Iran)**

	2016	2017	2018	2019	2020
UNSCR 2231 (Iran)	1 356 015	1 302 758	1 314 812	1 320 389	1*288*251
UNSCR 1718 (DPRK)	410 509	410 497	411 307	410 872	410*654

Source: German Authorities

245. Government authorities also take some other steps to identify assets. This includes the *Länder* land registers screening new entries against sanctions lists. There is no regular screening of other government sources (e.g., the Commercial Register, the Transparency Register, or BaFin's account retrieval system) to proactively identify if newly listed persons or entities hold assets in Germany; authorities note that this is, in part, for data protection reasons.

#### *FIs and DNFBPs' understanding of and compliance with obligations*

246. In general, FIs and DNFBPs were aware of proliferation-related TFS and the risks related to Iran and DPRK. Understanding in the financial sector is generally better, particularly in the banking sector, which reflects the Bundesbank's closer engagement with this a segment of this sector and the limited outreach to DNFBPs. Large FIs and DNFBPs, particularly banks, insurance companies, MVTS providers and legal and accounting firms, routinely screen all customers against sanctions lists at onboarding and on an ongoing basis using commercial databases. On-site discussions indicate that smaller FIs (particularly non-bank FIs) and DNFBPs also undertake sanctions screening, but are less likely to perform ongoing screening or have access to commercial databases. Some use the online, consolidated sanctions list, *FiSaLis* (maintained by the Ministry of Justice of North Rhine-Westphalia), while others manually check EU and UN lists. Some DNFBPs only undertake sanctions screening as part of enhanced due diligence rather than screening all customers. Smaller DNFBPs noted that where complex corporate structures were involved, issues identifying the beneficial owner would complicate sanctions screening. While many DNFBPs undertake screening, shortcomings in controls, especially in cash-intensive sectors (such as the gold sector) create a gap in TFS implementation that could be used to avoid mitigation measures adopted by FIs. Smaller FIs and DNFBPs were more risk averse and often stated they would not accept customers with links to Iran or DPRK.
247. As with terrorism-related TFS, the Bundesbank plays the primary role in raising awareness of proliferation-related TFS. The Bundesbank distributes circulars to approximately 1 800 FIs advising them of any changes to EU sanctions lists (or AWG orders). It also provides an email service to respond to questions via its website. Between 2014 and 2019, the Bundesbank received and responded to between 12 and 58 written enquiries annually on sanctions. These largely related to Iran, which is in line with Germany's context and the impact of the JCPOA over this period. The Bundesbank also offers a hotline, including to provide assistance in verifying potential false positives. The Bundesbank reports that the hotline is widely used by both FIs and DNFBPs, although no statistics are available. Private sector institutions met during the on-site were in some cases unaware of the Bundesbank's role. FIs and DNFBPs had inconsistent approaches in this area, with some approaching their AML/CFT supervisor (most of which do not have a role in proliferation-related TFS) or the FIU to verify false positives.

*Competent authorities ensuring and monitoring compliance*

248. For proliferation-related TFS, supervision of FIs is conducted solely by the Bundesbank (which monitors TFS implementation, including screening measures, freezing obligations, reporting requirements and authorisations for access to funds). BaFin does not have a statutory responsibility in this respect. While this difference (compared to supervision for terrorism-related TFS; see IO.3) was not always clear to FIs met during the on-site (including some large banks and MVTs providers), this does not appear to impede FIs' implementation of proliferation-related TFS. The Bundesbank conducts regular audits of its 2 500 supervised entities to supervise compliance. In July 2021, the FTE (full time equivalent) dedicated to TFS audits was increased, with 40 auditors now involved to some extent in supervising TFS compliance. The frequency of audits is based on a range of factors, including the size of the institution, previous results, and information from external sources. The number of inspections is low, but is complemented by other supervisory activities (such as surveys and questionnaires). Banks holding a combined total of 81% of all banks' balance sheets would be subject to inspection over the course of 10 years.

**Table 4.10. TFS audits by the Bundesbank**

	2017	2018	2019	2020*
Number of on-site audits with a TFS element	113	72	74	32

\* Due to COVID-19, fewer on-site audits could be conducted in 2020. This was mitigated by the use of a questionnaire for ~1 300 credit institutions.

Source: German Authorities

249. It is rare that the Bundesbank identifies actual sanctions breaches when conducting audits. Bundesbank detected 17 cases of potential TFS breaches at five institutions between 2017 and 2021. These were reported to the Main Customs Offices in order to carry out administrative offence proceedings (see IO.3).
250. There is a lack of clarity around DNFBP supervision for TFS, with no statutory supervisor for general TFS compliance for DPMS, REAs, casinos, TCSPs and insurance intermediaries.<sup>51</sup> There was some confusion expressed during the on-site by both entities and AML/CFT supervisors as to the roles and responsibilities in this area. This lack of clarity is acknowledged in Germany's AML/CFT strategy and contributes to issues implementing TFS, particularly by smaller DNFBPs (see IO.4, Chapter 5).
251. Outside of detection during supervisory activity, breaches of PF-related TFS obligations may be detected by the FIU, whose database systematically screens incoming STRs against UN sanctions lists and would disseminate any subsequent analysis.

<sup>51</sup> The customs administration monitors the import, export and transit of goods. Main Customs Offices audit, among other things, compliance with foreign trade law by businesses involved in the cross-border movement of goods, including relevant DNFBPs.

252. Customs is represented on various proliferation-related inter-agency groups, including on export credit and dual-use goods (see R.2), which would allow it to identify possible TFS breaches related to other proliferation-related sanctions breaches; however, there are no actual examples of this occurring in practice. The Bundesbank is not represented on these groups and is reliant on informal co-operation and information-sharing to remain abreast of the issues discussed in these groups, which may lead to TFS issues being overlooked.

4

## Overall conclusion on IO.11

Germany proposes EU designations under UNSCRs 1718 and 2231, but is less active at the UN level for political and contextual reasons. DNFBPs receive limited outreach and monitoring for compliance with proliferation-related TFS, contributing to some shortcomings in regular or ongoing screening of customers, including in some higher-risk sectors especially in cash-intensive sectors (such as the gold sector). DPMS, REAs, casinos, TCSPs and insurance intermediaries do not have a clear supervisor for general TFS compliance, and discussions with DNFBPs indicate that in practice, most entities are not subject to clear, effective monitoring. These factors impede TFS compliance and implementation in DNFBP sectors. These are major deficiencies in light of Germany's context and the risks of proliferation-related sanctions evasion within certain DNFBP sectors.

**Germany is rated as having a moderate level of effectiveness for IO.11.**

## Chapter 5. PREVENTIVE MEASURES

### Key Findings and Recommended Actions

#### Key Findings

- a) In general, FIs, including VASPs, apply a range of preventative measures commensurate with their risks. Larger FIs, particularly major banks (including online banks), MVTs, insurance providers, and VASPs, generally have a strong understanding of their ML/TF risks and AML/CFT obligations. Smaller FIs, including some regional/niche banks and money service businesses, show a less developed understanding.
- b) Risk understanding among DNFBPs is still developing with some entities (including certain REAs and accountants) displaying a nuanced understanding of risk. Larger DNFBPs, particularly major legal or REA firms or large-scale DPMS, and those with more supervisory contact generally implement preventive measures in line with risks. Nonetheless, some of these larger entities were not aware of their access to certain CDD measures (such as digital identity verification) and reported challenges aligning CDD and record-keeping obligations with data protection requirements. Smaller DNFBPs, including in higher risk sectors (such as notaries and legal professionals), face challenges implementing effective preventive measures, including in relation to CDD, PEPs and TFS.
- c) The development of a public-private partnership (the Anti-Financial Crime Alliance, AFCA) has increased the availability of risk information to a whole range of obliged entities and contributed to a better risk understanding in certain areas (including virtual assets, real estate and risk related to the COVID-19 pandemic).
- d) The obliged entity population in Germany's non-financial sector is very large (almost 1 million entities) and, in some sectors, changes year-to-year. This, combined with limited supervisory resources and an evolving risk-based approach in many sectors (see IO.3) means that certain DNFBP entities are less aware or unaware of their AML/CFT obligations, resulting in inadequate application of CDD and recording-keeping obligations and enhanced measures. The broad nature of the obliged non-financial sector inhibits supervisors from focusing their actions on higher-risk DNFBPs (see IO.3), resulting in deficiencies in entities' implementation of CDD obligations and enhanced measures.
- e) STR reporting numbers are particularly low for non-bank FIs and all DNFBP sectors and, until recently, were also lower than expected for banks. Almost all STRs (97% in 2020) come from the financial sector, mostly from banks

(90%). Reports from FIs, particularly banks, have increased exponentially from a relatively modest base for a range of reasons. A wide range of factors contribute to low DNFBP reporting, including lack of awareness, misunderstandings of the reporting threshold, poor implementation of preventive measures, and confusion surrounding professional secrecy obligations. Some FIs have misinterpreted recent enforcement actions by BaFin as imposing a strict reporting deadline (despite no such deadline existing in Germany's law of BaFin's interpretative guidance), leading them to rush their internal analysis prior to reporting. A lack of qualitative feedback from the FIU impacts the quality of reporting in both the financial and DNFBP sectors.

- f) Lawyers and other legal professionals, notaries and accountants met on-site all considered that their professional secrecy obligations inhibit STR filing. The legal profession's interpretation of legal professional privilege is broad: many lawyers and notaries consider that they are required to file a STR only where they have positive knowledge that they are being used for ML or TF. A 2020 ordinance requiring rules-based reporting by these sectors in real estate transactions (regardless of privilege) has increased reporting by notaries, but there is confusion among lawyers regarding the scope of the ordinance.

## Recommended Actions

- a) Improve STR reporting by:
  - a. Reviewing whether legal professional privilege requirements create confusion regarding STR reporting in practice and ensure that there are adequate measures (such as guidance) to encourage higher-risk sectors to fulfil their legal reporting obligations. Consider expanding rules-based reporting requirements for notaries and the legal profession to other high-risk areas (beyond real estate transactions).
  - b. Having the FIU routinely analyse the quality of STRs (beyond basic form requirements) and provide substantive feedback to reporting entities in high risk FI and DNFBP sectors and to their supervisors.
  - c. Ensuring the FIU and supervisors work with DNFBP sectors to provide sector-specific guidance on when to file a STR.
  - d. Considering further nuanced guidance or outreach for entities on timeframes for the submission of STRs to help reporting entities balance the need to analyse all relevant information, while complying with the requirement to file STRs promptly.
- b) Ensure DNFBPs, particularly higher risk institutions, consistently understand and implement their AML/CFT obligations, including the availability of relevant risk-based measures (such as digital identity verification).

- c) Ensure BaFin is targeting its supervisory and outreach activities to the sectors that require increased awareness and support, including by examining the findings of audit reports and STR data, in particular to:
  - a. continue to promote awareness of ML/TF risks and AML/CFT obligations, including the importance of having documented risk assessments and risk sensitive internal controls, among smaller bank and non-bank FIs, including VASPs;
  - b. support improvements to CDD processes in the securities and MVTs sectors; and
  - c. understand the root causes of sudden and dramatic STR increases from the banking sector to ensure there is no defensive reporting and, if there is an element of over-reporting, ensure that FIs have clarity on when STRs should be filed.
- d) Support further development of AFCA, including by proactively increasing involvement of DNFBPs and enhancing information-sharing on a broader range of issues (including compliance challenges, the use of new technologies, and specific ML/TF cases).
- e) Continue to engage and support supervisors, data protection authorities, FIs and DNFBPs to find workable solutions to enable comprehensive data collation and sharing consistent with data protection obligations.
- f) Review how identification requirements are applied in relation to refugees/asylum-seekers to ensure they are proportionate, appropriately risk-based, limit risk displacement and do not result in unintended financial exclusion.

253. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23, and elements of R.1, 6, 15 and 29.

#### Immediate Outcome 4 (Preventive Measures)

254. For the reasons of their relative materiality and risk in the German context, shortcomings in preventive measures were weighted most heavily for banks; heavily for MVTs and money service businesses, VASPs, real estate, notaries, lawyers and accountants; moderately heavy for securities, e-money and payment service providers (other than MVTs), DPMS, and TCSPs; and less heavily for casinos and the insurance sector. This weighting is based on the relative importance of each sector and Germany's risks, context and materiality. See Chapter 1, section 1.4.3 for more detail about the risk, materiality and weighting of each sector in Germany's context.
255. Meetings with the private sector did not reveal any fundamental concerns about the implementation of preventive measures. Overall, the assessors found that:
- **Most heavily weighted:** Larger banks demonstrated good awareness and implementation of preventive measures. Smaller banks have a less developed understanding and implementation.

- **Heavily weighted:** While MVTS, money service businesses, VASPs and real estate agents (REAs) are largely aware of and implement preventive measures, there are some deficiencies in these sectors, particular among smaller entities. Implementation is mixed among notaries, the legal profession (lawyers and tax advisors<sup>52</sup>) and accountants, with major deficiencies in these sectors, including in CDD obligations and STR reporting.
  - **Medium weight:** Securities, e-money and payment service providers (other than MVTS) are largely implementing their obligations, with some deficiencies in smaller entities' implementation of CDD and EDD measures among others. DPMS and TCSPs' understanding and implementation is mixed, with major deficiencies in several areas.
  - **Low weight:** Casinos and the insurance sector have a good understanding of their risks, and implement preventive measures accordingly.
256. Assessors' findings on IO.4 are based on: interviews with a range of private sector representatives, statistics, case files and examples of enforcement actions provided by BaFin and DNFBP supervisors, and information concerning the relative materiality and risks of each sector (including the NRA, Sub-National Risk Assessment (SRA) and *Länder* risk assessments). The assessors met with a range of FIs and DNFBPs. Nonetheless, given the large number of supervised entities, the wide diversity of the sectors, and the issues in supervision identified in IO.3, it is still difficult to generalise implementation across the sectors.

### *Understanding of ML/TF risks and AML/CFT obligations*

#### *FIs, including VASPs*

257. BaFin has observed a positive trend in FIs' risk awareness and knowledge of AML/CFT obligations. For example, Executive Board minutes indicate that ML/TF has become a regular discussion topic at many FIs' Executive Board level, which demonstrates a greater level of understanding of AML/CFT obligations and the importance of compliance. A range of banks, insurance providers, asset management companies and MVTS were directly involved in consultations on the NRA, in addition to associations representing banks, insurance intermediaries, securities providers, and payment and e-money institutions. This has helped promote consistent risk understanding among these sectors. FIs interviewed were unanimously aware of the NRA and used it in developing their own risk assessments. Various FIs, including several major banks, are also involved in the Anti-Financial Crime Alliance (AFCA; Germany's public-private partnership), which ensures they engage in and benefit from AFCA's work on emerging risk areas (see IO.1). AML/CFT monitoring through FIs' annual external audits and BaFin's supervisory activity ensure FIs receive regular feedback on their risk assessments and preventive measures promoting continuous improvement.

---

<sup>52</sup> Tax advisors are only captured in the FATF requirements (and covered in this report) to the extent that they fall within the definition of lawyers, other legal professionals or accountants undertaking the functions set out in R.22. In practice, tax advisors in Germany may be involved in the creation, operation or management of companies, legal persons or arrangements.

258. Banks have an adequate understanding of their ML/TF risks and AML/CFT obligations. The results from AML/CFT audits and BaFin's inspections reveal that the vast majority of banks have completed appropriate internal ML/TF risk assessments; more than 75% of shortcomings in this area were minor, with more serious deficiencies occurring in a very limited number of cases (under 3% of all findings).

### Box 5.1. Improvement of risk assessment at small bank

During a BaFin inspection of a small private bank, BaFin identified that the risk assessment did not clearly reflect the bank's risk situation. There were deficiencies in a range of areas, including: recording and identification of customer, product and transaction-related risks; categorisation and weighting/evaluation of identified risks; and review and refinement of preventive measures based on risk. BaFin directed the bank to completely revise the assessment as part of the post-inspection follow-up. Throughout this process, the bank was required to submit updated versions of the risk assessment to BaFin at specified intervals. When the revision was completed, BaFin assessed that it met regulatory requirements, meaning the institution is adequately aware of its ML/TF risks and obligations, and manages them appropriately.

Source: German Authorities (BaFin)

259. During discussions, larger FIs (particularly major banks, MVTs institutions, insurance providers, and VASPs) demonstrated a good understanding of ML/TF risks and AML/CFT obligations. Smaller institutions (including some regional/niche banks and money service businesses) have a less developed understanding. BaFin has noted that smaller FIs in the non-banking sector have particular difficulties in implementing requirements with respect to documentation of their AML/CFT policies and procedures. While the number of STRs from the financial sector has increased exponentially recently, the relatively modest base and low number of STRs from non-banks may suggest issues in entities' understanding and implementation of AML/CFT obligations.

#### *DNFBPs*

260. DNFBPs' understanding of their ML/TF risks has improved over the past five years, although it is still developing in certain areas. The large and changing nature of the supervised population, combined with challenges in supervision (e.g., limited supervisory resources: see IO.3) that may result in limited or no supervisory contact, means that certain entities, including within the legal, DPMS, and TCSP sectors, may be less aware or unaware of their AML/CFT obligations.

- 5
261. Understanding of ML/TF risks and AML/CFT obligations varies across the broad and diverse **REA, DPMS and TCSP** sectors, usually depending on the size of the entity and the level of supervisory engagement. REAs and DPMS were involved in the NRA through industry associations, rather than via direct representation. Some REAs consequently consider that the NRA does not provide sufficient detail or nuance. REAs generally display a good understanding of their ML/TF risks, which reflects the national focus on ML through real estate. Several REAs demonstrate an awareness of the risks posed by complex corporate structures and opaque legal entities (despite the relatively limited national understanding of these risks; see IO.1). DPMS also have a reasonable risk understanding, especially of the risks posed by cash, in line with the NRA. DPMS interviewed during the on-site had conducted an institution-specific risk assessment, although this is not the case across the whole sector; inspections of 50 gold dealers in 15 Länder in 2020 found that 60% had an adequate, documented risk assessment for their business. Standalone TCSPs (i.e., TCSPs that are not jointly operating as part of the legal, accounting or tax advisor professions) were not involved in the NRA. Larger REAs and DPMS have a good understanding of AML/CFT obligations, while smaller entities display some misunderstandings, particularly in relation to recent legislative changes. Challenges in supervision (such as a lack of resources and a large supervised population: see IO.3) mean certain entities, especially in the unlicensed DPMS and TCSP sectors, have limited to no supervisory contact and are less aware or unaware of their AML/CFT obligations (despite recent efforts by supervisors in certain sectors/regions). This is exacerbated in the TCSP sector as most supervisors have a limited understanding of risks in this area (see IO.3).
262. **Lawyers and other legal professionals (such as tax advisors), accountants and notaries** generally display a reasonable understanding of ML/TF risks and AML/CFT obligations. All entities interviewed had conducted an institution risk assessment. Notaries and legal professionals have a strong awareness of the ML risks related to their involvement in real estate transactions, consistent with the NRA and national focus on this area. Accountants interviewed during the on-site were aware of the risks posed by complex corporate structures, but notaries were less cognisant of risks in this area. Legal professionals and accountants noted that the shift towards risk-based supervision (see IO.3) has increased awareness of AML/CFT obligations as entities are aware they may be subject to inspection at irregular intervals.
263. **Casinos** demonstrate a good understanding of their risk and obligations. Entities are aware of the NRA, and have typically also conducted their own risk assessments. Casinos are very aware of the high inherent risks posed by the use of cash in their sector and entities interviewed on-site were able to explain how mitigation measures (both sectoral and specific) impacted these risks. Long-standing and active supervisory engagement contributes to casinos' strong understanding of their AML/CFT obligations.

264. DNFBPs that are involved in AFCA (namely certain REAs, casinos and notaries indirectly through the Federal Chamber of Notaries) benefit from direct exposure to discussions and assessments of existing and emerging risk areas. However, AFCA papers and risk-related resources are available only to obliged entities registered with the FIU. Entities are not required to be registered until 2024, and the number of registered non-financial institutions remains low (12 240) and comprises only a very small proportion of the non-financial obliged entity population (1.4%). Unregistered DNFBPs do not have access to AFCA's risk-related information, which may contribute to a lower understanding of risk.

### *Application of risk mitigating measures*

#### *FIs, including VASPs*

265. Banks typically apply adequate measures to mitigate risks. Findings from annual audits and BaFin's inspections over the last three years show that preventive measures in the banking sector are largely commensurate with risk; almost 90% of banks had only minor deficiencies, with more serious deficiencies in only a very small number of cases. A BaFin horizontal review in 2018 found that Money Laundering Reporting Officers (MLROs) were broadly effective in implementing risk mitigation measures of adequate quality across the banking sector. The study was based on a small sample size (only 28 institutions), with major and regional banks over-represented to maximise coverage of the market in terms of asset share.
266. Outside of the banking sector, risk management controls are weaker (including in certain MVTs and money service businesses), usually depending on the nature and scale of the business. BaFin has found that FIs subject to annual audits are largely effective in improving controls, with risk mitigation measures subject to ongoing improvement on the basis of auditors' recommendations. This is observed less in FIs that are not subject to annual audit requirements, meaning their risk management frameworks are not as regularly monitored and assessed (e.g. multiple agents providing payment services). VASPs demonstrated a particular interest in developing sector-specific tools in line with their risk profile, including in collaboration with the government. For example, one VASP developed specific tools for risk-based virtual asset blockchain analysis that are now also used by the BKA in its investigations.
267. FIs interviewed during the on-site generally had AML/CFT controls in place that were risk sensitive and informed by their risk understanding. However, the level of risk understanding is less developed among smaller FIs (including some regional/niche banks and money service businesses) which negatively impacts their ability to develop and implement preventive measures aligned to their ML/TF risks.

*DNFBPs*

268. Larger DNFBPs and those with good supervisory engagement, including major legal and accounting firms, large-scale REAs, and casinos, have a range of mitigating measures in place. Smaller DNFBPs and those with limited supervisory contact (including small scale notaries, solo legal practitioners, DPMS and TCSPs) may not have specific risk-mitigation measures and in some cases may not be applying preventive measures. REAs, DPMS and TCSPs are increasingly putting in place mitigating measures commensurate to their risks. Given the general risks in the real estate sector, REAs tend to have relatively strong controls that go beyond standard CDD and EDD. These include adverse media checks and involvement of compliance officers in vetting for clients meeting certain risk profiles, including links to higher-risk jurisdictions as identified in the NRA (which goes beyond the FATF and EU lists). DPMS are particularly sensitive to the risks posed by cash transactions; several entities had put in place cash transaction limits for payments over EUR 10 000 (the CDD obligation threshold is EUR 2 000). Entities also demonstrated other mitigation measures, for example, general limits on the volume and value of products that they would sell to a single client, and restrictions on the types and value of products that could be sold online. Limited mitigation measures were observed for smurfing or supply chain risks (e.g., laundering through recycled gold), although some DPMS demonstrated an awareness of these risks. Given the more limited supervisory engagement, TCSPs are less likely to have mitigation measures in place. As above, certain DPMS and TCSPs are less aware or unaware of their AML/CFT obligations and therefore do not implement adequate preventive measures.
269. **Lawyers and other legal professionals, accountants and notaries** have varying levels of mitigation measures in place, with measures having improved in the past 2-3 years. Mitigation measures are generally in line with risk areas of national focus, but are not always in line with sectoral risks. For example, most entities noted that they do not accept cash transactions in light of the nationally identified risk of cash-based ML. However, while this is relevant for real estate transactions, cash is otherwise not a significant risk for these sectors. Lawyers, tax advisors and accountants take additional measures for payments in virtual assets or from third parties. Additional steps are also taken for customers or transactions with links to higher-risk jurisdictions and entities generally look beyond FATF and EU lists in determining which jurisdictions fall into this category. Whether a lawyer is captured as an obliged entity depends on the nature of their work (consistent with R.22) and supervisors do not have a complete understanding on the scope of the obliged entity population. As a result, certain obliged entities are less aware of their AML/CFT obligations and may not apply adequate preventive measures.

270. **Casinos** generally have specific mitigating measures in line with their risks. In particular, casinos met on-site demonstrated a range of measures to mitigate the risks of cash. For example, for large or suspicious cash transactions (e.g., a large number of small used notes), some casinos will cash out chip using the same bills provided by the player upon entry into the casino. Casinos also do not issue certificates of winnings to avoid these being used to justify the proceeds of crime. Casinos interviewed also had automated processes to identify higher risk customers or transactions, based on sector-specific risk (e.g., first-time customers gambling large amounts, individuals changing money without playing, potential smurfing, etc.). Some casinos do not allow entry to certain foreign nationals to mitigate the risks posed by international junkets, but limited other measures were in place to address this risk.

### *Application of CDD and record-keeping requirements*

#### *FIs, including VASPs*

271. Overall, FIs (including VASPs) generally appear to have a good level of compliance with CDD obligations. From 2016-2018, external audits and BaFin's inspections found mostly minor shortcomings related to CDD. Banks are particularly strong in this area, with almost no very serious shortcomings identified. In 2018, 84% of bank audits identified no or minor shortcomings on CDD, 13.5% identified moderate shortcomings, and only 2.5% had major or serious deficiencies. Larger banks have centralised customer acceptance processes, with mandatory involvement of the AML or compliance department. Larger insurance companies and investment firms also increasingly use clear CDD and customer acceptance procedures that identify cases for MLRO or AML team involvement. In the MVTs sector, methods have been developed to involve the MLRO during the very rapid processing of walk-in customer business (see box below). Several major MVTs providers noted that they faced difficulties conducting CDD on refugees/asylum-seekers with certain types of government-issued documentation (e.g., a proof of arrival document, as opposed to an identity card). In such cases, these entities complied with their obligations and rejected such customers. BaFin has developed guidance on CDD for refugees, but could further review this issue in line with its broader financial inclusion efforts and to prevent the use of unlicensed channels.

**Box 5.2. MVTS involvement of the MLRO in the customer acceptance process**

In a special inspection of a relatively small MVTS, BaFin found that the MLRO has the option – despite not being physically present – of connecting to ongoing customer processing at the counter, via the institution’s IT system and video conferencing. This function is used for quality assurance of CDD, e.g., to monitor the process steps defined by work instructions. Employees also use the electronic hook-up with the MLRO to draw the MLRO’s attention to suspicious transactions without the customer’s awareness. In these cases, the MLRO can reject the payment order in real-time operation, e.g., by blocking it in the IT system.

Source: German Authorities (BaFin)

272. Most FIs, regardless of size or sector, now use IT systems to support CDD processes and maintain CDD records. The largely digital record keeping processes used by FIs has resulted in more complete customer records being maintained, which FIs can provide with relative ease to BaFin and LEAs as and when required. There has also been an increase in the use of customer identification technology with video identification being more commonly used and, to a lesser extent, electronic identification (eID). Entities demonstrated high standards for vendor due diligence. VASPs met at the on-site provided several examples of thorough 3<sup>rd</sup> party checks, including the rejection of a provider that was not able to meet the high qualitative standards set during an initial test. Many FIs are also using external IT solutions as part of their beneficial ownership identification process. Smaller FIs, especially in the securities sector and higher-risk MVTS sector, tend to use more manual processes. BaFin has observed that these have higher error rates.
273. Based on discussions with FIs, FIs generally do not enter a business relationship if the CDD process is not completed and terminate the business relationship if it is not possible to update CDD documentation or information. For sectors where the service is transactional in nature and a business relationship is not established (e.g. MVTS), FIs typically use IT systems which block transactions from proceeding when customer identification information is not entered and in such situations the customer is declined. Nonetheless, the low number of STRs outside the banking sector suggests not all FIs comply with the requirement to consider filing a STR in such cases (where CDD cannot be completed).

*DNFBPs*

274. Compliance in the DNFBP sectors is mixed due to some lack of understanding of basic obligations, difficulties implementing beneficial ownership obligations, and certain entities (accountants and the legal profession) facing challenges in knowing when to conduct CDD and maintain records without breaching data protection requirements. STR numbers suggest that most DNFBPs are not aware of the obligation to consider filing an STR where CDD cannot be completed.

275. Larger **REAs, DPMS and TCSPs** tend to have better CDD and record-keeping processes, often with automated and/or centralised components. Smaller entities across these sectors generally rely on manual processes. While most firms understand what CDD should involve, smaller DPMS are not always aware of when CDD is required (and, in particular, that Germany requires CDD for cash transactions over EUR 2 000 (see R.22)). Entities interviewed on-site had a good understanding of beneficial ownership requirements, although this may not be shared across all entities or all sectors: a 2020 review of gold traders found that almost 30% of entities did not ask about beneficial ownership. REAs, DPMS and TCSPs face challenges identifying the ultimate beneficial owner where more complex corporate structures are involved. Where CDD cannot be completed, entities interviewed do not continue the relationship or transaction, and most indicated they would also file a STR. However, the low number of STRs in these sectors and the small number of non-financial entities registered with the FIU (12 240 or 1.4% of the population) suggests that this is not reflective of the approach of these industries as a whole.
276. **Lawyers and other legal professionals, accountants and notaries** demonstrated a generally good understanding of CDD and record-keeping obligations, including beneficial ownership and ongoing CDD requirements. Larger legal and accounting firms with international clients cited difficulties verifying the identity of foreign customers or beneficial owners and were not aware of their ability to use video or digital identity verification processes. Firms providing a range of services also face difficulties knowing at which stage to conduct CDD. Lawyers are only required to conduct CDD for certain services (consistent with the FATF Standards), while accountants and tax advisors are subject to a blanket CDD requirement. Entities met during the on-site noted that firms offering several obliged entity services (e.g., legal and accounting services) face challenges knowing when to conduct CDD and maintain records without breaching data protection requirements. Larger or multi-service institutions, which are generally higher risk, often have several different supervisors (see IO.3). These firms considered that the complex supervisory regime, including different messaging from different supervisors, had an impact on their understanding of and compliance with relevant obligations. Entities were aware of the requirement not to conduct business and to consider filing a STR where CDD could not be completed. However, several factors inhibit compliance with this obligation, including restrictions on STR filing (see Chapter 5 below). Notaries' also have a duty to provide notarisation services unless it is for purposes that are recognisably illicit or unlawful. Discussions indicated this can cause difficulties for notaries in practice, although some notaries have strategies in place to deal with this conflict (see box below).

### Box 5.3. Notary strategies to deal with the conflict between an inability to complete CDD

In 2019, a notary based in Berlin was approached by a legal person customer that wanted to buy a property. In the course of undertaking CDD, the notary identified that the beneficial owner of the company had the same last name as an infamous Berlin clan of an organised crime group. The notary applied EDD and demanded a broad range of information from the client regarding the source of funds and asking numerous questions over a long period. The client's lawyer eventually contacted the notary, applying pressure to notarise the transaction. The notary indicated that they could refer the case to the regional court for decision. At this point the client withdrew their business. No STR was submitted as this case predated the reporting ordinance requiring reporting and the notary did not consider that they had positive knowledge of ML.

Source: On-site discussions.

277. **Casinos** have a strong understanding of CDD and record-keeping obligations. Several land-based casinos conduct CDD upon entry, using automated processes, regardless of the relevant thresholds. Others conduct CDD at the point of cash-out where thresholds are met (or, where there is potential smurfing). Supervisors noted that breaches in these areas are rare and a 2019 questionnaire found that casinos self-reported CDD breaches as medium-low.

#### *Application of EDD measures*

278. In general, larger FIs (particularly banks, MVTS and insurance providers) and DNFBPs (particularly large accounting and legal firms) are aware of and apply EDD measures. Smaller entities and those with less supervisory engagement, including entities in higher risk sectors (such as solo legal, accounting or notarial practitioners or REAs), face challenges implementing EDD measures, particularly relating to PEPs and TFS. The low number of STRs in Germany may indicate issues applying EDD.

#### *Politically exposed persons*

279. FIs (including VASPs) are aware that compliance with PEP requirements is a high priority area for BaFin and apply a range of measures. Most FIs, especially banks, uses off-the-shelf commercial software to automatically screen customers' PEP status, both at onboarding and on an ongoing basis. This is also the case for smaller banks, which typically belong to co-operative type structures that provide software solutions for all members. In addition to automated solutions, FIs also use manual processes; for example, client onboarding forms typically include a question on PEP status. FIs providing private banking services have even stricter screening standards and conduct additional research, including the use of private intelligence providers to establish the background of new clients and their possible PEP exposure. Some smaller FIs, particularly MVTS, indicated they would not accept PEP clients identified during onboarding.

280. FIs' PEP measures include obtaining information on the customer's source of funds and source of wealth. FIs across all sectors demonstrated a good understanding of these requirements. In order to address the specific risks of tax evasion, banks conduct additional checks to ensure that the client's funds have been properly taxed. In some instances, if the client uses legal persons or arrangements, particularly where there are connections to several jurisdictions, banks will request a legal opinion to certify that the structure is tax compliant. Banks and non-bank FIs also have processes in place to obtain senior management approval prior to onboarding or continuing a relationship with a PEP. Based on BaFin's on-site inspections, the use of automated processes ensures that the number of instances where an FI has failed to identify the presence of a PEP is extremely low.
281. DNFBPs displayed a mixed understanding of their obligations related to PEPs. Entities were generally aware of the obligation to identify PEPs. Larger DNFBPs, particularly casinos and major legal or accounting firms, often have access to PEP screening databases that they use to screen clients at onboarding and throughout the relationship. However, for the most part, DNFBPs, and especially smaller REAs, DPMS and solo legal practitioners or notaries, do not have access to these services and generally rely on self-disclosure. DNFBPs interviewed from these sectors recognised the drawbacks in this approach and indicated a need for additional government support (e.g., a searchable PEP database, similar to the TFS database). Awareness of other PEP requirements (including senior management approval and measures to identify the source of wealth and source of funds) was mixed and generally weaker in smaller entities, particularly small REAs, DPMS and solo legal practitioners or notaries. The Federal Chamber of Notaries has developed a questionnaire to help notaries in this respect by walking them through how to identify the source of wealth and source of funds.

### *Correspondent banking*

282. BaFin conducts ongoing supervisory outreach related to correspondent banking and has long recognised correspondent banking as a higher-risk area in its institution risk assessments. BaFin recognises the risk posed by intra-European relationships, and has promoted the need for enhanced attention on business relationships within the EU. BaFin's supervisory experience shows that banks have reduced their correspondent banking relationships since 2015 due to the inability to manage the risks of those relationships. This coincides with some highly-publicised instances of non-compliance resulting from conduct prior to 2015. BaFin regularly engaged with banks to understand which correspondent banking relationships were being terminated and why.
283. Although there have been major compliance issues in this area, in general correspondent banking is not a significant element of most banks' business. Approximately 40% of correspondent banking relationships are currently held by nine banks, with the largest share held by the two most globally active major banks in Germany, which are under intensified supervision by BaFin.

284. FIs are aware that BaFin considers correspondent banking to be potentially higher risk and take this into account in their approach to correspondent banking relationships. Senior management approval is required before entering into such a relationship and a dedicated processes is applied for initial and ongoing due diligence of the respondent bank. FIs with business activities on a global level use bespoke software solutions for monitoring the transactions routed on behalf of the respondent bank, which enables the correspondent bank to detect unusual transaction patters and potentially suspicious activity. Unfortunately, statistics on the number of STRs related to correspondent banking are not available.
285. Since 2018, correspondent banking relationships of certain banks have gradually increased in line with greater confidence in mitigation measures in this area.

#### *New technologies*

286. To address potential risks associated with new technologies, FIs have generally established processes for the creation of new products and technologies. These involve a thorough assessment of associated risks, with the involvement of both the compliance and risk functions. There is increased awareness among FIs of the risks relating to new technologies, in particular in relation to the area of Fintech and virtual assets. FIs are generally sensitive to the potential risks of new products and technologies and follow thorough product-approval processes, which include senior management approval, before they introduce any new products or changes to existing products. DNFBPs do not tend to encounter similar risks from new technologies, however, relevant sectors tended to be risk averse. For example, online casinos generally do not accept virtual assets.

#### *Wire transfer rules*

287. FIs are aware of the obligation for payment services providers to ensure that funds transfers are accompanied by certain information on the payer and payee. The information is added automatically and the payee's service provider monitors incoming transfers using automated procedures. BaFin's supervisory experience indicates that the majority of the institutions comply in full with the regulation. In a small number of instances where issues arise, the root cause is usually communication issues between the payer and payee institutions and is easily resolved. Shortly prior to the onsite visit, Germany implemented a new regulation that extended wire transfer rules to apply to VASPs (see R.15). VASPs were aware of this change, but were still in the process of developing and implementing systems to ensure compliance.

*Targeted financial sanctions (TFS)*

288. FIs across all financial sub-sectors have a reasonably good awareness of TFS obligations and risks. The vast majority of banks and large non-bank FIs use TFS screening software to automatically screen customers and transactions against all relevant lists, including the EU, UN and US Office of Foreign Assets Control lists. This is consistent with BaFin's findings. In 2018, BaFin identified TFS screening as a priority area and undertook a study on a sample of FIs' screening mechanisms. The study found that most FIs made use of electronic monitoring, generally from third-party providers, and typically updated daily. Nonetheless, deficiencies were identified at a number of institutions, including: failure to check that lists obtained from the external providers were up-to-date and complete (20% of sampled institutions); weak application of 'fuzzy matching' for screening names against the list (15%); and infrequent list updates (10%). Some confusion and a lack of clarity in supervisory responsibilities in this area (see IO.3) does not appear to impact FIs' compliance with TFS implementation in the financial sector. FIs interviewed were particularly sensitive to TFS compliance due to the potential for criminal penalties.

**Box 5.4. Implementation of TFS obligations by a financial services institution**

A financial services institution supervised by BaFin did not maintain any payment transaction accounts, meaning it was not required to implement an IT-based sanctions screening system. Nonetheless, the institution monitored changes in sanctions lists on a daily basis and evaluated any possible impact on the institution-specific risk situation. In order to implement specific EU financial sanctions, the institution analysed its customer base and blocked access to money market funds in the system for a subsidiary of a sanctioned company.

Source: German Authorities

289. DNFBPs generally displayed a reasonable understanding of their TFS freezing obligations. Many DNFBPs interviewed during the on-site visit, particularly larger entities, undertook routine sanctions screening in order to comply with TFS freezing obligations. The type and method of sanctions screening in the DNFBP sectors differs depending on the size and business model. Larger DNFBPs, particularly law and accounting firms, major REA firms, and large casinos, generally have access to sanctions screening databases that they use at onboarding and throughout the relationship. Some smaller entities use an online sanctions database provided by the Ministry of Justice of North Rhine-Westphalia, while others conduct manual screening. Some DNFBPs, including DPMS and casinos, only undertook sanctions screening as part of enhanced due diligence where another red flag had been raised. For smaller entities, including in higher risk sectors (such as legal professionals and DPMS), issues identifying the beneficial owner can complicate TFS implementation. No funds have been blocked or frozen in the DNFBP sectors as a result of TFS implementation. The absence of a proactive mechanism to immediately notify DNFBPs of new listings/de-listings and the lack of supervisory engagement on TFS in the DNFBP sectors contribute to an inconsistent level of understanding and compliance across and within all sectors (see IOs.10 and 11). While many DNFBPs undertake screening, shortcoming in controls create a gap in TFS implementation.

*High risk jurisdictions*

290. FIs, including VASPs, are aware of the obligation to apply EDD to business relationships with a nexus to a high-risk country. BaFin has observed that FIs take these obligations seriously. This was confirmed by FIs interviewed during the on-site visit; in many cases, FIs (particularly those in the banking, securities, insurance and MVTs sectors) applied enhanced measures for a wider range of jurisdictions than those on the FATF or EU lists. Many of these FIs drew on the NRA for this purpose, which includes several EU countries. This very conservative and overly-cautious approach can, in some cases, lead to over-compliance and unconditional de-risking (e.g., for clients or transactions with a link to Iran). In practice, where FIs engage in transactions involving high-risk countries, they will require an extensive range of documentation from the client to confirm that the transaction is legitimate. Documents requested include contracts, bills of lading, title deeds, etc.
291. DNFBPs also demonstrated a general awareness of their obligations relating to high risk jurisdictions. DNFBPs typically rely on the FATF and EU lists, although some entities take a broader approach; accountants in particular had a broad view of high-risk jurisdictions, including non-cooperative tax jurisdictions, based on supervisory guidance from the Federal Chamber of Accountants. Some entities, including casinos, took a risk averse approach and prohibited entry to customers from identified high-risk jurisdictions. As with all obligations, certain DNFBPs (particularly DPMS, TCSPs, and lawyers) may be less aware or unaware of all their AML/CFT obligations and therefore implement weak preventive measures or none at all, including in relation to high risk jurisdictions.

*Reporting obligations and tipping off*

292. FIs and DNFBPs interviewed were aware of their STR reporting obligations and the number of STRs has increased since Germany's last MER. Nonetheless, the number of reports from DNFBPs and non-bank FIs is low and, until recently, reports from the banking sector were also lower than expected taking into account Germany's risk and context. Reports have increased significantly year-on-year, with preliminary 2021 data indicating an exponential (~100%) increase. Where entities report, this is generally done promptly. Additional feedback from the FIU on the quality of reports could help encourage increased reporting.
293. FIs, including VASPs, appear to generally comply with their STR obligations. Audits of FIs routinely review STR policies and procedures, along with a sample of suspicions raised internally and STRs that were issued to the authorities. Audits do not identify a high number of major or serious deficiencies in relation to STR reporting, indicating that reporting systems generally function well. However, the number of reports from non-banks is low and, reports from banks have increased exponentially but from a relatively modest base in light of Germany's risk and context. As a result, there remains room for improvement (see table below).

**Table 5.1. FIs' audit findings relating to STR reporting (2017-2020)**

	No deficiencies/minor deficiencies	Moderate deficiencies	Major deficiencies	Serious deficiencies
2017	857	46	5	2
2018	979	37	11	1
2019	1 280	74	12	1

	No deficiencies/minor deficiencies	Moderate deficiencies	Major deficiencies	Serious deficiencies
2020	910	39	10	2

Source: German Authorities

294. In 2020, more than 97% of STRs originated from the financial sector, with the highest percentage (90%) coming from banks. Approximately half of the reports from banks come from the 33 institutions BaFin categorises as highest risk. Non-bank FIs are the second largest reporting group. STRs from the financial sector have steadily increased since 2014. STRs increased by approx. 50% from 2018 to 2019, largely due to increases in reporting by the financial sector and particularly the banking sector (see Table 5.2 below). Preliminary data for 2021 indicates that there has been an even more exponential increase (~100%) from 2020 to 2021.<sup>53</sup> In BaFin's view, increased reporting by the financial sector is due to FIs' improved awareness and more effective reporting procedures and monitoring systems. While some FIs agreed this was a factor, other FIs and the FIU pointed to increased awareness that MLROs may be personally liable for failing to report as a reason for the increase in reports. Some FIs have also misinterpreted recent enforcement action by BaFin as imposing a strict reporting deadline (despite no such deadline existing in Germany's law of BaFin's interpretative guidance), leading these institutions to hasten reports and limit pre-reporting analysis/investigation. These factors suggest there may be an increasing risk of over-reporting. Some FIs stated that reports likely increased further in 2021 due to the new 'all crimes' approach in the ML offence (see IO.7) and preliminary 2021 figures indicate this is the case.

### Box 5.5. Bank STR led to rapid solving of bomb attack case

On the evening of 11 April 2017, a bomb attack was carried out on the Borussia Dortmund football team bus. On the following morning, a bank employee noticed suspicious securities transactions relating to Borussia Dortmund shares. The employee immediately obtained further details on the transaction including the IP address through which the transactions were made. This revealed that the IP address came directly from the hotel where the Borussia Dortmund team had been staying. The employee sent internal reports to the bank's compliance department and the outsourced MLRO that same day (12 April 2017). The bank contacted the *Land* Criminal Police Office (LKA) and Federal Criminal Police Office (BKA) in addition to submitting a STR. Despite the Easter holidays, the bank employees stayed in subsequently constant contact with the investigators. Ultimately, the STR provided the crucial information enabling police to rapidly identify and arrest the perpetrator; prior to the attack, the arrested person had purchased put warrants (a type of security) to bet on a falling share price of the football club. The success of the case also inspired the bank to further strengthen the approach taken by its employees by launching a motivational campaign.

Note: A put warrant is a security that gives the holder the right to sell a set quantity of shares/assets for a specified price on or before a specified date.

Source: German Authorities

<sup>53</sup> Based on preliminary data, over 300 000 STRs were received in 2021; the exact number received as at the last day of the on-site is not available.

- 5
295. The non-financial sector (including DNFBPs) accounts for a disproportionately low number of STRs (2% in 2020), especially in light of the size of the obliged entity population (approximately 1 million entities; see Chpt.1) (see Table 5.2). Discussions with DNFBPs pointed to a wide range of factors that contribute to the low level of reporting. The vast majority of obliged entities are not yet registered with the FIU, indicating a lack of awareness of their obligation to file STRs. As at November 2020, 12 240 obliged entities were registered from the non-financial sector, representing approximately 1.4% of the covered population. Even where they are registered, REAs, DPMS and other smaller DNFBPs were deterred by the complexity of the STR filing process, noting that the GoAML system was targeted more towards FIs. DNFBPs also had misunderstandings regarding the reporting threshold; smaller entities and those with less supervisory engagement (such as sole trader REAs, small DPMS or TCSPs) sometimes see a STR as a criminal complaint, preventing filing for a mere suspicion. As a result, most entities only consider filing STRs where CDD cannot be completed, and even then, the low number of reports suggest this is not occurring systematically. In addition, entities do not always have a good understanding of possible red flags related to their business or services; almost all sectors expressed a desire for additional, sector-specific guidance on when to file with private sector input to ensure relevance. Certain sectoral bodies have adopted relevant tools; for example, the Federal Chamber of Notaries has developed a tool to help walk notaries through the STR filing process.
296. Despite legislative changes in this area since Germany's last MER, reporting by notaries and the legal profession remains limited by the sector's broad interpretation of legal professional privilege (see Germany's 2010 MER, para.902). Lawyers, tax advisors and notaries unanimously stated that they were only required to make a STR where they had positive knowledge that the client was using their services for ML or TF. This was considered the clear and unambiguous legal situation despite the legal changes and guidance that Germany has made since its last MER (see R.23). In practice, this is an extremely high threshold for filing (see Box 5.3 above where no STR was filed despite the suspected involvement of an organised criminal group). As a result, reporting from these sectors is very rare. Accountants also had a relatively strict approach to their professional duty of confidentiality and noted this could prevent STRs. Smaller accountants mistakenly believed that filing an STR in breach of this duty would result in criminal responsibility, although this is not the case under the relevant legislation. Accountants noted they would consult their supervisor to determine how to balance obligations, but felt they would benefit from clearer guidance on when they can and should file STRs.
297. In response to these issues, and in recognition of the risks related to real estate, Germany issued a reporting ordinance in October 2020 requiring rules-based reporting by notaries and the legal profession in specific 'red flag' situations related to real estate transactions. The ordinance has had a clear impact on reporting by notaries, which increased from 8 reports in 2018 to 4 500 as at September 2021. A similar increase has not been observed in the legal profession. This may be because these sectors do not participate in real estate activities to the same extent as notaries. However, it may also be due to confusion around the scope of the ordinance; lawyers and tax advisors met at the on-site had mixed awareness of their new obligations and some entities and authorities considered the ordinance applied only to notaries.

**Table 5.2. STRs received by sector (2018-2020)**

	2018	2019	2020
Credit institutions	65 132	103 697	129 108
Financial service institutions (incl. VASPs)	10 552	7 528	9 983
Payment and e-money institutions	264	290	238
Agents	35	650	730
Asset management companies	17	42	33
Insurance understandings	137	232	233
<b>Total STRs from the financial sector</b>	<b>76 137</b>	<b>112 439</b>	<b>140 325</b>
Lawyers and legal advisors	22	24	23
Notaries	8	17	1 629
Accountants	2	0	7
REAs	31	84	135
Gambling providers (incl. casinos)	150	754	252
Traders in goods (incl. DPMS)	368	554	436
TCSPs	1	15	13
Other*	15	64	359
<b>Total STRs from non-financial sector</b>	<b>597</b>	<b>1 512</b>	<b>2 854</b>
Other (e.g., supervisors)	518	963	826
<b>TOTAL STRs</b>	<b>77 252</b>	<b>114 914</b>	<b>144 005</b>

\* Other obliged entities in the non-financial sector include: financial companies (that are not FIs), insurance providers, and tax advisors.

Note: Data prior to 2018 was not provided due to the restructuring of the FIU (see IO.6). While there was a general increase in STRs from DNFBPs in 2020, the reduction in filings in certain sectors (e.g., gambling, traders in goods) could be explained due to limits in in-person activities as a result of COVID-19 containment policies.

Source: FIU Annual Report, 2020. [Some sectors are combined for simplicity]

298. The FIU noted that STRs are generally filed promptly, although there have been isolated cases in which issues are raised after the fact. For example, not long before the on-site a major FI provided a STR relating to conduct several years in the past. FIs and DNFBPs interviewed during the on-site had procedures in place to prioritise STRs where necessary and to ensure timely filing. Institutions reported that TF STRs are typically prioritised and filed within 24 hours of the transaction. Guidance on STR reporting timeframes varies and there is no clear, consistent guidance on timelines for filing. As a result, most entities enforce their own internal timelines for evaluating a case and filing a report. Timelines vary between several hours and 30 days after the transaction, depending on the size of the institution and the complexity of the filing process. Some FIs have misinterpreted recent enforcement action by BaFin as imposing a strict reporting deadline (despite no such deadline existing in Germany's law of BaFin's interpretative guidance), resulting in a misunderstanding about the timeframe within which they are required to report. These institutions consider that the quality of their STRs has decreased because they do not have sufficient time to analyse all information before submitting an STR and are concerned about breaching their obligations if they take more time. This represents a shift since Germany's last MER, which concluded that institutions were conducting overly lengthy examinations of transactions, resulting in a lack of filing. It is positive that entities are now more aware of the requirement to file promptly, but additional, nuanced outreach may be required to help FIs balance this requirement with the need to analyse potentially suspicious transactions.

299. In terms of quality, the FIU noted that larger FIs (particularly banks, securities and insurance institutions) tend to provide deep, high-quality STRs. More challenges are observed with STRs from newer entities, particularly payment service providers. In the non-financial sector, the overall low number of STRs makes it difficult to draw conclusions on quality, but the FIU found that 35% of STRs from DNFBPs were incomplete (i.e., not all fields in the form were filled out). As noted above, issues using GoAML, including the standard reporting form that is not adapted to DNFBPs' activities, may lead to poorer quality STRs from DNFBPs.
300. Both FIs and DNFBPs feel there is a lack of feedback from the FIU on the utility of their STRs. During the on-site, several entities referred to the FIU as a "black box", and noted they would often only be aware that their information was used when they are contacted by a prosecutor to seek evidence or testimony in relation to a case founded on the STR. For several entities, the lack of qualitative feedback discourages filing, which may further contribute to the low number of STRs in many sectors. Where feedback is received, it generally relates to the timeliness and completeness of the report (i.e., whether all fields are filled out) rather than its quality or utility. Nonetheless, entities across a range of sectors noted that the FIU provides useful information upon request.
301. Entities are broadly aware of their obligation to avoid tipping off customers when they make a STR. FIs take a number of practical measures to prevent tipping off. The specific measures vary depending on the organisation or structure of the FI. Measures include: work or staff instructions; contractual confidentiality obligations with employees or with outsourcing companies; company rules for employees and management (e.g., in the Code of Conduct); and training (e.g., online training courses or selective classroom training). Most DNFBPs also provide training and/or staff guidance on tipping off obligations. Avoiding tipping off is challenging in certain DNFBP sectors. REAs noted that their close relationship with their client often made it difficult to terminate the relationship upon filing a STR without tipping off the client. REAs interviewed during the on-site had a range of creative excuses they would provide, but this may not be the case across entire sector.

### *Internal controls and legal/regulatory requirements impending implementation*

#### *FIs, including VASPs*

302. BaFin's supervisory experience has found that FIs are aware of the obligation to have internal AML/CFT controls in place. The quality of policies and procedures is also generally good. FIs' internal control frameworks typically follow a 'three lines of defence' model. The first line of defence is the business side, which is the main point of contact with customers. The business side receives regular and ongoing AML/CFT training and performs relevant checks and controls, e.g., CDD at customer onboarding. The second line of defence is the compliance function, which develops and oversees implementation of the AML/CFT framework, including by conducting regular checks on the first line of defence. Finally, the audit function acts as the third line of defence, and scrutinises all relevant AML/CFT processes. Even smaller banks typically have good controls because they are part of a co-operative structure and therefore able to access products developed for member banks. In general, FIs' policies are updated regularly in response to legislative changes. BaFin has also

found that FIs have a wide range of training options at their disposal, including web-based solutions, workshops and newsletters.

303. FIs are aware of the obligation to apply group-wide AML/CFT policies. Audit report findings indicate that there are moderate improvements needed in this area.

**Table 5.3. FIs' audit findings relating to group-wide policies (2019)**

	No/minor deficiencies	Moderate deficiencies	Major deficiencies	Serious deficiencies
2017	270	11	3	0
2018	304	12	3	0
2019	476	28	3	1
2020	335	18	3	0

Source: German Authorities

304. BaFin and the FIs met during the on-site are of the view that regulatory requirements do not cause any major problems that impede FIs from complying with AML/CFT rules. Some global banks indicated that they face challenges due to divergent data protection obligations. This could theoretically be an impediment to collating global data for risk analysis purposes. However, institutions indicated that these challenges were usually resolved in a satisfactory manner. BaFin has also observed that these banks are actively working on solutions to appropriately balance their data needs against data protection requirements.

#### *DNFBPs*

305. Large DNFBPs, including legal and accounting firms, REAs and DPMS that are part of a national or international group, and casinos, have generally adopted AML/CFT compliance programs. These entities typically have compliance officers or departments, and offer training programs to their staff. Entities operating across borders are aware of their obligation to apply the stricter AML/CFT requirements.
306. Other DNFBPs, particularly smaller entities and sole-traders, have more limited programmes in place. While those interviewed tended to have a compliance officer, this function was not always independent. Staff training is not always regular and compliance programmes are not consistently documented. These issues are exacerbated at entities that receive limited supervisory engagement. In addition, as certain DNFBPs (particularly smaller DPMS, TCSPs and lawyers) are less aware or unaware of all of their AML/CFT obligations, they will not have relevant programmes in place.

## Overall conclusions on IO.4

Preventive measures in the financial sector (including VASPs) are steadily improving, although smaller entities (including some regional/niche banks and money service businesses) face challenges implementing effective AML/CFT measures. The need for sustained remediation measures in relation to several large banks suggests that the size, complexity and global reach of this sector is likely to continue to pose ongoing challenges in effectively mitigating their risks. While some larger DNFBPs, particularly major legal or REA firms or large-scale DPMS, generally understand their risks and obligations, there are major deficiencies in DNFBPs' implementation of preventive measures. CDD requirements, including relating to beneficial ownership, are not clearly understood across the DPMS sector. In the legal and accounting sectors, larger and multi-service institutions face challenges knowing when to conduct CDD and maintain records and the complex supervisory regime impacts understanding of their obligations. Smaller DPMS, TCSPs and sole legal or accounting practitioners are less aware or may be unaware of their AML/CFT obligations and therefore have more limited preventive measures or even none. These issues were weighted heavily as they apply to entities in some higher risk sectors.

There are also major shortcomings in obliged entities' compliance with their reporting obligations. STR reporting numbers are low for non-banks and DNFBPs and, until recently, were also lower than expected for banks in light of Germany's risks and context. This raises questions as to the depth of understanding and implementation of AML/CFT measures. Conversely, there are indications that recent increases in reports from FIs, particularly banks, may be in part due to defensive reporting. The extremely low reporting from DNFBPs is in part due to serious difficulties dealing with legal professional privilege. While notary reporting has increased in relation to real estate transactions, widespread confusion related to privilege restricts reporting in most other instances. Given the risks in these sectors, these shortcomings were weighted heavily.

**Germany is rated as having a moderate level of effectiveness for IO.4.**

## Chapter 6. SUPERVISION

### Key Findings and Recommended Actions

#### Key Findings

- a) All regulated activities under the FATF Standards are subject to AML/CFT supervision in Germany. BaFin, the main FI supervisor, implements a satisfactory framework for supervising the financial sector. BaFin has seen an evolution in its approach to AML/CFT supervision, including structural reforms in response to changing risks and instances of non-compliance. The assessment was undertaken against the backdrop of a recent high-profile failing in the financial sector. While AML/CFT supervision was not directly implicated, BaFin was subject to allegations regarding its operations, particularly the proper handling of its wider supervisory activities. This incident led to structural reforms in early 2021. BaFin has a strong understanding of the ML/TF risks in its supervisory population. Supervisory measures are generally applied in accordance with risk and are usefully informed by, but do not rely on, FIs' annual external audits. However, in some higher risk non-bank sectors there is a low level of independent supervisory activity from BaFin.
- b) The large number of DNFBP and other financial supervisors (over 300) and a lack of knowledge of the extent and features of the extensive supervisory population (approximately 1 million entities) create major difficulties in ensuring a consistent risk understanding. Risk-based supervision varies considerably between these supervisors. While risk is a consideration for DNFBP supervisors, they generally do not consider all relevant risk factors and variables in fully actualising a risk-based approach and supervisory strategy. Supervision in general is limited due to the large supervised population and a critical lack of resources for the supervision of almost all DNFBP sectors. Coordinating the large number of supervisors poses challenges resulting in an overlap in supervisory responsibilities and multiple obligations reporting entities have to address, and inhibiting a broader risk-based approach to DNFBP supervision.
- c) Supervision of terrorism-related TFS obligations is separate from other AML/CFT obligations. For most FIs, supervision of TFS obligations is shared by BaFin and the Deutsche Bundesbank. While this results in some overlap, FIs are generally subject to adequate supervision. However, information on shortcomings is not routinely shared between the two supervisors to ensure appropriate remedial measures

are taken. There is no clear supervisor of TFS obligations for casinos, REAs, DPMS, TCSPs or insurance intermediaries, and limited practical TFS supervision for other DNFBP sectors.

- d) BaFin appears to apply satisfactory measures to prevent criminals and associates from entering the market, although the low number of rejections and a lack of data on application withdrawals makes it difficult to definitively form a conclusion on the robustness of controls. A dedicated team takes steps to identify unauthorised FIs, but could take a more proactive approach to unlicensed MVTS providers, especially *hawala* operators. The remaining FIs not supervised by BaFin (certain insurance entities) are subject to measures to prevent and detect criminals and associates entering the market, although proactive ongoing checks to identify unauthorised operators are more limited.
- e) DNFBP sectors that are subject to licensing/authorisation (REAs, the legal profession, accountants, and casinos) tend to have measures in place to prevent and detect criminals and associates entering the market. The DPMS sector has more limited measures to safeguard market entry, and there are no measures in place for the TCSP sector. Outside the casino sector, measures to identify unauthorised DNFBP providers are largely reactive.
- f) BaFin applies a range of remedial measures and sanctions, including recently using business restrictions to positive effect. However, measures in particular cases (including involving major banks) have not always ensured prompt remediation of non-compliance or prevented repeated breaches. While a range of outreach is provided, guidance is often targeted at FIs with a retail and domestic business model and is not sufficiently tailored to all sectors.
- g) While DNFBP supervisors have access to a range of remedial tools, these are used to a limited extent and not always in a proportionate manner. Supervisors of the legal professions (lawyers and tax advisors<sup>54</sup>) have only recently been able to apply fines, so there are few instances of them using this tool in practice. The impact of supervisory engagement in DNFBP sectors is unclear.

<sup>54</sup> Tax advisors are only captured in the FATF requirements (and covered in this report) to the extent that they fall within the definition of lawyers, other legal professionals or accountants undertaking the functions set out in R.22. In practice, tax advisors in Germany may be involved in the creation, operation or management of companies, legal persons or arrangements.

## Recommended Actions

- a) Enhance DNFBP supervision by:
  - a. Substantially increasing the resources available for DNFBP supervision including both human capital and technical capabilities, in line with the risks posed by these sectors and the number of entities under supervision.
  - b. Adopting measures to develop a consistent approach to DNFBP supervision that goes beyond co-ordinating risk information and moves towards more harmonised supervision in line with the risk-based approach, including by considering a mechanism for oversight of DNFBP supervision across Germany.
  - c. Enhancing the sources of information available to DNFBP supervisors to strengthen their risk-based approach, including obtaining information on the size and activities of the TCSP sector, and using data from tax authorities on DNFBP sectors to provide a clearer picture of the supervised sectors.
  - d. Considering a more vigorous risk-based approach to the broad range of obliged entities in the non-financial sector to focus on high or medium risk activities.
- b) Improve awareness and compliance by:
  - a. Increasing supervisors' use of sanctions, including BaFin's use of business restrictions and personal accountability as appropriate in light of the level of dissuasiveness of these measures;
  - b. Working with the private sector to develop more tailored guidance and targeted outreach for specific FI and DNFBP sectors, and considering adopting outreach strategies to enhance effectiveness.
- c) Improve fit and proper checks by:
  - a. Ensuring all DNFBP sectors are subject to adequate fit and proper checks or other robust controls (at market entry and on an ongoing basis) and that these checks are sufficient to identify criminal associates and strawmen.
  - b. Adopting a more proactive approach by BaFin to the prevention and detection of unlicensed MVTS providers, including informal value transfer services, especially *hawala* operators.
- d) Keep BaFin's existing supervision model under review to ensure that it continues to deliver an effective and graduated risk-based approach to supervision. In this regard, BaFin should:
  - a. Consider introducing a multi-year element to its supervisory planning with a view to ensuring all higher risk entities are subject to inspection by BaFin over a defined period commensurate with their risk profile.
  - b. Assess the level of inspections it carries out itself each year of higher risk non-bank FIs to ensure entities are subject to regular supervisory activity by BaFin commensurate with their risk profile.
  - c. Continue with its plans to focus its supervisory activities on VASPs (particularly those newly captured as FIs) to enhance its risk understanding and apply an

appropriate level of supervision to ensure that adequate controls are in place to address the risks.

- e) Improve the data and statistics available in relation to supervision, in particular by maintaining statistics on applications, rejections and withdrawals in relation to fit and proper checks for the FI and DNFBP sectors.
- f) Consider whether BaFin's institution-level risk assessment would benefit from further exploiting any additional data and information available from prudential supervisors within BaFin, in other jurisdictions and the European Central Bank.

307. The relevant Immediate Outcome considered and assessed in this chapter is IO.3<sup>55</sup>. The Recommendations relevant for the assessment of effectiveness under this section are R.14, 15, 26-28, 34, 35 and elements of R.1 and 40.

### Immediate Outcome 3 (Supervision)

- 308. FIs are supervised by BaFin, with the exception of certain insurance entities that are supervised at the *Land*-level by DNFBP supervisors (see R.26). The assessment was undertaken against a backdrop of a recently publicised high profile failing in the financial sector and allegations of improper handling of prudential supervision by BaFin. The assessment team noted that in response to these matters, BaFin has gone through a period of structural reform, including changes in the senior leadership of the organisation.
- 309. There are over 300 different supervisors in the non-financial sector, including DNFBPs.<sup>56</sup> In many cases, there are multiple DNFBP supervisors per sector per *Land* (see R.28). For practical reasons, the assessors were not able to interview representatives of all the DNFBP supervisors but have relied on interviews from larger and smaller *Land* supervisors, including those operating in higher-risk regions.
- 310. Positive and negative aspects of supervision were weighted most heavily for banks; heavily for MVTs and money service businesses, VASPs, real estate agents (REAs), notaries, lawyers and other legal professionals (including tax advisors) and accountants; moderately heavy for securities, e-money and payment service providers (other than MVTs), DPMS, and TCSPs; and less heavily for casinos and the insurance sector. This weighting is based on the relative importance of each sector and Germany's risks, context and materiality. See section 1.4.3 for more detail about the risk, materiality and weighting of each sector in Germany's context, and section 1.4.6 for a description of Germany's supervision arrangements.

<sup>55</sup> When assessing effectiveness under Immediate Outcome 3, assessors should take into consideration the risk, context and materiality of the country being assessed. Assessors should clearly explain these factors in Chapter One of the mutual evaluation report under the heading of Financial Institutions, DNFBPs and VASPs, as required in the instructions under that heading in the Methodology.

<sup>56</sup> Germany's AML/CFT obligations apply to a broad range of non-financial institutions, beyond those covered by the FATF Recommendations. For the purposes of this report, references to "DNFBPs" refer only to those sectors defined as DNFBPs under the FATF standards (casinos; real estate agents; DPMS; lawyers, notaries and other independent legal professionals and accountants; and TCSPs). References to the "non-financial sector" refer to Germany's broader population of non-FI obliged entities.

311. The conclusions in IO.3 are based on: statistics and examples of supervisory actions provided by Germany; guidance issued by supervisors; discussions with BaFin, certain Länder supervisors and FI and DNFBP sector representatives and review of publicly available and confidential reports on the effectiveness of AML/CFT supervision in Germany.

### *Licensing, registration and controls preventing criminals and associates from entering the market*

#### *BaFin (FIs, including VASPs)*

312. BaFin applies controls to prevent criminals and their associates from infiltrating FIs. Controls include licensing (authorisation) procedures, procedures for acquisition of qualifying holdings, and fit and proper assessments. Fit and proper checks are conducted on FIs' proposed management board and administrative board members and beneficial owners. This occurs both at market entry and on an ongoing basis, including in relation to proposed acquisitions of qualifying holdings in a FI. A positive decision is not required for an appointment to the administrative board to be made; however, FIs often wait for positive feedback before appointing management board members in particular as BaFin has the power to remove unfit individuals.
313. Applicants are required to provide a signed declaration of any criminal or administrative offence proceedings, decisions under trade law, and insolvency or enforcement proceedings. BaFin cross-checks this information against the central register of criminal proceedings, a certificate from the Federal Office of Justice (BfJ) on the applicant's criminal conviction status, and certificates of good conduct from the individual's countries of residence over the last ten years. Relevant criminal or administrative convictions, pending proceedings, or enforcement or supervisory measures will raise material concerns regarding a proposed candidate. Where concerns arise, BaFin will conduct a more thorough investigation, including enquiries using commercial due diligence software/tools, information requests to the FIU and intensified media research, which would better enable the identification of criminal associates. In 2020, BaFin updated the process manual for banking supervision so that fit and proper checks include systematic commercial database screening and the intensified involvement of BaFin's AML/CFT Department. BaFin has issued guidance on fit and proper checks for each sector and also observes the EU Joint Guidelines on the assessment of acquisitions and qualifying holdings in the banking, insurance and securities sectors.

314. VASPs are licensed as financial service institutions under the Banking Act (KWG) in Germany, meaning these requirements apply equally to VASPs. In 2020, Germany created a specific license for virtual asset custody businesses (wallet providers) that were previously exempt from licensing requirements. As at November 2021, 20 entities are licensed by BaFin as virtual asset custody businesses (3 of which have finished the licensing process and 17 are operating under a preliminary license, having been grandfathered in under the new regime<sup>57</sup>). An additional nine applications are pending (without the right to conduct business). In addition to the regular fit and proper checks, BaFin's AML Department is conducting interviews with applicants prior to licensing.
315. In the banking sector, BaFin receives and processes approximately 1 100 notifications regarding management board members annually (see table 6.1 below). The number of rejected candidates is very low: 30 rejections in total between 2017 and 2020. BaFin considers that this is for two reasons. First, because institutions often make preliminary enquiries prior to submitting an application. And secondly, because institutions are aware of the robust controls and refrain from proposing candidates who would not meet the requirements. Given the high number of notifications processed by BaFin, it follows that there should be instances where FIs withdrew notifications after BaFin's enquiries identified concerns. However, while BaFin provided a small number of case examples of withdrawn notifications, no statistics on withdrawals were available to demonstrate the robustness of controls. Maintaining such statistics would allow BaFin to better track the effectiveness of its processes. Case studies of ML investigations and prosecutions provided by Germany included a very small number of cases where criminals were able to take ownership of FIs. However, these cases were largely historical (dating around 2010) and BaFin's controls have improved since this time, including: implementing a two-step process targeted at ML/TF prevention, fundamental revisions to BaFin's internal guidance on vetting management and supervisory body members, organisational changes to ensure consistency and effective information-exchange, and the establishment of internal whistleblowing platforms (with mechanisms for exchanging information received with licensing teams). The controls now in place are sufficiently robust to address the risk of instances of this nature reoccurring.

**Table 6.1. Fit and proper assessments in the banking sector**

	2017	2018	2019	2020
Notifications received	1 118	1 080	1 178	961
Approved	1 114	1 072	1 165	956
Declined	4	8	13	5

Note: Figures include all notifications regarding applicants and management board members. There is a two-step approach for applications from management board members – both the intention to appoint a management board member and the appointment itself must be notified to BaFin. These two notifications are counted separately.

Source: German Authorities

<sup>57</sup> These grandfathered VASPs are operating under a preliminary license, under which they are not allowed to conduct any virtual asset custody business. These institutions are subject to the same fit and proper checks as all other FIs.

316. BaFin's Integrity of Financial Systems Directorate (IFSD) is dedicated to combatting unauthorised business conduct in the financial sector. IFSD employs 23 FTE. On average, IFSD conducts 1 100 investigations and 85 enforcement proceedings annually. Investigations are triggered by various sources, including STRs, consumer complaints, media reports, and whistle-blower information. During an investigation, IFSD is able to exercise powers to request information, conduct on-site inspections, search premises, and seize evidence. If a breach is detected, IFSD can issue cease and desist orders and additional instructions, publicise orders, and appoint a suitable person to liquidate the business. IFSD exercises these powers not only against those conducting unauthorised business, but also against third parties aiding the unauthorised activity (e.g. internet service providers, intermediaries, trustees, etc.). Powers are also used against foreign entities actively marketing their services in Germany. IFSD takes a proactive approach to identifying unlicensed VASPs; however, they are less proactive with respect to unlicensed MVTs including informal value transfer services, especially *hawala* services.

**Table 6.2. IFSD investigations and enforcement actions (2017-2020)**

	2017	2018	2019	2020
New investigations	1 042	1 318	1 007	1 436
Enforcement actions	25	87	150	176

Source: German Authorities

#### *DNFBP supervisors*

317. DNFBP sectors that are subject to licensing tend to have measures in place to prevent and detect criminals and associates entering or operating in the market, while measures for unlicensed DNFBP sectors (DPMS and TCSPs) are more limited. In general, DNFBP licensing authorities take a reactive approach to detecting unauthorised business.<sup>58</sup>

<sup>58</sup> As with FIs, the licensing of DNFBPs is generally performed by a different team that AML/CFT supervision.

*Land and district governments (REAs, DPMS, TCSPs, casinos and certain insurance entities<sup>59</sup>)*

318. Casinos, REAs and insurance providers are required to be licensed, and are therefore subject to more intensive market entry requirements. Licensing of these sectors is the responsibility of *Land*/district governments, with the specific authority varying depending on the *Land*. Licensing and AML/CFT supervision do not always under the same responsibility of the same government institution. Licensing authorities conduct fit and proper checks upon authorisation and on an ongoing basis. This involves checking the applicants, management and third party representatives' criminal record, regulatory record and financial soundness. Authorities check registers and make requests to the tax authorities rather than relying on self-disclosure. In the case of casinos and insurance providers, information is also obtained on ownership structures, voting rights and shareholdings, which may help identify criminal associates. This is not the case for real estate agents, which are licensed as an individual and are not subject to checks on any broader firm structure. The Darmstadt Regional Administration (a local government) continuously reviews online gambling providers, providing an overall view of both legal and illegal operators (including illegal online casinos). The Darmstadt Regional Administration has identified 232 websites offering illegal online gambling services in Germany (including non-casino gambling services that fall outside the FATF scope). This information is shared with licensing and AML/CFT authorities, as well as the Ministry of the Interior in Lower Saxony, which can initiate proceedings with payment service providers to prevent payments to these services.
319. DPMS and TCSPs are not subject to a licensing regime, but are required to notify the relevant trading standards authority when they establish their business. For DPMS, the trading standards authorities conduct a reliability check, involving a criminal and regulatory record check. This occurs upon receiving notification (i.e., after the business is established); criminal ownership or involvement can therefore only be identified post-hoc. Reliability checks of DPMS are focused on the applicant, meaning there are no measures to proactively identify a criminal beneficial owner, or involvement of criminal associates. Authorities confirmed this would only be identified at a later stage, either in the course of regular supervisory activities or tip-offs. TCSPs are not subject to any registration, licensing or reliability check, which contributes to a lack of information on the size and activities of this sector.

---

<sup>59</sup> As explained in Chpt.1.4.3, Germany has three economically insignificant insurance companies and 81 061 insurance intermediaries that supervised at the Länder-level. The reference to "insurance entities" refers to these entities.

320. Courts and prosecution offices are required to notify licensing authorities (for REAs, casinos and insurance providers) of criminal convictions or civil proceedings relating to their licensed population. They must also notify the trading standards authority of any such proceedings relating to DPMS or TCSPs. This allows for some level of ongoing fit and proper checks for these sectors, although on a reactive basis. With the exception of casino supervisors, licensing and trading standards authorities are largely reactive in identifying unauthorised businesses and generally depend on consumer complaints and tip-offs. Statistics are available on the number of applications, withdrawals and rejections for all traders (including DPMS), but cannot be isolated for DNFBP sectors. This makes it difficult to determine whether fit and proper and reliability requirements are being applied effectively to these sectors in practice.

**Table 6.3. Trading permit applications, refusals and withdrawals (2018-2019)**

	2018		2019		2020	
	Owner-run businesses	Legal entities and associations	Owner-run businesses	Legal entities and associations	Owner-run businesses	Legal entities and associations
Registered persons/entities	309 861	22 291	343 612	22 672	341 235	23 890
Permits refused (2018)	246	78	298	139	301	141
Withdrawals and revocations (2018)	641	112	694	162	555	148
Bans imposed	4 612	333	4 342	344	3 760	330

Note: The figures above cover all trading entities. This includes DPMS, real estate agents, TCSPs and insurance intermediaries. It also includes other companies, such as those in the service sector.

“Bans imposed” refers to business prohibitions for businesses that do not require a separate license, which includes DPMS and TCSPs.

Source: German Authorities

*Professional body supervisors (accountants, notaries, and the legal profession)*

321. Accountants, notaries and members of the legal profession (lawyers and tax advisors) are subject to fit and proper checks upon authorisation and on an ongoing basis (including through the requirement for courts and prosecution offices to notify authorities of criminal convictions or civil proceedings). Authorisation is generally the responsibility of the same professional bodies as AML/CFT supervision, but may be undertaken by a different team/individual. Authorisation requirements apply to individual practitioners, management and beneficial owners of companies and partnerships. Most professional bodies check the criminal register (which shows criminal convictions), and request a self-disclosure on financial soundness. However, the Chamber of Accountants relies on self-disclosure for all elements, including criminal record checks. A criminal conviction, including for ML, is not a definitive ground for preventing an individual from practising (see box 6.1 below). There is no proactive strategy for identifying unlicensed providers. While no statistics are available, case studies suggest professional bodies actively respond to fit and proper issues when malpractice is identified, although sanctions are relatively weak. Revocations of authorisation are rare because the accused entity generally withdraws from the profession voluntarily (often with supervisory encouragement) as this is a mitigating factor for sanctioning in any related criminal

proceedings. Where bans are imposed, they can be relatively short given the identified misconduct (see box 6.1 below).

### Box 6.1. Bar association partial ban in response to ML

The Berlin regional court sentenced a lawyer to a suspended prison sentence of 18 months for three counts of ML. The lawyer had received a considerable amount of cash from his client and held it in safekeeping despite knowing that the money was the proceeds of crime. The Court noted that “An order banning the exercise of the profession ... was not considered as an option” as it was the lawyer’s first offence and he had since distanced himself from the client. Following a *MiStra* notification, the Berlin Bar Court imposed a partial ban on exercising activities in the field of criminal law for a period of 18 months.

Source: German Authorities.

### Supervisors’ understanding and identification of ML/TF risks

#### *BaFin (FIs, including VASPs)*

322. BaFin has a strong understanding of the ML/TF risks faced by its supervisory population. This understanding is informed by various sources, including its supervisory activities, data from FIs’ annual audits, questionnaires, feedback from the FIU on STRs, and engagement with policy and LEAs regarding emerging risks. BaFin contributed to the NRA and uses the NRA and the SNRA to inform its own risk understanding. Since 2017, BaFin has produced a financial sector risk assessment (SRA) at least annually, which provides a detailed, nuanced assessment. The SRA classifies risk by sector and subsector, and also ranks the inherent risk of products and services according to sector (acknowledging that the same product can pose a different risk in different sectors). In some cases, the SRA recognises that certain subsectors comprise institutions with very different characteristics; BaFin therefore breaks these subsectors down into even more specific groups to allow for a more detailed risk understanding.
323. As VASPs are required to be licensed as financial services institutions in Germany, the SRA does not consider each type of VASP as a separate sub-sector, but assesses the risks related to virtual assets as part of the product/service risk assessment. The exception is virtual asset wallet providers, which are licensed and assessed as a separate sector (“crypto custodians”). BaFin’s risk understanding related to VASPs is more developed than that reflected in the NRA. While the NRA rated the risk as medium-low, BaFin considers that the risks have evolved since this time as the NRA was based on information from before 2019, and this is a rapidly changing sector. Consequently, BaFin currently views VASPs as an emerging area of potential higher risk. Wallet providers are rated medium-high risk, in part due to the newness of the sector and the resulting limited supervisory information.

324. BaFin also assesses individual institution risk on an annual basis.<sup>60</sup> The risk assessment system (BAKIS) considers inherent risk factors, such as complexity of operations, geography, customers, products and services, and delivery channels. It then considers the quality of controls (with AML/CFT controls assessed separately to other preventive measures). These two elements are combined to give a residual risk score. Risk scores are subject to automated and regular cross-checking, and BaFin makes ad hoc updates if any new information arises. BaFin uses both qualitative and quantitative information to develop and support its risk model. Quantitative information includes data in relation to higher risk scenarios, such as the number of higher risk customers and also data with respect to the value and levels of activity. For newly licensed virtual asset wallet providers, BaFin’s AML Department has been conducting supervisory interviews to obtain information on the institution’s business model to feed into the risk assessment (both at an institution level and sectoral level). BAKIS information is shared with prudential supervisors and the European Central Bank, but incorporating further information from these sources in addition to the data already utilised could further enrich BaFin’s risk modelling.

**Figure 6.1. Individual risk classification in the banking sector (2020)**

	A	B	C	D
1	363	102	13	1
2	740	235	37	7
3	19	23	10	8

**Figure 6.2. Individual risk classification in the non-banking sector (2020)**

	A	B	C	D
1	651	19	24	6
2	334	31	23	6
3	26	5	3	2

<sup>60</sup> Individual risk assessments are updated every two years for smaller, lower-risk institutions.

Note: In Figures 6.1 and 6.2, A-D represent the quality of ML prevention/control environment with A denoting the highest quality. 1-3 represent the inherent risk with 1 denoting the lowest risk. Green represents lower risk, orange medium risk, and red higher risk. In total, 1 217 banks are lower risk (green), 292 are medium risk (orange), and 48 are higher risk (red).

The individual risk classification in the non-banking sector (Figure 6.2) is based on annual audit reports in 2020. No audit reports were available at that time for financial services institutions offering crypto custody business (as these were newly licensed institutions) and registered capital management companies (which were subject to reporting from mid-2021). MVTs agents are not subject to an annual audit requirement.

Source: German Authorities (BaFin)

325. BaFin engages with the FIU to further enrich its sectoral and institutional risk understanding. BaFin regularly requests information from the FIU on specific institutions as part of its supervisory activity (see below). With this information, BaFin creates its own STR analyses that compare the reporting activity of similar institutions. These analyses assist with the identification of issues with the completeness or timeliness of reporting by certain sectors or individual FIs. While the FIU does not include feedback on the quality of reports (for investigation purposes), these analyses help identify anomalies with respect to the level of reporting by FIs in comparison to their peers. BaFin uses these analyses to inform and target its supervisory activities at those outlier sectors and individual FIs.

#### *DNFBP supervisors*

326. The risk understanding amongst DNFBP supervisors is varied and efforts to understand risks are evolving, meaning risk understanding is impaired in certain areas. The large number of DNFBP supervisors poses challenges in achieving a consistent risk understanding, although the recent NRA and *Länder* risk assessments have helped in this respect. The lack of knowledge of the extent and features of the supervisory population hampers many DNFBP supervisors' risk understanding.

#### *Land and district governments (REAs, DPMS, TCSPs, casinos and certain insurance entities)*

327. The level of understanding of ML/TF risk varies between *Land* and district government supervisors responsible for AML/CFT supervision of REAs, DPMS, TCSPs, casinos and certain insurance entities. Developing and maintaining a holistic understanding of risk is a challenge for supervisors. Prior to 2020, supervisors' developed their own understanding of risk, resulting in an uneven and varied understanding. In 2020, for the first time, the *Länder* risk assessments presented a co-ordinated and holistic summary of authorities' risk understanding. The *Länder* risk assessments assess the regional risks in the non-financial sectors (including DNFBPs) and *Länder*-supervised insurance entities. These assessments take into account and are consistent with the NRA and SNRA findings. *Länder* risk assessments vary in depth and quality. In general, they are informed by available data (including STR data), law enforcement information and supervisory information. The risk factors considered are a mix of general and ML/TF specific factors, including the size of the sector, services performed, transaction numbers and values, customer profiles (which rarely includes PEP exposure), and exposure to higher ML/TF risk transactions or jurisdictions (based on the NRA). Information on each of these points is rarely included for every sector and in some cases only one or two factors are considered. For many sectors, the risk assessments include limited information on the extent of compliance controls (and consequential

vulnerabilities). The risk assessments are also limited by information gaps, some of which are significant (e.g., the number of TCSPs or exact number of DPMS operating in the region). The assessments draw on data on the number of companies and sales in relevant sectors. In light of the information gaps, additional data (e.g., from the tax administration) is required to provide a clearer picture of the size, operations and risks of the DNFBP sectors. The large number of obliged entities in the non-financial sector (including DNFBPs) and insufficient supervisory resources hamper supervisors' ability to develop a complete and consistent risk understanding.

328. Understanding of risk at the institution level is limited. The *Länder* or district government supervisors generally do not have tools or risk matrixes to consistently and comprehensively assess institution risk. Some supervisors use questionnaires to obtain certain institution-specific information; for example, the Bavaria supervisors of REAs and DPMS (the district governments) send questionnaires to certain entities to obtain information on business structure or volume of transactions. However, as efforts to understand risk are evolving, questionnaires are generally sent to a random sample of entities. Responses have typically been used to identify inherent sectoral risks or as a first step in the inspection process (e.g., to ensure the institution is an obliged entity). Nonetheless, some supervisors are increasingly using this information to identify subsectors or even institutions that present greater risks.
329. In practice, *Länder* and district government supervisors have a good understanding of the risks in their sectors as they relate to real estate and cash, in line with the NRA and Germany's national focus on this area. The understanding of the risk of DNFBPs being used for complex and international ML activity is weaker. While certain supervisors (e.g., in Berlin) have an emerging understanding of the risks related to TCSPs (due to their ability to help obscure ownership structures), most supervisors have a limited understanding of risks in this area. This is further limited by the lack of data on the number of TCSPs in Germany and the services provided.

*Professional body supervisors (accountants, notaries, and the legal profession)*

330. In 2020, AML/CFT supervisors for accountants (the Federal Chamber of Accountants) and the legal profession (27 regional bar associations and 21 regional chambers of tax advisors) summarised and documented their risk understanding for the first time. Each supervisory agency conducts its own, separate risk assessment, although these are based on agreed benchmarks. The risk assessments are based on a series of questionnaires from a sample of the total population, which for lawyers will include non-obliged entities. Legal professional supervisors (chambers of lawyers and tax advisors) generally send the questionnaire to a sample of up to 10% of registered professionals, while the Federal Chamber of Accountants sends questionnaires to 1% of accountants. The questionnaires provide a picture of risk, but are based on relatively blunt factors such as the number of higher-risk transactions and number of compliance breaches. Questionnaire responses are fed into a risk matrix that provides an institution-level risk rating for surveyed entities. While these efforts are positive, they remain recent. As a result, sectoral and institution level risk understanding remains limited and relatively high-level. A deeper and more nuanced understanding is also hampered by a lack of concrete knowledge of the number of obliged entities in the legal sector.

331. Until 2020, the 115 *Länder* courts that supervise notaries developed their own individual risk understanding. This was brought together into a documented, holistic assessment in the *Länder* risk assessments. The depth of assessment of notary risk varies between *Länder* assessments; in some cases the assessment is relatively shallow despite the recognised higher risk in this sector. In general, notary supervisors do not undertake institution-level risk assessments. One exception is the Berlin Notary Supervision Task Force (see Box 6.3). As with the legal profession, risk understanding of most notary supervisors is limited by the recency of holistic risk assessments and efforts to understand risk. As with other DNFBP supervisors, professional body and notary supervisors have a focus on the risks of ML through real estate and are sensitive to how their population can be used for such transactions. Understanding of risks relating to professional enablers, international ML schemes, or complex corporate structures is generally more limited.

### *Risk-based supervision of compliance with AML/CFT requirements*

#### *BaFin (FIs, including VASPs)*

332. BaFin applies a graduated risk based approach to supervision of FIs. BaFin moved to a risk-based supervisory approach in 2006 (although the approach was much less developed for the non-bank sectors), and has worked to refine this approach. Its current supervisory model, which increased the focus on risk-based supervision of the non-bank sector, has been in place since 2019. BaFin's risk-based approach is reflected in its organisational structure. BaFin's AML Department was restructured in 2017 and given 32 additional FTE to better respond to identified risks in the banking sector. An additional 12 FTE were added in January 2020 to respond to risks in the non-bank sectors. The Department contains eight divisions, with 130 FTE (as at November 2021, 105 staff were in place).<sup>61</sup> Staff are distributed according to risk with more staff dedicated to supervising the highest-risk institutions (see table below). In light of the recent staff increases, BaFin should continue to ensure that it recruits and retains staff with the appropriate mix of skills and experience, in particular those with practical experience and knowledge of the financial sector.

**Table 6.4. Structure and resources of BaFin's AML Department (as at November 2021)**

Division	Focus	Targeted FTE	Current FTE
GW 1	Europe and Strategy	15	14
GW 2	Policy Issues and FATF	13	12
GW 3	Supervision of 2 major banks, foreign branch offices	13	12
GW 4	Supervision of credit institutions under intensified supervision	14	10
GW 5	Supervision of other credit institutions, field relating to co-operative network institutions	23	13
GW 6	Supervision of non-banking financial sector (1)	13	10
GW 7	Supervision of non-banking financial sector (2)	9	8
GW 8	Management of account data retrieval system	30	26
	Total	130	105

Source: German Authorities

<sup>61</sup> Twenty additional positions were approved from 2022.

333. A notable feature of Germany's system is that most FIs are subject to an annual external audit,<sup>62</sup> which includes an AML/CFT element that assesses compliance with all statutory AML/CFT obligations. This also allows BaFin to collect ML/TF-related data, including on FIs' business activities and models. Auditors are appointed by the FI, but BaFin has the option of rejecting the appointed auditor and it provided examples where it exercised this option as necessary to ensure auditors' competence and independence. BaFin's involvement in the audit process varies according to risk; for higher risk entities, BaFin's AML Department designates priority areas for deeper review during the audit or provides staff to support the audit, which assists in ensuring consistency in the application of the process. In the wake of a recent financial sector scandal, BaFin has undertaken a transformation project which has included intensifying ML-related information-exchange with auditors. BaFin is not solely reliant on the audit process to deliver supervisory coverage; it has significantly increased its own resources to undertake its own supervisory activities to supplement the audits and verify their results.
334. In line with the NRA, BaFin's SRA identifies the banking sector as the highest risk. BaFin has consequently developed separate approaches for supervising the banking sector and the non-banking sectors. The banking sector is divided into four categories (I through IV) according to risk, while the non-banking sector is divided into three risk categories (low to high). The intensity of BaFin's supervision varies from simplified to intensified supervision according to the risk category (see tables 6.5 and 6.6 below).
335. BaFin uses a range of on-site and off-site tools to supervise its population. On-site tools include setting priority areas for external audits, support for external audits, inspections by BaFin (which can last from a few days to several months on-site), special inspections (by independent third parties), and supervisory visits. Priority areas for external audits are set in line with identified risks and areas of vulnerability, with the goal of improving compliance and/or obtaining more information in a particular area. In 2021, priority areas included: MVTs, STR reporting, VASPs and virtual assets, insurance-wrapping, third-party acquiring and opaque corporate structures. Since 2019, BaFin has produced an annual supervisory programme that sets out the type and frequency of supervisory actions, taking into account the FIs' risk ratings, the number of supervised FIs, staff capacity, and BaFin's supervisory priorities (which are determined annually based on the NRA, SRA and supervisory information). Prior to 2019, supervisory planning was unit-based (i.e., undertaken at the individual division level). In theory, the frequency, intensity and scope of actions is commensurate to the individual FI's risk rating (see tables 6.5 and 6.6 below). However, pursuant to the 2020 and 2021 programmes, few inspections or other measures were undertaken of the eight highest-risk non-bank FIs (although they were subject to an external audit). The COVID-19 pandemic has had an impact; for example, as a result of this uncertainty, the 2021 programme anticipated fewer on-site measures. While there was some increase in more flexible measures (such as increased audit support visits), it is not clear the reduction in on-site measures was entirely mitigated. The approach of developing an annual programme may inhibit BaFin's ability to take a holistic,

---

<sup>62</sup> A two-year audit cycle can be applied for institutions with total assets of less than €400 million, but only where it would be appropriate on basis of the institution's ML/TF risk profile. Agents are not subject to an audit requirement.

longer-term view to ensure all higher risk entities are subject to a regular inspection by BaFin.

**Table 6.5. Supervisory programme for the banking sector (2020 and 2021)**

	Category I: intensified supervision		Category 2: enhanced supervision		Category III: basic supervision		Category IV: simplified supervision	
	2020	2021	2020	2021	2020	2021	2020	2021
<b>On-site measures</b>								
External audit	100%	100%	100%	100%	100%	100%	100%	100%
BaFin defines priority areas for audit	68%	67%	20%	8%	1%	1%	0%	-
BaFin support for audit	20%	30%	20%	0%*	1%	0%*	0%	-
BaFin inspection	60%	27%	36%	17%	17%	3%	0.2%	0.3%
Special external inspection	8%	15%	-	-	-	-	-	-
Supervisory visit	100%	36%	11%	25%	2%	4%	0%	-
<b>Off-site measures</b>								
Supervisory interview	100%	100%	50%	100%	6%	4%	0.1%	-
Request for information	100%	100%	71%	17%	25%	12%	2%	1%
FIU query	100%	67%	36%	33%	17%	3%	1%	0.3%
Questionnaires	100%	94%	100%	42%	-**	-	-**	-

\* BaFin support for external audits was reduced in 2020 due to COVID-19.

\*\* Action in these areas was event-driven and not included in the programme.

Note: Questionnaires are typically used for data collection, while a request for information is generally used to request information in advance of an inspection or audit (i.e. to obtain a full suite of policies, procedures, etc. and data from which to select samples of CDD, STRs, etc.).

Source: German Authorities

**Table 6.6. Supervisory programme for the non-bank sector (2020 and 2021)**

	High risk: enhanced supervision		Medium risk: basic supervision		Low risk: simplified basic supervision		Agents; high risk	
	2020	2021	2020	2021	2020	2021	2020	2021
<b>On-site measures</b>								
External audit	100%	100%	50%	100%	50%	75%	-	-
BaFin defines priority areas for audit	50%	6%	0.5%	1%	-	-	-	-
BaFin support for audit	-	3%	0.7%	1%	-	-	-	-
BaFin inspection	-	3%	0.5%	1%	-	-	0.4%	0.2%
Special external inspection	-	9%	0.2%	0.5%	-	-	-	-
Supervisory visit	-	3%	0.5%	1%	-	-	-	-
<b>Off-site measures</b>								
Supervisory interview	13%	100%	1%	4%	-	-	(5 CCPs)*	(6 CCPs)*
Request for information	50%	11%	4%	3%	0.5%	-	0.8%	1%
FIU query	100%	29%	1%	1%	-	-	0.1%	1%
Questionnaires	-	-	3%	7%	-	-	-	-

\* CCPs (Central Contact Points) are an EU mechanism by which payment and e-money institutions that operate through agents and have their head office in another EU Member State establish one single contact point in the host country to facilitate supervision by and communication with host regulators and to improve compliance and reporting.

Note: Questionnaires are typically used for data collection, while a request for information is generally used to request information in advance of an inspection or audit (i.e. to obtain a full suite of policies, procedures, etc. and data from which to select samples of CDD, STRs, etc.).

Source: German Authorities

336. BaFin recognises the importance of group wide compliance. BaFin has previously been overly reactive (rather than proactive) in this area, including in response to some highly-publicised instances of non-compliance in the mid-2010s. In these cases, BaFin was alerted to non-compliance and took action to audit foreign branches. These institutions were then subject to closer ongoing supervision in this area. More recently, BaFin has shown more proactive action. When supervising Germany's most significant global banks, BaFin conducts onsite visits outside of Germany and co-operates closely with supervisory authorities in other jurisdictions.

**Box 6.2. Group-wide supervision by BaFin**

BaFin conducted an onsite inspection of a major Germany bank in 2018. This covered the bank's implementation of group-wide policies and procedures, including procedures for information-exchange within the group. As part of its group-wide supervision of the bank, in 2019, BaFin conducted two onsite inspections at the institution's branches in Italy and Spain. These visits found deficiencies in one branch's reporting to the parent institution. BaFin also identified weaknesses in the branches' monitoring system, which was no longer used at the head office. The institution responded by making staff changes at one of the foreign branches to address the identified reporting deficiencies and introducing a new monitoring system for all but one branches. This was subsequently monitored by BaFin through monthly meetings and in the institution's annual audit, which covered implementation of the new system (including the monitoring system exception for one branch).

Source: German Authorities

337. BaFin has identified VASPs as a supervisory focus since 2019. Institutions with significant virtual asset products/services were put under intensified supervision in 2020 on the basis of identified risks in this area. For 2021, BaFin conducted several questionnaire campaigns to identify higher risk institutions. The findings led to additional questionnaires, supervisory meetings, 82 off-site inspections and 29 on-site inspections. BaFin has also expanded its supervisory programme to include sessions to sensitise AML officers and staff to risks related to virtual assets and provide information (including AFCA papers) on relevant red flags. Virtual asset products and services were identified as a priority area for external audits in 2019, 2020 and 2021; auditors were required to report to BaFin on the extent, type and value of virtual asset transactions and the nature of related AML/CFT mechanisms. In early 2021, BaFin asked the FIU to analyse STRs related to virtual assets and used this information to target particular FIs for a direct supervisory exchange. As at November 2021, BaFin was seeking approval to increase its staff by a further 20 FTEs with the intention that the additional resources would focus especially on VASPs.<sup>63</sup>
338. Supervision of FIs' implementation of TFS obligations is shared between BaFin and the Deutsche Bundesbank. In the course of its AML/CFT supervision, BaFin monitors FIs' compliance with their broader IT obligations, including TFS screening. The Bundesbank monitors FIs' compliance with the EU sanctions regimes (including freezing obligations, reporting obligations and screening systems) through regular, risk-based on-site inspections (see IO.11 in Chapter 4). While the separate but overlapping competencies appears to cause some confusion (at least among FIs met during the on-site), it does not appear to impede FIs' implementation of TFS (see IO.4) and, between the Bundesbank and BaFin, FIs are subject to TFS supervision.

<sup>63</sup> Following the on-site visit, BaFin received approval for this staff increase.

*DNFBP supervisors*

339. DNFBP supervisors have been required to implement a risk-based approach since 2017. However, in practice, risk-based supervision varies considerably between supervisors. While risk is a consideration for some supervisors, for the most part, supervisors do not consider all relevant risk factors and variables in developing a supervisory strategy and applying a risk-based approach. Supervision in general is limited due to the large supervised population in the broader non-financial sector and a critical lack of resources. Co-ordinating the large number of supervisors (over 300) poses challenges resulting in overlap and inhibiting a broader, consistent risk-based approach towards DNFBP supervision. The statutory framework for TFS supervision of DNFBPs is subject to some confusion, including in higher risk sectors (such as DPMS).

## CHAPTER 6. SUPERVISION

**Table 6.7. Supervisory measures for the non-financial sectors, incl. DNFBPs (2018-2020)**

	REAs			Traders (including DPMS)			TCSPs			Gambling (incl. casinos)			Notaries			Lawyers			Accountants and tax advisors*		
	2018	2019	2020	2018	2019	2020	2018	2019	2020	2018	2019	2020	2018	2019	2020	2018	2019	2020	2018	2019	2020
<i>Size of population</i>	30 324			Approx. 800 000 (of which, approx. 7 993 DPMS)			Unknown			19 169 (of which, 28 casinos)			6 912			36 791			101 383		
On-site inspection	185	415	97	503	643	270	2	11	0	313	443	211	1 923	1 512	1 522	15	16	93	452	391	322
Written inspection	511	594	575	1 001	845	530	5	2	197	956	999	1102	90	87	113	1 135	1 656	1 317	952	935	1 082
Additional/ other (e.g., questionnaires)	191	774	266	1 206	867	322	17	3	3	33	552	729	198	12	87	459	171	459	1	61	40

\* Separate data is not available for these sectors.

Note: This data includes measures that cover AML, but are not specific to AML (e.g., regulatory inspections of notaries). As Germany includes a wide range of non-financial sectors as obliged entities (e.g., high value dealers, sports betting, etc.), it is not possible to isolate data on only DNFBP sectors.

Source: German Authorities

**Table 6.8. Supervisory FTEs for AML/CFT supervision in the non-financial sector (incl. DNFBPs)**

	2018	2019	2020	Number of obliged entities
Lawyers	30	24	25.85	Approx. 36 791
Tax advisors	22.3	10.4	10.6	86 625
Notaries	67.8	50.7	47.74	6 912
Accountants	1.5	1.5	1.5	14 758
Gambling (incl. casinos)	44.9	47.7	44.98	19 168
Other non-financial sector entities (incl. DPMS, TCSPs)	77.1	85	98.78	Approx. 800 000 (of which, approx. 7 993 DPMS)

Note: As Germany includes a wide range of non-financial sectors as obliged entities (e.g., high value dealers, sports betting, etc.), it is not possible to isolate data on only DNFBP sectors. Lawyers are obliged entities only where conducting certain transactions. The number of obliged entity lawyers is based on an estimate by legal supervisors that 22% of all lawyers conduct such transactions.

Source: German Authorities

*Land and district governments (REAs, DPMS, TCSPs, casinos and certain insurance entities)*

340. In 2017, Germany amended the ML Act (GwG) to require risk-based supervision. This amendment was followed by the development of the NRA in 2019, and subsequent *Länder* risk assessments in 2020. These summarise *Länder* and district government supervisors' risk understanding and provide a documented basis for more consistent risk-based supervision. While the approach to supervision has changed since the last MER, supervision remains fragmented with an inconsistent application of the risk-based approach, in part due to the large number of supervisors, the low level of resources, and the size of the supervised population. *Land* and district government supervisors have access to on-site and off-site supervisory tools, although these are not consistently applied in a risk-based manner considering all relevant risk factors and variables (e.g., some measures are applied to a random segment of the population, or a lack of resources limits supervisors' ability to apply measures to all higher risk entities). Supervision of casinos is more developed, given the long-standing requirements in this area. However, casino supervisors still do not have a supervisory strategy that is informed by the full range of risk factors (for example, each obliged entity subject to a regular annual inspection regardless of risk).

- 6
341. In other sectors supervised by Land and district government supervisors, the risk-based approach is severely hampered by the scope of the supervised population, a critical lack of resources, and difficulties co-ordinating the large number of supervisors. The size of the supervised non-financial sector and information gaps regarding the supervised population results in supervisors taking a relatively simple approach to identifying entities for supervision or, in some cases, choosing a random sample of entities as the starting-point. It is not clear that DNFBP supervisors have a systematic plan to broaden engagement in a way that ensures all higher-risk entities are subject to regular supervision. For better-equipped supervisors, the intensity of supervisory measures applied are determined based on a limited number of risk-related factors. For example, in 2018, REAs in Berlin were subject to increased measures if their activities were wide in scope or involved higher-risk products. The number of TCSPs in Germany is unknown meaning some high risk entities may never be inspected. The number of FTEs responsible for DNFBP supervision is low across all sectors; for example, in Berlin, six FTE are allocated for supervising all traders in goods (including DPMS), REAs, TCSPs and insurance entities (approx. 7 391 entities). For the larger sectors, there is one FTE per several thousand supervised entities. Even better-resourced supervisors (such as gambling sector (including casinos) supervisors) have only one FTE per several hundred entities. While a portion of these entities will be lower risk, and therefore require less engagement, these figures are nonetheless far too low to ensure robust risk-based supervision. REA and DPMS supervisors note that due in part to limited resources, they rely primarily on off-site measures (rather than selecting measures based entirely on risk). Nonetheless, the total number of on-site inspections of REAs is increasing (from 28 across all of Germany in 2017 to 415 in 2019).
342. Co-ordinating the approximately 123 individual supervisors of REAs, DPMS, TCSPs and insurance entities is a challenge. Many entities, especially larger companies or those operating in multiple *Länder* will have more than one supervisor. With proper co-ordination and information-sharing, this overlap could help mitigate resource challenges. However, in practice this is not the case; during the on-site several obliged entities noted that a lack of co-ordination results in certain entities experiencing multiple inspections per year. Some preliminary measures exist to encourage information-sharing between supervisors; for example, supervisors attend an annual national symposium, the Darmstadt Working Group on ML Prevention, to share experiences. There is also good ad hoc and informal co-operation among certain *Länder* supervisors that face shared risks (particularly Berlin and Brandenburg). However, this is largely informal and dependent on the initiative and commitment of particular individuals. As a result, there remains a lack of consistency and co-ordination between supervisors both within and across sectors, resulting in an inconsistent risk-based approach.

343. AML/CFT supervisors of casinos, REAs, DPMS and TCSPs do not have a statutory obligation or power to supervise these entities for compliance with TFS obligations. The Bundesbank and the Main Customs Offices have a TFS-specific monitoring role that is set out in the relevant TFS legislation. However, in practice these authorities do not undertake general monitoring of DNFBPs' compliance.<sup>64</sup> Germany's national AML/CFT Strategy recognises that "responsibilities for monitoring compliance with financial sanctions are not defined sufficiently clearly". This lack of clarity contributes to issues implementing TFS, particularly by smaller DNFBPs in these sectors, including casinos and DPMS (see IO.4 in Chapter 5).

*Professional body supervisors (accountants, notaries, and the legal profession)*

344. Like other DNFBP supervisors, professional body supervisors have been required to conduct risk-based supervision since 2017. Based on discussions with supervisors and obliged entities, in practice, supervisors are not yet consistently applying a risk-based approach to supervising their populations of obliged entities that is informed by relevant risk factors. Like district and government supervisors, professional body supervisors are hampered by a severe lack of resources.
345. Bar associations (that supervise lawyers) are limited in their ability to apply a risk-based approach due to the recency of efforts to determine the scope of the supervised population. In general, bar associations identify their supervisory pool based on a random selection of potential obliged entities, which is narrowed down based on self-reported risk factors. Additional measures are applied based on a limited range of risk factors, e.g., to entities that conduct a larger number or higher-value of high-risk transactions. Where inspections are performed, lawyers and tax advisors report that these are thorough. Statutory accountants are subject to regular, rules-based supervision through an audit every six years, which covers AML/CFT obligations.
346. Despite the identified higher risk posed by notaries, supervisors (the regional courts) view the sector as largely homogenous, so supervisors generally do not consider relevant risk factors and variables in applying supervisory measures. There are, however, regular inspections of this sector as AML/CFT supervision is conducted as part of the notary's regulatory review, every four years. Compared to other DNFBP sectors, this results in a relatively high amount of supervisory activity for this sector. Additional or more frequent inspections can be undertaken in response to identified anomalies or new notaries. Some supervisors do conduct additional AML/CFT-specific inspections on the basis of certain, relatively simple risk factors (e.g., notaries operating in large metropolitan areas), but this approach is inconsistent across the large number of supervisors. As with other supervisors, supervision in general is limited by a lack of resources. While it is one of the better resourced sectors, there are still approximately 150 notaries per one supervisory FTE. The Berlin Notary Supervision Task Force is a good example of more risk-based supervision in the sector. However, like most DNFBP supervisors, its level of resources is very low compared to the size of its supervised population, especially taken into account the higher risks in this region.

<sup>64</sup> The customs administration monitors the import, export and transit of goods. Main Customs Offices audit, among other things, compliance with foreign trade law by businesses involved in the cross-border movement of goods, including relevant DNFBPs.

**Box 6.3. Berlin Notary Supervision Task Force**

In January 2020, the Berlin Regional Court set up a specific AML/CFT Supervision Task Force for Notaries. The task force works under the direction of a presiding judge and consists of three inspectors (to supervise the 692 Berlin notaries). It is designed to supervise and raise AML/CFT awareness among notaries. The Task Force has a somewhat risk-based approach to supervision. Each notary's risk is calculated based on: self-reported information on the number of transactions they have assisted with that fall under the ML Act; the findings from the notary's regulatory reviews (which check compliance with official notarial duties, including the ML Act); and findings from any previous inspections. This information is then used to identify notaries for on-site and written inspections. The Task Force carried out 73 on-site inspections in 2020, and took desk-based measures in an additional 62 cases.

Source: German Authorities

347. As with other DNFBP supervisors, co-ordinating the large number of supervisors for the legal professions and notaries is difficult. Larger firms often have multiple supervisors as a result of operating across-regions, or providing a range of independently-supervised services (e.g., legal, accountancy and tax advice services). A lack of co-ordination may result in a single firm being subject to multiple inspections; one law firm noted that it had eight supervisors, and between prudential and AML/CFT supervision, it experienced 30-40 written or on-site inspections per year. Supervision is even more fragmented in the notary sector; with up to 22 regional court supervisors per *Land*. The regional bar associations and chambers of tax advisors have mechanisms for information-sharing, e.g., a bar association working group on ML that meets every two months. However, it is not clear there is sufficient co-ordination to prevent overlap. This impacts the ability for Germany to take a nation-wide risk-based approach to DNFBP supervision and in practice results in inconsistencies in supervision between and within sectors.
348. AML/CFT supervisors of lawyers, tax advisors, notaries and accountants (professional bodies) have a general power to supervise their populations for compliance with all relevant obligations, which includes TFS obligations in theory. However, in practice, entities and supervisors in these sectors met during the on-site visit were not always clear on the relevant responsibilities in this area.

*Remedial actions and effective, proportionate, and dissuasive sanctions**BaFin (FIs, including VASPs)*

349. BaFin has, and uses, a range of measures for remedying deficiencies and sanctioning violations of AML/CFT obligations. BaFin applies these measures in an escalating fashion with the aim of supporting strengthened compliance, as well as dissuading and sanctioning breaches. While a range of measures are used in practice, particular cases (including involving major banks) indicate that measures do not always ensure prompt remediation of non-compliance or prevent repeated breaches. Available measures include informal instruments such as telephone or written requests to address deficiencies, instruction letters to management or administrative board members, requests for regular updates on remediation progress, and the threat of further action. Informal measures are used in the context of an audit or inspection follow-up. Deficiency letters are issued on the basis of risk (i.e., higher risk institutions need fewer and less serious shortcomings to receive a deficiency letter and follow-up) and include a date by which the entity must provide an action plan with timeframes. BaFin monitors implementation of the action plan via written reports until all shortcomings are eliminated. BaFin has made creative use of available informal measures; in one case of serious shortcomings, at BaFin's request, a bank pegged the remuneration of management board members to progress in remedying AML/CFT deficiencies.
350. BaFin also has a formal supervisory toolkit that includes the power to impose fines, issue warnings, dismiss management board members, withdraw licenses and the ability to restrict business. The power to appoint a special representative to a FI is considered particularly influential, as it represents a significant intervention in the FI's business. The mandate of a special representative can take various forms ranging from that of a mere observer and reporter to that of a substitute member of an executive body. In addition to the power to replace some or all members of executive bodies, the special representative can draw up restructuring plans, rectify selected weak points in the FI's business organisation and monitor compliance with orders issued by BaFin. The special representative's permanent presence in the FI, combined with extensive rights of access and information, make the special representative effective useful supervisory tool.

**Box 6.4. Use of a special representative by BaFin**

In September 2018, BaFin appointed a special representative to a major Germany bank in response to issues related to correspondent banking. In February 2019, BaFin expanded the mandate of the special representative to monitor the bank's implementation of a BaFin instruction to review and, if necessary, adjust its group-wide risk management processes in relation to correspondent banking.

BaFin's preliminary assessment is that the institution has achieved substantial improvements in implementing BaFin's order. For example, the institution reviewed its correspondent banking relationships, identified more broadly-defines correspondent banking relationships, and adjusted its risk appetite in response to newly-identified risks resulting in a significant decrease in the number of correspondent banking relationships. However, various requirements have remained only partially met over a long period of time. As a result, BaFin maintains pressure on the institution. While BaFin states that it is prepared to use further instruments in this regard, e.g., administrative enforcement instruments, it is not clear under what circumstances these would apply.

BaFin has also observed a process of cultural change at the institution. This is evident, in particular, from the substantial restructuring of the Management Board in July 2019, which affected the members of the Management Board responsible for the ML shortcomings, forcing them to resign. This was not pursuant to a BaFin order, but was the result of informal personal warning letters by BaFin to these members of the Management Board, which were also brought to the attention of the Supervisory Council.

Source: German Authorities

351. BaFin regularly uses its power to impose administrative fines (see table 6.9 below). From 2015-2020, BaFin initiated 333 administrative offence proceedings against FIs (and, where appropriate, individuals). Following these proceedings, BaFin issued 201 fine notices resulting in 2 028 individual fines totalling EUR 83.6 million.<sup>65</sup> The use of fines appears risk-based; the majority of fines imposed (by both value and number) are imposed on higher-risk institutions. The quantum of fines appear proportionate in the context of the cases, and the number of cases pursued is significant.

<sup>65</sup> Including two fines imposed by a public prosecutor's office. The public prosecution offices have the ability to impose fines where criminal ML proceedings are pursued, and do not result in conviction but result in the identification of administrative breaches.

**Table 6.9. Administrative fines imposed by BaFin (2017-2020)**

	2017	2018	2019	2020
Agents and e-money agents (high risk)	76 fines EUR 55 300	91 fines EUR 65 150	41 fines EUR 20 400	-
High risk credit institutions	239 fines EUR 9 891 350	1 fines EUR 15 000	9 fines EUR 15 031 700	13 fines EUR 13 612 500
Medium risk credit institutions	20 fines EUR 220 000	12 fines EUR 150 000	3 fines EUR 24 000	
Low risk credit institutions	103 fines EUR 342 700		3 fines EUR 86 300	5 fines EUR 9 750
Foreign payment institutions (high risk)	-	115 fines 3 500 000	1 fine EUR 10 000	-
Insurance companies (medium risk)	-	1 fine EUR 15 000	-	-
Other (low risk)	-	-	-	1 fine EUR 20 000
<b>Total</b>	<b>438 fine</b> <b>EUR 10 509 350</b>	<b>220 fines</b> <b>EUR 3 745 150</b>	<b>57 fines</b> <b>EUR 15 172 400</b>	<b>19 fines</b> <b>EUR 16 642 250</b>
<i>High risk institutions</i>	<i>315 fines</i> <i>EUR 9 946 650</i>	<i>207 fines</i> <i>EUR 3 580 150</i>	<i>51 fines</i> <i>EUR 15 062 100</i>	<i>13 fines</i> <i>EUR 13 612 500</i>
<i>Medium risk institutions</i>	<i>20 fines</i> <i>EUR 220 000</i>	<i>13 fines</i> <i>EUR 165 000</i>	<i>3 fines</i> <i>EUR 24 000</i>	
<i>Low risk institutions</i>	<i>103 fines</i> <i>EUR 342 700</i>	<i>0 fines</i> <i>EUR 0</i>	<i>3 fines</i> <i>EUR 86300</i>	<i>6 fines</i> <i>EUR 29 750</i>

\* Figures include a fine imposed by a prosecutor.  
Source: German Authorities

352. FIs met during the on-site considered that BaFin's use of remedial measures was increasingly dissuasive, although repeated and continuing breaches by fined institutions suggest that fines may not always be a dissuasive sanction. Several other measures appeared particularly effective. The publication of instances of non-compliance has a deterrent effect on both the individual firm and the wider supervised sector due to fear of reputational damage. The information published on the breaches is also helpful in signalling BaFin's expectations to FIs. BaFin and FIs also noted the impact of the use of business restrictions and the ability to pursue individuals as very effective tools. BaFin has only recently begun to take advantage of these particular tools, which has hampered the dissuasiveness of their actions in the past. A recent case where BaFin restricted business growth is as an example of a particularly effective sanction.

**Box 6.5. BaFin's use of restriction of business growth as a sanction**

In 2021, BaFin conducted a prudential on-site inspection of a German bank. The inspection identified deficiencies in outsourcing management, IT-security and risk management as well as insufficient emergency and security management. The shortcomings related to outsourcing management had particular implications for the bank's AML/CFT compliance. All findings showed that in light of the complexity and size of the bank, the institution had no sufficient business organisation. BaFin issued an AML/CFT order in May 2021, instructing the bank to rectify these deficiencies and appointed a special representative to monitor the institution's compliance. The bank was not able to remediate the findings in a timely manner. As a result, BaFin ordered the implementation of risk mitigating measures, including a 50% limitation on customer growth.

To ensure compliance with these orders, BaFin extended the mandate of its special representative. The case demonstrated good co-operation between BaFin's prudential and AML supervisory teams, which worked together to prepare the orders relating to the bank, due to the cross-cutting nature of the deficiencies identified.

Source: German Authorities

353. In terms of measures related to TFS (where monitoring is split between BaFin and the Bundesbank), the Bundesbank identified 64 TFS control deficiencies at 38 institutions from 2017 to 2021 (e.g., incomplete data collection, incorrect filtering, using out-of-date lists, etc.).<sup>66</sup> These were addressed via letters and follow-up checks. An additional 17 cases of potential sanctions breaches were identified at five institutions and reported to Customs for investigation. Based on the case studies provided, information on shortcomings is not routinely shared with BaFin, which could pursue alternative or additional remedial measures.

*DNFBP supervisors*

354. While DNFBP supervisors have access to a range of tools, these are used to a limited extent. Certain supervisors, particularly professional body supervisors, are reluctant to use the full range of available sanctions in a proportionate manner.

<sup>66</sup> These deficiencies are not limited to terrorism-related TFS.

*Land and district governments (REAs, DPMS, TCSPs, casinos and certain insurance entities)*

355. Measures available to *Länder* and district government supervisors include informal measures (written feedback and follow-up monitoring) and repressive measures (formal warnings and administrative fines). After an inspection, supervisors provide feedback on any shortcomings. If the shortcomings are minor and the entity is co-operative, there will be no formal follow-up process. For more serious shortcomings, supervisors will request that these are addressed and the inspection process will remain open until the issue is resolved. For serious or repeated infringements, *Länder* and district government supervisors regularly impose formal warnings or fines.
356. Consolidated statistics for all DNFBP sectors across all *Länder* are not available. Nonetheless, available statistics suggest that the overall number of remedial measures is relatively low given the size of the sectors and issues with compliance in certain areas (e.g., the very low level of STRs from DNFBPs; see IO.4) (see table 6.10 below). This is likely as supervisory action is still relatively limited, and supervisors are still focused on initial awareness-raising and encouraging compliance rather than formal sanctions. Nonetheless, case studies reflected supervisors' ability to fine entities for compliance failures. Available statistics also show that the number of fines connected to follow-up inspections has increased, showing supervisors are responding more seriously to systematic shortcomings. Fines are generally much lower than in the financial sector, in reflection of the smaller size and lower financial resources of these entities. However, fines in the six-figure range have been imposed in isolated cases. No sanctions have been imposed on casinos in recent years, which may reflect the higher level of supervisory engagement and the resulting better controls.

**Table 6.10. Administrative fines against REA, traders (including DPMS) and TCSPs (2017-2020)**

	2017	2018	2019	2020
REAs	3 proceedings EUR 3 953	11 proceedings EUR 25 650	24 proceedings EUR 116 639	18 proceedings EUR 45 000
Traders (including DPMS)	22 proceedings EUR 103 069	30 proceedings EUR 65 437	41 proceedings EUR 730 256	41 proceedings EUR 270 781
TCSPs	-	10 proceedings EUR 5 500	4 proceedings EUR 1 950	4 proceedings EUR 15 624

Source: German Authorities

**Box 6.6. Sanctions by *Land* and district governments****Sanctions against a DPMS entity**

In 2018, customs discovered a large quantity of gold during inbound passenger checks. As proof of ownership, the individual presented five invoices, all totalling just under EUR 10 000. All invoices had been issued by the same branch of a DPMS, some on the same day and with serial invoice numbers. The customs office forwarded the facts to the relevant LKA, which referred the case to the supervisory authority (the Senate Department for Economics, Energy and Public Enterprises Berlin).

During its investigation, the supervisor questioned several witnesses, including former and current employees, which revealed that although the individuals involved in the transactions had received training when they started working for the company, nobody had any knowledge of smurfing. In response, the supervisor imposed a fine of EUR 2 000.

**Sanctions against a REA entity**

Due to identified compliance shortcomings, a REA was subject to monitoring by the Bavarian supervisory authority. A follow-up inspection was conducted for the period 1 July 2017 to 31 March 2018. This inspection revealed that the previously-identified shortcomings had not been remedied, with an additional 21 cases of considerable shortcomings identified in relation to identification requirements. A fine of EUR 48 234 was imposed on the real estate agent in 2019. Appeal proceedings are currently pending.

Source: German Authorities

*Professional body supervisors (accountants, notaries, and the legal profession)*

357. Professional body supervisors have access to the same remedial measures and sanctions as other DNFBP supervisors and take the same approach following inspections. Supervisors of lawyers and tax advisors (regional bar associations and chambers) have only been able to issue sanctions themselves since early 2020. Data and discussions with supervisors indicated that supervisors of notaries and the legal profession (lawyers and tax advisors) rarely apply sanctions. This is inconsistent with data indicating non-compliance in certain areas (such as STR reporting). Nonetheless, individual cases indicate that some regulators are increasingly taking a stricter approach to using sanctions. For example, in 2021, a Bar Association imposed a fine of EUR 22 000 on a lawyer indicted for ML based on their incorrect, untimely, incomplete provision of information, failure to provide information, and failure to submit documents. The Chamber of Accountants identifies a low number of breaches despite indicators of lacklustre compliance; for example, three cases of non-compliance were identified in 2019, in the same year that the sector made 0 STRs. The Chamber noted that breaches are typically remedied by the individual, but it demonstrated its ability to issue fines where this did not occur. Revocation of licenses/removal from the profession is rarely used by any professional body supervisors, even in serious cases, e.g., professional enablers

(see Box 6.1). This indicates that certain supervisors may be reluctant to use the full range of available sanctions in a proportionate manner.

**Table 6.11. Sanctions against accountants, tax advisors, lawyers and notaries (2018-2020)**

	2018	2019	2020
Lawyers	0 warnings -* 22 notices	48 warnings -* 87 notices	24 warnings 1 fine (EUR 1 000) 207 notices
Notaries	0 warnings 0 fines 28 notices	43 warnings 0 fines 64 notices	22 warnings 1 fine (EUR 1 250) 54 notices
Accountants and tax advisors	0 warnings 0 fines 5 notices	10 warnings 1 fine (EUR 500) 58 notices	37 warnings 15 fines (EUR 16 600) 29 notices

Note: Bar associations were only able to issue fines in 2020.  
Source: German Authorities

### *Impact of supervisory actions on compliance*

#### *BaFin (FIs, including VASPs)*

358. BaFin has observed that audit and inspection findings have improved over time, with findings now being more in the space of improvement, refinement or enhancement to controls, rather than significant weaknesses in, or absence of, key controls (as observed in previous years). However, data on this point is mixed. While BaFin retains audit findings, recent expansions of AML requirements and a stricter assessment system means audit findings in many areas do not illustrate a clear improvement in FIs' AML/CFT compliance. In addition, individual audit reports indicate repeat infringements in the same areas despite BaFin intervention. As a result, it is difficult to draw any clear conclusions on this basis.

359. BaFin points to the increasing number of STRs as one indicator of the effectiveness of its supervisory actions. The number of STRs has increased dramatically since Germany's previous MER, in part as a result of legislative changes to respond to the FATF's findings. STRs filed increased by fifteen times between 2008 and 2019, with a 50% increase between 2018 and 2019 alone. The vast majority of reports (98%) come from the financial sector.<sup>67</sup> Although some FIs shared the view that growing awareness was a factor in the increase, a number highlighted concerns regarding ML reporting officers' personal liability for failing to report as another reason for increased reporting, raising concerns of defensive reporting. Whereas the previous MER criticised FIs 'over-investigation' of potential STRs, discussions with FIs indicate that this is no longer the case. Some FIs have misinterpreted recent enforcement action resulting in significant fines for delayed reporting (e.g., a EUR 4.2 million fine in 2021) to mean there is a three-day deadline for reporting (although there is no such deadline in Germany's law or BaFin's interpretative guidelines). This misinterpretation has led some FIs to rush their pre-STR analysis. While BaFin's actions may have contributed to the increase in STR reporting, there is limited evidence that the quality of reporting has improved and indications of potential defensive reporting (see IO.4 for further analysis on this issue).
360. Since 2019, BaFin has extended its existing practice of closer involvement of management board members in supervisory interviews alongside the MLRO. This practice is consistent with the legislative requirement to have a board member responsible for AML/CFT compliance. BaFin considers this has led to increased risk awareness at the management level and an improved level of focus on AML/CFT matters. While FIs met during the on-site agreed that management awareness and general compliance had improved over the past several years, this could be attributable to other factors, including legislative changes in this area and enforcement activity by foreign supervisors. The assessment team also observed that significant deficiencies continue to persist in the quality and timely application of certain controls even within the major banks sector. On this basis, it is not yet clear that BaFin's increased supervisory activity in recent years has had a major impact.

#### *DNFBP supervisors*

361. Supervisory engagement in the DNFBP sectors is limited due to the size of the sector and the lack of resources, which makes it difficult to draw any conclusions on the overall impact of supervision. While there are some indications of improved awareness, it is not clear that this is linked to supervisory actions (as opposed to legislative or policy changes).

---

<sup>67</sup> The size of the financial sector (in terms of the number of supervised entities) did not increase significantly over this period, meaning the increasing number of STRs is not attributable to a growing number of FI reporting entities.

*Land and district governments (REAs, DPMS, TCSPs, casinos and certain insurance entities)*

362. Due to legislative changes and limitations in statistics until relatively recently, it is difficult to conclude that supervisory activity by Land and district government DNFBP supervisors has affected compliance. The number and amount of fines imposed in relation to initial inspections decreased in relation to the total volume of fines from 2017 to 2019, which supervisors consider suggests generally better compliance. However, the statistics cover a short period and there may be a range of factors at play, which makes it difficult to draw any clear trends from this data. In practice, supervisors have observed increased risk mitigation measures; as noted in IO.4, certain sectors are implementing measures, e.g., restricting cash transactions, which indicates a growing awareness of risk that may be partly due to supervisory activities.
363. STR reporting from the DNFBP sector is very low (less than 2% of all STRs are received from DNFBPs). Data cannot be broken down by DNFBP sector, but is available for the broader non-financial sectors covered under Germany's AML/CFT framework. There has been a steady increase in reporting from the broader traders in goods sector (which includes DPMS) and both traders and REAs saw a jump in reporting in 2019. Land and district government supervisors note that this coincides with increased inspections measures for these sectors in 2018 and 2019. It also coincides with national-level focus on the risks in this area.

*Professional body supervisors (accountants, notaries, and the legal profession)*

364. Similar to other DNFBP supervisors, it is difficult to draw conclusions on the impact of supervisory activity in the accounting, notary and legal professions (including tax advisors). Professional body supervisors point to increased demand for AML/CFT training and seminars and a growing number of AML/CFT enquiries as evidence of effective awareness-raising and outreach in this area. Discussions with obliged entities supported this, indicating an increasing appreciation for ML risks and obligations. STRs from the legal, notary, tax advisory and accounting sectors remain extremely low. Only notaries have seen a significant increase in reporting, due to an ordinance requiring rules-based reporting rather than as a result of any supervisory efforts. (See IO.4 for further information on this issue). Supervisors provided case studies and statistics that showed that follow-up monitoring rarely reveals further shortcomings; this suggests that direct supervisory engagement may positively affect compliance at the institution level.

*Promoting a clear understanding of AML/CFT obligations and ML/TF risks**BaFin (FIs, including VASPs)*

365. BaFin publishes regular guidance in the form of circulars, interpretation decisions and guidance notices. Circulars are generally used to alert institutions to risks (e.g., regular circulars on high-risk countries issued after FATF Plenaries), but can also be used to explain FIs' obligations (e.g., the 2017 circular on video identification requirements). Interpretive decisions help FIs understand their obligations under a particular law (e.g., decisions on the EU Funds Transfer Regulation or the Interpretation and Application Guidance to the ML Act (GwG)). Guidance notes tend to provide more specific information (e.g., guidance notes for agents working for a foreign FI). BaFin publishes its circulars and guidance on its website and via a newsletter that reaches 45 000 subscribers. Its website contains other relevant ML information, including the NRA. BaFin also issues a monthly new bulletin (*BaFinJournal*) which contains expert articles, interviews and reports on supervisory issues. Six detailed articles have been published on ML issues. BaFin's Annual Report also contains a special ML section on ML developments.
366. BaFin engages with FIs on a bilateral and multilateral basis. Since 2018, BaFin has organised an annual symposium for FIs, which attracts around 500 participants each year. During the event, staff from BaFin's AML Department are available at an information stand and at a 'Speaker's Corner' to answer specific questions. In addition, staff from the AML Department take part in external events to share information on supervisory topics. In the course of inspections, BaFin provides time for discussion on issues not related to inspection activities. For high-risk institutions, BaFin maintains an ongoing dialogue. Entities can also contact BaFin via telephone, e-mail or in writing. BaFin is also a member of AFCA (Germany's public private partnership; see IO.1) alongside 16 banks and uses this forum to share information and contribute to typologies. BaFin and Commerzbank together lead an AFCA working group on ML/TF risks and trends in the financial sector.
367. Feedback received from FIs was broadly positive in relation to the BaFin's outreach activities with most FIs confirming that BaFin guidance is helpful. Some larger FIs, particularly those with an international focus, indicated that, in their view, the guidance is more relevant to FIs with retail and domestic business models and that they would welcome guidance tailored for FIs that operate internationally. While it is clear that BaFin is utilising a range of outreach activities, consideration should be given to developing an outreach strategy to further enhance effectiveness.

*DNFBP supervisors*

368. DNFBP supervisors have issued sector-specific guidance for most sectors and professional body supervisors are particularly active in providing training. AFCA is a useful tool and would benefit from broader DNFBP engagement.

*Land and district governments (REAs, DPMS, TCSPs, casinos and certain insurance entities)*

369. Land and district government supervisors have collaborated to publish interpretation and application guidance on the GwG (the AML Law) for casinos and “other DNFBPs”. The guidance for other DNFBPs covers very diverse DNFBP sectors, including REAs, DPMS, TCSPs and insurance intermediaries, in addition to other non-financial sectors covered in Germany as obliged entities (e.g., traders in goods), which limits its ability to cater for sector-specific scenarios. As a result supervisors have jointly developed specific instruction sheets with frequently-asked questions and practical guidance for REAs, DPMS, and insurance intermediaries. The guidance is available on supervisors’ websites and may be handed out during supervisory visits. Supervisors also work with chambers of industry to distribute information and provide information packs to newly-registered entities. The size of Germany’s broader obliged entity population combined with the lack of supervisory resources poses challenges in this respect, especially in the case of traders in goods. This sector comprises approx. 800 000 entities, which makes it difficult for supervisors to make a commensurate effort to inform at-risk sub-sectors and entities, including DNFBPs, of their obligations.
370. DNFBPs interviewed during the on-site were generally aware of the interpretation and application guidance, and some noted that the development of standardised guidance was positive. Nonetheless, entities generally felt that the guidance was overly lengthy, complex, inaccessible for smaller entities, and more targeted at the financial sector. This may be a result of DNFBP supervisors using BaFin’s interpretation and application guidance as a starting point. Entities noted that there was very little industry involvement in the development of guidance, resulting in outdated provisions; for example, guidance for casinos includes information about deposit accounts, which casinos stopped providing several decades ago. Obligated entities were largely unaware of the sector-specific instruction sheets.

*Professional body supervisors (accountants, notaries, and the legal profession)*

371. Professional body supervisors have worked with other supervisors in their sectors to develop separate guidance on AML/CFT obligations for the legal profession (lawyers and tax advisors), notaries and accountants. This helps ensure a measure of consistency in interpretation within and across sectors. The guidance is published on supervisors’ websites and shared during training events. All legal and accounting supervisors (but not notary supervisors) offer seminars and training events on AML/CFT. Further guidance and awareness-raising products have been developed by different supervisory bodies. For example, the Hanseatic Bar Association of Hamburg provides specific guidance on the risk-based approach, general guidance on the AML Act (GwG), sample risk analyses, and questionnaires to enable members to determine whether they are an obliged entity. For notaries, seminars and training are offered by the federal and regional chambers of notaries, however, it is not clear that there is sufficient co-ordination with supervisors to ensure supervisory findings are being incorporated into these trainings.

372. Obligated entities generally found guidance and information from supervisors helpful. However, larger entities with multiple supervisors faced difficulties consulting and reconciling information and advice from multiple supervisors. In addition, while efforts appear positive, they are not having a meaningful impact in all areas. STR reporting among the legal profession remains extremely low despite supervisory engagement and recent rules-based reporting requirements intended to combat issues related to legal professional privilege (see IO.4).

## Overall conclusion on IO.3

BaFin has a strong understanding of risks across the financial sector, and largely supervises its population in line with its risks. BaFin's risk-based approach benefits from FIs' annual external audit requirement. However, the risk-based approach is more recent in the non-bank sector, where there is a lower level of independent supervisory activity by BaFin, particularly on-site inspections, and an insufficiently proactive approach to identifying unlicensed MVTs providers, especially *hawala* operators. The assessors gave more weight to these shortcomings in light of the identified risks in these sectors. While a range of remediation measures are used, including proportionate fines, instances of repeated non-compliance suggest that more impactful measures are required in some cases. Supervision of VASPs is improving, but the focus on this sector remains relatively new and supervision of certain types of VASP is at an early stage.

There have been improvements in Germany's supervision of DNFBPs since its 2010 MER, and there are some examples of specific supervisors demonstrating a developing risk-based approach. However, there remain major deficiencies with Germany's supervision of DNFBPs caused by challenges co-ordinating the over 300 supervisors, gaps in knowledge and understanding of the supervisory population, and a severe lack of resources. As a result, supervision in general is limited, including in some higher-risk DNFBP sectors. Supervisors generally do not consider all relevant risk factors and variables in developing a supervisory strategy, resulting in an ineffective and inconsistent risk-based approach.

Supervision of TFS obligations is separate to AML/CFT supervision. While there is overlap in the supervision of FIs, the sector is largely subject to adequate supervision. There is no clear TFS supervisor for casinos, REAs, DPMS and TCSPs, and in practice, most DNFBPs are not subject to clear, effective monitoring. This is a major deficiency given Germany's risk and context and the risks posed by some of these sectors.

**Germany is rated as having a moderate level of effectiveness for IO.3.**

## Chapter 7. LEGAL PERSONS AND ARRANGEMENTS

### Key Findings and Recommended Actions

#### Key Findings

- a) Germany has a variety of measures in place which prevent legal persons and arrangements from being misused for ML/TF to some extent. Whilst many of the previous measures were decentralised, Germany is currently taking steps to capture and make BO information centrally available through the Transparency Register. However, this is still in a process of implementation and while some information is available, there remain major issues with the current data pool which is not complete and there are issues with accuracy and information being up-to-date on the Transparency Register and other registers that pre-date the Transparency Register.
- b) A significant amount of information is publicly available on how to create different types of legal persons in Germany and, to a slightly lesser extent, legal arrangements.
- c) Germany has a reasonable understanding of the inherent vulnerabilities associated with different types of legal persons and legal arrangements due to a recent sectoral risk assessment. However, there is a gap in its understanding of the extent to which legal persons created in the country can be, or are actually, being misused for ML/TF as only limited objective data from the FIU, BKA, prosecutors and supervisory authorities has been used in the risk assessment.
- d) A number of mitigation measures have been introduced to prevent against abuse for ML/TF, including the use of various registers, the use of an automated account data retrieval system (providing BO information on account holders) and increased restrictions on bearer shares and the provisions on nominee directors/shareholders. However, taken together, major deficiencies remain, particularly in relation to material issues in the operation of registers but also in relation to proactively reducing the number of bearer shares, identification of nominee shareholders and the fact that the account data retrieval system has been used to a limited extent by the FIU and does not contain information on all legal entities/arrangements in Germany.
- e) Competent authorities (and obliged entities) can obtain adequate, accurate and current basic information through the Common Register Portal of the *Länder (Registerportal)* which provides timely access to information on the Commercial Register and the Co-operative, Associations and Partnership Registers held by the *Länder*. However, these registers do not capture

beneficial ownership information. The commercial registers do, however, contain information on the partners in commercial partnerships.

- f) BO information is available through the Transparency Register, directly from the legal entity, through LEA powers and to some extent through the Electronic Account Retrieval System. The Account Retrieval System is currently the most commonly used platform by authorities for finding BO information but this is also limited as it relies on the legal person or arrangement holding a German bank account.
- g) Germany has recently taken important steps to increase access and availability of adequate, accurate and current BO information on legal persons and arrangements in the jurisdiction with the implementation of the Transparency Register in 2017, and subsequent legislative amendments to its operation in 2021. Germany is now following a new, two-pronged approach to improve accuracy: i) Obligated entities verifying information available on the Transparency Register are required by Law to file discrepancy reports to the Transparency Register. ii) All relevant entities are required to directly file with the Transparency Register by the end of 2022. This approach will significantly improve the accuracy of available information to the benefit of competent authorities and the private sector.
- h) A deficiency exists in respect of information available on Civil Law Partnerships (GbRs), of which there were 572 139 civil law partnerships engaged in business activity in 2017. This is particularly the case as Germany acknowledge that the GbR is susceptible to money laundering and there are a relatively large number of partnerships in Germany. Some limited basic information exists through tax filings and information held on other registries (i.e. land registry). However, there is no comprehensive source of basic or beneficial ownership information available to authorities. Whilst reforms to German partnership laws have been passed, they will not be fully in effect until 2024 and it is unclear if they will comprehensively address all the requirements of the FATF Standards.
- i) Sanctions have been applied to some extent by the Transparency Register for failure to notify and failure to notify in a timely manner, along with a relatively small number of supervisory actions taken by BaFin.

## Recommended Actions

- a) In order to improve accuracy of beneficial ownership information, revisions to the structure and operation of the Transparency Register should be implemented in full by the end of 2022. This should have a particular focus on ensuring that there is compliance with discrepancy reporting and re-filing by all entities. The Transparency Register must be provided with the appropriate human/technical resources to process these significant data filings and update the register in a timely manner.
- b) Germany should look to deepen its understanding of legal persons and arrangements to fully understand the ML/TF risk they pose to Germany focussing specifically on enhancing the existing risk assessment in two areas:
  - a. Conducting an in-depth analysis concerning the risks foreign shareholders and beneficial owners (particularly focussing on foreign legal entities), connected to German legal entities, pose to Germany.
  - b. Conduct a holistic risk assessment combining the conclusions from the Sector Specific Risk Assessment on vulnerabilities of legal persons and arrangements with objective data on the misuse of legal persons and arrangements for ML/TF gathered from the FIU, law enforcement, supervisors, the private sector and other relevant stakeholders.
- c) Germany should proactively reduce the number of bearer shares in operation in Germany and achieve conversion to registered shares as this does not appear to have been actively reduced in recent years. Equally, authorities should address the remaining risks around abuse of nominee shareholders where beneficial ownership information may not be registered on the Transparency Register through mechanisms to strengthen enforcement of requirements.
- d) Germany should look to further enhance the benefits that the automated account retrieval system provides by ensuring direct automatic access to all relevant authorities to the system. In respect of the FIU direct access should be used to increase requests, particularly when conducting analysis of beneficial owners of legal entities linked to ML/TF.
- e) Germany should ensure that GbRs and other legal arrangements where inadequate information is available are brought into the scope of an appropriate regime allowing authorities access to relevant information in a timely manner. The scope of the law reforms should be reviewed to ensure they are adequate under the FATF Standards.
- f) Given the prominence of the Transparency Register in ensuring adequate, accurate and timely beneficial ownership information in Germany, a strategy should be developed to enforce filing obligations, including the use of dissuasive sanctions.

373. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25, and elements of R.1, 10, 37 and 40.<sup>68</sup>

### Immediate Outcome 5 (Legal Persons and Arrangements)

374. Germany's framework for capturing basic and beneficial ownership ("BO") information is complex and built on a series of inter-connected registers and portals. The system for capturing and verifying information relies on local courts, notaries and administration at the *Länder*-level. The system has also been subject to a series of progressive reforms since 2017 to introduce a national Transparency Register to capture all basic and BO information in a single database (see Chapter 1 for more information on the framework). The Transparency Register is currently run and managed by a private company (*Bundesanzeiger Verlag GmbH*) which has been empowered by the Federal Ministry of Finance by means of an ordinance to manage the register. In performing this function, it is considered an authority and can enforce compliance.
375. The assessment team based its findings on: statistics and police documents; interviews with the BMF, BMJ, the Federal Office of Administration, *Bundesanzeiger Verlag* (company running the Transparency Register), BaFin, BZSt, FIU, BKA, GBA, BfV, Federal Chamber of Civil Law Notaries and a selection of representatives from LKAs, tax investigation offices, local courts, notaries, case studies and interviews with the private sector.

### Public availability of information on the creation and types of legal persons and arrangements

376. Germany has numerous sources of information publicly available on the creation and types of legal persons. A large proportion of this information is held on Government websites to encourage a start-up culture in Germany. However, information on legal arrangements is much more limited.
377. The multilingual business start-up portal (*Existenzgründerportal*) operated by the Federal Ministry for Economic Affairs and Climate Action (BMWK) provides the most extensive publicly accessible information on the how to choose or change a legal form. This includes information extending from a Fact Sheet outlining the main selection criteria for legal forms and a discussion of decision-making criteria relevant to the choice of legal form. There are equally several e-learning modules available which look to educate the public on how the legal forms operate and duties and obligations under the legal forms. The website has significant and increasing amounts of traffic, demonstrating that it is used for information, receiving over 5 million page views in 2019 from 2.8 million individual visits.

<sup>68</sup> The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

378. The publicly available information is also accompanied by a number of expert forums where experienced associations and businesses offer initial guidance to founders and those interested in setting up a business. This allows for individuals to submit online question forms to request questions which are responded to in a matter of days. The BMWK Expert forum contains over 40 experts. There is equally the “Make it Germany” website which provides information for international qualified professionals and future business founders on how to start a company in Germany. The website has had over 9 million page views from 3.7 million individual visits in 2019.
379. With respect to legal arrangements, *Treuhand* describes trust like structures created under German law that are commonly used in Germany. Express trusts cannot be created under German law but foreign trusts can operate and are regulated under Germany’s AML law. There is no specific source of general information available on legal arrangements but specific statutes which regulate the creation and types of legal persons and arrangements are available publicly in German at [www.gesetze-im-internet.de](http://www.gesetze-im-internet.de). The Regulations on establishing European Legal forms are available in all European languages at [www.eur-lex.europa.eu](http://www.eur-lex.europa.eu).

### *Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities*

380. Germany has identified and assessed ML/TF risks and vulnerabilities of legal persons and arrangements to a reasonable extent. German authorities have taken positive steps towards a comprehensive understanding of risks with the development of the NRA in 2019 and a sector-specific risk assessment in 2020 looking at the inherent vulnerabilities of legal persons and arrangements. However, the sector-specific risk assessment only included limited information from operational agencies (particularly the FIU) which represents a gap in risk assessment and understanding. The assessment team based its findings on: the sectoral risk assessment, NRA and other risk analyses (including the 2020 NPO risk assessment), interviews with both the public and private sector and publically available information on the abuse of legal persons in Germany.<sup>69</sup>
381. While the sector-specific risk assessment was intended to capture “actual risk”, authorities confirmed that the assessment was focussed on the inherent features of legal persons and arrangements which could theoretically assist to obfuscate transparency. While this is an important preliminary exercise, the risk assessment was further supplemented with objective data and evidence from operational agencies (e.g. the FIU) only to a limited extent. Other sources of objective data from the private sector and the Transparency Register were not used in the exercise. The risk assessment could further benefit from cross-checking findings with external reports beyond the NRA (including similar risk assessments in other jurisdictions). The sector-specific risk assessment therefore provides a limited understanding of the actual risk situation in Germany and is not a comprehensive starting point for preventing legal persons and arrangements from misuse for ML/TF.

---

<sup>69</sup> Tax Justice Network, Financial Secrecy Index 2020.

382. The sector-specific risk assessment concluded that the main risks around legal persons and arrangements arose from the involvement of a third jurisdictions. However, there are significant flaws in the assessment. In particular, the risk assessment concluded, and authorities repeated during the onsite, that German legal persons tend to be poorly suited for use as ML vehicles due to mandatory registration requirements, including for legal arrangements such as *Treuhand*. However, for legal persons this underestimates the risk of straw men being used for concealing beneficial ownership behind a shareholder and therefore demonstrates a more limited understanding by the authorities of the true risk situation in Germany. Overall, the German authorities have generally not focussed on the involvement of legal persons in ML cases occurring in Germany from a law enforcement or investigative perspective. This process has therefore not led to any meaningful typologies being produced on the involvement of legal persons and arrangements in ML in Germany. Whilst the AFCA has conducted some initial work on the abuse of shell companies in Germany, this work generally amalgamates conclusions from international reports with some focus around where there has been a German nexus, however it does not represent a detailed understanding.
383. Despite the initial findings of the NRA identifying it as high-risk, there has been limited focus by Germany on understanding how legal persons and arrangements in Germany formed part of broader, cross-border ML schemes despite Germany's profile as an international financial centre. In relation to the real estate sector, whilst some positive action has been taken at a policy level in terms of the implementation of the Transparency Register and requirements to identify and register the ultimate beneficial owner of foreign legal entities who own property, the lack of detailed analysis on actual misuse of legal persons impedes the countries current risk understanding. It is also not clear if authorities have taken into account open source information suggesting potential ML occurring through the real estate sector in their risk assessment processes.<sup>70</sup>
384. Given the prominence of foreign ownership of German legal entities and focus by open source information on the risk of occurring, the assessment team considered understanding of ownership of German legal entities by foreign legal entities to be particularly important in the context of the country. Authorities are at an early stage of conducting analysis on the connection of foreign legal entities with German legal entities. Preliminary inquiries suggest that 5% of legal persons (89 000 out of 1.8 million legal persons entered on the Commercial Register) have at least one direct "foreign participant". The current findings are purely based on presence of foreign participants and not on the amount or size of the participation by the foreign legal person. Authorities intend to create a methodology to examine participation by foreign entities in more detail to better understand the risk. At the current time, Germany only understands the risk of involvement between German legal entities and foreign legal entities to a negligible extent and this remains a significant risk in the context of Germany.

<sup>70</sup> Rosa Luxembourg Stiftung, Christoph Trautvetter and Markus Henn (2021) *Transparency Register: No Transparency: A Research Report on Anonymity in Berlin's Real Estate Market*, available at: [www.rosalux.de/fileadmin/rls\\_uploads/pdfs/Studien/Studien\\_11-21\\_Transparency\\_en.pdf](http://www.rosalux.de/fileadmin/rls_uploads/pdfs/Studien/Studien_11-21_Transparency_en.pdf).

385. TF risk has been identified as primarily arising from the misuse of associations (*Vereine*) and other NPOs is complemented by the 2020 NPO risk assessment which examines the abuse of these legal forms for TF activity (see IO.10). Overall, Germany's understanding of TF risk is better than the understanding of ML risk in relation to the misuse of legal persons.

### *Mitigating measures to prevent the misuse of legal persons and arrangements*

386. Germany has taken several important steps to mitigate and prevent the misuse of legal persons and arrangements and achieves this to some extent. Measures have been put in place to mitigate the risk around bearer shares and some measures have been in place around nominee directors and shareholders that are somewhat effective. The development and implementation of registers that hold basic and beneficial ownership information is a positive development but they are still in varying stages of implementation with major deficiencies in the information held on the different registers. The existing mechanisms include the Commercial, Foundation, Partnerships and Association Registers, held by the *Länder*, that have existed for a long period of time. These registers are supplemented by the federal level Transparency Register which was first established in 2017, became public on 1 January 2020 and was subject to recent significant legislative amendments which came into force in August 2021. The operation of the registers and their ability to provide adequate, accurate and current basic and beneficial ownership information is discussed below in section 7.2.4 and 7.2.5.

#### *Bearer shares*

387. Bearer shares are still issued in Germany with the current number of bearer shares in circulation estimated at around 3 900 to 4 000. Germany authorities claimed that the number of bearer shares is declining but as there does not appear to be active monitoring, this could not be confirmed by the assessment team. German authorities assume that there has been a decline in numbers due to the adoption of the registered share as the standard form of securitisation for shares in a stock corporation or partnership limited by shares. New laws were put in place in 2016 to prevent abuse of bearer shares by requiring companies to issue registered shares. There are now only certain situations where bearer shares can be issued: either requiring the company to be listed and subject to detailed capital market reporting obligations or, in the case of a non-listed company, the company must have waived the right to issue individual share certificates and ensure that a global certificate is deposited with a legal depository. A share register must be kept until the global certificate has been deposited. With a global certificate, custodian banks (which know the depositor and therefore the shareholder) register the non-certificated individual shares in secure depositories.
388. German authorities state that these measures allow investigating authorities to obtain adequate information on the BO of bearer shares. However, it was not demonstrated how in all cases the BO would be identified by authorities when custodian banks held the global certificate of shareholders (as opposed to BOs). Some mitigation measures and checks remain in place, namely if a company requests an entry in the Commercial Register involving the issue of bearer shares, the courts are required by law to check the articles of association to verify that the right to issue individual share certificates has been waived. Overall, these measures reduce the risk to some extent of the remaining bearer shares being abused in Germany.

*Nominees shareholders and directors*

389. Germany has taken action to reduce the risk of nominee agreements through provisions in law to prohibit the appointment of legal persons as a director, member of the supervisory board or manager. Therefore, the risk of legal persons acting as nominee directors is mitigated as it is not permissible in Germany. However, it is not clear what measures are in place for natural persons acting as nominee directors.
390. Nominee shareholding arrangements are permissible. However, the risks in this area are mitigated as notaries must notarise the transfer and verify the identity of the ultimately beneficial owner. There is the possibility that a nominee arrangement may indicate a beneficial owner that differs from the legal ownership information held in the Commercial Register. In these circumstances, the German authorities have outline that it would be necessary to register these arrangements with the Transparency Register. However, these measures assume that the information on the registers is accurate and up-to-date and current deficiencies in the registers impacts the effectiveness of this measure in mitigating the risks of nominee shareholders.

7

*Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons*

391. Germany ensures timely access to adequate, accurate and current basic and beneficial ownership information on legal persons to a limited extent. A complex system of registers for capturing basic and beneficial ownership information has evolved in Germany. The existing arrangements are further complicated by the fact that the various registers are operated by different authorities at the *Länder* and Federal levels and that different requirements apply for access to different registers. The regime covers many types of legal persons but also duplicates information across registers and does not cover some categories of legal persons (particularly civil law partnerships). Issues with the maintenance and verification of information on the registers restrict their usefulness to LEAs as they cannot be relied upon for accurate and current information.

*Länder Registries: Commercial, Co-operative and Partnership Registers for legal persons*

392. A variety of registers exist at the *Länder* level to collect basic (and occasionally beneficial) ownership information for companies, partnerships, co-operatives, associations and foundations. The information held on the different registers and access to this information varies. While the majority of information can be accessed online, some registry information on foundations is only available by visiting the relevant *Länder* authority in the *Land* where the entity is registered. Generally, adequate, accurate and current basic information for Foundations, General Law Partnerships, Foreign Law Partnerships, Limited Partnerships and Partnership Companies are available on a series of Registers. They are accessed by competent authorities in the course of their work.

393. Basic information on legal persons on the Commercial Register can generally be considered adequate and accurate due to the strict requirement for information to be notarised upon initial registration and upon change. The notary system in Germany works effectively to ensure verification of basic information as the notary verifies information before it is entered onto the Register. The Commercial Register therefore only holds information on BO where the legal ownership and BO are the same. Supervisory processes work well to ensure that verification processes are taking place, and this involves checking of the process and documentation of verification, including during on-site inspections. Notary supervisors confirmed that on-site visits involve a random sample of files and that actions have been taken against individual notaries for failing to document adequate procedures for verification. The other registers for basic information operate in a similar fashion with notaries playing a role in verifying basic information before it is entered into the registers.
394. Direct and comprehensive access to information held in the different registers is provided by the Common Register Portal of the *Länder*, which has been in existence since 2007 and is operated by the *Land* of North Rhine-Westphalia on behalf of all Germany's *Länder*. This Portal creates a single point of central access to information collected and held by the *Länder* on the Commercial Register, Cooperative, and Partnership Registers and the Register of Associations. Anyone, including non-German authorities, can use the Common Register Portal to access. Data retrieval is subject to a charge in certain cases. However, this does not apply to bodies such as Federal or *Länder* LEAs and some other German and foreign public agencies.
395. The Common Register Portal of the *Länder* is easily accessible by both authorities in the public and private sector and was regularly used. Due to the strict notarisation requirements, it was reported as rare that information contained on the register was found to be inaccurate. In these circumstances, authorities noted they would contact the relevant register who would make amendments but examples were not provided.

396. Civil Law Partnerships (GbRs) are not currently required to register on the Commercial Register and will not be required to register on the Transparency Register. Germany estimates there were 572 139 civil law partnerships engaged in business activity in 2017 which is a significant number of entities that will not be required to register. Despite the majority (201 638 GbRs) of these generating a low-income of EUR 10 000 or less, Germany recognises that they do present a ML/TF risk given their relatively informal nature. The NRA has identified GbRs as susceptible to ML due to their diverse and flexible form. They can also be created with little red tape (there are no requirements to involve a notary or formally register the partnership) and can be created quickly to set up an ML scheme. Germany explained that the risk is mitigated to some extent as the partnership model is less vulnerable to abuse and less attractive for ML schemes as there is no limited liability and it is not possible to obtain anonymity in financial transactions to the same extent as is offered by limited liability companies. Germany does collect some basic information on GbRs through both tax filings and requirements to file with other authorities. If a GbR acquires land, all of the partners of a GbR must also be entered by name in a German real estate register (*Grundbuch*). Based on data collected in 2017, 190 621 GbR were engaged in letting and leasing activity. GbRs that acquire shares in a GmbH must be entered as a shareholder on the Commercial Register. Based on data from the Transparency Register, this concerns approximately 10 000 GbRs. Germany has also passed legislative reforms to introduce a Partnership Register in 2024 to address this gap. However, these reforms will not be in effect until 2024 and it is not clear that the new register will fully cover the provision of all basic and BO information. This issue is considered a deficiency due to the lack of a detailed risk understanding of the risk arising from GbRs and unavailability of accurate and up to date basic and BO information through a route that can be accessed in a timely manner.
397. In respect of foundations, the information and transparency obligations relating to disclosure of the beneficial owner (i.e. registration on the Transparency Register) is as applicable. Each of the foundation registers maintained by the *Länder* can also be accessed for information on foundations under private law with legal capacity domiciled in Germany. Anyone is allowed to inspect the registers without giving a reason. The registers provide details of the name, legal nature, registered office, purpose and address of the foundation. Information is also provided on the bodies and persons authorised to represent the foundation and the type of authorisation they hold, and on the competent supervisory authority. The foundation registers are continuously updated by the *Länder* and can be viewed free of charge at any time via the relevant websites. However, the online availability varies as not all *Land* have made register available online.

*Transparency Register*

398. The implementation of the Transparency Register in 2017, and subsequent legislative amendments to its operation in 2021 are critical steps for Germany in ensuring availability of adequate, accurate and current basic and beneficial ownership information. Information on the Transparency Register has been publicly available since 2020. However, due to the original remit of the Transparency Register relying on existing registered information on other Registries (such as the Commercial Register) and a lack of oversight to ensure required filing by the Federal Office of Administration, at the time of the on-site the Transparency Register had major deficiencies concerning the availability of accurate information. In particular, there were numerous missing or incorrect entries have been highlighted in open-source media and by civil society.<sup>71</sup>
399. A major issue with the functioning of the Transparency Register between 2017 and 2021 has been that if information on a legal entity was previously registered on the Commercial Register, registration would not be required on the Transparency Register unless there were very specific circumstances. This was the position even though the Commercial Register does not contain beneficial ownership information in most circumstances. This created the notion of a “fictional” beneficial owner. This has made the accuracy of the Transparency Register debatable as was noted by the private sector during the onsite. This has meant that until recent changes to the Transparency Register, it has not been regularly used by the private sector in carrying out their CDD obligations to identify beneficial ownership.
400. Since August 2021, there is a new, two-pronged approach to improve the accuracy of information on the Transparency Register by creating a full register of beneficial ownership information. Firstly, this will require obliged entities to verify information available on the Transparency Register when conducting CDD with a legal requirement to file discrepancy reports if the information is inaccurate. Secondly, the amendments introduced a direct requirement for all entities to file with the Transparency Register without delay, however these are generally subject to transition periods (determined by type of entity) which last up until the end of 2022. Taken together, these measures will significantly improve the accuracy of available information if the refiling and discrepancy reporting is properly enforced and is able to be dealt with through appropriate human resource in the Transparency Register. Germany will also require registration of information in higher risk sectors, notably property with foreign ownership where if there is a foreign company who directly or indirectly owns real estate in Germany they will be also required to file a report with the Transparency Register.
401. The Transparency Register has received 23 000 discrepancy reports between January 2020 and November 2021 and this requires an element of manual and automated processing to process. Given the significant new filing requirement along with the number of discrepancy reports expected to be received, Germany must ensure adequate human and technical resource in order to improve the accuracy of this information. Plans are in place to recruit new staff for this purpose but they were not in place at the time of the on-site.

---

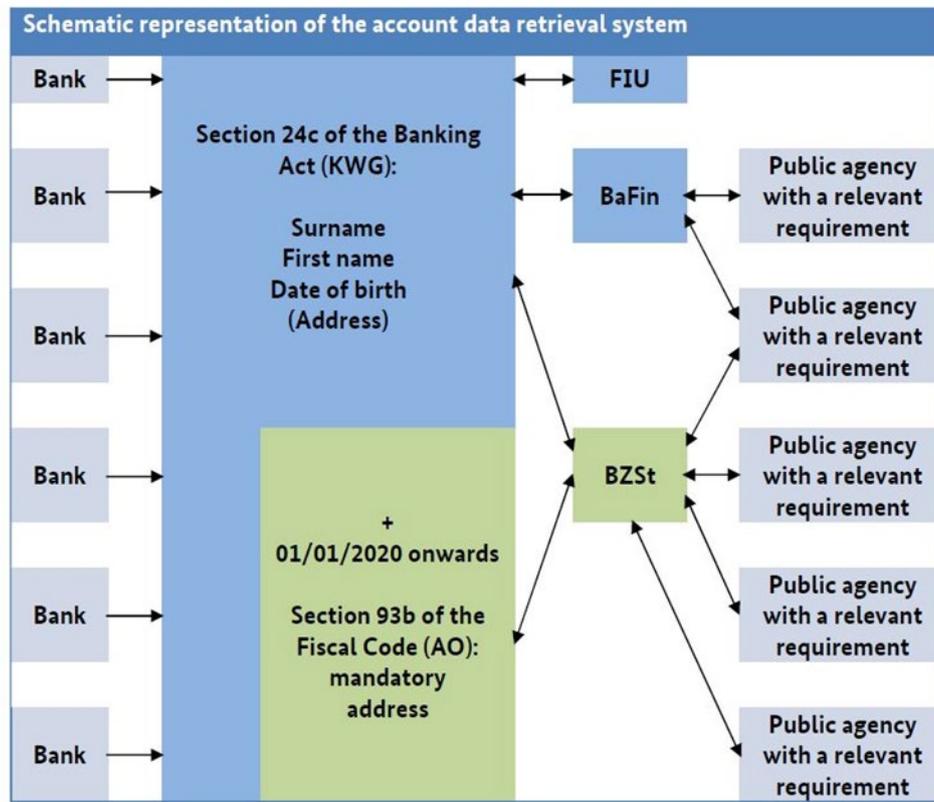
<sup>71</sup> Ibid.

402. A significant gap exists with respect to information on legal persons not currently required to register on the Commercial Register. While foundations, co-operatives and partnership companies will be required to register, associations are not required to register on the Transparency Register in all circumstances. Information on Associations will be fed into the Transparency Register from the current Register of Associations if the beneficial owners are the same persons who are registered as legal representatives of the Association but there will be no requirements for separate verification of the information which limits its accuracy and usefulness. In other circumstances, a separate registration on the Transparency Register is required.
403. After the implementation of all these changes, the Transparency Register will be a single point of access for basic and beneficial ownership information. The assessment team considers that this goal should be strongly pursued by Germany to simplify the search options for both the public and private sectors (potentially with the option of adding in connectivity to additional register, notably the *Land* (property) registers. This will ensure that when checks are made against the information there is more chance of a single check producing a comprehensive set of information and avoiding omissions. However, Germany needs to give consideration to how to cover the categories of legal persons not currently registered on the Commercial Register which are also vulnerable to abuse for ML and TF (such as GbRs).

#### *Identification of BO through bank account register*

404. Germany has a significant tool to limit the misuse of legal persons in the form of the Electronic Account Retrieval System which has been in place since 2003. This allows German competent authorities with a “relevant purpose” access to account and deposit account data as well as safe deposit box information held by German credit institutions and branches of foreign credit institutions operating in Germany.
405. Information can be retrieved on a variety of fields including information on the name, date of birth and address of beneficial owners of accounts held by legal persons. At 30 June 2021, 650 774 043 accounts were accessible via the data retrieval system, 344 061 288 were active accounts.
406. The retrieval system is operated by BaFin and the Federal Central Tax Office and these are routes that other authorities (such as law enforcement) can use to request information from the system (see the diagram below). Requests are processed on a case-by-case basis and the length of time it takes to complete a request depends on the complexity and nature of the request but most are processed within one working day.

Figure 7.1. Electronic Account Retrieval System



Note: While the FIU is meant to have direct access to the system, technical issues have prevented this from being implemented. At the time of the on-site, the FIU was accessing the system through requests to the BZSt.

Source: German Authorities

407. The system is regularly used by authorities with the greatest usage being police authorities with over 219 000 data retrievals made during 2020 (see IO.6). However, the FIU currently does not have direct access<sup>72</sup> and has made limited use of this system so far with a comparatively small number of data retrievals. The information in this database depends on the CDD undertaken by regulated entities (see in Chapter 5 for more information on the quality of this information). When information is changed on the owner of a bank account by a relevant entity, this is immediately updated on the system. Germany presented examples of the account retrieval system being used for investigations of suspected TF and where there was risk to life/risk of harm but these focused on identifying the accounts held by the natural persons. Germany did not demonstrate that the system was used to analyse the beneficial ownership of complex legal structures and understand their beneficial ownership. Along with the issues identified in IO.1 and IO.7 in relation to a lack of investigations involving legal persons in ML/TF, this suggests that FIU and law enforcement access and use of BO information to prevent legal persons and arrangements from being used for criminal purposes is limited. Equally, whilst the account data retrieval system is a positive mechanism in some circumstances, there is no requirement for legal persons / arrangements to hold a bank account in

<sup>72</sup> As part of the redesign of the system, the FIU will be integrated as a query centre and connected via its own interface and gain direct access in 2022.

Germany or with a German subsidiary. Germany was unable to provide general statistics on how many legal persons/arrangements in Germany held German bank accounts that were entered in the account data retrieval system. Whilst it is a positive aspect of the German regime and a useful tool for LEAs, this mechanism can only be considered to mitigate the risk of abuse of legal persons to some extent.

408. The Electronic Account Retrieval System does not interact with the Transparency Register or other Registers and there are no plans for the information on the Transparency Register or other Registers to be cross-checked or verified with the information available through the Electronic Account Retrieval System.

#### *Obligated Entities and CDD obligations*

409. Generally, CDD obligations carried out by obliged entities were found to be reasonable, with generally good procedures for identifying beneficial ownership identified for FIs and a more limited knowledge identified for DNFBPs. However, when questioned, the authorities did not tend to access basic or beneficial ownership information directly from obliged entities and instead relied upon the registers or the bank account retrieval system to obtain this information.

#### ***Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements***

410. Germany ensures timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements to a limited extent. The issues around the maintenance and verification of information on the different registers for legal persons also applies to legal arrangements and restricts their usefulness to LEAs as they cannot be relied upon for accurate and current information.
411. Express trusts cannot be created under German law but contractual relationships named *Treuhand* (a German trust-like arrangement) and foreign trusts are recognised and are required to comply with transparency requirements. Lawyers, legal advisors, notaries and trust and company service providers who act as trustees are required to obtain and hold information on the persons from who they have received assets for management and the persons for whose benefit they manage those assets and register this information on the Transparency Register.

#### ***Effectiveness, proportionality and dissuasiveness of sanctions***

412. Germany has applied both administrative fines and supervisory sanctions for failing to file basic and beneficial ownership information. Overall, Germany has implemented effective, proportionate and dissuasive sanctions to some extent. Overall sanctions were low and while they may be dissuasive for natural persons and small businesses, it is less dissuasive for legal persons. The assessment team based its findings on: statistics, case studies and interviews with competent authorities.

*Transparency Register*

413. The Federal Office of Administration is responsible for implementing sanctions for breaching reporting obligations in relation to the Transparency Register. The Federal Office of Administration has demonstrated a range of penalties were imposed and issued a schedule of penalties that could be applied to different situations. This takes into account a variety of factors including the seriousness of the conduct and the intention of the party. The highest penalty possible in 2020 for failures to notify is a fine of EUR 66 667 although under the GwG, a maximum penalty of EUR 5 million may be applied. Average fines from 2018 and 2019 (presented below) are low and may be proportionate and dissuasive for natural persons but are not be adequately dissuasive for legal persons.

**Table 7.1. Sanctions for breaches: Transparency Register, 2018-2019**

	2018	2019
Number of fines	1 889	4 218
Average amount of fine (EUR)	1 942.75	1 489.39

Note: Statistics were only captured from February 2018.  
Source: German Authorities

414. The sharp rise in the number of cases where a fine was applied in 2019 can be explained by the increase in staffing levels and advanced automation in the processing of individual cases. Authorities' abilities to identify non-filing and failure to notify in good time (change filing) is becoming more sophisticated through the adoption of modern technology.
415. However, the failure for the Federal Office of Administration to have an adequate process to ensure filings on the Transparency Register (as identified by missing information) still means that sanctions and fines may not be being adequately implemented. In this regard, Germany is encouraged to review the sanctions policies/procedures and levels in line with the significant amount of filing that will occur under the new Transparency Register legislation before the end of 2022 so that the can form a strategy for non-filing, along with dissuasive sanctions.

*Sanctions for obliged entities*

416. BaFin has responsibility for sanctioning obliged entities in the financial sector for offences related to beneficial ownership requirements. For obliged entities in the non-financial sector this responsibility lies with the supervisory authorities of the *Länder* and with the chambers. Between 2015 and 2019, BaFin issued 63 warnings and fines to natural persons and 13 to legal persons for breaches of obligations around beneficial ownership. As set out below, the average fines for natural persons was EUR 1 036 and for legal persons was EUR 6 364. These penalties may be proportionate and dissuasive for natural persons but may not always be adequately dissuasive for legal persons.
417. Fines are also available under different laws for failures to comply with obligations to register and update information on various *Länder* registers and disciplinary action is possible against notaries for verification failures. However, the extent to which this is used was not demonstrated to the assessment team.

**Table 7.2. Sanctions for breaches: BaFin, 2015-2019**

	<b>Number of fines</b>	<b>Fines (total amount)</b>
Fines imposed on natural persons	43	EUR 44 545 Average = EUR 1 036
Fines imposed on legal persons	9	EUR 57 280 Average = EUR 6 364
Warnings (with fines) imposed on natural persons	20	EUR 220
Warnings (with fines) imposed on legal persons	4	EUR 55

Note: Some, but not all warnings are accompanied by a nominal fine.

Source: German Authorities

7

## Overall conclusion on IO.5

Germany has taken positive steps to enhance transparency including conducting a sector-risk assessment on legal persons and arrangements and ongoing enhancements to the Transparency Register to make it a full register for basic and BO information. However, a number of these measures are yet to be fully implemented and were not in effect at the time of the on-site. Considerable gaps in the scope of entities covered by the Transparency Register, issues with the accuracy of information held remain as major deficiencies. Issues in relation to proactively reducing the risk of bearer shares and available information on GBRs is also material. Alternative measures, mainly the Electronic Bank Account Retrieval system, are used to some extent to access beneficial ownership information. It was not demonstrated that BO information was being regularly and routinely accessed via regulated entities, or through FIU or law enforcement channels. Considering Germany's risk profile as an international financial and economic centre, major improvements are needed.

**Germany is rated as having a moderate level of effectiveness for IO.5.**

## Chapter 8. INTERNATIONAL COOPERATION

### Key Findings and Recommended Actions

#### Key Findings

- a) Germany has an effective legal and operational framework in place for mutual legal assistance (MLA), extradition and asset recovery (including repatriation). Germany provides assistance promptly and its requests and responses are generally good quality. Assistance can be provided without a treaty to any country and the scope of assistance that can be provided is broad and includes all the tools that LEAs can use for domestic investigations.
- b) Germany's primary international partners are other EU member states and co-operation with these countries is simplified and streamlined through regional frameworks like the European Investigation Order (EIO) and European Arrest Warrant (EAW) schemes rather than standard, formal MLA and extradition processes.
- c) Germany actively seeks co-operation in ML, TF and predicate offence cases. Co-operation is facilitated by Germany's use of international networks, bilateral engagement and liaison officers. Germany seeks and provides assistance in asset recovery cases, although it is not clear that this is being pursued proactively in line with Germany's risks because statistics on asset repatriation are not kept.
- d) Germany's de-centralised model for co-operation means that, record keeping, case tracking and case management at a national-level remains a significant challenge for Germany. There are very limited statistics available on MLA and agency-level co-operation. This makes it more challenging for Germany to avoid duplication of efforts and conflicts of jurisdiction and identify new and emerging risks and trends and proactively prioritise resources.
- e) Germany routinely uses other forms of international co-operation in a timely manner both for exchanges of information and in operational and supervisory actions. Several LEA agencies have appointed liaison officers to strategically important countries to facilitate co-operation. BaFin makes active use of various channels to engage with foreign counterparts. The general quality and timeliness of informal co-operation is good.
- f) Germany can provide basic and beneficial ownership information on legal persons and legal arrangements to foreign partners but the effectiveness in this field is impeded by the limitations identified in IO.5 regarding the verification of the BO information.

## Recommended Actions

- a) Unify the different case management systems or find another solution to establish a consolidated national system for tracking international co-operation cases (both formal and informal), particularly for MLA and asset recovery and where it is currently not collected. This system should enable authorities to identify areas of duplication, avoid conflicts in jurisdiction, and allow for the collection of comprehensive national statistics.
- b) For extradition cases, implement a system for tracking the time taken to process and execute extradition requests.
- c) Proactively use international co-operation tools in asset recovery cases to target and, where appropriate, repatriate proceeds of crime coming into Germany from foreign countries.
- d) Continue to enhance engagement with international co-operation partners in alignment with Germany's risk profile and continue to proactively work to promote and enhance informal co-operation with priority countries.
- e) Consider implementing a mechanism for verifying or corroborating BO information obtained from different registers, particularly the Transparency Register and the Commercial Register, before disseminating information to foreign counterparts while the information pool is still being populated and verified.

418. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40 and elements of R.9, 15, 24, 25 and 32.

### Immediate Outcome 2 (International Cooperation)

419. Germany is an important international financial centre and faces significant risks as a destination country for foreign proceeds and transit country for funds to enter and leave the European single market. Germany's main international co-operation partners are EU-member states. Outside of the EU, the NRA has identified Switzerland, the UK, the US, Türkiye, Russia and the Balkan states as the highest risk countries for ML and TF. Germany makes use of two different regimes for co-operation with EU member states and other countries. The EU frameworks establishing the European Arrest Warrant (EAW) and European Investigation Order (EIO) simplify and expedite MLA and extradition between Germany and other EU member states. This is beneficial as the majority of outgoing and incoming requests involve EU member states. Germany's legal framework allows for the provision of MLA to all countries without a treaty or reciprocity. Extradition can also be executed without a treaty on the basis of reciprocity. However, bilateral and multilateral treaties facilitate the process and the majority of the remaining requests for cooperation flow through these channels.

420. Germany's takes a decentralised approach to international cooperation with the majority of requests dealt with at the *Länder*-level (MLA and extradition) and agency level (other forms of cooperation). In this context, co-ordination and co-operation between different domestic authorities is a particular challenge.
421. It should be noted that because of the de-centralised approach, statistics on international co-operation are not maintained consistently. While there are some limited national statistics on extradition matters, there are no comprehensive national statistics maintained on MLA and other forms of co-operation.

### *Providing constructive and timely MLA and extradition*

422. Germany provides constructive and timely assistance in MLA (including asset recovery) and extradition cases to a large extent. As mentioned above, Germany does not maintain comprehensive statistics on MLA. To demonstrate effectiveness, authorities compiled statistics for a period of 12 months from 1 June 2019 to 31 May 2020. Interviews with German authorities indicated that this was a broadly representative sample. To assess Germany's effectiveness over time, the assessment team relied on interviews with prosecutors (Bfj, GBA and *Länder* prosecution offices), LEAs (BKA, LKAs, Customs, BFV), case studies and feedback from FATF and FSRB (FATF-style regional bodies) delegations.

### *Mutual legal assistance*

423. Germany typically provides high quality, constructive and timely MLA and provides a wide range of assistance. Requests for assistance sent from EU member states under the EIO scheme can be sent directly to *Länder*-level courts and public prosecution offices who are responsible for deciding whether to accept or decline the request and executing the request. EIOs are the most commonly used channel for receiving requests for assistance. For requests from non-EU member states, the Federal Office of Justice (Bfj) acts as a central authority to review and disseminate requests to the relevant *Länder* competent authority. The Bfj also provides assistance to foreign countries making requests to Germany by reviewing draft requests and acting as a central point of contact for enquiries. While the Bfj monitors the requests it disseminates, it does not have a co-ordination or decision-making function. These powers and responsibilities have been delegated to the public prosecutor offices in the *Länder*. Where it is not clear which *Länder* has responsibility or where multiple *Länder* are involved, co-ordination is governed by *Guidelines on Relations with Foreign Countries in Criminal Matters* (RiVAST) and is done on an ad-hoc case-by-case basis. The RiVAST requires *Länder* to consult with each other on how to handle a request and determine one *Länder* to execute or coordinate the request or agree that each *Länder* will act independently on different parts of the request. Case studies, interviews with LEAs and feedback from delegations indicates that this system works well in practice. However, there is a risk of duplication of efforts. Germany has a decentralised model for case tracking management with different *Länder* operating different systems at the investigation level with no national sharing of information. In some cases, this can lead to duplication of efforts. In one case, it was found that authorities from two different *Land* had unknowingly attempted to seize the same bank account in two separate domestic investigations.

424. Germany receives a reasonably high number of MLA requests. In one 12 month period from 2019 to 2020, 392 ML-related requests were received and 14 TF requests were received. Approximately 6% of cases are refused because of lack of competence, practical obstacles such as a witness not being available, pending domestic investigations that could be compromised by providing assistance and deficiencies in the request. Liaison networks like Camden Asset Recovery Network (CARIN) and the European Judicial Network in addition to the European Union Agency for Criminal Justice Cooperation (Eurojust) are used to facilitate co-operation as much as possible by creating informal networks and communication channels for case work, reviewing and consulting on draft request and sharing information outside of the formal MLA process wherever possible.

**Table 8.1. Number of incoming requests for MLA in ML and TF cases**

	ML	TF
EU countries	325	12
Non-EU countries	67	2
<b>Total</b>	<b>392</b>	<b>14</b>

Note: These statistics cover the period 1 June 2019 to 31 May 2020 and includes both European Investigation Orders and from MLA requests. Statistics on other time periods were not available.  
Source: German Authorities

425. Under German law, requests for assistance (both EU and non-EU) are treated in the same way as domestic investigations, which means that all the investigative measures available in domestic investigations can be used to support a foreign investigation. A wide variety of assistance is provided by Germany, including access to bank records and other financial information, searches and telecommunications intercepts. Most ML/TF requests received are for information on bank accounts; Germany is able to process such requests quickly and easily using BaFin's central bank account register (the Electronic Account Retrieval System). Feedback from foreign counterparts, including key partners, indicates that the assistance provided by Germany is high-quality and contributes to international AML/CFT efforts.

**Table 8.2. Incoming requests for MLA: types of assistance requested**

	ML	TF
Interviewing a witness	137	6
Interviewing a suspect	44	1
Identification of person by phone number or IP address	3	1
Traffic information	6	1
Information on bank and other financial accounts	193	1
Telecommunications intercepts	3	0
Observation of people	1	0
Search of homes and businesses and business records	13	0
Seizure and confiscation	7	0
Freezing of assets (temporary measures)	22	0
Restitution (transfer of assets to a victim of crime)	1	0
Other (e.g. requests for documents, investigation of the accused's income)	75	0

Note: These statistics cover the period 1 June 2019 to 31 May 2020. Statistics on other time periods were not available. One MLA request may request multiple types of assistance, which is why the totals here do not match Table 8.1.

Source: German Authorities

426. MLA is generally provided in a timely manner. EIO requests have time limits set out in law and in directives to competent authorities. Public prosecutors must confirm receipt of the request within one week, approve or decline the request within 90 days and then execute the request within a further 90 days. Delays that would exceed these time limits trigger reporting obligations and requirements to consult with the requesting country. Requests outside of the EIO framework are not subject to strict legal time limits. However, under the RiVAST, there is a general requirement for decisions on MLA requests to be made within 30 days and requests to be executed within 90 days. Case studies, statistics and feedback from co-operation partners indicate that these timeframes are complied with for the majority of requests. From 2019 to 2020, approximately 75% of requests were executed in three months or less (see table 8.3 below). Prosecutors have systems in place to prioritise cases identified as urgent or otherwise time sensitive by the requesting country are prioritised. The reasons provided for delays are reasonable (for example, difficulties in identifying a witness; potential to jeopardise domestic investigations; missing information in the request or lack of necessary guarantees/assurances). For example, information provided by two *Länder*, Bavaria and Baden-Württemberg, shows that almost all requests were executed within a period of 1 to 3 months, in many cases even within a period of less than one month. Only in very few cases did the execution of an incoming take 3 to 6 months or longer. In very rare cases it took 9 to 12 months. In each of these cases, there were objective reasons for this, for example numerous reciprocal and interrelated requests with the initially requesting state which delayed the final resolution of the request.

**Table 8.3. Incoming requests for MLA in ML and TF cases 2019-2020: time taken to execute the request**

	ML	TF
Less than 1 month	61 (22%)	2 (22%)
1-3 months	143 (52%)	4 (44%)
3-6 months	58 (21%)	3 (33%)
6-9 months	5 (2%)	0
9-12 months	6 (2%)	0
<b>Total</b>	<b>273</b>	<b>9</b>

Note: These statistics cover the period 1 June 2019 to 31 May 2020 and includes both EIO and MLA requests. Statistics on other time periods were not available. The total number of requests does not align with the figures presented in tables 8.1 and 8.2 because statistics were only collected for a limited period and refers only to requests executed over the 12 months and would include requests received before 1 June 2019 but would not include requests executed after 31 May 2020. The figure does not include requests that were declined in 12 month period.

Source: German Authorities

*Asset recovery and asset sharing*

427. As with other forms of MLA, Germany is able to provide assistance with tracing, seizing, freezing and confiscating assets using the same tools as would be available for a domestic investigation. Germany is able to share assets with foreign countries (see R.38). There were no statistics available on the total number of cases involving asset recovery and asset sharing and a limited number of case examples. However, Germany provided information on the type of assistance requested in ML or TF-related MLA requests; 6% of these requests were for assistance in asset recovery (see Table 8.2 above). Germany provided some case examples where assets had been confiscated and repatriated to a foreign country pursuant to an MLA request. It is clear that asset recovery and repatriation cases are being pursued to some extent in Germany. However, because statistics on asset repatriations are not kept, it is not clear that asset repatriation is being fully in line with Germany's risk profile. Germany's FIU has access to an immediate freezing power that allows it to freeze transactions for one month where there it has reason to believe that the transaction is connected to ML or TF. The FIU uses this power where additional time is required to analyse the transaction. This tool would be particularly useful in the context of MLA requests related to asset recovery. In 2019, this tool was used successfully in 5 cases to temporarily block transactions of more than EUR 4 million.
428. Since 2020, the EU has established strict time limits requiring freezing orders to be recognised in 48 hours and freezing to be executed in the next 48 hours. The implementation of these requirements by Germany remains in a planning stage and German authorities did not seem to have the resource capacity to respond to requests within these limits. Case studies indicate Germany faces challenges freezing assets within this short a time period.

**Box 8.1. Case study: provisional asset freezing (FIU-INT-2)**

In this case, a foreign FIU requested information from the German FIU about a company making a number of transactions to German bank accounts. The funds comprised about EUR 100 000 in proceeds of crime generated from an IT fraud.

The German FIU retrieved and reviewed the information and found that the accounts in Germany were payable-through accounts and a large amount of funds transferred into the German accounts had already been transferred out to other accounts in Germany and other countries. Upon the request of the foreign country, the FIU initiated a freeze on the funds still held in German bank accounts as an urgent measure and successfully blocked the movement of EUR 50 000 in funds.

The foreign country subsequently submitted a formal MLA request for the further freezing of the funds. The proceedings are ongoing.

Source: German Authorities

**Box 8.2. Case study: MLA and asset repatriation (BY-GW-46)**

In this case, a French company conducting an international transaction had funds fraudulently stolen when paying a supplier in Vietnam via an intermediary in Switzerland. Funds to be transferred to the intermediary in Switzerland were fraudulently diverted to an account in Germany.

On 12 February, 2019 the Public Prosecution Office in Nuremberg-Furth received an EIO from French justice authorities for assistance in investigating the offence and freezing of EUR 3 921 752 in assets related to the case.

On 18 February, the MLA request was granted for assistance in sharing account information and interviewing witnesses. On 14 May 2019, a German court approved the freezing of EUR 1 866 955.87 in assets held in a German bank account and returned these funds to France in full. While there was some delay in the granting of the asset freeze (including across a weekend), German authorities had been proactive in commencing a domestic investigation and using other powers to freeze the assets while the court proceedings were ongoing.

Source: German Authorities

*Extradition*

429. There are two extradition regimes in operation in Germany: a simplified extradition process for EU member states under the European Arrest Warrant (EAW) framework and a standard procedure for non-EU members. Germany receives a high number of requests for extradition. EAW alerts with these cases making up approximately 80% of the extradition requests received by Germany. Such requests can be implemented quickly, with an extradition case taking on average between 43 days from arrest to the granting of the extradition request. In half of all EAW cases, the subject of the request consents to their extradition and the time between arrest and the granting of the extradition is approximately 20 days. Germany is able to extradite in approximately 80-85% of cases although it is difficult to compare figures across years as cases may not be finalised in the same year that the extradition is requested.
430. For EAW requests, the main reason for refusing extradition are on human rights grounds or where a judgement has been entered in absentia. Statistics are not kept on why the request was refused for non-EAW requests which may hamper Germany's ability to identify or quantify over-reliance on specific grounds for refusal or issues with requests from particular countries or *Länder*. Germany does not extradite German nationals to non-EU member states. Germany has refused to extradite on this ground, but could not confirm how many cases there had been. There is a general obligation and framework in place to prosecute in lieu of extradition in such cases, and Germany cited one recent case where this had happened. However, in the absence of further information, it is not clear that Germany is systematically prosecuting where extradition is refused based on nationality.

431. Unlike MLA, Germany maintains national statistics on extradition, although these cannot be broken down by specific offence beyond broad categories so it is only possible to see what cases relate to terrorism but not TF. Discussions with authorities indicate that Germany receives a reasonable number of extradition requests related to ML and some requests for TF. However, it is not clear what percentage of these cases were carried out and what percentage were refused.
432. Germany was not able to provide statistics on the timeframes in which extradition cases must be carried out for non-EAW extradition requests as these statistics are not currently collected and this could not be assessed.

**Table 8.4. Incoming requests for extradition 2017-2019**

	2017	2018	2019	2020	Total
<b>Total requests received (EAW and non-EAW extradition requests)</b>	1 721	1 760	1 686	1 545	6 712
<b>EAW alerts</b>	1 419	1 423	1 346	1 640	5 828
<b>Requests granted</b>	1 423	1 498	1 485	1 294	5 700
<b>Requests rejected</b>	284	265	378	403	1 330
<b>Requests otherwise disposed of</b>	106	124	114	139	483
<b>ML requests (includes receipt of stolen goods)</b>	59	49	80	52	240
<b>ML requests granted</b>	52	40	63	44	199 (83%)
<b>Terrorism requests</b>	24	26	68	62	180
<b>Terrorism requests granted</b>	14	5	7	1	27 (15%)

Note: Requests otherwise disposed of refers to cases that were concluded by other means, for example, if the wanted person has died or the requesting country has withdrawn the request. Note also that the figures refer to terrorism cases as statistics on TF were not available. A high number of terrorism-related requests were denied due to an unusually large number of requests being received in 2018-2019 from one country where there were concerns that individuals were being sought for political purposes. "EAW alerts" means extradition requests made under the EAW framework.

Source: German Authorities

### *Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements*

433. Germany is a financial centre and because of the exposure to international financial flows, many of Germany's ML, TF and predicate offence cases have an international element. Germany actively seeks MLA and extradition in these cases, including pursuing requests for asset freezing and confiscation. The assessment team's findings are based on: available statistics on MLA (from a 12 month period of June 2019 to May 2020) and extradition, interviews with prosecutors and LEAs, case studies and feedback from FATF and FSRB delegations.

*Mutual legal assistance*

434. The decision to request MLA is generally made by a public prosecutor following the Guidelines set out in the RiVAST. Over a 12-month sample period, Germany made 446 requests for assistance in ML cases and 14 requests for assistance in TF cases. The majority of these requests (88% for ML and 71% for TF) were made to other EU member states under EIOs. Case studies, feedback from foreign counterparts, and discussions with German authorities indicated that EU countries regularly account for the vast majority of Germany's requests. Germany provided a sample table of the types of assistance being requested and it shows a broad range of assistance is being requested by Germany in ML cases. Most requests are for bank and other financial account records and interviews of suspects and witnesses.
435. Feedback from FATF and FSRB delegations indicates that Germany sends requests that are good quality. This is facilitated by Germany's extensive participation in international networks/agencies including Eurojust and the European Judicial Network, which it actively uses to establish contacts, seek help drafting requests, and obtain informal co-operation in advance of formal MLA. Germany has established regular bilateral engagement with key international co-operation counterparts to facilitate MLA. For example, in 2019, Germany had 20 bilateral meetings with EU member states and non-EU states including Brazil, India, the US and the United Arab Emirates. Germany is also proactive in engaging higher-risk countries including Türkiye, Russia and Balkan States. Germany has also taken the step of having staff exchanges and establishing liaison officers in priority countries. For example, Germany established a reciprocal staff liaison posting for a German judge in the French Minister of Justice and a French liaison judge based in the German Ministry of Justice to facilitate co-operation.

**Table 8.5. Outgoing requests for MLA in ML and TF cases**

	ML	TF
EU countries	397	10
Non-EU countries	44	4
<b>Total</b>	<b>446</b>	<b>14</b>

Note: These statistics cover the period 1 June 2019 to 31 May 2020. Statistics on other time periods were not available.

Source: German Authorities

**Table 8.6. Outgoing MLA requests: types of assistance requested**

	ML	TF
Interviewing a witness	60	5
Interviewing a suspect	193	0
Identification of person by phone number or IP address	3	1
Traffic information	6	1
Information on bank and other financial accounts	280	2
Telecommunications intercepts	0	1
Observation of people	5	1
Search of homes	22	1
Seizure and confiscation	11	0
Freezing and confiscation of assets	8	0
Restitution	2	0
Other (e.g. requests for documents, investigation of the accused's income)	78	2

Note: These statistics cover the period 1 June 2019 to 31 May 2020. Statistics on other time periods were not available.

Source: German Authorities

### *Asset recovery*

436. Germany actively requests assistance in asset recovery cases. Looking specifically at ML and TF cases, over a 12-month sample period, 19 requests for assistance were made. Case studies demonstrate that Germany is seeking assistance from foreign countries, to freeze and confiscate assets but the number of asset recovery requests is low. Considering there were a total of 460 outgoing requests for assistance in ML and TF cases, assistance with asset freezing and confiscation was only sought in 4% of cases. Requests are being made in line with the country's risk profile for the most part but request to higher-priority non-EU countries seems low. For example, in the 2019 sample period, there were no asset freezes in the UK, US or Russia which were all countries identified by Germany as important for international crime co-operation.

**Table 8.7. Asset frozen overseas in German cases: 2019**

Country	Number of cases	Assets frozen (EUR)
Lebanon	1	3 000 000
Kosovo	3	2 289 691
Latvia	1	1 164 194
Netherlands	6	1 056 050
Poland	1	1 000 000
Türkiye	2	646 519
Finland	3	526 292
Czech Republic	4	339 988
Lithuania	3	275 290
Slovakia	1	272 026
Belgium	3	250 900
Norway	1	248 689
Switzerland	3	180 200
United Arab Emirates	1	171 200
Spain	5	137 746
Austria	2	133 500
Romania	3	108 999
Slovenia	1	62 577
France	1	23 900
Hungary	1	23 000
Luxembourg	1	22 000
<b>Total</b>	<b>47</b>	<b>11 932 761</b>

Note: EU-countries are highlighted.

Source: German Authorities

### *Extradition*

437. As with MLA, the decision to request extradition is led by the public prosecutor in charge of a case. The EAW regime is the most commonly used framework and the majority of requests are to EU member states, which is largely in line with Germany's risks. While Germany does not have statistics on the total number of requests made under the EAW regime, authorities report that in 2017, 1 367 people were extradited or surrendered to Germany and 90% of these cases (1 234 people) were surrendered or extradited under the EAW scheme. In 2018, Germany reported that 87% of people were extradited or surrendered under the EAW scheme (1 185 people out of a total number of 1 367). In 2019, 86% of people were extradited or surrendered by the EAW scheme (1 117 people out of a total number of 1 293). Germany makes active use of extradition. From 2017 to 2019 it made 68 requests for extradition in ML cases and six requests for assistance in terrorism cases (including TF). The overall number of extradition requests seems reasonable and rose significantly in 2019. Feedback from FATF and FSRB delegations indicates that Germany's requests for assistance were generally of good quality.

**Table 8.8. Outgoing extradition requests: 2017-2020**

	2017	2018	2019	2020	Total
Total requests outgoing	1 316	1 308	1 351	1 095	5 070
Requests granted	1 367	1 367	1 293	1 068	5 095
Requests rejected	56	60	61	52	229
Requests otherwise disposed of	61	73	68	48	250
ML requests	18	21	33	19	91
ML requests granted	16	18	30	17	81
Terrorism requests	3	4	1	1	9
Terrorism requests granted	3	3	0	1	7

Source: German Authorities

### *Seeking and providing other forms of international cooperation for AML/CFT purposes<sup>73</sup>*

438. Germany is actively engaged in a range of networks to facilitate informal co-operation. Other forms of co-operation are sought and provided to a large extent. The assessment team's findings are based on: available statistics; interviews with prosecutors, LEAs, supervisors and the FIU; case studies; and feedback from FATF and FSRB delegations.

#### *Law enforcement agencies*

439. Police-to-police cooperation is channelled through the BKA as the central agency for police information and intelligence. The BKA co-operates extensively with foreign counterparts through Eurojust, Interpol and Europol. The BKA has an extensive network of 65 liaison officers posted in 50 countries, including Germany's key partners and jurisdictions identified as posing ML/TF risks. These offices facilitate the international exchange of information and execution of requests for international co-operation, including ML and TF cases but are not specialised in financial investigations. Germany presented a number of cases to show how liaison officers have been used to facilitate international cooperation through both formal and informal channels.

**Table 8.9. Interpol requests for ML and TF searches 2016-2020**

	2016	2017	2018	2019	2020
Outgoing requests for ML-related searches	27	21	13	10	34
Outgoing request for TF-related searches	0	0	0	1	1
Incoming request for ML-related searches	76	94	164	184	177
Incoming request for TF-related searches	16	10	16	22	18

Source: German Authorities

<sup>73</sup> This section covers core issues 2.3 and 2.4.

440. Customs plays a role in investigating Customs-related offences, including ML-cases involving cross-border smuggling of cash or goods. Customs is active in pursuing bilateral co-operation with its own network of Customs liaison officers. At the time of the on-site, Customs has posted liaison officers to 19 countries, including key partners, to facilitate international co-operation. Participation in five Joint Centres with France, Luxembourg, Belgium, Denmark, Poland and the Czech Republic play an important role in co-ordinating cross-border operations. As part of broader EU initiatives, Germany participated in operation Joint Customs Operation Cerberus in 2017 and in operation Daphne in 2019, both targeting cash smuggling. Customs is also able to share information spontaneously with foreign counterparts. Prosecutors in Germany play an active role in investigations and can exchange information with counterparts through a variety of networks/agencies including Eurojust and the European Judicial Network. Germany is an active participant in asset recovery networks including the EU network of Asset Recovery Offices (AROs) through the Bfj and CARIN through the Bfj and BKA. German LEAs and prosecutors make extensive use of Joint Investigation Teams (JITs) with other EU member states under a simplified EU framework. In 2020, Germany was a participant in 23 JITs and was active in 9 JITs as of June 2021.
441. Prosecutors are able to informally share information that would normally require an MLA request outside of the MLA framework as a “spontaneous exchanges of information” in cases where the information is necessary to facilitate criminal prosecutions or avert threats. This is a useful tool that can be used in urgent cases to share important information with international counterparts for example, in the context of a joint investigation Eurojust investigation into ISIL money mules with France. Statistics on the number of times this mechanism is used are not collected by Germany but several case studies were provided to show that it had been useful in a number of cases, particularly in TF matters.

### Box 8.3. Case example: co-operation through a joint investigation team and Eurojust (NI-GW-114)

Prosecutors and police in Germany established a JIT with Finnish police in June 2014, supported by Eurojust, and undertook a joint cross-border initial action. The case was initially triggered by an STR filed by a German bank in July 2012 that identified a Finnish company and a Finnish national in a suspected case of financial crime.

Through the investigation, it was found that the criminal assets were funds that had been derived from embezzlement and corruption from a Russian partly state-owned company by means of deliberately excessive invoicing by supplier companies. The criminal proceeds were forwarded via Latvia, Jersey, Germany and Panama using invoices for commission.

Italian authorities also joined the JIT after Italy's involvement in the case was discovered.

It was decided ultimately that charges should be brought in Italy and Finland. Funds were seized in Germany after domestic proceedings were initiated and pending the conclusion of the criminal cases in Italy and Finland, authorities expect to confiscate these funds.

Source: German Authorities

### *FIU*

442. The FIU has established two dedicated units with 36 staff to handle European and international requests and spontaneous exchanges of information. The FIU participates in the Egmont Group and uses Egmont channels to exchange the majority of FIU-related information. The FIU is able to exchange information and co-operate with counterparts without a treaty or memorandum of understanding (MOU) but has concluded nine MOUs with countries whose national law requires an MOU as a basis for co-operation. In 2020, there were information exchanges with 145 countries; co-operation was highest with France, Luxembourg, Malta, Italy and the UK. There is a high number of both incoming and outgoing disseminations from Germany. There was a significant rise in spontaneous outgoing request for assistance in 2019 and then a drop in 2020. The FIU explains that this variation was brought about by changes to the risk prioritisation model implemented in 2019. Feedback from other delegations indicated that co-operation with the FIU was effective and the FIU provided quality assistance in a timely manner.

**Table 8.10. FIU international information exchanges: 2018-2020**

	2018	2019	2020
<b>Outgoing disseminations</b>			
Spontaneous	3 737	8 734	4 977
On request	1 255	1 218	1 592
<b>Incoming disseminations</b>			
Spontaneous	517	804	1 451
On request	846	1 109	1 250
<b>Total</b>	<b>6 355</b>	<b>11 865</b>	<b>9 270</b>

Source: FIU annual report 2020, 2019 and 2018.

### *Supervisors*

443. FI and DNFBP supervisors are empowered under the GwG to exchange information and co-operate with foreign counterparts. BaFin regularly co-operates and exchanges information in AML/CFT matters with foreign counterparts. BaFin exchanges information in the context of institutionalised working groups and committees as well as on an ad hoc basis. This co-operation happens proactively as well as upon request and feedback from delegations confirmed co-operation is timely and constructive. BaFin can cooperate with foreign counterparts without a treaty or MOU in place but is a party to 142 bilateral and multilateral MOUs which facilitate the process. BaFin is an active member in many international bodies, including the European Supervisory Authorities' Joint Committee Sub-Committee on Anti-Money Laundering (AMSLC), European Banking Authority Working Groups and the European Commission's Working Group on ML/TF (EGMLTF). BaFin also closely engages with prudential supervisors on topics related to AML. For significant institutions, this co-operation is done with the respective Joint Supervisory Team from the European Central Bank, for less significant institutions, this is done with the respective department at BaFin as BaFin is an integrated financial supervisory authority.
444. BaFin has conducted on-site inspections abroad of branches of German obliged entities in order to check compliance with group-wide strategies and procedures. When BaFin does so, it engages with the foreign country's supervisory authority in order to get an idea of the country's specific legal requirements of the branch. Sometimes, the other country's supervisory authority also attends the on-site inspection of BaFin and the branch. Once BaFin has completed its supervisory work, it shares its findings with the other country's supervisory authority.
445. The extent to which DNFBPs supervisors participate in international co-operation exchanges could not be determined. Considering the size and nature of the Germany's DNFBP sectors and the large number of supervisors, there are likely to be challenges in this area.

**Box 8.4. Case examples: joint on-site inspections of German FI's foreign branch****Case example: co-operation with the UK FCA**

BaFin was contacted in 2017 by the UK Financial Conduct Authority (FCA) about a branch of a German financial institution that had significant deficiencies in its AML controls. This included deficiencies in know-your-customer processes, compliance awareness amongst staff and issue with the electronic transaction monitoring system. This report promoted BaFin, in consultation with the FCA, to conduct a joint on-site inspection of the bank branch. In May 2018, BaFin and the FCA participated in a two-day on-site inspection, which confirmed the deficiencies previously reported by the FCA. Following the inspection, the FCA appointed a Skilled Person to monitor the remediation of these deficiencies and provided copies of the Skilled Person's reports to BaFin so that the deficiencies could be assessed from a group wide perspective by BaFin as the group supervisor.

Both BaFin and the FCA have asked the bank to take remedial action and the branch has recruited more staff to reduce the backlog in know-your-customer processing.

**Case example: co-operation with the Swiss Financial Market Supervisory Authority**

Between 2016 and 2017, BaFin submitted two written requests to the Swiss Financial Market Supervisory Authority to conduct on-site inspections of four branches of four German banks in Switzerland and at three additional subsidiaries of one of these three German banks. This was prompted by suspicions of ML arising out of the Panama Papers case.

The on-site inspections took place in March and September 2017 and looked at over 100 client files at seven Swiss entities belonging to four German parent firms to facilitate BaFin's examination of the firms' group-wide implementation of procedures.

Source: German Authorities

***International exchange of basic and beneficial ownership information of legal persons and arrangements***

446. Information on basic information is exchanged to a large extent and beneficial ownership information is exchanged to some extent. The assessment team's findings are based on: interviews with prosecutors, LEAs, the FIU and feedback from FATF and FSRB delegations.
447. German authorities have access to a wide range of information sources for obtaining basic and beneficial ownership (BO) information and it can be freely shared with foreign LEAs. Basic and BO information is available through the Transparency Register, Commercial Register and other *Länder* registers (see Chapter 7 in IO.5). Information can also be found through the Electronic Account Retrieval System. Some information (like the *Länder* registers) is publicly available and can be accessed without a request for assistance. Access to the Transparency Register was also made public in 2020 and can be directly accessed by foreign LEAs. However, information on bank accounts through the Electronic Account Retrieval System can only be obtained through an MLA request.

448. While registry information is available, it is not clear how Germany would provide assistance to obtain BO information when the information could not be obtained through a register. It was also not clear how Germany would verify information on the register or corroborate the information. German authorities indicated that they would not generally check the accuracy of the information found on the registers if they were asked to make enquiries on behalf of a foreign country. As noted in IO.5, there is a significant amount of information on the Transparency Register which may be incomplete or inaccurate. This may impede the ability of German authorities to provide accurate information in a timely manner. It could be useful to establish a process or mechanism for corroborating and verifying BO information with FIs, DNFBPs or other public agencies before information is disseminated to foreign counterparts while the Transparency Register improves its data holdings.

## Overall conclusions on IO.2

Germany has a good framework for providing a broad range of assistance to a wide range of counterparts through both formal and informal channels. Feedback indicates that the assistance provided by Germany is good quality and timely. International co-operation is used extensively and proactively in Germany by most competent authorities, evidenced by the high number of MLA, extradition cases and high number of information disseminations from the FIU. Specific procedures and measures exist for key partner jurisdictions to facilitate co-operation in line with risks.

Data collection at the national level remains a challenge and the statistics collected on MLA, asset recovery and police-to-police co-operation are not sufficient to allow Germany to have a holistic view and hamper Germany's ability to monitor and detect emerging risks and take proactive action. The assessment team was not able to conclude that asset recovery and repatriation was occurring fully in line with Germany's risk profile as an international financial centre and destination country for proceeds of crime because statistics on asset repatriation were not available. The process for sharing BO information could also be improved to ensure that there is some verification of the information to ensure that information shared with foreign counterparts is accurate.

Considering the overall risk and context of Germany, these deficiencies are considered moderate.

**Germany is rated as having a substantial level of effectiveness for IO.2.**



## TECHNICAL COMPLIANCE

This section provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerical order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2010. This report is available [here](#).

### Recommendation 1 – Assessing risks and applying a risk-based approach

This is a new Recommendation, which was not assessed in the previous MER.

**Criterion 1.1** – Germany finalised its first NRA in October 2019. It primarily draws upon the work of four interagency working groups, including law enforcement and supervisory bodies from both federal and *Land* authorities, meeting over a period of 14 months (from December 2017). The NRA builds on other risk assessments and sources, including the supra-national EU risk assessment (SNRA), sector-specific or issue-specific assessments by federal and *Land* authorities and input from the private sector and academics.<sup>74</sup> The NRA identifies high-risk proceeds-generating offences and assesses the residual risks of ML and TF at the sectoral level using the World Bank NRA Tool (adapted for national circumstances).<sup>75</sup>

**Criterion 1.2** – The Federal Ministry of Finance (*Bundesministerium der Finanzen*, BMF) co-ordinates national risk assessments (Money Laundering Act, *Geldwäschegesetz* (GwG), s.3a).

**Criterion 1.3** – Germany’s first NRA was commenced in 2017 and completed in 2019. BMF has committed to update it in two to three years. In addition to the NRA, assessments by the FIU and BaFin are updated annually. Germany also contributes to the SNRA which the European Commission is required to update every two years (AMLD, art.4(1)).

**Criterion 1.4** – Germany has several mechanisms to provide information on the results of the NRA to all relevant competent authorities and self-regulating bodies (SRBs), FIs and DNFBPs. The NRA is available publically on the BMF, BaFin and FIU websites and an overview of the NRA was published in the *BaFinJournal* (a FI industry news bulletin). *Länder* supervisory bodies, industry associations and SRBs have

<sup>74</sup> These include: BaFin’s regular risk assessments for the financial sector; *Länder*-level risk assessments; FIU annual reports and typologies reports; the Federal Criminal Police Office (BKA) reports on organised crime (2017), clan crime (2018), human smuggling (2017), gun crime (2017), and TF (2013); academic studies on ML (2016) and TF (2017) and input from the private sector. Germany has also undertaken separate risk assessments on the NPO sector in 2019/2020 (see R.8) and legal persons in 2020 (see R.24).

<sup>75</sup> See: World Bank “Risk Assessment Support for ML/TF” (2016), accessible at: [www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support](http://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support)

disseminated the NRA to all FIs and DNFBPs and Federal agencies (BaFin and the FIU) have also undertaken outreach to the private sector, including at the *Länder*-level.

**Criterion 1.5** – Federal authorities allocate resources in line with ML/TF risk, but it is not clear that there is a whole-of-government approach or if authorities at the *Länder*-level are allocating resources and implementing measures based on risks identified. At the national level, risk-based resourcing decisions are taken within the framework of the National Strategy to Counter ML/TF (see R.2) while budgetary decisions are made by the German Bundestag (with input from the relevant agency). Such decisions have included increasing BaFin, customs and BKA AML/CFT resources and expanding FIU resources including new liaison officers

At the *Länder* level, states are independently responsible for resourcing decisions. Germany provided examples of certain *Länder* establishing agencies or bodies in higher risk areas (such as organised crime), but it is not clear that all *Länder* consider the NRA and other risk assessments in resourcing and budgetary decisions. Risk-based resourcing decisions are also taken at the agency level, for example, BaFin and the FIU have reorganised internal operations and personnel to respond to specific risk areas.

Germany has also demonstrated that it implements AML/CFT measures to address risks including under its National Strategy to Counter ML/TF (National AML/CFT Strategy) and by going beyond the minimum requirements in the FATF standards when required. For example, in light of risks Germany imposes CDD obligations on property leasing agents and has lowered the threshold at which dealers in precious metals and stones need to undertake CDD (GwG, s.10).

**Criterion 1.6** – There are no wholesale exemptions from AML/CFT obligations for particular sectors. While BMF has the ability to exempt entities from AML/CFT obligations (GwG, s.2(2)), it has not done so. Certain VASPs are temporarily exempt from requirements relating to virtual asset transfers for pragmatic, rather than risk-based reasons (see c.15.9).

**Criterion 1.7 – (a)** Germany requires FIs and DNFBPs to take enhanced measures where higher ML/TF risks are identified (GwG, s.15). Supervisory authorities may order FIs and DNFBPs to apply enhanced measures in sector-specific high-risk situations, e.g., for high-risk countries (GwG, s.15(8)).

**(b)** FIs and DNFBPs are required to undertake a risk assessment. When doing so, they must pay particular attention to certain high risk factors and to incorporate the findings of the NRA (GwG, s.5(1)).

**Criterion 1.8** – Germany allows FIs and DNFBPs to apply simplified due diligence to business relationships or transactions that have been identified as low ML/TF risk (GwG, s.14(1)). The list of low-risk factors that FIs and DNFBPs should consider includes factors that are not based on an assessment of risk (e.g., registration or residence in an EU Member State; GwG, Annex 1). (See c.10.18).

**Criterion 1.9** – Supervisors and SRBs are required to ensure that FIs and DNFBPs are implementing their obligations under the GwG, including the requirements of R.1 (GwG, ss.50, 51). There are some limitations in the risk-based approach applied by *Länder*-level supervisors (see analysis of R. 26 and R. 28).

**Criterion 1.10** – FIs and DNFBPs are required to identify and assess the ML/TF risks associated with their business activities (GwG, s.5(1)). This includes being required to:

- (a) document their risk assessment (GwG, s.5(2))
- (b) consider various risk factors, including customers, products, services, transactions, delivery channels and geographic elements, and the NRA, in determining the overall ML/TF risks and mitigation measures (GwG, ss.5(1), 6(1))
- (c) regularly review and update the risk assessment (GwG, s.5(2)), and
- (d) make the risk assessment available to their supervisor on request (GwG, s.5(2)). In addition, most FIs (including banks, insurance providers and securities providers) must provide their risk assessment as part of their regular audit (see c.18.1(d)).

#### **Criterion 1.11 –**

- (a) FIs and DNFBPs are required to have principles, procedures and controls in place to manage and mitigate identified ML/TF risks (GwG, s.6(1)). These must be approved by a member of executive management (GwG, 4(3)).
- (b) FIs and DNFBPs are required to monitor the functionality of internal controls and safeguards and update them where necessary (GwG, s.6(1)).
- (c) FIs and DNFBPs are required to take enhanced measures to manage and mitigate identified higher risks (GwG, s.15 – see c.1.7).

**Criterion 1.12 –** Germany allows simplified due diligence for lower-risk business relationships or transactions (see c.1.8), however c.1.9 is not fully met as there are some limitations in DNFBP supervisors' application of a risk-based approach. Simplified measures are not permitted where the FI or DNFBP suspects ML/TF (GwG, s.10(3)).

### **Weighting and Conclusion**

Germany finalised its first NRA in October 2019, with the participation of a variety of sectors, under the co-ordination of the BMF. Germany has implemented the main aspects of R.1 and has only a small number of outstanding deficiencies. It is not clear that there is a whole-of-government approach or if authorities at the *Länder*-level allocate resources and implement measures to prevent and mitigate ML/TF. This deficiency is weighted the most heavily due to its possible broader reach, but the existence of informal structures mean it is only a minor shortcoming. Other minor deficiencies are: certain VASPs are exempt from certain requirements for pragmatic, transitional reasons (rather than on the basis of risk), the list of low-risk factors to consider in applying simplified due diligence includes factors not based on risk, and there are some limitations in the risk-based approach to supervision.

**Recommendation 1 is rated largely compliant.**

### **Recommendation 2 - National Cooperation and Co-ordination**

In its previous MER, Germany was largely compliant with these requirements as there was no effective co-ordination with authorities responsible for DNFBPs, and policy co-ordination focused primarily on FATF policy matters rather than developing policies and activities to combat ML and TF in Germany. In 2019, new co-ordination mechanisms were introduced.

**Criterion 2.1 –** Germany develops and implements national AML/CFT policies that are based on identified risks. In December 2019, Germany adopted its National AML/CFT Strategy. The Strategy identifies 11 areas and concrete actions to improve

Germany's AML/CFT system. The identified actions are a mix of measures to respond to regional and international standards (including EU and FATF requirements) and to respond to regional and national risks. Germany has committed to updating the Strategy on a regular basis. The Steering Committee for Combating ML/TF (see c.2.2 and 2.3) provides a mechanism and forum for keeping the Strategy up-to-date. Germany also enacted policies to address risks identified during the NRA process, prior to the formal adoption of the NRA and the National AML/CFT Strategy. For example, in response to vulnerabilities posed by a low number of STRs in the real estate sector, Germany extended obligations so that certain real estate transactions automatically trigger a STR.

**Criterion 2.2** – The Steering Committee for Combating ML/TF (RÜST GW/TF) provides a forum for high-level decision-making on AML/CFT policies. RÜST GW/TF was created in 2019 and meets twice per year. Its focus to-date has been on monitoring implementation of the National AML/CFT Strategy, dissemination of the NRA and preparing for the FATF evaluation. While it provides a platform for co-ordinating policy development this has not been the focus. RÜST GW/TF operates on the basis of a working agreement. Its decision-making power is based on the co-operation and agreement of all participating agencies (rather than having a binding authority). RÜST GW/TF includes representatives from 14 federal agencies and, since 2020, two *Land* representatives from the *Land* co-ordinating offices (see c.2.3) (currently Bavaria and Brandenburg).<sup>76</sup> Germany intends that the *Land* representatives will rotate and act as liaisons between the RÜST GW/TF and the other *Land* co-ordinating offices, although there is no formal mechanism to ensure this would occur.

**Criterion 2.3** – Germany has in place a range of mechanisms for co-ordination and information-exchange between competent authorities (see Table A.A.1 below), however, operational co-ordination on ML could be enhanced and policy level co-ordination could include a wider range of stakeholders as described below.

As set out in c.2.2 above, the RÜST GW/TF provides a platform for high-level policy co-ordination, but it is not clear that *Länder* authorities are sufficiently and systematically involved in its decision-making (see c.2.2). This is to some extent addressed through a new system of co-ordinating offices at the *Länder* level, although it is not clear how these offices co-ordinate on policy-making.

At the operational law enforcement level on ML, the FIU and Federal Criminal Police Office (BKA) co-ordinate and share information with *Länder* police offices. Inter-agency guidance for LEAs encourages information-sharing on organised crime, but not ML. There are no formal mechanisms (e.g., working groups or MOUs between agencies) for law enforcement co-ordination on ML.<sup>77</sup> At the operational level on TF, there are a number of co-ordination mechanisms including the informal TF Working Group, ten national security centres, the Joint Counter-Terrorism Centre (GTAZ) and

<sup>76</sup> BMF, BMJ, BMI, the Federal Ministry for Economic Affairs and Climate Action (BMWK), the Federal Foreign Office (AA), BaFin, the Federal Criminal Police Office (BKA), the Federal Office for the Protection of the Constitution (BfV), the Federal Intelligence Service (BND), the Central Office of the German Customs Investigation Service (ZKA), the Federal Prosecutor General (GBA), the FIU and the Deutsche Bundesbank.

<sup>77</sup> Specific Commissions bring together LEAs to co-ordinate on priority areas (e.g., on organised crime or national security), but there is no commission specifically targeting ML.

the Joint Centre for Combating Extremism and Terrorism (GETZ), although the FIU is not a regular member of these centres.

From a supervisory perspective, there are co-operation mechanisms, including between the FIU and BaFin under a MOU; through the federal-*Land* working group for supervisors and the FIU (the *Bund-Länder-Arbeitskreis* (BLA)); and co-ordination among *Land* supervisors in specific sectors. However, these mechanisms do not always include all relevant supervisors, and DNFBP supervisors of some sectors have no co-ordination mechanisms. The Darmstadt Working Group provides a voluntary opportunity for discussion and knowledge-sharing between all DNFBP supervisors. (See Table A.A.1 below).

**Table A.1. Overview of certain AML/CFT co-ordination mechanisms and bodies**

Co-ordination mechanism/body	Scope of mandate and responsibilities	Federal agencies involved	<i>Länder</i> agencies involved
<b>Policy co-ordination</b>			
RÜST GW/TF	High-level co-ordination on ML/TF policy, including on the development and implementation of the National ML/TF Strategy.	14 federal agencies: BMF, BMJ, BMI, the Federal Ministry for Economic Affairs and Climate Action (BMWK), the Federal Foreign Office (AA), BaFin, the Federal Criminal Police Office (BKA), the Federal Office for the Protection of the Constitution (BfV), the Federal Intelligence Service (BND), the Central Office of the German Customs Investigation Service (ZKA), the Federal Prosecutor General (GBA), the Federal Court of Justice, the FIU and the Deutsche Bundesbank	Two <i>Länder</i> members (Bavaria and Brandenburg).
<i>Länder</i> co-ordinating AML/CFT offices	High-level co-operation and information-sharing relating to AML/CFT policies, operational work and risk assessments.	One co-ordinating office per <i>Länder</i> , plus a federal office within BMF.	All 16 <i>Länder</i> represented at the Ministerial level.
<b>Operational co-ordination</b>			
Federal- <i>Länder</i> Working Group, <i>Bund-Länder-Arbeitskreis</i> (BLA)	Co-ordination on legislative drafting and interpretation, best practices, and trends relating to AML/CFT.	BMF, the FIU.	DNFBP supervisors (excluding SRBs).
ML Working Group on Gambling	Co-ordination to develop AML/CFT guidance, provide GwG interpretation, and ensure uniform application of national standards	BMF	Gambling supervisors from all 16 <i>Länder</i> .
ML Working Group of Bar Associations	Co-ordination to develop AML/CFT guidance, provide GwG interpretation, and ensure uniform application of national standards	Federal Bar Association.	Bar Associations from all 16 <i>Länder</i> .
Darmstadt Working Group	Forum for discussion of supervisory issues and best practices.	Regular invitation to: BMF, FIU, and other relevant agencies.	Open invitation to all supervisors from 16 <i>Länder</i> .
Working Group on TF	Preparation of a regular joint situation report on TF.	The BND, BfV, and BKA.	
FIU liaison officers in <i>Länder</i> police offices	Information-sharing on ML and TF investigations.	FIU	<i>Länder</i> criminal police offices (LKAs)
Anti Financial Crime Alliance	Public-private information sharing on ML/TF policy and strategy.	Board member and members of working groups: The FIU, BaFin, the BKA, and the ZKA. Private sector representatives from: 20 FIs, 7 from the non-financial sector (including 3 representatives from the real estate sector), and 2 non-obliged entities	Members of working groups: The Berlin Senate Administration for the Economy, Energy and Public Companies; the Brandenburg Ministry for Economy, Employment and Energy; the Hessen Ministry of

	(including the Federal Chamber of Notaries).	the Interior; and the Baden-Württemberg Ministry of the Interior
--	--	--

Source: German Authorities.

**Criterion 2.4** – Germany has mechanisms in place to monitor and implement PF-related TFS. Germany has established an inter-ministerial co-ordination group on sanctions comprising the ministries of foreign affairs, economics and finance. The group’s mandate is to co-ordinate all sanctions matters, including PF-related TFS. In addition, a Ministerial Working Group for Export Control and a Prohibition Discussion Group<sup>78</sup> meet twice annually to deal with export control and sanctions-related issues (see R.7 and IO.11). These mechanisms ensure co-operation on PF-related TFS, and to some extent provide a platform for co-operation on broader PF issues (beyond TFS). Information is also shared on an *ad hoc* basis between the central bank, supervisors and law enforcement to promote TFS supervision and the identification and investigation of sanctions breaches.

**Criterion 2.5** – Germany has co-operation and co-ordination mechanisms in place to ensure AML/CFT requirements comply with data protection and privacy rules, including the European General Data Protection Regulation. Authorities are in place at the *Länder* and federal level to supervise the public and private sectors’ compliance with data protection rules. The Dusseldorf Group brings together the relevant *Länder* authorities and BaFin every year to discuss data protection issues, with a standing agenda item on AML/CFT topics. Federal AML/CFT authorities have held meetings with the Federal Data Protection Officer. Germany has also amended its AML/CFT framework to ensure consistency with regional data protection regulations and to exempt data users from data protection requirements where the use is necessary for AML/CFT obligations (GwG, s.51a). All draft legislation affecting the use of personal data must be submitted to the Federal Data Protection Officer (European General Data Protection Regulation, art.36(4)). Before the introduction of processes that involve personal data, a Data Protection Impact Assessment must also be conducted (European General Data Protection Regulation, art.35).

### Weighting and Conclusion

Germany has in place a range of mechanisms for co-ordination and information-exchange between competent authorities with only minor deficiencies. RÜST GW/TF does not have binding authority and the rotating and representative involvement of the *Länder* is not formalised to ensure their co-ordinated engagement. Operational and policy co-ordination mechanisms exist, but do not include all relevant stakeholders (notably the FIU). There are no formal mechanisms for law enforcement co-ordination on ML. Supervisory co-operation mechanisms do not always include all relevant supervisors, and DNFBP supervisors of some sectors have no co-ordination

<sup>78</sup> The Ministerial Working Group comprises 16 relevant agencies including: the Federal Ministry for Economic Affairs and Climate Action (BMWK); Foreign Office (AA); Federal Office for Economic Affairs and Export Control (BAFA); Federal Intelligence Service (BND); Federal Ministry of the Interior, Building and Community (BMI); the Federal Office for the Protection of the Constitution (BfV); the Federal Prosecutor General (GBA); the Federal Ministry of Finance (BMF); and the Central Office of the German Customs Investigation Service (ZKA) amongst others. The Prohibition Discussion Group comprises: BMWK; AA; BMF; licensing authority; ZKA; Federal Public Prosecutor General; intelligence services and, where relevant, other ministries and agencies.

mechanisms. Although authorities co-operate on PF-related TFS, there is no general PF co-ordination mechanism in this area.

**Recommendation 2 is rated largely compliant.**

### Recommendation 3 - Money laundering offence

In its previous MER, Germany was partially compliant with these requirements due to gaps in criminal liability for self-laundering and the list of offences considered to be predicate offences to ML,<sup>79</sup> as well as insufficient sanctions. Germany has amended its ML offence several times since its previous MER, and the latest set of changes came into force in March 2021.

**Criterion 3.1** – Germany criminalises ML at the federal level in line with the Vienna and Palermo Conventions and the ML offence applies in all German *Länder* (Basic Law, *Grundgesetz* (GG), s.72, 74(3)).

The ML offence explicitly covers the following activities: acquiring, possessing or using proceeds; concealing or disguising the true nature, source or location of the proceeds, or the method involving the disposition, movement or ownership of the proceeds or rights related to them; and (as of March 2021) transferring and converting proceeds (German Criminal Code, *Strafgesetzbuch* (StGB), s.261).

**Criterion 3.2** – All unlawful acts under German law are predicate offences under the ML offence (StGB, s.11(1)(no.5) and s.261(1)).<sup>80</sup> Germany has criminalised activity in all 21 categories of designated predicate offences.

**Criterion 3.3 – (N/A)** As of March 2021, Germany no longer applies a threshold approach for designating predicate offences for ML.

**Criterion 3.4** – The ML offence uses the term ‘objects’ instead of property but in practice this covers all types of property required by the FATF Standards, regardless of value and both the direct and indirect proceeds of crime (StGB, ss.73, 261). For example, German courts have confirmed that virtual assets fall within the definition of ‘objects’.<sup>81</sup>

**Criterion 3.5** – It is not necessary for there to be a prosecution or conviction for the predicate offence to prove that property is the proceeds of crime and this is not an element of the money laundering offence.

**Criterion 3.6** – Predicate offences includes conduct that occurred in another country if the conduct would constitute a criminal offence in both countries or is a criminal offence under certain provisions and conventions of the European Union (StGB, s.261(9)).

**Criterion 3.7** – The ML offence applies to self-launderers to the extent possible under the fundamental principles of German law. Since the previous MER, Germany has extended its ML offence to offenders or participants who take actions to circulate and thereby conceal the unlawful origin of the objects of crime (StGB, s.261(9)). A predicate crime offender that possesses the proceeds of crime without a separate

<sup>79</sup> Counterfeiting and piracy of products and insider trading and market manipulation were not predicate offences for money laundering.

<sup>80</sup> The revised money laundering offence entered into force on 18 March 2021. Prior to March 2021, Germany had a combined approach to defining predicate offences for ML using both a threshold and list of designated predicate offences.

<sup>81</sup> Federal Court of Justice judgement dated 27 July 2017 (1 StR 412/16, margin no 6).

action to circulate the funds is not covered under the ML offence as it is considered to be the same course of conduct as the predicate offence and is inconsistent with fundamental principles of German law that no person may be punished for the same act more than once (GG, art.103(3)).

**Criterion 3.8** – For the purposes of the ML offence, intent and knowledge can be inferred from objective factual circumstances. While there is no explicit provision referring to objective factual circumstances, judicial authorities rely on the broad principle of free evaluation of evidence which includes the capacity for this inference to be made (Criminal Procedure Code, *Strafprozessordnung* (StPO), s.261).

**Criterion 3.9** – Proportionate criminal sanctions apply to natural persons convicted of money laundering. Offences are punishable by a term of imprisonment not exceeding 5 years or a fine (StGB, s.261). Aggravated offences are punishable by a term of imprisonment from 6 months to 10 years. An offence committed by an obliged person under the Money Laundering Act (GwG) is punishable by a term of imprisonment from 3 months to 5 years. Courts can issue fines for ML ranging from EUR 5 to EUR 10 800 000 depending on the seriousness of the conduct and the income/means of the offender (StGB, s.40). Fines cannot be applied in conjunction with a term of imprisonment. Fines are used in cases involving less serious conduct where a term of imprisonment would not be appropriate, or where special circumstances exist that make a fine the more appropriate punishment (StGB, ss.261(1),261(6), 47(1)). These penalties are similar to those applied for other criminal offences like bribery, counterfeiting, drug trafficking and fraud.

**Criterion 3.10** – The concept of criminal liability for legal persons is not recognised in German law and was considered to be against the fundamental principles of domestic law at the time of the previous evaluation (see paragraph 167 of the previous MER). However, legal persons are subject to administrative fines for ML (also referred to as regulatory fines) (Administrative Offences Act, *Gesetz über Ordnungswidrigkeiten* (OWiG), ss.30, 130) which are proportionate and dissuasive. Fines are calculated from the sum of two elements: a punitive element (up to EUR 10 million) and an uncapped ‘confiscation’ element equivalent to the financial benefit obtained from the offence (OWiG, s.17(4)). These sanctions do not preclude parallel civil proceedings or criminal proceedings related to natural persons.

**Criterion 3.11** – Ancillary offences for ML include abetting (including incitement), aiding and attempt. Neither the attempted aiding nor the attempted abetting of an ML offence is punishable under German law but aiding or abetting an attempted ML offence is punishable (StGB, ss.23, 26, 27). Conspiracies (agreement or plan to commit ML) are criminalised as a general offence under s.129 of the Criminal Code (forming criminal organisations).

### Weighting and Conclusion

All criteria are met.

**Recommendation 3 is rated compliant.**

### Recommendation 4 - Confiscation and provisional measures

In its previous MER, Germany was largely compliant with these requirements for effectiveness deficiencies (which are now covered under IO.8) and issues around access to information held by DNFBPs subject to professional secrecy.

**Criterion 4.1** – Germany has the following conviction-based measures in place for the confiscation of assets either held by criminals or third parties:

- (a) Laundered property (referred to as the “objects of crime”) (StGB, ss.74(2), 74(a));
- (b) and (c) Proceeds of (including income or other benefits derived from such proceeds), or instrumentalities used or intended for use in ML, predicate offences and TF (StGB, ss.73-73b, 74, 74a);
- (d) A sum of money or assets of corresponding value if the tainted asset itself cannot be confiscated or has diminished in value (StGB, ss.73c, 74c).

Property that is the proceeds of crime can be confiscated from third parties if the property was transferred to the third party without remuneration or without legal justification, the third party was aware or should have been aware the property was the proceeds of crime, or the third party was directing the offender (StGB, s.73b). Property that is the instruments of crime may also be confiscated from third parties if the third party contributed at least recklessly to the property being used as an instrument of crime or acquired the property in the full knowledge of the circumstances which would have allowed for its confiscation (StGB, s.74a).

Non-conviction based confiscation measures are available when the perpetrator cannot be identified; or for reasons of death, absence from the country or unfitness, cannot stand trial (StGB, ss.76a(1), 76a(2), 261(10)). In addition, property of unclear origin may be confiscated if it was seized in an investigation into certain listed offences, including ML, if the court is convinced that it derives from an unlawful act even if the underlying act cannot be identified (StGB, s.76a(4)).

**Criterion 4.2** – Germany has measures in place to allow competent authorities to:

- (a) Identify, trace, and evaluate property that is subject to confiscation through the broad powers available to LEAs in the Criminal Procedure Code and available in all criminal investigations including seizure of documents and searches of databases (StPO, ss.94, 95, 98, 102, 103, 161(1), 161a, 163(1); Banking Act, *Gesetz über das Kreditwesen* (KWG), s.24c(3); GwG, s.32(3));
- (b) Carry out provisional measures ex parte and without prior notice, including seizing property to prevent its transfer or disposal prior to confiscation (StPO, s.111b), including property of equivalent value (StPO, s.111e);
- (c) Prevent or void actions that prejudice the ability to seize or recover property subject to confiscation (StPO, s.111d(1), 111h(1)). When property is seized for confiscation, a general prohibition on disposal of the asset comes into effect and any transactions entered into in contravention of the prohibition are considered void, unless the transaction was done in good faith (Civil Code, *Bürgerliches Gesetzbuch* (BGB), s.136);
- (d) Take other investigative measures as set out in R.31.

**Criterion 4.3** – German law protects the rights of bona fide third parties with legitimate interests in property at both the seizure and confiscation stages (StGB, s.73b(1), 73e(2); StPO, s.111n(3) and (4)).

**Criterion 4.4** – Mechanisms are in place to manage, and where necessary, dispose of seized and confiscated assets (StPO, ss.111k, 111m, 111p). The power to manage and dispose of assets is given to the public prosecution office but can be delegated to investigators, a bailiff or another appropriate person (Courts Constitution Act,

*Gerichtsverfassungsgesetz* (GVG), s.152). Confiscated assets can also be used to compensate injured parties (StPO, s.459h).

### *Weighting and Conclusion*

All criteria are met.

**Recommendation 4 is rated compliant.**

### **Recommendation 5 - Terrorist financing offence**

In its previous MER, Germany was largely compliant with these requirements because some conduct was not adequately criminalised and a minimum value attached to the definition of 'funds'. In February 2016, the FATF clarified that R.5 requiring countries to criminalise the financing of travel for terrorist purposes (c.5.2<sup>bis</sup>).

**Criterion 5.1** – Germany has largely criminalised TF in line with the TF Convention by:

- Introducing a specific offence for financing of terrorist acts and individual terrorists (StGB, s. 89c) in 2015.
- Using a broader membership and support offence (StGB, s.129a) to cover financing of a terrorist organisation as a member (StGB, ss.129a(1) and (2)) and as a non-member (StGB, s.129a(5)). Section 129b(1) extends section 129a to membership of and support for foreign terrorist organisations. Participating as a member or supporting a terrorist organisation as a non-member covers both the collection and provision of funds.<sup>82</sup>

A terrorist act for the purposes of the TF offences covers a range of violent acts, including those covered in the treaties listed in the annex to the TF Convention. The TF offences are consistent with Article 2(1)(b) of the UN TF Convention (regarding specific intent TF offences), but inconsistent with Article 2(1)(a) as they require an additional element of intent to “seriously intimidate the public,” for the offences identified in the treaties listed in the UN TF Convention annex. Terrorist purpose can be inferred from the nature of the actions considering the objective factual circumstances of the case. Nevertheless, this is an additional element which goes beyond the TF Convention.

<sup>82</sup> The collection and provision of funds constitutes punishable participation of a member as the promotion of the illegal purposes of the terrorist organization from the inside is sufficient; see MüKoStGB/Schäfer/Anstötz, 4th edn. 2021, section 129a, margin no. 57, referring to section 129 margin no. 82; Kindhäuser/Hilgendorf, StGB, 9th edn. 2022, section 129a margin no. 26; for jurisprudence see, e.g., Federal Court of Justice decision of 14 May 2020 (AK 8/20); Federal Court of Justice decision of 7 May 2019 (AK 13/19). Criminal support of terrorist organisations by non-members equally covers the collection and provision of funds as it can have a positive effect on the possibilities of action and purpose of the organisation in any way and thus strengthens its danger; see LK/Krauß, StGB, 13th edn. 2020, section 129a, margin no. 90; for examples in jurisprudence see Federal Court of Justice decision of 9 January 2020 (BeckRS 2020, 468, para. 27). Even the mere promise of a non-member to provide funds to a terrorist organization can amount to support punishable by section 129a of the Criminal Code. See LK/Krauß, StGB, 13th edn. 2020, section 129a, margin no. 97. For jurisprudence see, among others, Federal Court of Justice decision of 28 April 2020 (StB 13/20).

**Criterion 5.2** – The TF offences cover the direct and indirect collection or provision of funds or assets in full or in part with the intention or knowledge, that the funds or assets be used to carry out a terrorist act (StGB, s.89c) or provided to a terrorist organisation (StGB, ss.129a (1), (2) and (5), 129b(1)). However, the offences do not extend to cover financing of an individual terrorist for any purpose as the s.89c offence requires proof that the person knows or intends for the funds to be used for a specified offence. Prosecutors note that it suffices for the perpetrator to know, or to have merely intended, that the funds provided are to be used for an offence even if the act does not occur or is thwarted or is not fully planned.

**Criterion 5.2 bis** – Germany criminalises the collection or provision of funds or assets for the purposes of funding travel for an individual for terrorist purposes which includes travel for the purposes of preparing, planning of participating in a terrorist or receiving terrorist training (StGB, ss.89a(2a) and 89c(1) no.8). The offences include situations where the person is self-funding their travel (s.89(2a)) and covers funding of a third party (ss.89a(2a), 89c(1) no.8). Additional offences apply to situations of self-funding and funding of a third party if there is a link to a terrorist organisation (ss.129a(1), (2) and (5)).

**Criterion 5.3** – There is no definition of assets, funds or property in the terrorist financing offence but Germany provided legal texts and cases to show that it is interpreted broadly to include movable or immovable property or rights, virtual assets and material support whether they are derived from a legitimate or illegitimate source.<sup>83</sup>

**Criterion 5.4** – The TF offences do not require funds or assets to be **(a)** actually used to carry out or attempt a terrorist act(s) or **(b)** be linked to a specific terrorist act(s) if the funding is related to a terrorist organisation (StGB, 129a(5)). However, as set out in c.5.1, there is a limited deficiency as funding individual terrorists does require proof of knowledge or intention to commit an offence (StGB, s.89c(1)).

**Criterion 5.5** – Intent and knowledge can be inferred from objective factual circumstances (StPO, s.261). Under German law, the principle of free evaluation of evidence operates so that the facts of the case be inferred from circumstantial evidence and intent and knowledge of the offender can be inferred from objective factual circumstances.

**Criterion 5.6** – Natural persons convicted of financing terrorist acts or individual terrorists are subject to terms of imprisonment between three months and ten years (StGB, s.89c). The penalty for financing a terrorist organisation ranges from six months to 10 years depending on the seriousness of the offence and up to 15 years imprisonment for leaders of a terrorist organisation (StGB, s.129a). The penalties available are proportionate and dissuasive compared to similar offences in Germany.

**Criterion 5.7** – The concept of criminal liability for legal persons is not recognised under German law but administrative penalties apply – the analysis at 3.10 also applies here although the uncapped ‘confiscation’ element which is calculated

<sup>83</sup> Germany provided legal commentaries to support the interpretation: MüKoStGB/Schäfer, 3rd edition (2017), margin no. 12 regarding section 89c of the Criminal Code and Federal Court of Justice decision of 27 July 2017 (1 StR 412/16, NStZ 2018, 401 (404)). In Germany, legal commentaries outline the general interpretation of legal provisions that is currently dominant in jurisprudence and academia.

according to the financial benefit obtained from the offence is less dissuasive in a TF context as TF is not usually profit driven.

**Criterion 5.8** – Germany has criminalised ancillary offences as follows:

(a) It is an offence to attempt to provide financing to a terrorist organisation (StGB, s.129a) and to designated persons and groups (Foreign Trade and Payments Act, *Außenwirtschaftsgesetz* (AWG), s.18(6)) but it is not expressly an offence to attempt to finance terrorism not involving a terrorist group or designated groups of individuals;

(b) Participation as an accomplice in a TF or attempted TF offence (StGB, ss.25(2), 27(1), 30);

(c) Organising or directing others to commit a TF offence or attempted offence (StGB, s.23, 25, 26, 27, 30 and s.89c or s.129a) and instructing others to provide financing to designated persons and groups (AWG, ss.18(1), 18(6));

(d) Contributing to the commission of one or more TF offence(s) or attempted offence(s) by a group of persons with a common purpose (StGB, ss.25, 129a).

**Criterion 5.9** – TF offences are designated predicate offences for money laundering (StGB, s.261(1)(5)).

**Criterion 5.10** – The TF offences (StGB, ss.89c, 129a) apply regardless of the location of the financier or the terrorist/terrorist organisation if there is a jurisdictional nexus to Germany under the Criminal Code (i.e. the offender or the injured party is a German national or is physically present in Germany) (StGB, ss.89c (3), 129b(1)).

### *Weighting and Conclusion*

Germany enacted new offences in 2015 (StGB, s.89c) to cover financing of terrorist acts and individual terrorists to address the previous gaps identified. However, a range of minor issues remain. The TF offences incorporate an additional element of terrorist purpose which also goes beyond the TF Convention and the provision of funds to an individual terrorist for any purpose (or attempt to do so) is not covered. This gap is limited due to the availability of TFS offences for making any funds available to designated individuals or those connected with designed entities.

**Recommendation 5 is rated largely compliant.**

### **Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing**

In its previous MER, Germany was partially compliant with these requirements. The following deficiencies were identified: (a) except for credit institutions, financial services institutions and investment companies, no other person is subject to requirements to freeze the assets of EU-internals; (b) there was a lack of effective procedures to freeze assets other than funds for EU-internals where the Banking Act applies; (c) professional secrecy was interpreted broadly and there were strict conditions for obtaining such information which hindered the location and tracing of terrorist funds; and (d) there were no appropriate measures to monitor compliance with relevant obligations.

**Criterion 6.1** – In relation to designations under UNSCRs 1267/1989/2253 and the 1988 regime (collectively referred to as “UNSCR 1267 etc.”):

**(a)** The Federal Foreign Office, *Auswärtiges Amt* (AA), is the competent authority for proposing designations to the relevant UN Committee via Germany's Permanent Representation to the UN (this is not explicitly prescribed in a legal provision, but is implicit based on the AA's foreign affairs role).

**(b)** An undocumented national process is in place to identify targets for designation. Targets are initially identified by the federal or *Länder* police with input from other operational agencies (including the relevant prosecution office and ZKA) and are submitted to the BKA. The BKA proposes the designation to the Federal Ministry of the Interior, Building and Community (BMI) which assess the proposal for completeness and plausibility. The BMI liaises with the AA which undertake an initial assessment of the proposal to determine whether it meets the UN Committee criteria. If so, the proposal will be submitted for confirmation to an inter-ministerial committee (*Ressortkreis*) made up of relevant agencies that is formed on an *ad hoc* basis to consider proposals.<sup>84</sup> If approved by the *Ressortkreis*, the AA makes the final decision on the proposal and submits it to the UN with the necessary evidence and documents (as per c.6.1(a)). This national process and the factors to consider in deciding to propose a designation (beyond the UN criteria) are not written or formalised, but are based on convention.

**(c)** When assessing a proposal for designation, the *Ressortkreis* and the AA consider whether there is reliable information that provides reasonable grounds to believe that the UN designation criteria is met. This includes reviewing police and intelligence findings, information from judicial authorities and publicly accessible information. Criminal proceedings may be an indication in favour of a designation, but they are not mandatory.

**(d)** Germany uses the standardised UN forms when submitting designation applications.

**(e)** Germany provides the UN Committee with evidentiary information in an annex when submitting designation applications. This includes the name, aliases, identifying information, the basis for the proposal (including specific findings and reasoning), supporting evidence, and a statement on whether Germany can be identified as the designating state.

**Criterion 6.2** – Germany implements UNSCR 1373 designations primarily through the EU mechanism (Common Position (CP) 2001/931/CFSP; EC Regulation 2580/2001). Germany also has the possibility to issue national freezing/prohibition orders (AWG, ss.4(2), 6; KWG, s.6a).

**(a)** *At the EU level*, the EU Council (through the Council's Working Party on the Application of Specific Measures to Combat Terrorism (COMET)) is responsible for designating persons or entities that meet the criteria set forth in UNSCR 1373 (EU Regulation 2580/2001, art.2(3); CP 2001/931/CFSP, art.1(4)). *At the national level*, the AA is the competent German authority for submitting requests to the EU and for co-ordinating Germany's position on designations proposed by other EU Member States.

**(b)** *At the EU level*, proposals for listing can be submitted by member states' competent authorities (the AA for Germany) as well as by the High Representative for Foreign Affairs and Security Policy (CP 2001/931/CFSP, art.1(4); CD

<sup>84</sup> The AA, the BMI, the Federal Ministry of Justice (BMJ), the Federal Ministry for Economic Affairs and Climate Action (BMWK) and the BMF.

2016/1693/CFSP, art.5)). COMET prepares and makes recommendations for designations, including assessing whether the information available meets the specific criteria for designation under UNSCR 1373 (CP 2001/931/CFSP, art.1(2) and EU Regulation 2580/2001, art.2(3)). *At the national level*, the process by which Germany identifies targets to propose to the EU for designation under UNSCR 1373 is the same as that described above for UNSCR 1267 and subject to the same deficiencies (see c.6.1(b)).

**(c)** *At the EU level*, when a request for designation is received (from an EU or non-EU country), the European External Action Service or relevant Member State will carry out a first basic scrutiny of the proposal and gather relevant information, including requesting additional information from the requesting country (doc.14612/1/16 REV 1 on establishment of COMET WP, Annex II, art.3). COMET delegations (all EU Member States) have 15 days to review the proposal, which does not permit a prompt determination. This timeframe can be shortened in exception cases (doc.14612/1/16 REV 1 on establishment of COMET WP, Annex II, arts.8-9).

*At the national level*, if Germany receives a request for designation directly from another country (i.e., where a request is made to Germany and not directly to the EU), the AA would examine the request. There is no fixed timeframe for this examination to ensure such determinations are prompt. If the proposal is sufficiently detailed and credible, the AA would consult other German authorities before making a proposal for designation to the EU.

**(d)** *At the EU level*, when deciding on a proposal, COMET decides on the basis of a decision by a competent national body, irrespective of criminal proceedings (CP 2001/931/CFSP, art.1(4)). *At the national level*, Germany applies a 'reasonable grounds' threshold for proposing designations, following the approach described in c.6.1(c). Authorities consider police and intelligence findings, publicly available information, and other pertinent findings to determine if this threshold is met. Targets are proposed to the EU on the basis of a national decision by Germany (CP 2001/931/CFSP, art.1(4)), which could be an order from BMI banning an organisation from operating (see c.8.4), or a court judgment against an individual. The precise factors are dependent on each case. Proposals are not conditional on the existence of a criminal proceeding.

**(e)** Where Germany proposes a designation at the EU level, it provides as much information as possible to support the designation and help EU countries to identify the designated person or entity, including names, aliases, addresses and other identifying information. This information can be shared with non-EU members upon request provided EU member states agree. There is no EU or national procedure for *requesting* non-EU countries to give effect to EU designations or domestic freezing/prohibition orders under the AWG. However, there is an approximation procedure that allows non-EU Member States to adopt the EU sanctions lists.

### **Criterion 6.3 –**

**(a)** *At the EU level*, all Member States are required to provide each other with all available relevant information to identify persons meeting the criteria for designation (CP 2001/931/CFSP, art.4; EC Regulation 2580/2001, art.8; EC Regulation 881/2002, art.8). *At the national level*, German operational agencies and LEAs have relevant powers to collect information to identify targets for designation (see R.29-31). The *Ressortkreis* relies on this information when assessing or proposing designations, in addition to other information it is able to collect or request (e.g., publicly available

information, supervisory information, etc.). However, there is no legal authority or domestic framework that entitles the *Ressortkreis* to solicit the necessary information to identify potential targets for designation.

**(b)** *At the EU level*, designations take place without prior notice (EC Regulation 1286/2009, preamble para.5). *At the national level*, where a domestic freezing/prohibition order is issued under the AWG, no notification or advance notice is given to persons or entities implicated by such orders (Administrative Proceedings Act, *Verwaltungsverfahrensgesetz*, s.28(2)).

**Criterion 6.4** – For TFS under UNSCR 1267 etc., Germany can issue freezing/prohibition orders (by way of an administrative act) that apply domestically to reduce the implementation delays seen under the EU mechanism (AWG, s.6(1)). The national order will remain valid until the EU designation enters into force. Germany has systematically used this framework for EU designations under UNSCR 1267 etc. Since its entry into force, all UNSCR 1267 designations have been implemented without delay (within 24 hours) by way of orders under the AWG. However, AWG orders cannot be issued on weekends or holidays and a delay has been observed in the implementation of another sanctions regime.<sup>85</sup> This means that the current framework does not allow implementation without delay for sanctions issued by the UN immediately prior to weekends (including Fridays) or holidays.

For TFS under the UNSCR 1373 mechanism, these measures are implemented without delay through the EU mechanism. Once the decision to freeze has been taken, EC Regulation 2580/2001 is immediately applicable within all EU member states. Where the EU mechanism does not apply (e.g. for EU internals), BaFin has the power to issue a freezing order for specific accounts (KWG, s.6a(1)). However, these orders apply only to accounts/funds held by credit and financial service institutions (not all natural and legal persons) (KWG, s.1).

**Criterion 6.5 – (a)** *At the EU level*, under EU regulations, all natural and legal persons within or associated with the EU shall freeze without prior notice and delay the funds or other assets of designated persons and entities (EC Regulation 881/2002, arts.2(1), 11; EU Regulation 753/2011, arts.3, 14; EC Regulation 2580/2001, arts.2(1)(a), 3(1), 10). However, for 1373 designations, there is no requirement to freeze assets of listed individual or entities that are “EU internals” (i.e., persons who have their roots, main activities, and objectives within the EU). Such entities are only subject to increased police and judicial co-operation (CP 2001/931/CFSP (and amendments), Annex 1, footnote 1).

*At the national level*, where Germany issues a freezing/prohibition order under the AWG (in advance of an EU designation), such orders prohibit all natural and legal persons from making funds or economic resources available to the designated person or entity (AWG, s.6(1); template Order to Restrict Capital and Payment Transactions with certain Persons or Partnerships). As these orders operate as a temporary measure to pre-empt an EU listing of a UN designation, they would normally not concern EU internals. BaFin freezing orders prohibit credit and financial services institutions from disposing of funds (KWG, s.6a(1)). While these orders can cover EU

<sup>85</sup> Assessment of other sanctions regimes is not within the scope of R.6; however, as the national implementation system is the same, this is included as relevant context when determining the likelihood of delays.

internals, they apply only to certain FIs (not all natural or legal persons), so are limited in scope (see c.6.4).

**(b)** *At the EU level*, freezing actions for UNSCR 1267 etc. apply to all funds and economic resources belonging to, owned, held or controlled, either directly or indirectly, by a designated person or entity, or by a third party acting on their behalf or at their direction. This extends to interest, dividends or other income on or value accruing from or generated by assets (EC Regulation 881/2002, arts.1(1), 2; EU Regulation 753/2011, arts.1(a), 3). This does not explicitly cover jointly-owned assets, although this interpretation is taken in non-binding EU Best Practices on sanctions implementation (EC document 8519/18, para.34-35).

Under the EU mechanism on UNSCR 1373, the freezing obligation applies to all funds, other financial assets and economic resources belonging to, or owned or held by the designated person or entity (EC Regulation 2580/2001, arts.1(1), 2(1)). There is no explicit reference to funds or assets controlled by, indirectly owned by, derived from assets owned by, or owned by a person acting at the direction of a designated person or entity. However, this gap is largely mitigated by the EC's ability to designate any legal person or entity controlled by, or any natural or legal person acting on behalf of, a designated person or entity (EU Regulation 2580/2001, art.2(3) (iii) and (iv)). As above, the notion of joint-ownership is not explicitly covered, although this interpretation is taken in non-binding EU Best Practices (EC document 8518/18, para.35).

*At the national level*, orders under the AWG (issued in advance of an EU designation) apply to all funds and economic resources owned by the designated person, and not just those that can be tied to a particular terrorist act, plot or threat. The definition of funds and economic resources covers funds or other assets derived or generated from such funds. The template Order makes it clear that the AWG covers funds or assets that are directly or indirectly in the possession or under the control of a designated person or entity. The definition of "control" set out in the template Order is such that this would cover the funds or other assets of persons or entities acting on behalf of or at the direction of designated persons or entities (template Order to Restrict Capital and Payment Transactions with certain Persons or Partnerships). As with the EU orders, jointly-owned assets are not explicitly covered. However, as these orders are explicitly made to pre-empt an upcoming EU designation, they are likely to be interpreted broadly to mirror the scope of the EU regulations.<sup>86</sup>

**(c)** *At the EU level*, natural and legal persons are prohibited from making funds, other assets or economic resources available unless authorised (EC Regulation 881/2002, art.2(2), (3); EU Regulation 753/2011, art.3(2); EC Regulation 2580/2001, art.2(1)(b)). Regulations apply to any natural or legal person, entity, body or group in respect of any business done in whole or in part within the EU. The EU UNSCR 1373 mechanism explicitly extends to the provision of financial services (EC Regulation 2580/2001, art.2(2)). While there is no similar explicit prohibition in the EU UNSCR 1267 mechanism, this is covered by the broad definition of funds and other assets and the prohibition to make available assets that can be used to obtain such services (EC Regulation 881/2002, art.1(2); EU Regulation 753/2011, art.1(c)).

*At the national level*, orders under the AWG (in advance of EU designations) prohibit natural and legal persons from making funds or economic resources available

<sup>86</sup> The order template is currently under revision.

(template Order to Restrict Capital and Payment Transactions with certain Persons or Partnerships).

**(d)** Germany has mechanisms in place to publicise designations for FIs and DNFBPs. Proactive notification measures are focused on FIs (including VASPs), particularly banks. Germany publicises designations and provides guidance on freezing obligations through national websites and gazetting, as well as relying on EU mechanisms. Information on EU designations is included in the EU's Financial Sanctions Database (which includes a newsletter service to which FIs and DNFBPs can subscribe). A link to the EU database is provided on the BMJ website with other information and guidance on TFS obligations. The Ministry of Justice of North-Rhine Westphalia maintains an online financial sanctions database (*FiSaLis*). Relevant agencies (including the Bundesbank and Customs) also provide information and guidance on their websites, including links to *FiSaLis* and the EU sanctions lists). EU designations are published in the Official Journal of the EU (EC Regulation 881/2002, art.13; EU Regulation 753/2011, art.15; EC Regulation 2580/2001, art.11). Designations under the AWG are published in Germany's Federal Gazette (AWG, s.6(1a)). However no mechanism in place to immediately notify new designations to all FIs and DNFBPs. Proactive communication/notification measures are taken to notify most FIs of new designations. The Deutsche Bundesbank proactively disseminates designations to 1 800 FIs (including all banks and VASPs) through a proactive circular. Circulars are typically transmitted on the same day as the listing or prohibition. There is no similar service to immediately and proactively notify other FIs or DNFBPs of new designations. BaFin orders under the KWG are directed at a specific institution, which is immediately notified. These orders are communicated to the FIU and are available to all those who communicate with the FIU. This ensures widespread distribution.

**(e)** *At the EU level*, FIs and DNFBPs are required to report assets frozen or actions taken in relation to designated persons or entities to competent authorities (in Germany, the Deutsche Bundesbank) (EC Regulation 881/2002, art.5(1); EU Regulation 753/2011, art.8; EC Regulation 2580/2001, art.4). This requirement does not explicitly extend to reporting attempted transactions, although this is covered by the requirement to report of "any information which would facilitate compliance" with the relevant Regulations. When the Deutsche Bundesbank issues circulars advising banks of new designations, it informs them of this reporting obligation. It also requests that they submit a negative report if no relevant funds are held, although there is no obligation to do so.

*At the national level*, there is no separate obligation for FIs and DNFBPs to report assets frozen in accordance with orders under the AWG or attempted transactions related to such orders. However, as AWG orders are used as a temporary measure to pre-empt an EU designation, the EU reporting obligations will typically be triggered by a corresponding EU designation shortly after the AWG order.

**(f)** *At the EU level*, for 1267 designations, third parties acting in good faith are protected (EC Regulation 881/2002, art.6; EU Regulation 753/2011, art.7). No similar provisions exist under the EU 1373 mechanism. However, the EU Best Practices on sanctions implementation state that good faith third parties should not be held liable and German civil law protections would extend to third parties implementing EU requirements (EU Document 8519/18, para.37). *At the national level*, third parties applying AWG orders or EU regulations are protected under the rules of German civil law (BGB, ss.276, 280).

**Criterion 6.6** – The following de-listing, unfreezing and access procedures apply:

**(a)** *At the EU level*, for designations under the 1267 mechanism, there are procedures to submit de-listing requests to the relevant UN Sanctions Committee in line with Committee procedures (EC Regulation 881/2002, art.7c; EU Regulation 753/2011, art.11(4)). *At the national level*, there is no publicly known procedure regarding delisting as such designations are generally implemented through temporary AWG orders, which expire automatically upon implementation of an EU designation (or, if not renewed, one month after entry into force). The AA as the competent authority can submit a request for de-listing to the UN Sanctions Committee directly. This decision is based on the procedure and criteria set out in c.6.1 and is in line with UN Committee procedures.

**(b)** *At the EU level*, de-listing procedures are available for designations under the 1373 mechanism under EC Regulation 2580/2001. *At the national level*, orders under the AWG operate as a temporary measure and expire automatically after one month (unless actively renewed) or upon implementation of the designation at the EU level. BaFin is required to repeal orders under the KWG soon as and insofar as the reason for the order no longer exists (KWG, s.6a(4)).

**(c)** *At the EU level*, a person or entities designated under the 1373 mechanism can write to the EU Council to have the designation reviewed or may institute a proceeding before the EU Country of Justice (Treaty on the Functioning of the European Union, arts.263(4), 275(2)). *At the national level*, orders imposed under the AWG or KWG can be challenged by petitioning the ordering authority, or before the German courts (Code of Administrative Court Procedures, *Verwaltungsgerichtsordnung*, ss.68, 81; KWG, s.6a(5)).

**(d) & (e)** *At the EU level*, persons designated under UNSCR 1267 etc. and 1988 are informed of applicable de-listing procedures (EC Regulation 881/2002, art.7(a); EU Regulation 753/2011, art.11(4)). *At the national level*, the Deutsche Bundesbank provides contact a dedicated financial sanctions hotline and contact addresses through which individuals can seek advice on de-listing.

**(f)** *At the EU level*, there are procedures to handle cases of mistaken identity (EC document 8519/18, paras.8-17, 37). *At the national level*, brief national guidance has been provided.<sup>87</sup> Funds mistakenly frozen under AWG orders (e.g., following a false positive) can be released following legal action on the basis that only the assets of listed persons must be frozen. The process for doing so is a standard court appeal (i.e., the process is not specifically communicated in relation to TFS). However, AWG orders are generally only temporary and are lifted when a corresponding EU designation comes into force.

**(g)** De-listings are communicated in the same way as new listings (see c.6.5(d)).

**Criterion 6.7** – *At the EU level*, there are procedures to authorise access to frozen funds, where necessary for basic expenses or the payment of certain expenses (EU Regulation 753/2011, art.5; EC Regulation 881/2002, art.2a; EC Regulation 2580/2001, arts.5, 6). *At the national level*, for freezing/prohibition orders under the AWG, BMWK has the authority to grant access to funds frozen where necessary to satisfy basic expenses or pay certain reasonable expenses such as legal fees (AWG, s.6(1); template Order to Restrict Capital and Payment Transactions with certain Persons or Partnerships). As such orders are temporary, requests for access to funds

<sup>87</sup> Available at: [www.finanz-sanktionsliste.de/fisalis/](http://www.finanz-sanktionsliste.de/fisalis/)

are rarely if ever received in practice. BaFin has the authority to grant access to funds frozen under the KWG for equivalent purposes (KWG, s.6a(3)).

### *Weighting and Conclusion*

Germany predominantly relies on the EU regime for implementing TFS. There is a national mechanism to mitigate the delay in the EU framework, however the current framework does not allow implementation without delay for sanctions issued by the UN immediately prior to weekends (including Fridays) or holidays.<sup>88</sup> This is considered a major shortcoming for two reasons. First, the inability to consistently implement TFS without delay undermines the other measures Germany has in place, meaning this criteria is weighted heavily. Secondly, the important TF risks in Germany and the materiality of Germany's financial sector mean that even an occasional delay in implementation could have significant consequences, meaning this deficiency creates a major gap. There are other shortcomings in both the EU and national framework, with deficiencies in the national framework generally given less weight as national orders are used exclusively as an interim measure prior to the adoption of an EU designation.

The national process for proposing designations is not documented, meaning the process is not always clear. Certain competent authorities do not have clear powers to solicit information to identify targets, although they are able to rely on other agencies with sufficient powers. Requests for designation received by Germany or the EU may take several weeks to be considered, which does not allow for a prompt determination. There is no EU or national procedure to request non-EU countries to give effect to EU or national designations, although the EU does have an approximation procedure. The EU 1373 mechanism does not require freezing for "EU internals" and national mechanisms that can be used in such cases are limited, which is a major deficiency given Germany's risks and context. There are minor gaps or lack of clarity in the application of EU and national mechanisms to all types of funds, assets and persons covered in criteria 6.5(b). There is a very minor delay in reporting obligations for the short period between a national and EU designation. Communication mechanisms for designations and de-listing could be improved at the national level.

**Recommendation 6 is rated partially compliant.**

### **Recommendation 7 – Targeted financial sanctions related to proliferation**

These are new requirements that were not assessed in Germany's previous MER.

**Criterion 7.1** – UN financial sanctions are implemented by way of EU Regulations that have direct effect in Germany. UNSCR 1718 and its successor Resolutions on the Democratic People's Republic of Korea (DPRK) are transposed into the EU legal framework through Council Decision (CFSP) 2016/849 and EU Regulation 2017/1509. UNSCR 2231 on Iran is transposed into the EU framework through Council Decision (CFSP) 2010/413 and EC Regulation 267/2012 and amendments. Germany can issue a domestic freezing/prohibition order to reduce the

<sup>88</sup> Delays have been seen in the implementation of other sanctions regimes under this system. Assessment of these regimes is not within the scope of R.6; however, as the implementation system is the same, this is relevant context when determining the likelihood of delays under this system.

implementation delays seen under the EU mechanism (AWG, s.6(1)). The national AWG order remains valid until the EU designation enters into force. As noted in c.6.4 above, AWG orders cannot be issued on weekends or holidays, meaning there will be a delay in implementation of UN designations issued immediately prior to weekends or holidays.<sup>89</sup>

**Criterion 7.2** – Germany’s supervisory framework for implementing and enforcing PF-related TFS is the same as that described in c.6.5 (also see c.2.4 on PF co-operation and co-ordination more generally).

**(a)** *At the EU level*, the EU regulations require all natural and legal persons within the EU to freeze the funds or other assets of designated persons or entities as soon as a designation is published (EC Regulation 267/2012, art.49; EU Regulation 2017/1509, art.1). *At the national level*, AWG orders prohibit natural and legal persons from making funds or economic resources available to the designated person or entity (AWG, s.6(1); template Order to Restrict Capital and Payment Transactions with certain Persons or Partnerships). As noted in c.7.1, there is a risk of delays in implementation.

**(b)** *At the EU level*, the freezing obligation extends to all funds and economic resources belonging to, owned, held or controlled by designated persons or entities. This includes funds or other assets derived or generated from such funds. Jointly-owned assets are not explicitly covered but this is touched upon in non-binding EU Best Practices on sanctions implementation. While the definition does not explicitly cover funds or assets of persons acting on behalf or at the direction of a designated person or entity, this is largely captured by the coverage of funds ‘controlled’ by the designated person. In addition, the EU has the ability to list those working on behalf of designated persons or entities (EC Regulation 267/2012, arts.1, 23(1)-(2); EU Regulation 2017/1509, arts.2, 34; EC document 8519/18, para.35). *At the national level*, the template Order makes it clear that the AWG covers funds or assets that are directly or indirectly in the possession or under the control of a designated person or entity. The definition of “control” set out in the template Order is such that this would cover the funds or other assets of persons or entities acting on behalf of or at the direction of designated persons or entities (template Order to Restrict Capital and Payment Transactions with certain Persons or Partnerships). As with the EU orders, jointly-owned assets are not explicitly covered. However, as these orders are explicitly made to pre-empt an upcoming EU designation, they are likely to be interpreted broadly to mirror the scope of the EU regulations (see c.6.5(b)).<sup>90</sup>

**(c)** *At the EU level*, EU nationals and natural and legal persons within the EU are prohibited from making funds and other assets available unless otherwise authorised or notified in compliance with the relevant UNSCRs (EU Regulation 267/2012, art.23(3); EU regulation 2017/1509, art.34(3)). Regulations apply to any natural or legal person, entity, body or group in respect of any business done in whole or in part within the EU. *At the national level*, orders under the AWG prohibit natural and legal persons from making funds or economic resources available (template Order to

<sup>89</sup> Since the national system came into force in 2020, a delay has been seen in the implementation of another sanctions regime. Assessment of other regimes is not within the scope of R.7; however, as the national implementation system is the same, this is relevant context when determining the likelihood of delays.

<sup>90</sup> The order template is currently under revision.

Restrict Capital and Payment Transactions with certain Persons or Partnerships) (see 6.5(c)).

**(d)** Germany uses the same mechanisms described in c.6.5(d) to communicate designations and provide guidance in relation to PF TFS and the same deficiencies apply.

**(e)** *At the EU level*, natural and legal persons (including FIs and DNFBPs) are required to immediately report any information on accounts and amounts frozen to competent authorities (the Deutsche Bundesbank) (EU Regulation 267/2012, art.40; EU Regulation 2017/1509, art.50). This requirement does not explicitly extend to reporting attempted transactions, although this is covered by the requirement to report “any information which would facilitate compliance” with the relevant Regulations. *At the national level*, there is no separate obligation for FIs and DNFBPs to report assets frozen in accordance with orders under the AWG or attempted transactions related to such orders. However, as noted in c.6.5(e), AWG orders are used as a temporary measure to pre-empt an EU designation, so the EU reporting obligations will typically be triggered by a corresponding EU designation shortly after the AWG order.

**(f)** *At the EU level*, protections are in place for third parties acting in good faith (EU Regulation 267/2012, art.42; EU Regulation 2017/1509, art.54). *At the national level*, protections exist for third parties in relation to orders under the AWG (see c.6.5(f)).

**Criterion 7.3** – Monitoring and enforcement of proliferation-related TFS is largely the same as for terrorism-related TFS (see c.6.5). The Deutsche Bundesbank and the Main Customs Offices are specifically authorised to monitor compliance with EU and AWG TFS obligations (AWG, s.23). Both agencies can conduct audits, can demand business documents or other relevant information, and have the power to undertake on-site examinations (AWG, s.23(1)). The Bundesbank supervises FIs’ compliance while the Main Customs Offices monitors businesses involved in cross-border movements of goods (including, where relevant, DNFBPs). Outside the financial sector, professional bodies (of lawyers, tax advisors, notaries and accountants) have a general duty to monitor their sector’s compliance with all obligations, which could include TFS. There is no clear monitoring or enforcement responsibility for other DNFBPs (REAs, DPMS and TCSPs) not engaged in the cross-border movement of goods. A breach of the freezing and prohibition orders (at the EU level or AWG orders) is punishable by a prison sentence of up to five years (AWG, s.18). There are no sanctions for breaching reporting requirements (c.7.2(e)).

**Criterion 7.4** – The following de-listing, unfreezing and access procedures apply:

**(a)** *At the EU level*, listed persons are informed of their ability to petition the UN Focal Point for de-listing. This takes place via a notice in the official journal of the EU containing the designation decision. *At the national level*, listed persons may approach the AA which will, on a case-by-case basis, provide a recommendation to the petitioner on a possible course of action.<sup>91</sup>

**(b)** Procedures for unfreezing funds due to a false positive are the same as those described under c.6.6(f).

<sup>91</sup> The recommended course of action would usually involve referring the petitioner to submitting a de-listing request to the Focal Point or providing information on other avenues for seeking redress.

**(c)** The Deutsche Bundesbank has the authority to grant access to frozen funds in accordance with EU Regulations and in line with the UNSCR exemption conditions (Regulation EU 267/2012, arts.24-28, 28b; EU Regulation 2017/1509, arts.35-36).

**(d)** Mechanisms for communicating de-listings are the same as those described in c.6.5(d).

#### **Criterion 7.5 –**

**(a)** The EU Regulations permit the payment of interest or other earnings to frozen accounts as well as payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the UNSCR provisions (EU Regulation 2017/1509, art.34(9); EU Regulation 267/2012, art.29). There is an equivalent provision under national AWG orders (template Order to Restrict Capital and Payment Transactions with certain Persons or Partnerships).

**(b)** Provisions in the EU Regulations authorise the payment of sums due under a contract entered into prior to the designation of such person or entity, provided the payment does not contribute to an activity prohibited by the regulation and after prior notice is given to the UN Sanctions Committee (EU Regulation 267/2012, arts.24, 25). The Deutsche Bundesbank is responsible for authorising payments and assesses applications against the factors set out in c.7.5(b)(i)-(iii). While there is no similar allowance under national AWG orders, such orders are temporary, and superseded by an EU designation (see c.6.5(e)).

### *Weighting and Conclusion*

As in R.6, Germany predominantly relies on the EU regime for implementing PF-related TFS. There is a national mechanism to mitigate the delay in the EU framework, however the current framework does not allow implementation without delay for sanctions issued by the UN immediately prior to weekends (including Fridays) or holidays.<sup>92</sup> This is considered a major shortcoming for two reasons. First, the inability to consistently implement TFS without delay undermines the other measures Germany has in place, meaning this criteria is weighted heavily. Secondly, the materiality of Germany's financial sector mean that even an occasional delay in implementation could have significant consequences, meaning this deficiency creates a major gap. There are minor gaps in both the EU and national frameworks, with deficiencies in the national framework weighted less strongly because these orders are used as a temporary stopgap prior to EU designations. There is a minor lack of clarity as to the coverage of all types of funds, assets and persons listed in criteria 7.2(b). There is a very minor delay in reporting obligations for the short period between a national and EU designation. There is a gap in monitoring for REAs, DPMS and TCSPs (unless these institutions are involved in the cross-border movement of goods). At the national level, communication mechanisms for designations and de-listing could be improved.

**Recommendation 7 is rated partly compliant.**

<sup>92</sup> Delays have been seen in the implementation of other sanctions regimes under this system. Assessment of these regimes is not within the scope of R.7; however, as the implementation system is the same, this is relevant context when determining the likelihood of delays under this system.

## Recommendation 8 – Non-profit organisations

In its previous MER, Germany was largely compliant with these requirements, however the requirements in R.8 have changed considerably since then.

### Criterion 8.1 –

**(a)** Germany has assessed its large civil society sector and identified a sub-set of organisations<sup>93</sup> that it considers fall within the FATF definition of a NPO. Germany conducted a NPO risk assessment in 2019/2020 which uses a range of relevant sources (including statistics and sector analysis, case studies, STRs and FIU analysis, information from LEAs and intelligence services, experience of NPOs, self-assessment by NPOs (including a large-scale survey of NPOs), and the findings of the NRA). The NPO risk assessment identifies the features and types of NPOs which are at risk of TF abuse and outlines nine criteria as particularly high risk (see IO.10 for further information).

**(b)** The NPO risk assessment identifies the nature of threats to NPOs including those that arise from the exploitation of a legitimate NPO (as medium-low risk), and threats from the use of sham NPOs (as medium-high risk) (see IO.10).

**(c)** Germany has taken steps to review the adequacy of measures that relate to at-risk NPOs. In the NPO risk assessment, Germany considered the measures applicable to NPOs (to assess regulatory vulnerabilities) and made recommendations accordingly.

**(d)** The 2019/2020 NPO risk assessment was the first comprehensive assessment of the NPO sector's TF risk. Germany intends that it is updated as part of the NRA process (see c.1.3). Germany also uses existing TF risk assessment mechanisms to assess new information on the NPO sector (e.g., the TF situation report issued every three years, *ad hoc* information reports by the BKA (see R.2)).

### Criterion 8.2 –

**(a)** While the government has not issued written guidance on NPO governance, it has supported civil society organisations' efforts to promote accountability, integrity, and public confidence in the administration and management of NPOs (including a voluntary Seal of Approval and transparency standard for NPOs that fulfil transparency criteria, advice to NPOs and the public on donations, a public online library of good practices for NPOs, and principles of good foundation practice).<sup>94</sup> NPOs are also subject to measures and obligations that aim to increase transparency and accountability and prevent TF (see c.8.3).

**(b)** Germany has undertaken outreach to raise awareness of TF risks and measures to combat TF. E.g., BMI has regular contact with representatives of certain religious NPOs and held two events in 2019 and one event in 2021 on TF risk management for 30 at-risk NPOs; the AA provided TF risk training to humanitarian NPOs in 2020; and

<sup>93</sup> NPOs are not an independent type of organisation in Germany. Germany's NPO sector is made up of associations, foundations, and non-profit private companies. The common feature is that such organisations are not for-profit.

<sup>94</sup> These measures are offered by civil society organisations and groups (including the German Central Institute for Social Issues, *Das Deutsche Zentralinstitut für soziale Fragen* (DZI); VENRO, an umbrella organisation for humanitarian aid NPOs; the Association of German Foundations; and the Transparency Civil Society Initiative, *Initiative Transparente Zivilgesellschaft* (ITZ)) with support from government authorities.

*Länder* security agencies also hold events for target NPOs.<sup>95</sup> Germany has also worked with NPOs and FIs to prevent and mitigate de-risking (e.g., the 2020 Global Forum on Illicit Financial Flows and Sustainable Development). For donors, the BMI circulated a brochure on the TF risks of donating and encouraging responsible donations. More generally, the German Central Institute for Social Issues, *Das Deutsche Zentralinstitut für soziale Fragen* (DZI) provides advice to donors, including on its website<sup>96</sup> and through a donor advisory service that encourages or warns against donating to specific agencies on the basis of DZI's research.

**(c)** Germany has worked with VENRO, an umbrella organisation of NPOs, DZI and other NPOs to fund and develop guidance and workshops on risk management, integrity, transparency and anti-corruption. To-date, guidance or best practices have not covered measures to address the specific TF risks and vulnerabilities.

**(d)** It is not clear that Germany has encouraged NPOs to conduct transactions via regulated financial channels, beyond explaining the risks of cash during outreach initiatives.

**Criterion 8.3** – Germany has taken steps to monitor NPOs to demonstrate that measures are being applied to prevent TF abuse. Measures for associations are largely sufficient, but are not fully in line with the recent NPO risk assessment.

NPOs typically operate as associations, foundations or non-profit companies and are required to be registered in line with their legal person status; there is no separate registration as a NPO (see R.24). To be eligible for non-profit status, NPOs must submit information to the relevant *Länder* tax authority, including prior to commencing operations. This includes financial reporting requirements (Fiscal Code, *Abgabenordnung* (AO), ss.51, 60, 63). These measures apply to NPOs on a general level. Associations are considered at higher risk than foundations or companies (NPO Risk Assessment, pg.52). The information provided by associations upon registration is more limited than foundations or companies which reduces the ability of registrars to identify possible abuse. Nonetheless, associations that seek non-profit status are subject to scrutiny from the tax authorities which may help detect the misuse of funds for TF purposes. This leaves only a very minor gap for associations that do not seek non-profit status. Foundations are subject to more stringent registration and monitoring, despite the identified lower risk of these entities.

There are some risk-based measures to detect specific at-risk NPOs. The BfV works to detect sham NPOs with extremist tendencies. NPOs seeking government grants must submit detailed information on their management, funding and operations. The awarding of grants or contracts is based on a risk-assessment of the specific NPO. At the law enforcement level, the monitoring and investigation of NPOs suspected of TF is subject to risk-based prioritisation (e.g., within the FIU). (For more information on monitoring and supervision of NPOs, see c.8.4(a)).

**Criterion 8.4** –

**(a)** Germany has in place some monitoring of NPOs for compliance with the requirements of R.8. All NPOs with non-profit status are subject to monitoring by the *Länder* tax authorities. This monitoring includes undertaking research on affiliated

<sup>95</sup> Further outreach is foreseen in the communication strategy of the published NPO Risk Assessment.

<sup>96</sup> DZI “Donation tips” (<https://www.dzi.de/pressemitteilungen/spenden-tipps-zum-jahreswechsel/>).

entities or persons and reviewing available information for any indications of extremist tendencies. Foundations and companies are also subject to additional monitoring by *Länder* registrars (for foundations) and the Commercial Register (for companies); although this is not focused on R.8 requirements (see R.24). For NPOs conducting government-supported projects abroad, particularly in high-risk countries, there is enhanced and ongoing scrutiny, including on-the-ground, from the AA or independent third-parties. NPOs may also be monitored by law enforcement or security agencies where there are indications of extremism (which is one of the risk factors identified in the NPO risk assessment) or a suspicion of misconduct. There is a very minor gap in oversight for associations that do not seek non-profit status (including sham NPOs) where there is no indication of extremism (see c.8.3). Germany estimates that there are only a small number of associations without non-profit status (~5% of registered associations), but the exact number is not recorded.

**(b)** Germany largely has the ability to apply effective, proportionate and dissuasive sanctions for violations of the requirements applicable to NPOs. NPOs with indications of extremism are identified in a public report. For associations, failure to comply with registration requirements (including notifying the register of a relevant change) is subject to a coercive fine of up to EUR 1 000 (BGB, s.78; Introductory Act to the Criminal Code, art.6). For foundations, these fines are imposed by administrative authorities (who manage the registers) according to the relevant *Länder* legislation (e.g., Administrative Enforcement Act for Baden-Württemberg, s.19). *Länder* legislation also gives administrative authorities the power to remove foundation members (e.g., Foundation Law for the Saarland, s.14). A breach of the tax and financial reporting obligations can be sanctioned by the revocation of non-profit status and significant financial disadvantages (e.g., repayment of tax benefits). For entities receiving government funding, breaching relevant reporting and oversight requirements can be sanctioned by the termination of any contract and an order to repay the funds awarded. The BMI is able to permanently ban any NPO whose aims or activities contravene criminal law or are directed against the constitutional order. Such NPOs must thereafter be dissolved. A banned NPO will typically also have its assets seized and no successor or replacement association may be formed (Basic Law, art.9(2)). Germany is also able to take measures where NPOs breach TFS obligations (see R.6, 7) or are involved in TF (see R.5). Criminal sanctions are available for natural persons where the individual has committed a criminal offence in the context of their NPO activity. Administrative sanctions can be applied to natural persons only where the individual has extensive decision-making power in the relevant area and the necessary knowledge and skills (OWiG, s.9), which may not cover all those acting on behalf of an NPO.

#### **Criterion 8.5 –**

**(a)** Germany has measures in place to promote co-operation, co-ordination and information-sharing between competent authorities. Co-operation is facilitated by broad disclosure powers that apply to all relevant agencies. These also extend to the tax authorities, which are permitted to disclose tax information (including that covered by tax secrecy provisions) where there is a public interest to do so and/or where it helps prevent, detect or combat ML and TF (AO, ss.30(4), 31b(1)). Information-sharing is enhanced through the public nature of the various registers. Federal and *Länder* law enforcement and security agencies co-operate regularly and productively within the framework of the GTAZ and GETZ (see R.2). However, the FIU is not a regular member of these fora and instead co-operates with law enforcement bodies on an *ad hoc* basis (through written communication and meetings) on

identified risk areas, including NPOs. Co-operation with administrative monitoring bodies (such as association or foundation registrars) is also *ad hoc*.

**(b)** The German security agencies and judicial authorities have the investigative expertise and capability to examine NPOs suspected of TF abuse. Specialised units for investigating and prosecuting TF have been established at the federal level and in different *Länder*. These have TF-specific expertise.

**(c)** Competent authorities have access to information on the administration and management of NPOs in the course of an investigation. Registry information on associations, foundations and companies is public and available on online portals for each of the *Länder*. Other information can be sought pursuant to a production order (see R.31) or obtained from relevant competent authorities (see c.8.5(a)).

**(d)** Registrars or other bodies that may develop suspicions that a NPO is being misused (e.g., the DZI or the AA) are subject to a general duty to report offending, and are able to report any suspicion to law enforcement or the security agencies (StGB, s.138(2)). There is no formal mechanism or established reporting channel for registrars to share relevant information with the BKA, *Länder* police and/or the FIU. A single point of contact has, however, been appointed in the AA to receive information related to NPO misconduct. Tax authorities are obliged to report suspicions to the FIU, which will then disseminate them to the relevant authority (AO, s.31(b)). Federal and *Länder* LEAs and security agencies can also share information and report suspicions within the framework of the GTAZ and the GETZ.

**Criterion 8.6** – International requests for information regarding particular NPOs suspected of TF abuse are dealt with in the same way as any other request for information. Competent authorities (including security or investigation agencies, the FIU, and tax authorities) can provide information as described in R.40. Foreign authorities are able to access the public NPO registers.

### Weighting and Conclusion

Germany has a framework in place for preventing and detecting TF abuse through NPOs and only minor deficiencies remain. In part due to the recency of Germany's NPO risk assessment, existing guidance and best practices do not yet cover measures to address the specific TF risks and vulnerabilities identified. It is not clear that Germany has explicitly encouraged NPOs to conduct transactions via regulated financial channels. Germany has taken steps to monitor NPOs, but there are limited measures for the very small number of associations that do not seek non-profit status. This is given limited weight as this is likely a small number of entities. Sanctions for natural person NPO representatives are limited. Mechanisms are in place for co-operation, which could be enhanced through more regular and systematic involvement of the FIU and administrative monitoring bodies (such as association or foundation registrars). While avenues for reporting exist, there is no formal mechanism for registrars to share relevant information with the BKA, *Länder* police and/or the FIU.

**Recommendation 8 is rated largely compliant.**

## Recommendation 9 – Financial institution secrecy laws

In the previous MER, Germany was compliant with these requirements.

**Criterion 9.1** – There are no financial institution secrecy laws that inhibit the implementation of AML/CFT measures in Germany.

*Access to information by competent authorities:* There are no legal duties that prevent FIs and DNFBPs sharing information with competent authorities. The FIU and supervisors have powers to compel information from entities in line with their responsibilities (GwG, ss.30(3), 51; KWG, s.44(1); Insurance Supervision Act, *Versicherungsaufsichtsgesetz* (VAG), s.305(1); Investment Code, *Kapitalanlagegesetzbuch* (KAGB), s.14; Payment Services Supervision Act, *Zahlungsdiensteaufsichtsgesetz* (ZAG), s.19(1)). Supervisors are exempt from applicable data protection requirements where data use is necessary for their functions (GwG, s.51a). See also R.27, 29 and 31.

*Sharing of information between competent authorities:* Supervisory authorities are required to co-operate fully and share information with competent authorities (GwG, s.55(1)). While there is a general duty of confidentiality, this does not apply to disclosures of information to other AML/CFT supervisors, prudential supervisors, LEAs, or the FIU (GwG, s.54(3)). Mechanisms exist to facilitate co-operation and information-sharing between competent authorities; see R.2. Information can also be shared internationally with foreign competent authorities (GwG, s.54(3)); see R.40).

*Sharing of information between FIs:* FIs and DNFBPs may share information, including customer and STR information, with other entities in the same group (GwG, ss.9(1), 47(2)). FIs may also share information on suspicions outside a group where it would aid in the other entity's risk assessment or STR reporting (GwG, s.47(5)). See also R.13 and 16-18.

### Weighting and Conclusion

All criteria are met.

**Recommendation 9 is rated compliant.**

## Recommendation 10 – Customer due diligence

In its last MER, Germany was partially complaint with CDD requirements on the basis that: reasonable measures to verify beneficial ownership were not always required, the definition of beneficial ownership of a trust was incomplete, there were broad CDD exemptions without risk assessment, and there was no requirement to consider filing an STR where CDD could not be completed.

Most AML/CFT obligations, including CDD, are contained in the GwG, which applies to all FIs and DNFBPs. A small number of requirements for FIs are contained in sector-specific laws. The law relating to insurance providers (the Insurance Supervision Act, *Versicherungsaufsichtsgesetz* (VAG)) does not apply to insurance intermediaries acting as independent agents; such entities are instead covered by the Trade Regulation Code. This has a minor impact on Germany's compliance with parts of R.10 below (c.10.12 and c.10.13), as well as parts of R.12, 18 and 26.

**Criterion 10.1** – Germany prohibits the use of a fictitious name for opening or maintaining an account and does not permit anonymous accounts (Fiscal Code, *Abgabenordnung* (AO), s.154).

**Criterion 10.2** – FIs are required to undertake CDD when:

- (a) establishing a business relationship (GwG, s.10(3)1)
- (b) carrying out transactions outside an existing business relationship of EUR 15 000 or more (GwG, s.10(3)2(b)), including where the transaction is carried out in several linked operations (GwG, s.1(5))
- (c) carrying out occasional wire transfers of EUR 1 000 or more (GwG, s.10(3)2(a))
- (d) there is a suspicion of ML/TF, regardless of other thresholds or exemptions (GwG, s.10(3)3)
- (e) there are doubts about the veracity and adequacy of previously obtained customer identification data (GwG, s.10(3)4).

**Criterion 10.3** – FIs are required to identify the customer (any “contracting party”, whether a natural or legal person) and verify that identity using one of the specified reliable sources, such as an official identity document or various forms of digital identity (GwG, ss.1(3), 10(1), 11-13).

**Criterion 10.4** – FIs are required to verify that any person acting on behalf of a customer is authorised to do so, and identify and verify the identity of that person (GwG, s.10(1)). The same identification and verification requirements apply to those opening an account on behalf of another person (see c.10.3).

**Criterion 10.5** – FIs are required to determine whether the customer is acting on behalf of a beneficial owner and, if so, identify the ultimate beneficial owner (GwG, s.10(1); BaFin Guidance on the GwG, section 5.2.2.1; Guidance on the GwG for goods dealers, real estate agents and other non-financial undertakings, section 4.5.2 (applicable to FIs not supervised by BaFin)). FIs are required to verify the information gathered by taking reasonable (risk-appropriate) measures (GwG, s.11(5); BaFin Guidance on the GwG, section 5.2.3.2). There is no requirement that verification must use information or data from a “reliable source”, although it is not sufficient for FIs to rely on the transparency register (GwG, s.11(5)). There is a limited requirement that identification and verification processes be sufficient to satisfy the FI that it knows who the BO is.

**Criterion 10.6** – FIs are required to obtain information on the purpose and intended nature of the business relationship where this is not already clear beyond doubt (GwG, s.10(1)3).

**Criterion 10.7** – FIs are required to conduct ongoing due diligence on the business relationship (GwG, s.10(1)5), including:

- (a) continuously monitoring transactions to ensure they are consistent with the documents and information available to the FI on the customer (including the beneficial owner), their business activity and customer profile and, where necessary, the source of wealth, and
- (b) ensuring that CDD documents, data or information are updated at appropriate intervals in line with risk.

**Criterion 10.8** – For customers that are not natural persons, FIs are required to take adequate measures to understand the customer’s ownership and control structure (GwG, s.10(1)2; BaFin Guidance on the GwG, section 5.2.2.1). This requirement covers legal persons, but does not extend to legal arrangements as they cannot be customers in Germany (the customer is the natural person administrator of the legal

arrangement, i.e., the trustee for foreign trusts and the administrator of *Treuhand* assets). For legal arrangements, FIs may collect some of this information when identifying the beneficial owner (see c.10.10). There is an implicit obligation to assess available information on (in order to understand) the nature of the customer's business activity and profile (GwG, s.10(1)5).

**Criterion 10.9** – For customers that are legal persons, FIs are required to identify and verify the customer through:

- (a) The name, legal form, and proof of existence (GwG, ss.11(4)2, 12(2)).
- (b) The names of members of its representative body or the names of its legal representatives (GwG, s.11(4)2). This would generally cover representatives from senior management level, particularly board members, although this is not explicit. FIs must also obtain an extract from the commercial or co-operative register, or a company's founding documents (GwG, s.12(2)).
- (c) The address of the registered office or head office (GwG, s.11(4)2). Guidance clarifies that this should be a physical location (BaFin Guidance on the GwG, section 5.1.4.1). However, there is no clear obligation for FIs to also obtain the address of the principal place of business, if different.

These requirements do not apply to legal arrangements (including *Treuhand*). As outlined in c.10.8, legal arrangements cannot be customers in Germany; the administrator of the arrangement is the customer. If the administrator is a legal person, that legal person will undergo the CDD process outlined above (GwG, ss.11(4)2). If the administrator is a natural person, no specific obligations apply in identifying the legal arrangement, but the legal arrangement should be identified in the process of identifying the beneficial owner (GwG, s.11(4)2; see c.10.11). The specific information required under (a) to (c) above are not explicitly covered as these elements are expected to be gathered in establishing the beneficial owner of an administrator's account.

**Criterion 10.10** – For customers that are legal persons, FIs are required to identify the beneficial owner by verifying the identity of the natural person who ultimately owns or controls the arrangement or the natural person at whose instruction a transaction is ultimately carried out or a business relationship is ultimately established (GwG, ss.10(1)2, 3(1), 1(3); see c.10.5).

(a) and (b) For legal persons except foundations with legal capacity, this includes any person who holds more than 25% of the capital or controls more than 25% of the voting rights or exercises control in a comparable manner (GwG, s.3(2); BaFin Guidance on the GwG, section 5.2.2.1).

(c) Where no natural person is identified under (a) and (b) above, FIs may verify the identity of the legal representative, managing partner or partner (GwG, s.3(2)). This would typically require the identification and verification of board members, chief executives or partners.

These requirements do not apply when the legal person is publicly listed in Germany, or the European Economic Area (EEA), or subject to equivalent transparency requirements (GwG, s.3(2)), which is in line with footnote 35 of the Methodology.

For foundations with legal capacity, FIs must identify and verify the identity of any natural person who is a member of the board, any natural person or class of persons who is a beneficiary, and any natural person directly or indirectly exercising a

controlling influence who is a member of the board or a designated beneficiary (GwG, ss.3(3), 10(1)2).

**Criterion 10.11** – In the case of legal arrangements, FIs are required to identify the beneficial owner by verifying the identity of the natural person who ultimately owns or controls the arrangement, or the natural person at whose instruction a transaction is ultimately carried out or a business relationship is ultimately established (GwG, ss.10(1)2, 1(3), 3(1); see c.10.5). For trusts or trust-like arrangements, this requirement includes identifying and verifying the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over management of assets or property or the distribution of income (GwG, s.3(3)).

**Criterion 10.12** – In the insurance context, in addition to the CDD measures required for the customer and the beneficial owner, insurance undertakings are required to conduct the following measures on the beneficiary of life insurance and other investment related insurance policies, when entering into a business relationship:

**(a)** for a beneficiary that is identified as a specifically named natural or legal person or legal arrangement - obtaining the name of the person (VAG, s.54(1); GwG, s.11(5)), and

**(b)** for a beneficiary that is designated by characteristics or by class or by other means - obtaining sufficient information on the characteristics or categories used to designate beneficiaries to be able to determine and verify the identity of the beneficiary at the time of the payout (VAG, s.54(1)).

**(c)** For both the above cases - the verification of the identity of the beneficiary must occur no later than the time of the payout (VAG, s.54(2)).

Insurance intermediaries are only subject to the first of these requirements under the GwG ((a) above).

**Criterion 10.13** – There is a general requirement for FIs to take into account customer risk factors in deciding whether to apply enhanced CDD (GwG, s.15(2)), although there is no specific requirement for FIs to include the beneficiary of a life insurance policy as a relevant risk factor. If the policyholder or a beneficiary is a legal person or association, insurance undertakings are required to identify the beneficial owner no later than the time of payout (VAG, s.54(1)). Insurance intermediaries are not subject to this requirement. This does not apply to legal arrangements (which cannot themselves hold or be the beneficiary of an insurance contract). There is no explicit requirement to take other enhanced measures.

**Criterion 10.14** – In general, FIs are required to identify and verify the customer and beneficial owner *before* establishing a business relationship or executing an occasional transaction (GwG, s.11(1)). Verification may be completed during the course of establishing the business relationship where (GwG, s.11(1)):

**(a)** this occurs “without delay” (defined as “without culpable hesitation”: BGB, s.121(1)),

**(b)** this is necessary to avoid interrupting the normal course of business, and

**(c)** there is a low risk of ML/TF.

Credit and financial service institutions are permitted to verify a customer’s identity without delay *after* the opening of a bank or securities account, but in such cases no

funds can be withdrawn from the account and any funds received can only be paid back to the depositor (KWG, s.25j) (see c.10.15).

**Criterion 10.15** – In general, FIs must identify and verify the customer and beneficial owner *before or during* the establishment of a business relationship meaning there is no ability to utilise a business relationship prior to verification (see c.10.14). There is some limited scope for credit and financial service institutions to conduct verification *after* the opening of a bank or securities account (see c.10.14). To manage this risk, Germany has imposed strict conditions under which a customer may utilise the business relationship prior to verification to ensure this occurs only in limited and low-risk cases (no funds can be withdrawn and any funds received can only be paid back to the depositor) (KWG, s.25j).

**Criterion 10.16** – FIs are required to apply CDD requirements to existing customers on the basis of risk and materiality, and at an appropriate time, particularly when the relevant circumstances change (GwG, s.10(3a)). There is no explicit obligation to take into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained, although this may be factored into the risk-based decision to apply CDD. These elements may also be captured to some extent by the obligation to take into account a change in the customer's circumstances, but this will not always be the case.

**Criterion 10.17** – FIs are required to perform enhanced due diligence where they identify, either through a risk analysis or by taking into account a non-exhaustive list of risk factors, a higher risk of ML/TF (GwG, s.15(2)).

**Criterion 10.18** – FIs may apply appropriate simplified CDD measures where they have established that the business relationship or transaction presents a low risk of ML/TF, taking into account a non-exhaustive list of risk factors (GwG, s.14). This list includes factors that may not be based entirely on an assessment of risk, for example, registration or residence in an EU Member State (GwG, Annex 2; see also c.1.8). Simplified measures are not permitted where the FI or DNFBPs suspects ML/TF (GwG, s.10(3)). There is no explicit prohibition on simplified measures where specific higher risk scenarios apply, but there is guidance in the legislation on higher risk factors where simplified measures would not be appropriate (where there is a higher risk, enhanced due diligence is required (see c.10.17)).

Criterion 10.19 –

**(a)** Where a FI is unable to complete CDD, a business relationship must not be established and no transactions may be executed. Where a business relationship already exists, it is required to terminate the relationship (GwG, s.10(9)).

**(b)** In such cases, non-binding guidance states that FIs must review whether filing a STR is appropriate (BaFin Guidance on the GwG, section 5.8.1 (which applies to most FIs); Guidance for other DNFBPs, section 4.10.1 (which applies to insurance intermediaries not supervised by BaFin)).

**Criterion 10.20** – There is no explicit provision allowing entities to omit CDD and file a STR where they believe that the CDD process would tip-off the customer, however, this is implicitly covered. Where postponing a transaction (e.g., due to time taken to undertake CDD) could “frustrate proceedings in relation to a suspected criminal offence” (including by tipping off a customer), FIs may perform the transaction provided they file a STR without delay (GwG, s.46(2)).

### Weighting and Conclusion

While most of Germany's CDD measures meet the FATF Standards, minor deficiencies exist. Deficiencies related to beneficial ownership have been weighted most heavily. Requirements on identifying and verifying the beneficial owner could be clearer in some areas. Requirements to understand a customer's ownership and control structure do not clearly extend to legal arrangements. Small gaps exist in the requirements on information collection and verification related to legal persons, and these requirements do not apply to legal arrangements. In the insurance context, there is no specific requirement for FIs to include the beneficiary of a life insurance policy as a relevant risk factor for enhanced due diligence and insurance intermediaries are not subject to all of the insurance-specific CDD requirements. Finally, certain requirements are not sufficiently explicit including the requirement to take into account whether and when CDD measures were previously undertaken and the adequacy of data obtained, and the requirement to consider filing a STR where a FI is unable to complete CDD. The decision to undertake simplified due diligence includes factors that are not entirely risk-based. These are weighted less heavily as implicit or mitigating requirements are generally in place.

**Recommendation 10 is rated largely compliant.**

### Recommendation 11 – Record-keeping

In its previous MER, Germany was largely compliant with these requirements on the basis of uncertainty about what information would be acquired and retained on low-risk customers.

**Criterion 11.1** – FIs are required to retain data and information collected on domestic and international transactions for at least five years (GwG, ss.8(1), 8(4)).

**Criterion 11.2** – FIs are required to retain data collected and information gathered through CDD measures and results of any risk analysis for five years following the termination of the business relationship or after the date of the occasional transaction (GwG, ss.8(1), 8(4)). Commercial and tax obligations require FIs to maintain account books and business correspondence, including customers' account files for at least six years (Commercial Code, *Handelsgesetzbuch*, s.257; AO, s.147).

**Criterion 11.3** – Transaction records must include information that could be necessary for the investigation of transactions (GwG, s.8(1)1). For banks, there is also an additional requirement that records be sufficient to permit effective supervision (KWG, s.25a(1)).

**Criterion 11.4** – FI are required to ensure that records can be retrieved within a reasonable period of time (GwG, s.8(3)), and are required to swiftly ("without culpable hesitation") provide requested information to competent authorities, including supervisors and law enforcement agencies (GwG, s.6(6) BaFin Guidance on the GwG, Chpt.3.9; BGB, s.121(1)). See also R.27, 29 and 31.

### Weighting and Conclusion

All criteria are met.

**Recommendation 11 is rated compliant.**

## Recommendation 12 – Politically exposed persons

In its previous MER, Germany was partially compliant with these requirements based on the following deficiencies: there were no requirements with respect to PEPs that were beneficial owners of the customer; provisions did not apply to foreign PEPs residing in Germany; and approval to commence or continue the business relationship was not specific to be at a senior management level. Since its previous MER, the FATF Standards in this area have been expanded to include domestic PEPs and Germany has amended its PEPs requirements.

**Criterion 12.1** – Germany does not distinguish between domestic and foreign PEPs and the definition of a PEP is in line with the FATF Glossary definition (GwG, s.1(12)). In relation to domestic or foreign PEPs, their family members, or close associates, in addition to performing CDD, FIs are required to:

**(a)** Use risk-management procedures to establish whether a customer or beneficial owner is a PEP (GwG, s.10(1)).

**(b)** Obtain senior management approval before establishing or continuing a business relationship (GwG, s.15(4)).

**(c)** Take reasonable measures to establish the source of funds involved in the business relationship or transaction of customers and beneficial owners identified as PEPs (GwG, s.15(4)). The German term for source of funds (*“Herkunft der Vermögenswerte”*) is interpreted broadly and would generally, but not always, also cover the requirement to establish the source of wealth of the PEPs.

**(d)** Conduct enhanced, ongoing monitoring of the business relationship (GwG, s.15(4)).

**Criterion 12.2** – The measures set out in c.12.1 apply to domestic PEPs and persons entrusted with a prominent function by an international organisation (GwG, s.1(12)).

**Criterion 12.3** – The measures set out in c.12.1 apply to the family members and close associates of all types of PEPs (GwG, ss.15(3), 15(4)). The definition of family member is “close relative” of a PEP, such as a spouse, child or parent. While this list is not exhaustive, it is not clear that the definition would include extended family members (e.g., aunts and uncles, brothers- and sisters-in-law, grandparents, etc.). Similarly, the definition of close associate is a person who has a “close business relationship” or is a co-beneficial owner of a legal person or arrangement with the PEP which does not cover close social associates (GwG, s.1(13)-(14)).

**Criterion 12.4** – Insurance undertakings and intermediaries are required to use risk-oriented procedures to establish whether a beneficiary or beneficial owner is a PEP (VAG, s.54(2); GwG, s.10(1)). For insurance undertakings, it is specified that this should occur, at the latest, at the time of the payout (VAG, s.54(2)). Where higher risks are identified, insurance undertakings are required to conduct enhanced scrutiny on the whole business relationship (VAG, s.55(2)), to examine whether the conditions for making a STR are met (VAG, s.55(3)); and to inform a member of senior management before the payout (VAG, s.55(1)). Insurance intermediaries are only subject to the general requirement required to use risk-oriented procedures to establish whether a beneficiary or beneficial owner is a PEP.

### Weighting and Conclusion

Germany covers domestic and foreign PEPs in its laws; however, some minor gaps exist: the requirement to establish the source of wealth is not always covered; the definition of family members and close associates does not clearly extended family or close social associates; and insurance intermediaries are not subject to the life insurance-specific obligations.

**Recommendation 12 is rated largely compliant.**

### Recommendation 13 – Correspondent banking

In its previous MER, Germany was rated partially compliant with these requirements as special measures applied only to non-EU correspondent relationships and approval for continuing business relationships was not specified to be at the senior management level.

**Criterion 13.1** – In relation to cross-border correspondent banking or other similar relationships with a third-country respondent institution outside the EEA, FIs are required to:

**(a)** obtain sufficient information about the respondent to understand the nature of their business, their reputation, and the quality of supervision. While not explicit, this is broad enough to cover understanding whether the institution has been subject to an investigation or AML/CFT action (GwG, s.15(7)1).

**(b)** obtain sufficient information to understand the respondent institution’s AML/CFT controls (GwG, s.15(7)2)

**(c)** obtain approval from senior management before establishing the relationship (GwG, s.15(7)2), and

**(d)** determine and document the respective responsibilities of each institution in fulfilling due diligence requirements (GwG, s.15(7)3). There is no obligation to determine and document the other AML/CFT responsibilities of each institution (e.g., record-keeping, suspicious transaction reporting).

For correspondent banking relationships within the EEA, a case-by-case, risk-based approach is taken (GwG, s.15(3)4). This is inconsistent with R.13 which requires these measures to be applied to all cross-border correspondent banking relationships.

**Criterion 13.2 – (N/A)** Germany does not permit FIs to maintain “payable-through accounts” for respondents (KWG, s.25m). FIs are required to take measures to ensure respondent institutions do not permit payments through payable-through accounts (GwG, s.15(7)5).

**Criterion 13.3** – Credit and financial services institutions in Germany are prohibited from entering into, or continuing, correspondent banking or other business relationships with shell banks (KWG, s.25m). This captures the FIs that are engaged in correspondent banking relationships. In addition, all FIs are required to take measures to ensure that they do not establish or continue a business relationship with a respondent whose accounts are known to be used by a shell bank (GwG, s.15(7)4).

### Weighting and Conclusion

There is no obligation for FIs to determine and document all AML/CFT responsibilities of third-country respondent institutions. Mandatory enhanced due diligence measures for correspondent banking relationships apply only to respondent institutions outside the EEA. This is a moderate deficiency due to the significant role of the German financial sector in the EU.

**Recommendation.13 is rated partially compliant.**

### Recommendation 14 – Money or value transfer services

In its previous MER, Germany was largely compliant with these requirements based on effectiveness deficiencies which under the current evaluation are considered in the assessment of IO.4.

**Criterion 14.1** – Money or value transfer services (MVTs) providers, whether natural or legal persons, must be licensed by BaFin (Payment Services Supervision Act, *Zahlungsdiensteaufsichtsgesetz* (ZAG), ss.10(1), 11(1)). Licensed FIs (e.g., banks and e-money institutions) can provide MVTs without a separate license.

**Criterion 14.2** – BaFin monitors MVTs providers to investigate and enforce licensing requirements and sanction breaches (ZAG, ss.7, 8, 63, 64). A specialised BaFin unit is responsible for investigating and sanctioning the unlicensed provision of MVTs. Information from various sources may trigger an investigation (e.g., STRs, whistleblowing, consumer complaints, information from other national or international authorities etc.). Providing MVTs without a license is subject to proportionate and dissuasive sanctions, including imprisonment of up to five years or an unspecified fine (ZAG, s.63(1)). BaFin can also order the immediate cessation of business operations (ZAG, s.7).

**Criterion 14.3** – MVTs providers are subject to monitoring by BaFin for compliance with the GwG (GwG, ss.2(1) and 50).

**Criterion 14.4** – Agents for MVTs providers are required to be registered with BaFin before commencing operations (ZAG, s.25). MVTs providers providing services through an agent must provide BaFin with information on the agent (including name and address) and notify BaFin of any changes (ZAG, s.25(1)).

**Criterion 14.5** – MVTs providers that use agents, which are obliged entities themselves, are required to ensure that the agent “meets the legal requirements when providing payment services” (ZAG, s.25(2)) and must provide BaFin with a description of the agent’s internal control mechanisms (ZAG, s.25(1)2). Nonetheless, there is no specific obligation to include the agent in their AML/CFT programme or to monitor their ongoing compliance.

### Weighting and Conclusion

MVTs providers are licensed and supervised by BaFin. Agents for MVTs providers are obliged entities under the GwG and need to be registered with BaFin. While MVTs providers need to provide BaFin with all necessary information on the agent and its internal control mechanisms, there is no specific obligation for MVTs providers to include agents in the AML/CFT programme or monitor their compliance.

**Recommendation 14 is rated largely compliant.**

## Recommendation 15 – New technologies

In its previous MER, Germany was largely compliant with these requirements as there were no specific obligations to take measures to prevent the misuse of technological developments. Since then, R.15 has been amended significantly to include new requirements relating to virtual assets and virtual asset service providers.

**Criterion 15.1** – Germany has identified and assessed the ML/TF risks related to new technologies, products and services (NRA; BaFin’s sectoral risk assessment (SRA)). FIs are required to identify and assess the ML/TF risks associated with the business activities in which they engage, including new products and new business practices, new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products (GwG, s.5(1), Annex 2).

Criterion 15.2 – FIs are required to:

**(a)** Undertake and regularly update their risk assessments (GwG, s.5(2); BaFin Guidance on the GwG, pg.18), although it is not explicit that this must occur prior to the launch or use of such products, practices and technologies, and

**(b)** implement appropriate internal safeguards to manage and mitigate the ML/TF risks posed by new products and technologies (GwG, s.6(2)).

**Criterion 15.3** –

**(a)** Germany’s NRA includes a chapter on virtual assets which identified and assessed the general ML/TF risks (NRA, chpt.6). Risks related to virtual asset service providers (VASPs) are considered to a lesser extent in the NRA. BaFin’s *Subnational Risk Assessment* (SRA) generally does not look at each type of VASP as a separate sub-sector (with the exception of wallet providers), but assesses the risks of virtual assets as a product/service. The SRA provides a more detailed assessment than that of the NRA, although BaFin is still obtaining information on the scope and activities of FIs in this area. Virtual assets and VASPs are categorised as a high-risk sector and were a priority area for BaFin’s supervision in 2020 and 2021. Germany is in the process of completing a more comprehensive risk assessment for this sector, but this was not yet complete at the time of the on-site.

**(b)** Germany is applying a risk-based approach to measures to counter the misuse of virtual assets/VASPs for ML/TF to a large extent. BaFin considers the risks related to VASPs in its supervisory activity. Policy authorities are also considering risks associated with virtual assets in their approach to AML/CFT, although this approach is limited by a less nuanced understanding of risk and how these entities are misused. Measures are sometimes aimed at obtaining more information on this sector and responding to potential risks, rather than being fully risk-based.

**(c)** VASPs are subject to the same requirements as FIs to take appropriate steps to identify, assess, manage and mitigate their ML/TF risks as set out in c.1.10 and 1.11.

**Criterion 15.4** –

**(a)** VASPs in Germany are required to be licensed or registered as a financial services institution (KWG, s.32(1)). In 2020, Germany created a specific license for virtual asset custody businesses (wallet providers), which were previously exempt from

licensing requirements. The definition of a financial services institution captures institutions that:<sup>97</sup>

- i. provide exchange between “cryptoassets” and fiat currencies or between one of more forms of cryptoassets (KWG, ss.1(1a)1b, 1d, 4; 1(11)10);
- ii. institutions that transfer cryptoassets (KWG, ss.1(1a)4, 6; 1(11)10);
- iii. institutions that provide safekeeping and/or administration of cryptoassets or cryptographic keys which enable control over cryptoassets (KWG, s.1(1a)6); and
- iv. institutions that participate in and provide financial services related to an issuer’s offer and/or sale of a cryptoasset (KWG, ss.1(1a)1b, 1c, 1d, 4; 1(11)10).

The definition of “cryptoassets” is broad and aligns with the FATF definition of virtual assets (KWG, s.1(11)).

Like other financial services, licensing requirements apply to VASPs created, operating, or providing business or services in Germany, or targeting the German market (even if their office or residence is outside Germany) (KWG, s.32(1)1). This covers legal person VASPs created in Germany and natural person VASPs where their place of business is in Germany.

**(b)** VASPs are subject to fit and proper requirements under the KWG as set out in c.26.3.

**Criterion 15.5** – A specialised BaFin unit takes action to identify natural or legal persons that carry out unlicensed financial services, including VASP activities, and applies appropriate sanctions to them (KWG, s.32(1)). Unlicensed providers commit a criminal or administrative offence and are subject to appropriate sanctions upon conviction, including imprisonment of up to five years, monetary penalties of an unspecified amount, or cessation of business operations (KWG, ss.37(1), 54(1)). Monetary penalties can be applied to legal persons.

**Criterion 15.6** –

**(a)** BaFin supervises VASPs under the same systems for ensuring compliance with national AML/CFT requirements as other FIs (see R.26), meaning that VASPs are subject to AML/CFT regulation and risk-based supervision (GwG, ss.2(1), 50(1)(b), 51(1)). In 2020, BaFin identified cryptoassets as a priority area for supervisory engagement.

**(b)** BaFin has powers to supervise and ensure VASPs’ compliance with AML/CFT requirements (GwG, s.51(2)). These powers are the same as those available for FIs; see R.27.

**Criterion 15.7** – Guidance and feedback has been provided to FIs and applies equally to VASPs (see R.34), however, information specific to VASPs is somewhat limited particularly as it relates to AML/CFT obligations. BaFin has issued guidance on: licensing and authorisation requirements for cypto-token issuers; the definition of a crypto-custody business; and licensing applications for crypto-custody businesses. These do not go into detail on ML/TF issues. The FIU has issued a typology paper on

<sup>97</sup> BaFin “[Virtual Currency](#)” (December 2017)

red flags in virtual asset transactions (December 2020). BaFin has published the FATF *Guidance on Virtual Assets and VASPs* on its website,<sup>98</sup> and has a dedicated section on virtual currency on its website which includes contact forms for VASPs.<sup>99</sup> Direct feedback is given to VASPs during the registration and licensing process, as well as through annual audits and AML/CFT inspections. BaFin also works with the private sector using the Anti-Financial Crime Alliance (see R.2) to share information on risks among members; however, this information is not accessible to the industry writ large.

#### Criterion 15.8 –

(a) The sanctions available for FIs apply equally to VASPs (see c.35.1).

(b) These sanctions would generally apply equally to VASP’s directors and senior management, although there may be situations where this is not possible (see c.35.2).

**Criterion 15.9** – VASPs are subject to the requirements set out in R.10 to 21 in the same manner as for FIs, and are subject to the same minor deficiencies.

(a) For transactions outside a business relationship/occasional transactions, CDD must be conducted where the transaction is over EUR 1 000 (GwG, s.10(3)2(c)).

(b) Germany requires all FIs, including VASPs, to apply the obligations in the EU Money Transfer Regulation *mutatis mutandis* to all transfers involving virtual assets; see R.16. This includes the obligation to collect, store and transmit data for transfers between VASPs as well as for transfers that do not exclusively involve VASPs (Crypto Value Transfer Ordinance 2021, *Kryptowertetransferverordnung* (KryptoWTransferV), ss.3, 4). However, VASPs that were operating prior to the entry into force of this requirement are entitled to an exemption of up to two years where they notify BaFin that they are unable to fulfil their obligations (e.g., where it is not yet technically possible to obtain all required information) (KryptoWTransferV, s.5).

**Criterion 15.10** – Germany’s mechanisms for proactive communication/notification of new TFS listings and de-listings (specifically the Bundesbank circular) extend to VASPs, including newly-licensed virtual asset custody businesses (wallet providers). Deficiencies identified in c.6.5(d), 6.6(g), 7.2(d) and 7.4(d) (a lack of proactive communication for some FIs and DNFBPs) do not apply to VASPs.

**Criterion 15.11** – Germany has mechanisms in place to provide international cooperation (see R.40). BaFin is able to disseminate supervisory information internationally to relevant international or foreign authorities for AML/CFT purposes, including information on VASPs (GwG, s.54(3); see c.40.12-16).

### Weighting and Conclusion

There is a minor deficiency as it is not explicit that an FI’s update of its risk assessment must occur prior to the launch or use of new products, practices and technologies. On virtual assets and VASPs, Germany has a licensing and registration regime in place and as of 2020, all VASPs are subject to AML/CFT obligations. The NRA is somewhat

<sup>98</sup> BaFin “FATF Guidance – Virtual Assets and Virtual Asset Service Providers” (July 2019) ([www.bafin.de/SharedDocs/Downloads/EN/Bericht/dl\\_gw\\_fatf\\_guidance\\_virtual\\_asset\\_s\\_en.html](http://www.bafin.de/SharedDocs/Downloads/EN/Bericht/dl_gw_fatf_guidance_virtual_asset_s_en.html))

<sup>99</sup> BaFin “Virtual Currency” (December 2017) ([www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual\\_currency\\_artikel\\_en.html](http://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_artikel_en.html)).

limited in its assessment of VASPs, resulting in a less comprehensive understanding of risk at the national level. However, this is given less weight as BaFin's SRA provides a more detailed understanding of VASP and virtual asset risk. Guidance specific to VASPs is somewhat limited. VASPs are subject to the same AML/CFT obligations as FIs (including preventive measures, fit and proper requirements, sanctions, and TFS) and as a result are subject to some of the same minor deficiencies (namely on sanctions). For VASP-specific requirements, Germany has implemented the travel rule, but it is subject to a transitional period under which certain VASPs are exempt from its requirements.

**Recommendation 15 is rated largely compliant.**

### Recommendation 16 – Wire transfers

In its previous MER, Germany was compliant with these requirements. Since then, the EU has adopted new regulations relating to wire transfers that are directly applicable in Germany (EU Regulation 2015/847).

**Criterion 16.1** – FIs must ensure that cross-border wire transfers<sup>100</sup> over EUR 1 000 are accompanied by: **(a)** required and accurate<sup>101</sup> payer (originator) information (name, account number or, in the absence of an account, unique transaction reference, and address, document number, customer ID, or date and place of birth), and **(b)** required payee (beneficiary) information (name, account number or, in the absence of an account, unique transaction reference) (EU Regulation 2015/847, art.4).

**Criterion 16.2** – The requirements regarding batch files are consistent with the FATF requirements regarding originator and beneficiary information (EU Regulation 2015/847, art.6(1)).

**Criterion 16.3** – A *de minimis* threshold of EUR 1 000 applies to the application of requirements in c.16.1. The requirements for the originator and beneficiary information that must accompany all transfers below EUR 1 000 are consistent with the FATF Standards (EU Regulation 2015/847, art.6(2)).

**Criterion 16.4** – For transfers of less than EUR 1 000, originator information must be verified where there are reasonable grounds for suspecting ML/TF or the funds were received in cash or anonymous e-money (EU Regulation 2015/847, art.6(2)).

**Criteria 16.5 & 16.6**– For domestic wire transfers (which in this case includes intra-EU wire transfers), ordering FIs need only provide the payment account numbers (or unique transaction identifiers) when executing the transfer. If requested by the beneficiary, the ordering FI must be able to provide complete information on the originator and the beneficiary within three working days, which is consistent with the second part of criterion 16.5 and criterion 16.6. FIs are obliged to respond fully and without delay to requests from authorities on originator and beneficiary information, including by means of a central contact point (EU Regulation 2015/847, arts.5, 14). LEAs may also compel such information from FIs by way of a production order (see R.31). BaFin requires the appointment of a central contact point in cases where the criteria of Commission Delegated Regulation (EU) 2018/1108 (art.3) are met (ZAG, s.41(1)).

<sup>100</sup> Wire transfers taking place entirely within the borders of the EU are covered under c.16.5 pursuant to footnote 41 in the 2013 FATF Methodology.

<sup>101</sup> Originator information has to be verified (EU Regulation 2015/847, art.4).

**Criterion 16.7** – The ordering and beneficiary FIs are required to retain information on the originator and beneficiary for five years (EU Regulation 2015/847, art.16(1)).

**Criterion 16.8** – The ordering FI is not allowed to execute the wire transfer if it does not comply with the requirements set out in c.16.1-16.7 (EU Regulation 2015/847, art.4(6)).

**Criterion 16.9** – An intermediary FI must retain, with the cross-border wire transfer, all accompanying originator and beneficiary information (EU Regulation 2015/847, art.10).

**Criterion 16.10 – (N/A)** Technical limitations cannot be used to justify non-compliance with c.16.9. Accordingly, this criterion is not applicable.

**Criterion 16.11 and 16.12** – Intermediary FIs are required to take measures to identify wire transfers missing required information and to have risk-based policies and procedures for determining (a) when to execute, reject, or suspend such wire transfers and (b) the appropriate follow-up action (EU Regulation 2015/847, arts.11, 12).

**Criterion 16.13** – Beneficiary FIs are required to detect whether any required information on the originator or beneficiary is missing (EU Regulation 2015/847, art.7).

**Criterion 16.14** – For cross-border wire transfers of over EUR 1 000, the beneficiary FI is required to verify the identity of the beneficiary and maintain this information for five years (EU Regulation 2015/847, arts.7(3), 16(1)).

**Criterion 16.15** – Beneficiary FIs are required to have risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking the required originator or required beneficiary information; and (b) the appropriate follow-up action (EU Regulation 2015/847, art.8).

**Criterion 16.16** – The obligations listed above also apply to MVTS providers and their agents (EU Regulation 2015/847, arts.2(1), 3(5)).

**Criterion 16.17** – In cases where a MVTS provider controls both sides of a wire transfer:

**(a)** The MVTS provider must, as a payee (beneficiary) or intermediary institution, take into account information from both sides as a factor when assessing whether an STR has to be filed (EU Regulation 2015/847, arts.9, 13).

**(b)** While there is no explicit requirement for the MVTS provider to file an STR in any country affected by the transaction, taking into account 16.17(a) and the permissions for intra-group sharing of STR data (GwG, ss.47(2); see c.18.2(b)), MVTS providers are obliged to report in the countries of the ordering and beneficiary sides of the transaction (GwG, ss.43(1), (3)). In addition, relevant to EU passporting, compliance officers are required to file an STR with the FIU of the EU member state in whose territory the MVTS provider is established, i.e., the MVTS provider's headquarters (EU Directive 2015/849 and amendments, art.33; GwG, s.43(3)).

**Criterion 16.18** – FIs are subject to the requirements of the EU regulations which give effect to UNSCR 1267, 1373 and successor resolutions (see R.6).

### *Weighting and Conclusion*

All criteria are met. **Recommendation16 is rated compliant**

## Recommendation 17 – Reliance on third parties

In its previous MER, Germany was largely compliant with these requirements as there was no national assessment of the suitability of the specified institutions and professions which may act as introducers.

**Criterion 17.1** – FIs are permitted to rely on third-parties to perform elements of CDD (identification of customer, identification of beneficial owner, understanding nature of the business, establishing whether the customer or beneficial owner is a PEP) (GwG, s.17(1)). The ultimate responsibility for CDD remains with the FI relying on the third party (GwG, s.17(1)3).

**(a)** FIs must ensure that third-parties transmit the relevant CDD information to the FI directly and immediately (GwG, s.17(3); BGB, s.121(1)).

**(b)** FIs must take appropriate steps to ensure that copies of identification and verification information is made available from the third-party upon request without delay (GwG, s.17(3)), and

**(c)** Third-parties must be subject to Germany’s AML/CFT requirements, in another EU jurisdiction subject to the EU Regulation 2015/847, or subject to equivalent CDD and record-keeping requirements and supervised in a manner consistent with EU Regulation 2015/847 (GwG, s.17(1)). However, there is no specific requirement that the obliged entity must satisfy itself that the third party is regulated, supervised, and has measures in place for compliance with R.10 and 11, nor is there clear guidance on this.

**Criterion 17.2** – FIs are prohibited from engaging third-parties that are established in a high-risk “third country”, i.e., a country outside the EU (GwG, ss.17(2), 1(17)). This prohibition does not apply to EU member states or a third-party that is a branch or majority-owned subsidiary of an EU FI with group-wide AML/CFT policies and procedures (GwG, s.17(2)). Reliance on third-parties that are established in an EU Member State is not based on an assessment of the level of country risk, and reflects a presumption that all EU member states implement harmonised AML/CFT provisions.

**Criterion 17.3** – A FI can rely on a third-party introducer which is part of the same financial group for (a)-(c) of the CDD measures set out in R.10 if the following conditions exist (GwG, s.17(4)):

**(a)** the financial group applies CDD and record-keeping requirements and its AML/CFT policies and procedures are consistent with EU Regulation 2015/847 or equivalent provisions (which are largely in line with R.10-12 and 18),

**(b)** the financial group is supervised for compliance with AML/CFT requirements at a group-level by a home or host supervisor, and

**(c)** Group-wide AML/CFT measures, including internal safeguards, are based on risk analysis (GwG, s.9(1)). However, there is no explicit requirement that the risk analysis considers EU member states’ country risk.

The assumption that all EU countries apply adequate AML/CFT controls in other recommendations has an impact on the application of this criterion.

### Weighting and Conclusion

While there are measures in place for the use of third-parties, there are deficiencies stemming from the general assumption that all EU member states apply adequate AML/CFT controls. There are no explicit requirements that FIs must satisfy itself that third parties in EU member states are regulated, supervised, and have adequate CDD and record-keeping measures in place.

**Recommendation 17 is rated largely compliant.**

### Recommendation 18 – Internal controls and foreign branches and subsidiaries

In the last MER, Germany was partly compliant with the requirements on internal controls. Compliance officers were not required by all insurance intermediaries, and did not have full access to CDD information. There were no obligations on staff training or hiring procedures. In the last MER, Germany was largely compliant with requirements regarding foreign branches and subsidiaries as measures did not sufficiently extend to branches and subsidiaries in the EEA.

**Criterion 18.1** – FIs are required to have in place effective ML/TF risk management systems, appropriate to their ML/TF risks and the nature and size of their business (GwG, ss.4(1), (2)). These systems must include the following internal policies, procedures and controls:

- (a) appointing a compliance officer and deputy at management level (GwG, ss.6(2) and 7)
- (b) screening procedures to ensure high employee standards, including when hiring (GwG, s.6(2); BaFin Guidance on the GwG, section 3.5)
- (c) an ongoing employee training programme (GwG, s.6(2))
- (d) an independent audit, where appropriate given the nature and size of the business (GwG, s.6(2)). Such audits are required for most FIs, regardless of their size or the nature of their business, with the exception of some insurance intermediaries (KWG, s.25a(1); VAG, s.30(1); KAGB, s.28(1); ZAG, s.24(1)).

**Criterion 18.2** – Financial groups are required to implement group-wide AML/CFT programmes, which must be applicable and appropriate to all branches and majority-owned subsidiaries of the financial group (GwG, s.9(1)). These should include the measures set out in c.18.1 (GwG, s.9(1)).

(a) Programmes must also include procedures for sharing information within the group (via a group-level AML Officer) to prevent ML/TF (GwG, s.9(1)). This obligation is broad enough to cover the sharing of information for the purposes of CDD and ML/TF risk management. This broad interpretation is highlighted in non-binding guidance (BaFin Guidance on the GwG, pg.90).

(b) Programmes must also cover the provision, to the group-level AML Officer, of necessary information, which includes customer, account and transaction information, information on envisaged or submitted STRs, and information concerning contact with supervisors or other competent authorities (GwG, s.9(1); BaFin Guidance on the GwG, pg.90). The group AML Officer is to use this information for group-wide risk management (BaFin Guidance on the GwG, pg.90). This includes sharing information within the group and providing information to branches and

subsidiaries where appropriate for risk management (GwG, s.9(1); BaFin Guidance on the GwG, pg.89).

**(c)** Programmes must include coherent internal controls and safeguards for the protection of personal data; these requirements are broad and cover safeguards for other confidentiality purposes and to prevent tipping-off (GwG, ss.9(1)4, 6(2), 9(1)1).

**Criterion 18.3** – FIs are required to ensure that their foreign branches and majority-owned subsidiaries comply with Germany’s AML/CFT requirements where the minimum requirements of the host country are less strict than those of the GwG. If the host country does not permit implementation of the GwG requirements, the FI must (a) ensure that the relevant branch or subsidiary takes appropriate measures to manage the ML/TF risks and (b) inform their home supervisor (GwG, s.9(3)).

### *Weighting and Conclusion*

FIs are required to develop and implement programmes against ML/TF and are required to implement internal policies at the group level, including on data protection and information sharing within the group. However, it is not clear that an independent audit function is obligatory for some insurance intermediaries.

**Recommendation 18 is rated largely compliant.**

### **Recommendation 19 – Higher-risk countries**

In its previous MER, Germany was rated partly compliant with these requirements as there were no explicit obligation to pay special attention to relationships and transactions involving countries with inadequate AML/CFT standards.

**Criterion 19.1** – FIs are required to apply enhanced due diligence to business relationships and transactions with natural and legal persons (including FIs) from a “high-risk third country identified by the European Commission” (EC) (GwG, s.15(3); EU Directive 2015/849, art.9(2) as amended by EU Directive 2018/843, art.1(5)). When identifying countries, the EC is required to take into account relevant evaluations by international organisations in relation to the ML/TF risks posed by non-EU countries, and this has included adopting the FATF public statement. In addition, each supervisor has the power to require entities under its supervision to conduct enhanced due diligence for other high-risk countries based on evaluations, reports or assessments from national or international agencies (GwG, s.15(8)). This section is explicitly intended to allow Germany to require enhanced due diligence for EEA countries designated as high-risk by the FATF or for any country designated by the FATF but not included on the EC list (Explanatory Note to GwG). The BMF also has the power to issue statutory ordinances which would require all FIs and DNFBPs to conduct enhanced due diligence in certain cases where there is a higher ML/TF risk, including based on the country involved (GwG, s.15(10)1).

**Criterion 19.2** – Supervisors have the power to order the application of countermeasures proportionate to the risks for high-risk countries identified by the EC (GwG, s.15(5a)), or for other countries where there are facts, evaluations, reports, or assessments that justify doing so (GwG, s.15(8)).

**Criterion 19.3** – BaFin and the FIU regularly publish information on their websites on the status of jurisdictions listed by the FATF and the EC. Obligated entities that subscribe to the BaFin newsletter are informed about all new publications on the website of BaFin on a regular basis.

### *Weighting and Conclusion*

All criteria are met.

**Recommendation 19 is rated compliant.**

### **Recommendation 20 – Reporting of suspicious transaction**

In its previous MER, Germany was partly compliant with these requirements as a result of the following technical deficiencies: the scope of the reporting obligation related only to ML and did not cover all predicate offences; deficiencies in the TF offence limited reporting; and the threshold for reporting was high. Since then, reporting requirements have been updated.

**Criterion 20.1** – FIs are required to make a STR to the FIU without delay if there are reasonable ground to suspect that funds originate from a criminal offence, or are related to TF (GwG, s.43(1); Explanatory Note to the GwG; this is also emphasised in non-binding guidance: BaFin Guidance on the GwG, pgs.78, 80; Guidance for other DNFBPs (which applies to insurance intermediaries), pg.2).

**Criterion 20.2** – FIs are required to report all suspicious transactions, including attempted transactions (GwG, s.43(1); Bundestag printed paper no. 18/11555, pgs.122-123; this is also emphasised in non-binding guidance: BMF guidance on the interpretation of suspicious transaction reporting; BaFin Guidance on the GwG, pg.78; Guidance for casinos (pg.54)).

### *Weighting and Conclusion*

All criteria are met.

**Recommendation 20 is rated compliant.**

### **Recommendation 21 – Tipping-off and confidentiality**

In its previous MER, Germany was largely compliant with these requirements on the basis that the tipping-off provision applied only to reports that have already been filed.

**Criterion 21.1** – Any person who makes a STR is exempt from criminal and civil liability for breach of any restriction on disclosure of information provided the STR was not made maliciously or with gross negligence (GwG, s.48(1)). This applies to legal and natural persons, including FIs, directors and employees (including where employees report internally to a superior or in-house body) (Explanatory Note to GwG; GwG, s.48(2)1).

**Criterion 21.2** – FIs must not disclose the fact that an STR is being or has been filed, an investigation has been launched, or a demand for information has been made (GwG, s.47(1)). This includes where the STR has not yet been filed. Corresponding sanctions are available for natural persons, including directors and employees (GwG, s.56(2)). Reasonable exceptions to this prohibition ensure it does not interfere with information-sharing within a financial group, between EEA institutions, or intra-group as contemplated by R.18 (GwG, s.47(2)).

### *Weighting and Conclusion*

All criteria are met. **Recommendation 21 is rated compliant.**

## Recommendation 22 – DNFBPs: Customer due diligence

In its previous MER, Germany was rated not compliant with these requirements on the basis of the following deficiencies: no arrangements for casinos to link identification-on-entry data to individual transactions within the casino; registered legal advisors that are not subject to professional secrecy were included in the carve-out for legal and professional privilege; and no requirements to identify PEPs, or consider filing a STR where CDD cannot be completed, or to establish beneficial ownership.

**Criterion 22.1** – The CDD requirements set out in R.10 are required to be applied in the following situations (and are subject to the same technical deficiencies noted in R.10):

**(a)** Casinos<sup>102</sup> – when customers win or bet amounts equal to or above EUR 2 000, including in linked transactions (GwG, ss.1(5), 2(1)15, 10(1), 10(5)). This is more stringent than the EUR 3 000 threshold in the Standards. Customer identification may be conducted upon entry to the casino premises, provided the casino can attribute each transaction to the particular customer (GwG, s.10(5)). Casinos are required to ensure that they are able to link CDD information for a particular customer to the transactions that the customer conducts. These requirements apply equally to ship-based casinos.<sup>103</sup> Online casinos are subject to stricter measures and must undertake CDD irrespective of the amount involved in the transaction (GwG, s.16).

**(b)** Real estate agents<sup>104</sup> – when they are involved in the purchase of property (GwG, ss.1(11), 2(1)14, 10(1), 10(6)). CDD requirements must be fulfilled for both parties to the transaction (i.e., buyer and seller) as soon as a “serious interest” is expressed in a purchase contract is expressed, and the contracting parties are determined (GwG, s.11(2)).

**(c)** Dealers in goods, including precious metals and stones – when engaging in (i) any cash transaction of EUR 10 000 or more, including linked transactions, (ii) cash transactions of EUR 2 000 or more relating to high-value goods<sup>105</sup> (GwG, ss.1(5), 1(9), 1(10), 2(1)16, 10(1), 10(6a)). These requirements are more stringent than the threshold and scope of the FATF standards.

**(d)** Lawyers, notaries, and legal advisors (the legal profession) – when they prepare for, or carry out, transactions for a client concerning: buying and selling of real estate or business entities; managing money, securities or other assets; opening or managing bank, savings or securities accounts; organising contributions for the creation, operation or management of companies; creating, operating or managing

<sup>102</sup> Germany also goes beyond the FATF requirements to extend AML/CFT obligations to most organisers and brokers of games of chance, including, e.g., online lotteries and sports betting.

<sup>103</sup> Ship-based casinos are permitted in only two of Germany's *Länder* (Schleswig-Holstein and Mecklenburg-Western Pomerania) and can operate only as a branch of a terrestrial casino. [As at March 2021], there were no ship-based casinos licensed to operate by either *Länder*.

<sup>104</sup> Germany also goes beyond the FATF requirements to extend AML/CFT obligations to real estate agents involved in high-value leasing.

<sup>105</sup> High-value goods are goods that, on account of their quality, value, or intended use, stand out from articles of daily use, or on account of their price, do not constitute daily purchases. This includes precious metals and stones, jewellery and watches, art, motor vehicles, ships and aircraft (GwG, s.1(10)).

legal persons or arrangements (GwG, ss.2(1)10, 10(1)). The legal profession is not required to comply with c.10.19 where they are providing legal advice or representation (in line with legal professional privilege), unless they are aware that the advice is being used deliberately for ML/TF (GwG, s.10(9)).

Germany applies CDD requirements to all accountants, regardless of the nature of the transaction or relationship (GwG, s.2(1)12).

**(e)** Trust and company service providers, that are not already covered as lawyers, accountants or tax advisors – when they prepare for or carry out transactions for a client concerning: the formation of a legal person or partnership; acting or arranging another person to act as a director, manager or partner; providing a registered office, business administrative or correspondence address or related service for a legal person, partnership or arrangement; acting or arranging another person to act as a trustee of a legal arrangement; or acting or arranging another person to act as a nominee shareholder (GwG, s.2(1)13).

**Criterion 22.2** – DNFBPs are required to comply with the same record-keeping requirements as FIs under the GwG – see analysis of R.11.

**Criterion 22.3** – DNFBPs are required to comply with the same PEPs requirements as FIs under the GwG and are subject to the same deficiencies – see analysis of R.12.

**Criterion 22.4** – DNFBPs are required to comply with the same new technologies requirements as FIs under the GwG and are subject to the same deficiencies– see analysis of R.15.

**Criterion 22.5** – DNFBPs are required to comply with the same third-party reliance requirements as FIs under the GwG and are subject to the same deficiencies – see analysis of R.17.

### *Weighting and Conclusion*

DNFBPs are subject to the same CDD requirements as FIs, as set out in R.10. Minor deficiencies identified in R.12, 15 and 17 apply equally to DNFBPs and impact the rating.

**Recommendation 22 is rated as largely compliant.**

### **Recommendation 23 – DNFBPs: Other measures**

In its previous MER, Germany was not compliant with these requirements. While the legislation applicable to DNFBPs at that time imposed requirements similar to those for FIs, the previous report highlights a range of exemptions and limitations resulting in technical deficiencies, as well as a number of effectiveness issues now covered under IO.4.

**Criterion 23.1** – DNFBPs are subject to the same STR requirements as FIs (as set out in R.20), subject to the following qualifications:

**(a)** Lawyers, notaries, other independent legal professionals – when they are involved in the activities listed in c.22.1(d) (GwG, s.2(1)10). The legal profession is exempt from making STRs where the reportable matter related to information received in the course of legal advice or representation, unless they are aware that the advice is being used deliberately for ML/TF or where rules-based reporting obligations occur (only in specific situations relating to real estate transactions) (GwG, s.43(2); *GwGMeldV-Immobilien*, 2020 Ordinance on Real Estate Reporting under the GwG). Germany has

narrowed the scope of this exemption since its previous MER, and the exemption as set out in law aligns with Germany's concept of legal professional privilege (statement of grounds given with the GwG amendment: BT-Drs.19/13827, pg.98; GwG Interpretation Guidance for Lawyers (pgs.36-37); for Notaries (pgs.39-42)). The requirements on STR reporting apply to accountants in the same manner as for FIs (see R.20).

**(b)** Dealers in goods, including precious metals and stones, are subject to the same STR reporting requirements as FIs (GwG, s.43(1); see R.20). Relevant thresholds (see c.22.1(c)) apply only to CDD requirements, risk management and internal controls.

**(c)** Trust and company service providers, that are not already covered as lawyers or accountants – when they provide any of the activities listed in c.22.1(e) (GwG, s.2(1)13).

**Criterion 23.2** – DNFBPs are required to comply with the same internal control requirements and group-wide measures as FIs in the situations set out in c.23.1 – see analysis of R.18.<sup>106</sup> For traders in goods, these requirements must be in place if the trader undertakes any transaction meeting the relevant threshold: (i) a cash transaction of EUR 10 000 or more, (ii) a cash transaction of EUR 2 000 or more relating to high-value goods,<sup>107</sup> or (iii) an art transaction of EUR 10 000 or more (GwG, s.4(5)).

**Criterion 23.3** – DNFBPs are required to comply with the same higher-risk countries requirements as FIs – see analysis of R.19.

**Criterion 23.4** – DNFBPs are required to comply with the same tipping-off and confidentiality requirements as FIs – see analysis of R.21.

### *Weighting and Conclusion*

All criteria are met.

**Recommendation 23 is rated compliant.**

### **Recommendation 24 – Transparency and beneficial ownership of legal persons**

In its previous MER, Germany was non-compliant with these requirements as there were no mechanisms to ensure timely access to information on the control and beneficial ownership (BO) of legal entities except for publicly listed stock companies and issues related to bearer shares.

Foundations, cooperatives and associations are considered a sub-set of corporations but are subject to different legal, regulatory and reporting requirements than other commercial corporations.

<sup>106</sup> The deficiency identified in R.18 relates to obligations on payment service providers and e-money institutions, and is not relevant for DNFBPs.

<sup>107</sup> High-value goods are goods that, on account of their quality, value, or intended use, stand out from articles of daily use, or on account of their price, do not constitute daily purchases. This includes precious metals and stones, jewellery and watches, art, motor vehicles, ships and aircraft (GwG, s.1(10)).

**Criterion 24.1** – Germany has measures in place to identify and describe the different types, forms and basic features of legal persons. Information on how to obtain basic and beneficial ownership information is also publicly available.

Information on how to form legal persons (both corporations and partnerships) is publicly available on the websites of the Federal Ministry for Economic Affairs and Climate Action (BMWK) and on the websites of the Chambers of Industry and Commerce at the *Länder*-level.<sup>108</sup> In addition, the website of the [Federal Ministry of Justice](#) (BMJ) and websites of state ministries of justice provides information on associations. The website of the [Association of German Foundations](#) contains comprehensive information on creation and features of foundations. Basic information on foundations can also be found on the BMWK website. Information set out in German legislation on all legal persons is available online in German and in all the languages of the European Union.<sup>109</sup>

Information is available online on how to obtain basic and beneficial ownership information and obligations for recording this information can be found through the website [Common Register Portal of the German Federal States](#), the website for the [Transparency Register](#) (*Transparenzregister*), and [the website of the company register](#) (*Unternehmensregister*).

**Criterion 24.2** – Germany has completed a sectoral risk assessment of legal persons and legal arrangements. However, it is not clear if all relevant data has been consulted and the focus is on risks emanating from foreign jurisdictions rather than analysis on how this impacts the risks associated with legal persons in Germany.

**Criterion 24.3** – Germany has a complex system of registers with multiple registers used to capture basic information on different legal persons with information held by different *Länder* and federal authorities. However, partnerships which are small businesses (*Kleingewerbetreibende*), civil law partnerships, and foundations are not required to register on one of the public registries. There are also gaps in the information required to be collected on the register of foundations.

#### *System of registers*

Germany has consolidated information contained on multiple registries into the Company Register ([Unternehmensregister](#)) and the Common Register Portal of the German Federal States ([Gemeinsames Registerportal der Länder](#)) which is also referred to as the Commercial Register Portal ([Handelsregisterportal](#)). The public can access information from the following registers through these two portals:

- The Commercial Register (*Handelsregister*) for limited liability companies (GmbH and UG), stock corporations (AG), European stock corporations (SEs), commercial partnerships under the commercial code (oHG) and limited commercial partnerships (KG) and partnerships limited by shares (*Kommanditgesellschaft auf Aktien* (KGaA))
- Register of Cooperatives (*Genossenschaftsregister*) for cooperatives and European cooperatives, and

<sup>108</sup> See: [www.existenzgruender.de/DE/Gruendung-vorbereiten/Rechtsformen/Auf-einen-Blick/inhalt.html](http://www.existenzgruender.de/DE/Gruendung-vorbereiten/Rechtsformen/Auf-einen-Blick/inhalt.html); for the *Länder*, see for example, Berlin: <https://www.ihk-berlin.de/service-und-beratung/recht-und-steuern/firma-und-rechtsformen/rechtsformen-3433304>.

<sup>109</sup> German legislation is available at [www.gesetze-im-internet.de](http://www.gesetze-im-internet.de) and in other EU languages at [www.gesetze-im-internet.de/Teilliste\\_translations.html](http://www.gesetze-im-internet.de/Teilliste_translations.html)

- Partnerships Register (*Partnerschaftsregister*) for partnership companies (PartG).

For Associations, there is a separate Register of Associations (*Vereinsregister*) which can be accessed through the Common Register Portal of German Federated States but not through the Company Register.

Foundations are not required to register on a public registry but information on the name, legal status, purpose of the foundation and address of the foundation are kept on a public directory by the *Länder* authorities responsible for supervising foundations (BGB, s.80). This information can be accessed by the public through the Transparency Register and through the *Länder* authorities but methods of accessing information held by different *Länder* can vary.

While there are numerous registers, civil law partnerships (GbRs) are not required to register on any register which is a gap in Germany's system noting that these entities can be particularly susceptible to ML.

#### *Basic information available on the registers*

Commercial trading companies are required to register the following basic information on the Commercial Register: name of company/legal person, proof of incorporation, legal form and status, address, and list of directors (Limited Liability Companies Act, *Gesetz betreffend die Gesellschaften mit beschränkter Haftung* (GmbHG) ss.8, 10; Stock Corporation Act, *Aktiengesetz* (AktG) s.39; Commercial Code, *Handelsgesetzbuch*, ss.106, 162).

For partnerships, information held on the Partnership Register includes the name and address of the partnership, list of partners, basic information on the nature of the partnership and the powers of representation of the different partners (Partnership Register Regulation, *Partnerschaftsregisterverordnung*, s.5). However, there are no registration requirements for civil law partnerships (GbRs).

Associations must register information on the name of the association, registered office, list of management board members and their powers of representation on the Register of Associations (Civil Code, *Bürgerliches Gesetzbuch* (BGB) s.64).

The Register of Cooperatives contains information on the name of the cooperative, place of business, name of management board members, names of holders of general commercial powers of attorney and representation requirements (GenRegV, ss.15. 26).

Foundations, are not required to register and while some basic information is captured on a public directory as outlined above, it appears that information on basic regulating powers and directors of the foundation are not required to be captured.

**Criterion 24.4** – Information held on the registries and additional information on shareholders, shareholdings and members are required for most legal persons. However, it is not clear what information needs to be held by small businesses and partnerships not required to be registered under German law (see c.24.3).

Limited liability companies must provide a list of shareholders, when registering on the Commercial Register (GmbHG, s.8(1) no. 3) and inform the register when there is a change in shareholdings (GmbHG, s.40(1)). Information on share classes and rights and obligations associated with each shareholding is included in the articles of association which are also kept at the Register. Companies are not required to retain these records separately and the records on the Commercial Register are considered

definitive. Stock corporations are required to maintain a share register (AktG, s.67) of registered shares. Stock corporations which issue different classes of shares must register this information, which is also contained in the articles of association, in the Commercial Register (AktG, ss.11, 12, 23 (3) no.4). As with limited liability companies, records on the Commercial Register are considered definitive.

Some types of partnership companies (oHG, KG and KGaA) are also required to register on the Commercial Register, or in the case of partnership companies for freelancers (PartG) in the Partnership Register, and maintain the same information as limited corporations or stock corporations depending on the legal form of the partnership. However, it is not clear what type of information must be held by other types of partnerships not required to register on the Commercial Register (PartG). Civil law partnerships (GbR) are currently not required to register or maintain any information.

Cooperatives are required to keep a detailed list of members (Cooperatives Act, *Genossenschaftsgesetz* (GenG), s.32). Members of the general public with a legitimate interest may request a list of members directly from the cooperative. In the event that a cooperative refuses to grant access even though a legitimate interest exists, courts may enforce the right to access.

Some information on associations is available to the public through the Register of Associations. Information on the management board of the association must be entered on the Register of Associations (BGB, s.64). However, there is no requirement to maintain a list of members of an association.

**Criterion 24.5** – In general, Germany requires legal persons to update the relevant registers and fines apply for non-compliance, but it is not clear that these requirements ensure that information is updated on a timely basis. The accuracy of information is ensured through the involvement of a notary in registering legal persons on the various registers. There are no provisions in place for non-company partnerships.

Germany has established legal obligations on limited liability companies and stock corporations registered on the Commercial Register to keep the information on the Register accurate and up to date (AktG, ss.67, 81; GmbHG, s.39). Courts of registration can issue fines of up to EUR 5 000 for failing to submit documents to the Commercial Register (Commercial Code, s.14). However, there is no clear time period in which changes must be reviewed and updated.

For cooperatives, changes in the identity of a director or in director powers of representation must be updated in the Register of Cooperatives (GenG, s.28). The management board of a cooperative is required to keep a list of members. Any change concerning the board of directors or other authorised representatives has to be submitted for entry in the cooperatives register without undue delay (GenRegV, s.18).

Associations are obliged to update information filed with the Register of Associations on the composition of the board and articles of association (BGB, ss.67, 71). Failing to update information in the Register on the changes in the board can result in coercive fines being issued by the court (BGB, s.78). Courts, public prosecution authorities, police, municipality authorities, notaries and finance authorities (i.e. federal and *Land* tax and revenue collection agencies) are also under an obligation to notify the courts of incorrect, incomplete or omitted registrations to the Commercial Register and Register of Associations (Act on the Procedure in Family Matters and in Matters of

Non-contentious Jurisdiction, *Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit* (FamFG), s.379).

Foundations are required to regularly notify the public authorities that maintain the directory or the foundation supervisory authority of changes to entries in the *Länder* directories up to date (e.g., Berlin Foundation Law, *Stiftungsgesetz Berlin*, s.8(1); Foundation Law for Baden-Württemberg, *Stiftungsgesetz für Baden-Württemberg*, s.9).

**Criterion 24.6** – Germany uses a combination of the registry and existing information approaches to obtain and determine the beneficial ownership of legal persons. However, the approach taken does not cover all legal persons as non-registered partnerships (that is partnerships which are not partnership companies) are not required to record, retain or collect BO information.

Legal persons are required to collect, record and retain BO information and enter relevant information in the Transparency Register (GwG, s.19, 20). Relevant information includes the name, date of birth, place of residence, type and scope of interests held by beneficial owners collected as part of customer due diligence (see also R.10). In addition, there is a legal obligation on beneficial owners and shareholders to provide their information to legal entities and partnerships (GwG, ss.20(3), 20(4)). However, these obligations do not extend to cover partnerships except for partnership companies that are required to register on the Commercial Register or the Partnership Register.

BO information is available via the Transparency Register website which complements the information held on other Registers. Legal persons are required to collect, record, maintain and actively notify the Transparency Register of changes and updates to BO information (GwG, ss.20(3)-(4)).

BaFin and other competent authorities are also able to access the Electronic Account Retrieval System in Germany with credit institutions which also contains BO information in relation to those accounts (KWG, s.24c).

**Criterion 24.7** – There are requirements in place for legal persons, obliged entities and competent authorities (including law enforcement, supervisors and other public authorities) to provide and/or keep BO information accurate and up-to-date. However, there is no specific guidance on when information BO information must be updated and verification of information on the registers is done on an ad hoc basis rather than in a systematic manner meaning that it is likely not all of the BO information recorded is as accurate and up-to-date as possible.

Legal persons who are obliged entities are required to keep BO information on their customers up-to-date (GwG, s.10) and update the relevant registers (GwG, s.20(1)). Beneficial owners and shareholders are obliged to notify legal entities of changes to information to enable them to fulfil these obligations without undue delay (GwG, ss.20(3), 20(3a), 20(4)). Obligated entities are also required to keep customer BO information up-to-date under ongoing CDD requirements which is another method for updating information on German legal entities with a bank account in Germany (see c.10.7). However, while there is a general obligation for information to be obtained and relevant registers to be updated without undue delay there is limited guidance on what time frame would be considered to be without delay.

All obliged entities and legal persons are required to cooperate to provide complete and accurate information for the Transparency Register (GwG, ss.19(3), 20(1), 21(1)).

Missing, late or incorrect entries are subject to fines (GwG, s.56 – see c.24.13). If an entry on the relevant register is unclear, the office maintaining the register may contact the legal entity for clarification (GwG, s.18(3)).

With respect to the Transparency Register, the office maintaining the Register (*Bundesanzeiger Verlag*) checks updates to the register to see if the information is incomplete, unclear, or if there is any doubt about the information provided (GwG, s.18(3)). FIs and DNFBPs are also required to report discrepancies in beneficial ownership information (GwG, s.23(a)).

The failure to report the correct beneficial ownership information in a timely manner and to report changes regarding the beneficial owner is an administrative offence which can incur an administrative fine up to a maximum of EUR 150 000. In case of serious, repeated, or systemic violations, a fine of up to EUR 1 000 000 – or twice the amount of the financial benefit – can be applied. All legal persons are obliged to respond to queries, and a non-answer of those queries is an administrative offence and can incur an administrative fine up to a maximum of EUR 5 000 000 or 10% of the total revenues of the legal entity (GwG, s.56(3)).

**Criterion 24.8** – Companies are required to provide information to competent authorities in determining the beneficial owner however there are no specific measures in place to ensure that there is a natural person or a representative DNFBP in Germany that can provide this information.

Obligated entities are subject to a general obligation to cooperate with supervisory authorities to provide information and documents. This broad obligation extends to cooperation with supervisory authorities (GwG, s.52(1)).

Legal persons who are obliged to provide information to the Transparency Register also have a duty to cooperate to ensure the accuracy and completeness of information on the Transparency Register (GwG, ss,18(3), 20(1), 21(1)).

(a) There is no specific obligation for legal persons to have a natural person in Germany to assist competent authorities with accessing basic and beneficial ownership information.

(b) Board members and employees of obliged entities are required to cooperate with supervisory authorities (GwG, s.52(1)) and provide information and surrender documents including information on beneficial ownership.

**Criterion 24.9** – While there are record keeping requirements for limited liability companies, stock corporations, cooperatives, foundations and obliged entities who service legal persons; there are limited record keeping requirements for associations. In line with R.11, FIs and DNFBPs are subject to comprehensive record keeping obligations and must retain records for five years from the year in which a business relationship is terminated (GwG, s.8(4)).

The records of limited liability companies, stock corporations and cooperatives must be maintained for a period of ten years after the dissolution of the company (GmbHG, s.74(2), AktG, s.273(2), GenG, s.93).

Associations are required to keep some limited records of basic information (appointment of the board, articles of association) and are required to have these records available for the financial auditing purposes but there is no legal provision on how long these records must be kept for or that they must be kept for any period of time after the association has been dissolved (BGB, ss. 27, 666).

There are no specific record keeping requirements for associations or partnerships with respect to beneficial ownership.

The requirements for foundations are at the *Länder*-level. The foundation authority may obtain information regarding individual matters pertaining to the foundation and the foundation is obliged to provide information and submit documents. The foundations records are generally retained for a period of at least ten years after the foundation ceases to exist but the exact requirements vary between *Länder* (for example, Foundation Law of North Rhine Westphalia, *Stiftungsgesetz*, (NRW), s.7 and Foundation Law of the Land of Bavaria, *Bayerisches Stiftungsgesetz*, s.16).

**Criterion 24.10** – Competent authorities have a range of powers to obtain basic and beneficial ownership information in a generally timely manner. However, law enforcement agencies do not have direct access to the Central Database of Accounts, which makes retrieval of this information less timely.

Basic information on the Commercial Register, Register of Cooperatives, Register of Associations and Register of Partnerships is publicly available and can be accessed online by the general public and all competent authorities.

Public prosecutors have a general power to request information, conduct searches and examinations (StPO, ss.102, 103, 161(1) 161a), including on legal persons and obliged entities, in order to obtain basic and BO information in a timely manner (see R.31).

Supervisory authorities, the FIU, and law enforcement agencies also have full access to the BO information in the Transparency Register (GwG, ss.20(5), 23(1)). Furthermore, BaFin, the Federal Central Tax Office (BZSt), the Customs Investigations Service, the Illicit Employment Monitoring Authority and the FIU have access to a central database of accounts run by credit institutions which also contains beneficial ownership information in relation to those accounts (KWG, s.24c). With regards to the beneficial owner, banks are required to make the name, and if available, the address of the beneficial owner of the account available on the Central Database of Accounts (KWG s.24c(1)).

**Criterion 24.11** – Bearer shares and bearer share warrants are allowed under German law. The shares are to be issued as shares registered in the names of their holders.

Stock corporations which are not publicly listed can only issue bearer shares as a global certificate, which uniformly certifies the rights of several shareholders and guarantees that the administration is able to obtain sufficient and current information about the identity of the shareholders.

Germany has immobilised bearer shares by requiring that they must be deposited with a custodian bank that knows the depositor/shareholder (AktG, ss.10(1)) if they are issued by stock corporations that are not publicly listed. Share warrants are allowed in Germany.

**Criterion 24.12** – Nominee shares and nominee directors are not explicitly prohibited in law in Germany, and there are only partial measures in place to ensure they are not misused.

Stock corporations and limited liability companies are prohibited from having nominee directors and members of the supervisory board, however, this prohibition

is not expressly included in law and is read in as being inherent to the position of director that the role must be performed personally.

If a nominee arrangement leads to a beneficial ownership structure that is different from the one indicated in the Commercial Register, this arrangement must be registered with the Transparency Register (GwG, s.20(1)).

Nominee shareholders are possible in stock corporations, and their identity does not have to be disclosed to the company. However, if the nominee is the beneficial owner, she/he needs to be registered with the Transparency Register. Nominee shareholders do not need to be licensed.

While authorities are not aware of the use of nominees with regard to cooperatives, associations and foundations, there is no express prohibition against using them.

**Criterion 24.13** – A range of sanctions can be applied to legal and natural persons to ensure compliance with transparency and record keeping requirements with respect to the Transparency Register, however it is not clear that there are sanctions in place for non-compliance with requirements with respect to other Registers or the directory of foundations.

The general regime establishes the following sanctions to ensure compliance:

- Managing directors, shareholders of a limited liability company and founders and supervisory board members of a stock corporation incur criminal liability if they knowingly provide false information during the process of forming a company (GmbHG, s.82, AktG, s.399(1)). False representation of facts can lead to imprisonment not exceeding three years or to payment of a fine (AktG, s.400). Administrative fines between EUR 25 000 and EUR 500 000 can also be applied.
- Members of the boards of stock corporations can be fined up to EUR 5 000 for violations of record-keeping requirements (AktG, s.407).
- Any issuance of bearer shares in violation of the provisions described in c.24.11, leads either to the share issue being voided or if bearer shares are issued before they are fully paid, constitute an administrative offense.
- Penalties of up to EUR 5 000 000 may be applied for failure to fulfil obligations to provide information to the Transparency Register (GwG, s.56(1) no.54-66).
- Courts of registration can issue fine of up to EUR 5 000 for failing to submit documents to the Commercial Register (Commercial Code, s.14), or for failing to submit documents to the Register of Partnerships (Partnership Companies Act, *Partnerschaftsgesellschaftsgesetz*, (Partg GG), s.5(2)). Courts of registration can also issues a fine of up to EUR 5 000 for failing to update the Register of Cooperations (GenG s.160(1)). These penalties can be repeatedly issued until the required update is complete.
- Failure to update the Register of Associations can result in a coercive fine of up to EUR 1 000 (BGB, s.78).

For foundations, compliance is enforced through coercive fines ranging from EUR 50 000 to EUR 100 000. It is unclear whether consistently dissuasive and proportionate

finances are levied against non-compliant foundations across the *Länder* and *Länder* directories of foundations.

Overall, where there are sanctions in place, they are proportionate and dissuasive for non-compliance with the Transparency Register but may not always be proportionate and dissuasive for non-compliance with obligations in respect of other registers.

**Criterion 24.14 –**

**(a)** Basic and **(b)** beneficial ownership information available in entries in the public registers are open to the general public, including foreign LEAs for a fee.

**(c)** Assistance can also be provided to foreign counterparts in accessing information held on the central database of bank accounts and beneficial ownership information in relation to account holdings listed on the Transparency Register but this assistance can only be provided pursuant to a mutual legal assistance request.

**Criterion 24.15** The monitoring of assistance received from foreign countries through formal mutual legal assistance and between competent authorities on an agency-to-agency basis is done on an ad hoc basis. There is currently no central process for capturing this information.

### *Weighting and Conclusion*

Germany has implemented a number of measures to improve transparency and capture basic and BO information for legal persons through the launch of the Transparency Register and restrictions on the use of bearer shares. However, some deficiencies and gaps remain. Basic information is not collected on a public register for small companies and non-company partnerships (specifically civil law partnerships, although the risks are more limited in this area) and the risk assessment is primarily an assessment of inherent vulnerabilities rather than a detailed understanding of ML/TF risk.

There are small inconsistencies in information captured among the various registers and BO information is not being captured for some partnerships, foundations and associations. There is no detail on the timeframes in which basic and BO information should be updated which means that registry information may not always be up-to-date. Furthermore, the accuracy of information contained on the registries is not assured as there is no systematic obligation to verify information but rather an ad hoc, passive approach where obliged entities and government officials are only obliged to verify the information if they incidentally become aware the information on the register is incorrect or in respect of the Transparency Register, a discrepancy report is filed.

While Germany has taken steps to register bearer shares and share warrants, the situation with respect to nominee shareholders and directors is less clear. Nominee shareholders are permitted and there is no obligation for information on their nominator to be recorded by the company or elsewhere except in situations where the nominee is also the beneficial owner.

Finally, while BO information is available immediately to the FIU and BaFin through the Transparency Register and the Central Database of Accounts, it is not as available as quickly to LEAs (police and prosecutors) which means that access to information is not as rapid as it could be.

**Recommendation 24 is rated partially compliant.**

## Recommendation 25 – Transparency and beneficial ownership of legal arrangements

In its previous MER, Germany was non-compliant with these requirements due to deficiencies in transparency measures over *Treuhand*.

**Criterion 25.1** – Common-law express trusts cannot be created under German law, but foreign trusts can be created in Germany under another jurisdiction’s law, and foreign trusts established abroad can also operate in Germany. Legal arrangements set up under foreign law are allowed and legal arrangements established under foreign law that are intended to be identical in substance to a trust, but named differently, are to be treated as trusts (GwG s.1(6)). However, the GwG does not specify how to deal with legal arrangements that are only similar to trusts (*trustähnliche Rechtsgestaltungen*) but not identical in nature.

German law permits the creation of *Treuhandverhältnisse* or “*Treuhand*” which are a product of contractual agreements and operate similarly to express trusts and fall within the FATF definition of trusts and similar legal arrangements. *Treuhänder* are regulated for AML/CFT purposes (GwG, s.21(2)).

**(a)** Lawyers, legal advisors, notaries and trust and company service providers who act as trustees are required to obtain and hold information on the persons from who they have received assets for management and the persons for whose benefit they manage those assets (GwG, s.2(1) nos. 10, 11, 13 and s.8(1) no 1(a)). These trustees must also register information on the beneficial owners on the Transparency Register (GwG, s.(1)(6) sentence 2). Information collected for the register includes the name, date of birth, place of residence and nationality, nature and extent of the beneficial interest (GwG, s.21(1) and s.19(1)). Registration requirements extend also to trustees even if they do not have their registered office or place of residence in Germany, but there must be a relevant business connection with Germany (GwG s.21(1)).

**(b)** The GwG requires trustees who are obliged entities to hold general information obtained in the course of fulfilling due diligence requirements (see. R.10) which may contain information on regulated agents and service providers (GwG, s.8(1) no 1(a) and (b)). In addition, all trustees must hold information and supporting documents on expenditures under the Civil Code to meet their obligations from section 666 of the BGB. According to this, trustees have an obligation to give notices, to inform on the status of transactions and to render an account after completing their mandate. If trustees making use of third parties in performing their duties, they may also have to provide information on agents and service providers. While, there is no specific obligation to obtain and hold this information, in section 666 of the BGB, trustees must be able to furnish a rendering of accountability within the statute of limitations (in general 3 years), which in practice leads to an obligation to hold this information.

**(c)** Professional trustees are required to keep records for a period of five years after the termination of a business relationship (GwG, s.8(4)). Information related to the trust on the Transparency Register is never deleted from the register but is merely struck through so is kept indefinitely.

**Criterion 25.2** – Beneficial ownership information on the Transparency Register must be updated immediately by trustees to the office maintaining the register (GwG, s.21). Missing, late or incorrect entries are subject to fines (GwG, s.56).

If an entry on the relevant register is unclear, the office maintaining the register may contact the trustee for clarification (GwG, s.18(3)). With respect to the Transparency

Register, both obliged entities and competent authorities are required to report discrepancies in beneficial ownership information (GwG, s.23(a)).

Information not required to be reported to the Transparency Register, including information on contracting parties and business relationships; that trustees are required to collect and retain as obliged entities under the GwG, must be updated at risk-appropriate times (GwG, s.10(3a) no 2).

While the law specifies that the information must be updated without delay, there is no concrete guidance on what this means in practice and what timeframe would be considered without delay. Furthermore, verification of information on the registers is done on an ad hoc basis rather than in a systematic manner meaning that it is likely that not all of the BO information recorded is as accurate and up-to-date as possible.

**Criterion 25.3** – Trustees are required to disclose their status to financial institutions and DNFBPs when forming a business relationship or carrying out transactions (GwG, ss.11(6), 11(7), 21).

**Criterion 25.4** – Information on the Transparency Register is available to competent authorities (GwG, ss.23(1), 23(4)). Information is also available to other obliged entities to fulfil their due diligence obligations (GwG, s.23(2)). Legal professionals acting as trustees have to meet transparency obligations (GwG s.21(1)). No exemption is provided in cases where the trustee is a legal professional and legal professionals cannot decline to provide information to supervisors, FIUs and obliged entities on the basis of professional secrecy or other legal professional law provisions.

**Criterion 25.5** – As above, LEAs have access to information on the Transparency Register.

Trustees must also provide authorities with all required information and documents upon request (GwG, s.52(1)). The FIU and supervisory authorities also have powers to inspect information held by trustees or have it presented to them (GwG, s.21(3)).

Law enforcement authorities can use general investigative powers including powers of search, seizure and compulsory examination to obtain information in a criminal investigation (see also c.31(1)(a) for powers available to LEAs).

**Criterion 25.6** –

**(a)** Basic information is available to foreign law enforcement through the Transparency Register. However access to this register requires a mutual legal assistance request to be submitted which means that information may not always be provided rapidly.

**(b)** Upon request or by way of spontaneous information exchange, German competent authorities may provide information on trusts beyond what is publicly available on the public registers. Supervisory authorities can also cooperate with other supervisory authorities in cross-border cases (GwG, ss.54 and 55).

**(c)** Under the law on mutual legal assistance, the same investigative powers that can be used in domestic cases can be used to assist foreign counterparts in cross-border cases (see also R.37).

The FIU is also authorised to exchange data with Member States of the EU and with FIUs in other countries (GwG, ss.33, 34) (see also R.40).

Assistance can also be provided to foreign counterparts in accessing beneficial ownership information in relation to account holdings through the Central Account

Database but this assistance can only be provided pursuant to a mutual legal assistance request.

**Criterion 25.7** – Proportionate and dissuasive administrative penalties are available to authorities for dealing with trustees that fail to comply with their obligations. Administrative penalties of up to EUR 100 000 (up to EUR 150 000 when done wilfully) apply to persons and entities who do not comply with obligations related to basic and beneficial information for trusts (GwG, s.56(1)). For very serious, repeated or systematic breaches, the fine may be increased to EUR 5 000 000 and applies to natural persons, legal persons, and partnerships considered to be “obliged entities” (GwG, s.56(3)).

Legal persons who are obliged entities may also be subject to increased penalties of up to 10% of the total revenue of the legal person in the fiscal year before the fine (GwG, s.56(3)) for all serious, repeated or systematic violations.

**Criterion 25.8** – Information on basic and beneficial ownership held by trustees must be provided “without delay” to supervisory authorities and the FIU (GwG, s.21(3)). The Money Laundering Act (GwG) sets out a general regime of proportionate and dissuasive administrative penalties for violations of provisions of the Act including not providing information in a timely manner. (see. c.25.7). “Without delay” in German law means without hesitation or undue delay. There is no concrete timeline for this term, but should be done without too much time passing.

### Weighting and Conclusion

Overall, Germany has created a transparent system related to legal arrangements however some minor deficiencies remain. There are a few minor gaps related to the definitions of trusts which excludes trust-like legal arrangements and the collection of basic and beneficial ownership information relies of entries being made to the Transparency Register. With respect to the Register, there are also no concrete rules or guidance on the timeframe in which information must be updated and verification is only done on an ad hoc basis so the information on the Register may not be completely accurate or up-to-date. Sharing information with foreign counterparts is possible but requires a mutual legal assistance request to access even basic information.

**Recommendation 25 is rated largely compliant.**

### Recommendation 26 – Regulation and supervision of financial institutions

In its previous MER, Germany was largely compliant with these requirements. The following deficiencies were identified: uncertainty about the legal basis for BaFin’s ability to apply fit and proper testing for members of supervisory boards of investment companies, and lack of effectiveness in aspects of supervisory practice. Effectiveness issues are now covered under IO.3.

**Criterion 26.1** – Germany has designated BaFin as the competent supervisor for most AML/CFT obligations and for the vast majority of its FIs (GwG, s.50). Supervision of the insurance sector is split between BaFin and the *Länder*. BaFin supervises all private insurance undertakings of material economic and financial significance, and all public insurance undertakings that operate across *Länder* borders. The remaining insurance companies (the smaller or localised entities) are supervised by the *Länder*

ministry with economic/financial responsibility (VAG, ss.320, 321).<sup>110</sup> Insurance intermediaries are supervised by the supervisory authorities of the *Länder* (s.50, GwG). Supervision of TFS obligations is separate. BaFin supervises FIs for compliance with the TFS screening obligation (KWG, s.6), while the Deutsche Bundesbank has responsibility for monitoring compliance with other EU and AWG TFS obligations (AWG, s.23).

**Criterion 26.2** – All FIs, including Core Principles FIs, MVTs, money or currency exchangers, and insurance intermediaries are required to be licensed or registered (KWG, s.32; VAG, s.8; ZAG, s.10; KAGB, s.20; Trade Regulation Code, *Gewerbeordnung* (GewO), ss.11a, 34d, 35). Banks are required to have their head office and legal domicile within Germany, meaning authorisation will not be granted to a shell bank (KWG, s.33(1)6).

**Criterion 26.3** – Supervisors take regulatory measures to prevent criminals or their associates from holding or being a beneficial owner of a significant or controlling interest, or a management function, in a FI.

Upon application for a license or where relevant circumstances change, most FIs must provide information to their supervisor on the FI itself, its owners, managing directors, board members, and persons with a “qualifying holding”<sup>111</sup>. Insurance intermediaries are subject to a basic reliability check (including a criminal record check) and supervisors (the *Länder* Chambers of Industry or Chambers of Commerce) can seek additional information as necessary. Courts and public prosecutors are obliged to inform supervisors of criminal proceedings regarding these persons or any other person relevant for supervisory measures (including criminal proceedings of close associates). In addition, a co-operation agreement between BaFin and the FIU covers information sharing for the purpose of licensing and authorisation, qualifying holdings, and fit and proper assessments. While there is no equivalent co-operation agreement between the FIU and *Länder* supervisors for the small number of entities not supervised by BaFin, co-operation and exchange of information between the FIU and the responsible supervising authorities can take place on the basis of the GwG (GwG, s.28(1)2). All supervisors’ assessments include a criminal records check, as well as a review of administrative proceedings. (KWG, ss.2c(1), 2c(1b), 25c(1), 25d(1), 60a; ZAG, ss.12(4), 12(5), 14(1), 20(4), 65; VAG, ss.16,-18, 24(1), 47(1), 334; KAGB, ss.19(1), 21(1)4, 22(1)4, 18(4), 341; Trade Regulation Code, s.34d; Order on Notifications in Criminal Matters (MiStra), ss.25, 25a, 25b, 25c, 29, 39; BaFin Guidance Notices on management, board members and members of administrative and supervisory bodies). Germany makes use of international co-operation to undertake the same checks and obtain equivalent information in respect of foreigners or individuals not residing in Germany.

<sup>110</sup> As at 31 December 2018, BaFin supervised 555 insurance companies, with the remaining 715 companies and all intermediaries supervised at the *Länder level*. The insurance companies under supervision of the *Länder* are mostly pension funds, death insurers, property insurers and animal insurers—only three qualify as FIs under the FATF Recommendations. The insurance companies subject to *Länder* supervision are all located in nine *Länder*.

<sup>111</sup> A person will have a “qualifying holding” where they hold, directly or indirectly, 10% or more of the institution’s voting rights, capital or control.

**Criterion 26.4 –**

(a) Germany's Financial Sector Assessment Program (FSAP) report was conducted in 2016. Overall, the technical requirements for regulation and supervision of FIs was in line with the core principles. Germany had a reasonably high level of compliance/observance with the principles of banking supervision, insurance supervision<sup>112</sup> and those related to securities commissions. This includes the application of consolidated group supervision (GwG, s.9).<sup>113</sup>

(b) Other FIs, including MVTs and money or currency exchangers, are subject to AML/CFT supervision having regard to the ML/TF risks in the sector (GwG, ss.50, 51).

**Criterion 26.5 –** BaFin's risk-based approach for the FIs it supervises takes into account:

(a) the ML/TF risks and the policies, internal controls and procedures associated with the institution or group,

(b) the NRA and the ML/TF risks present in Germany, and

(c) the characteristics of the FIs or groups in particular the diversity and number of FIs and the degree of discretion allowed to them under the risk-based approach.

This approach is set out in a combination of legislation<sup>114</sup> (GwG, ss.50, 51(3)), BaFin's *AML Risk Classification Manual*, BaFin's *Subnational Risk Assessment for the Financial Sector 2019-2020*, and the European Banking Authority *Joint Risk-Based Supervision Guidelines*. There are no equivalent manuals for *Länder* supervisors for the supervision of insurance companies and intermediaries not subject to BaFin supervision.

**Criterion 26.6 –** Supervisors must review FIs' risk profile at regular intervals and when important events or developments occur (GwG, s.51(3)).

**Weighting and Conclusion**

BaFin takes a risk-based approach to supervision and has issued manuals and guidelines articulating their approach, however, it is unclear if supervising entities across the *Länder* apply consistent guidance and a similar risk-based approach. This is a minor deficiency given the nature and low risk of FIs supervised at the *Länder* level.

**Recommendation 26 is rated largely compliant.**

**Recommendation 27 – Powers of supervisors**

In its previous MER, Germany was largely compliant with these requirements due to effectiveness issues which under the current evaluation are considered in the assessment of IO.3.

<sup>112</sup> The 2016 FSAP did not cover ICP18 on intermediaries. The previous 2011 FSAP found that the relevant ICP was largely observed with deficiencies related to effectiveness issues.

<sup>113</sup> IMF (June 2016) *Germany: Financial Sector Assessment Program, Financial System Stability Assessment* (available at: [www.imf.org/external/pubs/ft/scr/2016/cr16189.pdf](http://www.imf.org/external/pubs/ft/scr/2016/cr16189.pdf)).

<sup>114</sup> The inspections of payment and e-money institutions and DNFBPs must be based on the entity's ML/TF risk profile.

**Criterion 27.1** – Designated supervisors (BaFin and *Länder* supervisors) are required to exercise supervision over FIs and may take appropriate and necessary measures and issue orders to ensure compliance with AML/CFT obligations (GwG, ss.51(1)-(2)). BaFin is the supervisor of most FIs, except public sector insurance undertakings and insurance intermediaries that are subject to supervision by *Länder* supervisors (GwG, s.50) (see c.26.1).

**Criterion 27.2** – BaFin and *Länder* supervisors have the authority to conduct inspections of FIs to review compliance with AML/CFT obligations (KWG, s.44(1); VAG, s.306(1); ZAG, s.19(1); KAGB, s.14; GwG, ss.50, 51(3)).

**Criterion 27.3** – BaFin and *Länder* supervisors can compel (without a court order) FIs to provide them with any information and documents on their business activities, including on compliance with AML/CFT requirements (KWG, s.44(1); VAG, s.305(1); ZAG, s.19(1); KAGB, s.14; GwG, s.51(2)).

**Criterion 27.4** – BaFin and *Länder* supervisors are authorised to impose sanctions for non-compliance with AML/CFT obligations (although the sanctions themselves are subject to some minor deficiencies: see R.35). This includes powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the FI's licence (GwG, ss.51, 56, 57; KWG, ss.35(2)6, 36; VAG, ss.303, 304(3); ZAG, s.13(2)5, 20; KAGB, ss.39(3)7, 40(1)).

### Weighting and Conclusion

All criteria are met.

**Recommendation 27 is rated compliant.**

### Recommendation 28 – Regulation and supervision of DNFBPs

In its previous MER, Germany was non-compliant with these requirements due to a combination of technical and effectiveness deficiencies. The technical deficiencies included the lack of adequate authority to supervise real estate agents and dealers in precious metals and stones and insufficient powers to monitor lawyers and tax advisors.

**Criterion 28.1** – Casinos in Germany are subject to AML/CFT regulation and supervision.<sup>115</sup>

**(a)** All casinos are required to be licensed by the *Länder* in which they operate (Interstate Treaty on Gambling, *Glücksspielstaatsvertrag* (GlüStV)<sup>116</sup>, s.4(1)). This includes online and ship-based casinos, where permitted (see c.22.1(a)). Operating without a license is a federal criminal offence, which is enforced by local LEAs, and punishable by a fine or up to five years' imprisonment (StGB, s.284).

**(b)** Measures are in place to prevent criminals or their associates from owning, managing or operating a casino. Applicants for a casino license must provide evidence on the reliability of the applicant and the persons designated to manage the casino, and information on ownership, voting-right structures, and shareholdings. Licensing

<sup>115</sup> These regulations also extend to sports betting which is not covered under the FATF standards and therefore not discussed here.

<sup>116</sup> The Interstate Treaty on Gambling, *Glücksspielstaatsvertrag* (GlüStV) (15 December 2011) has been ratified by all of the *Länder* and sets out a uniform legal framework for casinos (and the gambling sector more broadly).

authorities confirm the individual's financial situation, criminal record, and regulatory record. This process is repeated if there are any changes, as well as on an occasional basis to detect discrepancies. Criminal convictions are grounds for establishing a lack of suitability. Ongoing criminal proceedings involving license-holders are reported to licensing authorities by the courts. (Requirements are set out in *Länder* legislation, e.g., Baden-Württemberg Gambling Act, *Landesglücksspielgesetz Baden-Württemberg*, s.28(2); Rhineland-Palatinate Casino Act, *Spielbankgesetz Rheinland-Pfalz*, s.3a(2); Order on Notifications of Criminal Matters, no.39). Case law has shown that an applicant may be considered unreliable where they are under the influence of another, unreliable person (such as a criminal).

**(c)** Casinos in Germany are supervised for most AML/CFT obligations by the *Länder* authorities responsible for broader gambling supervision unless otherwise specified in *Länder* law (GwG, ss.50, 51(1)). In most cases, supervision is conducted by the *Länder* Ministry of the Interior.<sup>117</sup> There is no clear responsibility for the supervision of TFS obligations; the enforcement of breaches is undertaken by the Central Customs Authority (GZD) and federal or *Länder* police.

**Criterion 28.2** – The vast majority of DNFBP supervision is decentralised in Germany and undertaken by authorities or self-regulatory bodies (SRBs) at the *Länder*-level (see Annex B). The sole exception are accountants, who are supervised by the Federal Chamber of Accountants. The legal profession (including lawyers and tax advisors) are supervised by the relevant self-regulatory body, while notaries are supervised by the relevant regional court (GwG, s.50(1)). Real estate agents, DPMS and TCSPs (that are not already covered as lawyers, accountants or tax advisors) are supervised for most AML/CFT obligations by their relevant regulatory supervisor at the *Länder* level (GwG, s.50(1)). However, there is no clear supervisor of TFS obligations for these sectors (unless they are engaged in the cross-border movement of goods).<sup>118</sup> The GwG and other federal legislation sets out the overarching responsibilities and powers of all designated supervisors, including DNFBP supervisors. For certain sectors, *Länder* legislation determines which authority is empowered to execute the federal law (for the remaining sectors, the federal law provides this authority).

**Criterion 28.3** – Designated DNFBP supervisors are required to monitor obliged entities for compliance with AML/CFT obligations (GwG, s.51(1)). Supervisors have systems in place for monitoring compliance either alongside regulatory supervision or independently. There is a gap in TFS supervision, which is taken into account in c.28.2.

**Criterion 28.4** –

**(a)** Designated DNFBP supervisors and self-regulatory bodies have adequate powers to perform their supervisory function, including to inspect supervised entities, access information, and take appropriate measures to ensure compliance (GwG, ss.51, 55,

<sup>117</sup> Exceptions are: Baden-Wuerttemberg (District Government), Bremen (police authorities), Lower Saxony (Ministry of Finance), and Saxony (State Office). Regulatory and licensing supervisors differ from AML/CFT supervisors in two *Länder*: Rhineland-Palatinate and North Rhine-Westphalia. In these *Länder*, AML/CFT supervision is conducted by the District Government and State Administrative Office respectively.

<sup>118</sup> The customs administration monitors the import, export and transit of goods. Main Customs Offices audit, among other things, compliance with foreign trade law by businesses involved in the cross-border movement of goods, including, where relevant, DNFBPs.

56; supplemented by relevant *Länder* legislation which grant general powers to DNFBP supervisors execute federal laws and impose coercive fines, e.g., Hamburg Administrative Enforcement Act, *Hamburgisches Verwaltungsvollstreckungsgesetz*, s.14).

**(b)** Measures to prevent criminals or their associates from being professionally accredited as a DNFBP differ in intensity between sectors. Licensing authorities must deny the license or accreditation of lawyers, legal advisors and other legal professionals, notaries, tax advisors, accountants and real estate agents if the proposed licensee has had a criminal conviction in the preceding five years (Federal Code for Lawyers, s.7; Legal Services Act, s.12; Federal Notarial Code, ss.6, 49; Act Regulating the Accountancy Profession, s.16; Tax Consultancy Act, s.40; Trade Regulation Code, ss.34c). DPMS are subject to a “reliability” check upon application. While not explicit, a criminal conviction would generally point towards a lack of reliability resulting in a rejection, suspension or loss of accreditation (Trade Regulation Code, ss.35, 38). Managers and shareholders in law and accounting firms must be members of the profession, and are therefore subject to equivalent checks (Federal Code for Lawyers, ss.59c to 59h; Act Regulating the Accountancy Profession, ss.27-34; Tax Consultancy Act, ss.49-55). For TCSPs, supervisory authorities may remove senior managers or prohibit operations if senior managers or shareholders are deemed unreliable, but there is no proactive check (GwG, ss.51(5b), 2(1) no.13). Outside of these sectors, rules generally focus on the applicant, operator and/or manager of the entity. There are limited measures in place to ensure criminals’ associates are not accredited.

**(c)** Designated DNFBP supervisors, including SRBs, have sanctions available in line with R.35 to deal with non-compliance with AML/CFT requirements. These include issuing orders or warnings, imposing administrative fines, and publication (GwG, ss.51, 56, 57). Supervisors, including SRBs, are empowered to impose the sanctions available under relevant federal laws, including the GwG.

#### **Criterion 28.5 –**

**(a)** The frequency and intensity of supervisory inspections must be based on the risk profile of the obliged entity (GwG, s.51(3)). This legislative obligation does not explicitly apply to other supervisory activity (ss.5(4), 6(8), 7(3) GwG), although Germany considers that this is an implicit obligation. *Länder* risk assessments are taken into account by supervisors and largely consider the characteristics of DNFBP sectors, including their diversity and number. However, there is no model guidance or similar document to ensure the approach is consistent across all of the over 300 DNFBP supervisors or to give advice on how these supervisors should apply the risk-based approach.

**(b)** Pursuant to their supervision of DNFBPs, there is an implicit obligation that supervisors take into account the risk profile of DNFBPs, and the degree of discretion allowed to them under the risk-based approach when assessing the adequacy of internal controls (s.6(1), GwG).

### ***Weighting and Conclusion***

Measures to prevent criminals and/or criminals’ associates from owning, managing or operating a DNFBP differ in comprehensiveness between sectors. The requirement that supervisory activity beyond on-site inspections must be based on the risk profile of the obliged entity is implicit. In the absence of guidance or similar measures, it is

not clear that the large number of DNFBP supervisors apply a consistent risk-based approach; this is given more weight given the large number of DNFBP supervisors and the risks in these sectors. There is no clear supervisor for TFS obligations for casinos, REAs, DPMS and TCSPs.

**Recommendation 28 is rated largely compliant.**

### Recommendation 29 - Financial intelligence units

In its previous MER, Germany was largely compliant with these requirements. The main technical deficiencies focused on the de-centralised nature of STR receipt, analysis and dissemination and limitations in strategic analysis. Other deficiencies were also identified in relation to the quality of STR reporting and analysis, resourcing organisation of the FIU, and poor guidance to the private sector but these effectiveness issues are now considered separately under IO.6. Since the last MER, the FIU has been restructured and moved from under the umbrella of the Federal Criminal Police Office (BKA) to the GZD.

**Criterion 29.1** – The German FIU (*Zentralstelle für Finanztransaktionsuntersuchungen*) is an independent administrative body within the GZD and is the national centre for receipt and analysis of suspicious transaction reports and other relevant information related to ML, associated predicate offences and TF; and for disseminating the results of this analysis (GwG, ss.27(1), 28(1)).

**Criterion 29.2** – The FIU serves as the central agency for the receipt of disclosures filed by obliged entities, including:

**(a)** STRs filed by reporting entities (GwG, ss.28(1), 30(1), 43, 44).

**(b)** (N/A) Germany does not require any other forms of reporting from obliged entities of cash transactions, wire transfer and or any additional types of threshold based activity apart from cross border cash declarations (Customs Administration Act (*Zollverwaltungsgesetz*) (*ZollVG*), s. 12a) and other notifications from tax authorities (AO, s. 31b)

**Criterion 29.3** – In relation to obtaining and accessing information:

**(a)** The FIU has the power to obtain and use additional information from reporting entities as needed to perform its analysis properly and regardless of the existence of a STR (GwG, s.30(3)).

**(b)** The FIU has access to information from domestic public authorities, including a wide range of financial, administrative and law enforcement information, on request (GwG, ss.31(1)-(2)). The requested authorities are obliged to comply with the FIU's requests, unless there are "transmission restrictions". The FIU also has direct access to data on: the BKA police information database (INPOL) which contains information on federal and some *Länder* cases, Central Public Prosecutions Register (*Zentrales Staatsanwaltschaftliches Verfahrensregister*), information held by tax authorities, and information held on the Customs Database (INZOLL). The FIU can also request and receive information held by the Federal Employment Agency (*Bundesagentur für Arbeit*), and information held on the civil register (GwG, s.31(3)-(7)). The FIU also automatically receives reports from tax authorities for analysis and dissemination, when there is a suspicion of ML or TF activity (AO, s.31(b)).

**Criterion 29.4** – Under German law, the FIU is empowered to:

(a) Conduct operational analyses, including the assessment of suspicious transaction reports and other information (GwG, s.28(1)); and

(b) Conduct strategic analyses and produce reports on the basis of these analyses (GwG, s.28(1)).

**Criterion 29.5** – The FIU is required to disseminate the result of its analysis and all other relevant information to LEAs, supervisory authorities and tax authorities spontaneously and without delay (GwG, ss.32(1), 32(2)) and upon request, (GwG, s.32(3)). When information is shared, it is sent through secure channels including through secure email server using end-to-end encryption.

**Criterion 29.6** – The FIU protects its information in the following ways:

(a) A security plan is in place to ensure that employees can only access the data they need to perform their functions and data access is restricted to select groups of employees on a need to know basis.

(b) All employees at the FIU are subject to a security clearance process with employees working on TF matters required to have the highest level of security clearance.

(c) Physical access to the FIU premises is limited to FIU staff and is secured through access cards. Access to the FIU database and IT system is also restricted to FIU staff.<sup>119</sup>

**Criterion 29.7** – In relation to operational independence and autonomy, the FIU:

(a) Is established, by law, as an operationally independent entity that makes autonomous decisions to analyse, request or disseminate information (GwG, s.27(2));

(b) Can independently exchange information with other domestic authorities as well as with foreign FIUs (GwG, s.28(1));

(c) While the FIU is part of the GZD and has administrative links with the parent agency, it has distinct and separate core functions as set out by law and;

(d) Makes independent budget requests to budget authorities.

**Criterion 29.8** – The German FIU has been a member of the Egmont Group since 2003. Its Egmont membership was renewed in July 2017, after the FIU was moved from BKA to GZD.

### *Weighting and Conclusion*

All criteria are met.

**Recommendation 29 is rated compliant.**

### **Recommendation 30 – Responsibilities of law enforcement and investigative authorities**

In its previous MER, Germany was rated largely compliant for these requirements. Identified deficiencies related to effectiveness issues which are now assessed under IO.7.

<sup>119</sup> Germany has enacted laws to enable automatic data retrieval of FIU information by law enforcement agencies (GwG, s.32(4)). However this had not been implemented at the time of the on-site.

**Criterion 30.1 –***Money laundering and associate predicate offence investigations*

In general, law enforcement is the responsibility of the *Länder* governments. However, the Federal Prosecutor General (*Generalbundesanwalt* (GBA)) as the sole federal prosecution office, is responsible for law enforcement in certain instances as set forth in section 142a in conjunction with section 120 of the GVG.

In each *Land*, ML and predicate offences are investigated by public prosecution offices who lead the cases and direct law enforcement agencies in the conduct of the investigation (RiStBV, s.1). Specialised law enforcement teams and special prosecution offices are in place in various *Länder* to deal with ML and predicate crime cases. For example, there are numerous joint investigation groups targeting ML in different *Länder*.

Cases involving multiple *Länder* can be investigated concurrently by authorities in different *Länder* or prosecutors may come to an agreement for one office to take over responsibility for the entire case. In cases where prosecution offices cannot reach an agreement, the Federal Prosecutor General (*Generalbundesanwalt* (GBA)) will decide which *Länder* prosecution office will lead a case (GVG, s.143(3)).

At the federal level, the competent authorities are, in addition, the Federal Criminal Police Office (BKA), the Central Office of the German Customs Investigation Service (ZKA) and the Customs Investigations Offices (ZFAs) and the Illicit Employment Monitoring Authority.

*Terrorist financing investigations*

Standard TF cases are handled by LEAs at the *Länder* level in the same way as ML cases. Specialised law enforcement teams and special prosecution offices are in place in various *Länder* to deal with TF cases. For example, the Centre for Combatting Extremism and Terrorism in Bavaria and the terrorism prevention centres in Hesse and North Rhine-Westphalia handle some TF cases.

Complex, international and otherwise significant TF cases are normally investigated by the Federal Prosecutor General (GBA) and the Federal Criminal Police Office (BKA) (Federal Criminal Police Office Act, *Bundeskriminalamtgesetz*, (BKAG), s.4(1)). Cases can also be referred by the GBA to prosecution offices in the *Länder*. At the federal level, the designated authorities are: the Federal Prosecutor General (GBA) and the BKA.

In addition to the law enforcement agencies outlined above, terrorism financing cases are also supported by the Joint Counter-Terrorism Centre (GTAZ) and Joint Centre for Combating Extremism and Terrorism (GETZ) who play a role in detecting TF activity and co-ordinating TF cases. The customs administration has a Counter-Terrorism Co-ordination Office which centralises and processes all information on TF for customs and also supports the GTAZ and GETZ.

**Criterion 30.2 –** Public prosecution offices at the federal and *Länder*-level are required to take action regarding all prosecutable criminal offences, including ML/TF under the principle of mandatory prosecution provided there are sufficient factual indications (StPO, s.152(2)). Parallel financial investigations will be routinely carried out if there is an indication of ML/TF activity. Parallel financial investigations related to the investigation of ML/TF and their predicate offences are by default led by the

public prosecution offices but usually executed by the involved police or custom authority or tax investigation services.

**Criterion 30.3** – German prosecutors are obliged to pursue confiscation of proceeds of crime in all cases of proceed- generating crimes and practice an asset-focused approach on all levels as the Criminal Code establishes an obligation to consider seizure and confiscation in all criminal cases, (StGB, s.73; StPO, s.111b). The obligation to pursue confiscation of proceeds of crime applies also vis-à-vis third party beneficiaries. Legal entities can be subject to confiscation as third party beneficiaries. All *Länder* and federal public prosecution offices have special personnel for the purpose of investigating asset recovery cases and both federal and *Länder* police authorities have special financial investigation units housed with the BKA and the LKAs.

**Criterion 30.4** – In Germany, criminal investigations are led by the competent public prosecution office and no public authorities other than LEAs are tasked to investigate crimes. Tax and customs authorities are considered to be LEAs (AO, s.404). These authorities have powers of criminal investigation in their areas of purview and may identify, trace and secure any assets associated with the crimes under investigation consistent with R.30.

**Criterion 30.5** – Specialised corruption units within the different federal and *Länder* law enforcement agencies investigate cases of corruption. These units have the same powers to trace, identify, seize and freeze assets available to other law enforcement units investigating ML cases.

### *Weighting and Conclusion*

All criteria are met.

**Recommendation 30 is rated compliant.**

### **Recommendation 31 - Powers of law enforcement and investigative authorities**

In its previous MER, Germany was largely compliant with these requirements due to effectiveness issues that are now assessed under IO7. Since the previous MER, the requirements in R.31 have been updated.

**Criterion 31.1** – Law enforcement authorities involved in the investigation of ML, TF and predicate offences are able to access necessary documents and information for use in investigations, prosecutions and related actions. All criminal proceedings carried out by competent authorities (including Customs and the tax fraud investigations office) are governed by the Criminal Procedure Code (StPO).

**(a)** Public prosecutors can compel natural persons to produce written documentation or to act as a witness to give information that might constitute evidence in relation to a criminal investigation. Failure to comply with this obligation may be punished with coercive fines or coercive detention (StPO, ss. 95, 161a, 163(3)). Legal persons (FIs and DNFBPs) can be requested to hand over relevant documents however they cannot be compelled to do so. If legal persons do not voluntarily comply with the request for production of documents, responsible natural persons are compelled to supply the documents or summoned as witnesses to give evidence as described above.

**(b)** Investigative authorities have the powers to conduct searches of persons and premises (StPO, s.102) as well as other persons and their possessions and premises

(StPO, s.103). This requires a judicial order or an order by the public prosecutor or investigative authorities (StPO, s.105). The requirement for an order may be deviated from when the matter at hand is pressing or urgent. An order can be granted where there are “actual indications that a crime was committed” as well as the possibility of locating evidence or taking the accused person into custody.

**(c)** Witnesses and experts are obliged to appear before the public prosecution office if summoned, and make a statement on the subject matter or to render their opinion (StPO, ss.161a, 163(3)). Failure to comply with this obligation is punishable with coercive fines or coercive detention (StPO, s.161a(2)). Coercive fines and coercive detention both constitute means of order. Unlike fines and imprisonment, their purpose is not to sanction criminal offences committed. Instead they are intended to ensure orderly proceedings and may be imposed by the court or, as the case may be, the public prosecutor in case of culpable violations of procedural obligations or regulations. Unless otherwise provided in the statutory law, coercive fines shall amount to at least EUR 5 and at a maximum EUR 1 000.

**(d)** Objects that may be used as evidence can be taken into custody or secured if they are surrendered voluntarily. When there is lack of such willingness, seizure may be ordered (StPO, ss.94 (1), 94(2)). Seizure must primarily be done by court order. In exigent circumstances (that is to say an emergency situation or pressing issue), the seizure may be ordered by public prosecutors or investigators however the order must later be confirmed by a court afterwards if this is requested (StPO, ss.98 (1), 98(2)).

**Criterion 31.2** – Law enforcement authorities are able to use a wide range of investigative techniques in investigations including the following:

**(a)** Undercover operations can be used in TF investigations and ML investigations related to an organised criminal group or where the offences occur on commercial or habitual basis (StPO, s.110a). Undercover operations can also be used in relation to predicate offences where they: constitute an offence of substantial significance (which is an offence considered especially dangerous to the public),<sup>120</sup> are related to the illegal trade of drugs or weapons or counterfeiting of money or official stamps, are done on a commercial or habitual basis or involve an organised criminal group (StPO, s.110a).

**(b)** Communications can be intercepted and recorded in the course of a criminal investigation (StPO, s.100a). The types of communications covered includes call records from land lines and mobile phones, content of SMS and MMS messages, faxes and communications via the internet.

**(c)** Computer systems can be accessed as part of ongoing communication intercepts and also covert access and search of data stored on computer systems (StPO, ss.100a, 100b).

**(d)** Controlled deliveries are possible (StPO, ss.161, 163 and elaborated on in the Guidelines for Criminal Proceedings and Administrative Fine Proceedings (*Richtlinien für das Strafverfahren und das Bußgeldverfahren* (RiStBV), numbers 29a, 29b, 29c and 29d).

<sup>120</sup> These crimes are required to be of at least medium criminality and capable of disturbing the legal concord considerably and impairing the public’s feeling of security.

**Criterion 31.3 –**

**(a)** BaFin, the FIU and the Central Tax Office (BZSt) have access to a centralised bank account register, through the Electronic Bank Account Retrieval system, in which credit institutions input information on the name of the account holder, individuals authorised to draw on the account and any beneficial owners. In practice, law enforcement agencies can request that BaFin or BZSt retrieve this information for LEAs when it is requested (KWG, s.24c(3); AO, s.93b). Information on beneficial owners is also listed and accessible in the Transparency Register and other registers that are publicly available (see R.24).

**(b)** Law enforcement authorities may obtain the information of bank account owners and beneficial owners without the consent or prior knowledge of the person concerned based on the general authorisation to conduct investigations (StPO, ss.161 (1), 163 (1)).

**Criterion 31.4 –** Law enforcement authorities can request information from the FIU and the FIU has an obligation to provide information on all crime types when requested to do so (GwG, s.32(3)).

**Weighting and Conclusion**

All the criteria are met.

**Recommendation 31 is rated compliant.**

**Recommendation 32 – Cash Couriers**

In its previous MER, Germany was largely compliant with these recommendations due to weaknesses in measures for alerting passengers from outside the EU on their declaration obligations and a limited period for retaining declarations.

**Criterion 32.1** For travellers entering or leaving the EU via Germany, Germany applies a declaration system for accompanied cash under and unaccompanied cash under EU Regulation 2018/1672 (the EU Regulation). Germany also applies a disclosure system that applies to passengers travelling within and outside of the EU, as well as transportation of cash by mail or cargo (Customs Administration Act (*Zollverwaltungsgesetz* (ZollVG), ss. 5(1), 12a). Both systems apply to cross-border cash or BNI movements over EUR 10 000.

**Criterion 32.2 and 32.3** Under the EU declaration system, natural persons entering or leaving the EU must declare in writing cash or bearer negotiable instruments (BNIs) over EUR 10 000 (EU Regulation, Art.3).

Under the German disclosure system, passengers are required to verbally disclose when they hold cash or equivalent means (including BNIs, precious metals and stones and stored value cards) over EUR 10 000 and are required to give a truthful answer upon request from a customs officer (ZollVG, s.12a).

Since June 2021, a declaration system has also come into effect with respect to unaccompanied cash (cash transported through mail and cargo) to require the sender to disclose via declaration amounts over EUR 10 000 (EU Regulation, Art.4).

**Criterion 32.4** Customs officials can seek additional information on the origin and intended use of the cash, including documentation to verify the source of the cash, the beneficial owners or intended use (ZollVG, s.12a(5)).

**Criterion 32.5** Germany has proportionate and dissuasive sanctions in place for making false declarations or disclosures. Failing to comply with the declaration/disclosure requirements or making a false declaration/disclosure is an offence punishable by a fine of up to EUR 1 million per violation (ZollVG, ss.31a(1) and 31a(2)).

**Criterion 32.6** Information on declarations is recorded on the database of the Customs agency (INZOLL). Information related to disclosures (both disclosures and failures to disclose leading to further action) is recorded in a table by the responsible supervision unit of the GZD. The FIU has direct access to the Customs database INZOLL and the information on disclosures recorded by GZD. (EU Regulation 2018/1672, Art.9 and ZollVG, s.12a(8)).

**Criterion 32.7** Information on the INZOLL database relating to cash declarations is directly accessible by the BKA and members of Joint Financial Investigation Groups (GFGs) and FIU. Other investigation agencies (LKAs, tax investigators) can also obtain information by submitting requests for information to Customs. Cooperation in investigations is achieved through the broader mechanisms for co-ordination and co-operation between law enforcement agencies.

At the strategic level, a specialised unit of directorate VI of the GZD collects and analyses cross border cash movement data and detected undisclosed/undeclared cash movements. A specialised unit of the ZKA collects and analyses data of cash movements related to ML, TF and other crimes. The analysis of these data leads to reports on new trends, methods, routes, etc. Both units also regularly report to the Federal Ministry of Finance (BMF).

**Criterion 32.8** Customs officers can stop or restrain currency and BNIs for a period of five business days (which can be extended by three months) where there is reason to believe the assets are being transported for the purposes of ML or TF (ZollVG, s.12a(7)). There is no specific provision for seizure in cases of making a false declaration but German authorities noted that in practice the provision of false information would normally be grounds for suspicion of ML activity triggering the power to seize the assets.

**Criterion 32.9** To facilitate international co-operation and assistance, Germany records all information obtained under the disclosure and declaration regime including declarations/disclosures, non- or false declarations/disclosures and suspicions of illegal activity. Customs and the FIU may store data on cross-border cash movements for a period of five years from the date on which the data were obtained. The period of retention may be extended up to an additional three years if customs or the FIU deems in necessary. Customs can share cash declaration information with countries within and outside the EU (EU Regulation 2018/1672, Art.10 and 11, ZollVG, ss.11, 11a).

**Criterion 32.10** The disclosure/declaration requirements do not restrict: (i) trade payments between countries for goods and services or (ii) freedom of capital movements.

**Criterion 32.11** Persons transporting currency or BNIs relating to ML, TF or predicate offences are subject to:

**(a)** Penalties that apply to ML and TF offences (see R.3 and R.5) and administrative fines of up to EUR 1 000 000 for failing to declare or providing false information (ZollVG, s.31a), and

**(b)** Customs may seize cash or equivalent means of payment when there is suspicion of ML or TF and ultimately confiscate the cash if a criminal conviction is achieved (see R.4).

### *Weighting and Conclusion*

All criteria are met.

**Recommendation 32 is rated compliant.**

### **Recommendation 33 – Statistics**

In its previous MER, Germany was partially compliant with these requirements.

**Criterion 33.1** – Germany keeps statistics on the following:

**(a)** STRs received, subject to analysis and disseminated to the various authorities such as *Länder* criminal police offices, public prosecution offices, tax fraud investigation offices, Federal Police and with a breakdown of categories and sub-categories. The STRs are broken down by priority risk areas.

**(b)** Partial data and statistics on ML/TF investigations, prosecutions and convictions are kept at both the federal and *Länder*-level. Adequate statistics on TF investigations and prosecutions are not available as they are not counted as a distinct category of offences from terrorism. There are no clear statistics on ML investigations. The statistics on prosecutions do not include all ML proceedings; they only record the main focus (*Schwerpunkt*) of the case. Since 2017, Germany collects supplementary data on ML-related court decisions (convictions, acquittals, terminated proceedings and cases in which the court dispensed with a penalty) but these do not cover earlier stages of the process.

**(c)** Data and statistics on property frozen, seized and confiscated is kept but does not comprehensively detail the predicate offence and . Statistics are not kept on asset repatriation and until 2019, asset confiscation figures included numbers on corporate fines and could not be separated out.

**(d)** There is no central data or uniform statistics kept on mutual legal assistance cases. However, there are national-level statistics on extradition and other requests for international co-operation related to police-to-police and FIU-to-FIU co-operation.

### *Weighting and Conclusion*

Germany does not maintain national statistics on key parts of the AML/CFT system such as international co-operation (mutual legal assistance) and ML and TF investigations and prosecutions. Some of these issues arise at both the federal and *Länder*-level and is a major deficiency.

**Recommendation 33 is rated partially compliant.**

### **Recommendation 34 – Guidance and feedback**

In the last MER, Germany was partially compliant as there was uncertainty in some parts of the financial sector on the status of abrogated circulars, certain guidance was limited in scope, and there was a lack of guidance in the insurance intermediaries sector.

**Criterion 34.1 – Guidance and feedback by supervisors:** Supervisors are required to regularly provide supervised entities with up-to-date interpretation and application guidance on implementing their AML/CFT obligations (GwG, s.51(8)).

FIs: In May 2020, BaFin published its *Interpretation and Application Guidance on the GwG*, which provides assistance in applying the GwG. BaFin has also issued sector-specific guidance on complying with GwG obligations for BaFin-supervised insurance entities (January 2020). *Länder* insurance company supervisors reportedly also apply this guidance, while insurance intermediary supervisors instead apply the general guidance applicable to DNFBPs. BaFin provides feedback bilaterally and multilaterally, including through industry bodies, the BaFinJournal, and an annual AML/CFT symposium. Bilateral feedback is a component of supervisory inspections for *Länder* supervisors.

DNFBPs: Sector-specific guidance on complying with GwG obligations has been issued for the gambling sector, lawyers and patent attorneys, notaries, and accountants, as well as general guidance for other DNFBPs. *Länder* supervisors have published this guidance on their websites. Specific guidance has also been provided to DNFBPs on risk-based organisation measures, STR reporting, documentation for natural and legal persons, and the implementation of enhanced due diligence requirements. Guidance documents for DNFBPs are co-ordinated across *Länder* and at the federal level, so apply and are valid to DNFBPs in all 16 *Länder*. DNFBP supervisors provide feedback bilaterally (e.g., during and after audits or on-site inspections). DNFBP supervisors (sometimes in co-operation with individual chambers) also provide feedback and seminars, workshops or training courses on a multilateral based.

*Guidance and feedback by the FIU:* The FIU has a department responsible for sharing information and providing guidance and feedback to obliged entities. The FIU issues an annual report that identifies trends and methodologies, provides specific typology reports, organises workshops on sectoral risks, and provides general feedback to obliged entities on STR reporting (e.g., *FIU Guidance on Registration and Reporting on goAML*; a FAQ on the FIU website). In addition, the FIU is in regular contact with reporting entities, including through meetings and targeted discussions with certain groups, to raise awareness of case patterns and typologies, to provide specific feedback on STRs, and to give ongoing informal guidance.

### Weighting and Conclusion

Guidance and feedback is provided by BaFin, DNFBP supervisors, and the FIU. It is not clear that sufficient guidance and feedback is provided to FIs not supervised by BaFin (certain insurance undertakings and insurance intermediaries).

**Recommendation 34 is rated largely compliant.**

### Recommendation 35 – Sanctions

In the previous MER, Germany was rated partially compliant with these requirements. The deficiencies identified were: (a) administrative fines were not proportionate or dissuasive, maximum fines were too low, and high penalties could be applied only for gross negligence or deliberate intent; (b) administrative fines were not being applied effectively; (c) there were no administrative fines for certain sector-specific requirements relating to internal safeguards and enhanced due diligence; and (d) failure by supervisory boards to supervise management may have

resulted in uncertainty as to whether administrative fines applied to individual members of such boards.

**Criterion 35.1** – A range of sanctions criminal and administrative sanctions are available to deal with natural or legal persons that fail to comply with AML/CFT requirements. Legal persons can be liable for administrative sanctions where an offence was committed by a legal representative, chairperson, or similar managing official, or was a result of their failure in supervision (Administrative Offences Act, *Gesetz über Ordnungswidrigkeiten* (OWiG), ss.30(1), 130).

(a) For breaches of TFS obligations (R.6), criminal sanctions of up to five years' imprisonment are available for any natural or legal person who breaches an AWG or EU freezing/prohibition order (AWG, s.18(1)). The same sanction is available for breaches of licensing requirements (AWG, s.18(1)). Legal persons, including FIs and DNFBPs, can be sanctioned by means of an administrative fine of up to EUR 500 000 (AWG, ss.19(1), 18(1)). TFS supervisors (the Deutsche Bundesbank and the Main Customs Offices) have access to certain supervisory measures to enforce the implementation of TFS, as described in IO.10.

(b) For breaches related to NPOs (R.8), there are a range of sanctions available for NPOs themselves, although available sanctions for natural persons (such as NPO officers) are more limited (see c.8.4(b)).

(c) For breaches of preventive measures and reporting obligations (R.9-23), administrative sanctions may be imposed by the relevant supervisor. Available sanctions range from warnings, administrative fines, suspension, and deregistration. Warnings, fines, and prohibitions (e.g., from acting in certain positions) are also available for natural persons (see also c.35.2).

All obliged entities that breach their obligations under the GwG may be subject to administrative fines of up to EUR 100 000 (GwG, s.56). Where there is wilful intent, the fine may be up to EUR 150 000 (GwG, ss.56(1)2, (2)2). And where the breach is serious, repeated or systematic, the fine may be up to EUR 1 million or twice the economic benefit derived from the offence (GwG, s.56(3)1). In imposing a fine, supervisors are required to take into account the significant of the offence and the financial circumstances of the perpetrator (OWiG, c.17(3)). In addition, sanctions, once final, are published with acts as a further deterrent (GwG, s.57(1)). Higher sanctions are available for FIs – the fine may be up to EUR 5 million (for natural or legal persons), or 10% of total annual revenue (for legal persons) (GwG, s.56(3)). These sanctions are not available for DNFBPs. Administrative fines under the GwG may be imposed by the relevant FI or DNFBP supervisor.

Additional administrative sanctions are also available for FIs for breaches of sector-specific requirements.

- Breaches of the KWG (which apply to credit and financial services institutions) are subject to an administrative fine depending on the nature of the breach. For natural persons, the fine may be up to EUR 5 million or, for legal persons, EUR 5 million or 10% of the annual revenue (KWG, s.56). These fines may be increased to ensure they exceed the economic benefit derived from the offence (KWG, s.56(6c)). Sanctions imposed under the KWG are published (KWG, s.60b(1)).
- Breaches of the ZAG (which apply to payment service and e-money providers) are subject to administrative fines of up to EUR 1 million (ZAG, s.64).

- Breaches of the KAGB (which apply to asset management services) are subject to administrative fines of up to EUR 5 million (KAGB, s.340(1)). Legal persons may incur fines of up to 10% of their annual revenue. Fines may be adjusted to ensure they exceed the economic benefit derived from the offence (KAGB, s.370(7)). Sanctions imposed under the KAGB are published (KAGB, s.341a).
- Breaches of the VAG (which apply to insurance undertakings (but not intermediaries)) are generally subject to administrative fines of up to EUR 200 000. Higher fines of up to EUR 5 million or 10% of annual revenue may be imposed on legal persons for serious, repeated, or systematic offending (VAG, s.332). Sanctions imposed under the VAG are published (VAG, s.319(1)). These sanctions do not apply to insurance intermediaries.
- Breaches of the GewO (which applies to insurance intermediaries) are generally subject to administrative fines of up to EUR 50 000. Persistent breaches may be sanctioned by up to one year imprisonment or a fine (GewO, s.144).

In respect of other AML/CFT requirements, breaches of the AO (see c.10.1 and c.11.1) are subject to an administrative fine of up to EUR 5 000, imposable by the tax authorities (AO, s.379). Breaches of the Commercial Code (see c.11.2) constitute a criminal offence punishable by imprisonment of up to two years or a fine (StGB, s.283b). Finally, breaches of the wire transfer requirements in R.16 (Regulation (EU) 2015/847) are subject to a fine of up to EUR 200 000 (KWG, ss.56(4), 56(6)).

**Criterion 35.2** – The administrative sanctions for preventive measures are applicable to natural persons provided the individual has extensive decision-making power in the relevant area and the necessary knowledge and skills (OWiG, s.9). This would generally cover authorised representatives, managers, or persons appointed to perform specific duties, but, depending on the circumstances, there may be situations where sanctions cannot be applied to FI or DNFBP directors or senior managers.

Breaches of the TFS obligations are subject to criminal sanctions for natural persons (see c.35.1(a)). Sanctions apply to any natural person who themselves breaches the freezing obligation (including on behalf of a FI or DNFBP) or who assists another to do so (AWG, s.18(1); StGB, ss.26, 27). Sanctions also apply to any natural person who is responsible for preventing such offending and knowingly, intentionally or foreseeably fails to do so, which would generally cover managers (StGB, s.13).

For NPOs, it is not clear that sanctions are equally applicable to authorised representatives, managers, or persons appointed to perform specific duties within NPOs that breach the relevant requirements (see c.8.4(b)).

### *Weighting and Conclusion*

Overall, Germany has measures in place to apply sanctions for non-compliance with AML/CFT measures. However, there are minor deficiencies in the applicability of NPO-related sanctions to natural persons. It is not always clear that sanctions are applicable to all FI and DNFBP directors and senior managers.

**Recommendation 35 is rated largely compliant.**

## Recommendation 36 – International instruments

In its previous MER, Germany was partially compliant with these requirements. The technical deficiencies were: gaps in the ML and TF offences and deficiencies in TFS requirements under UNSCR1373 in relation to EU-internals. Since the last MER, Germany has revised its laws to address these issues.

### Criterion 36.1 –

Germany has signed and ratified the Vienna, Palermo, Merida and TF Conventions (see the table below).

**Table A.1: Germany’s ratification of relevant international instruments**

International Instrument	Signed	Ratification
Vienna Convention 1988	19 Jan 1989	22 July 1993
TF Convention 1999	20 July 2000	17 June 2004
Palermo Convention 2000	12 Dec 2000	14 June 2006
Merida Convention 2003	9 Dec 2003	12 Nov 2014

### Criterion 36.2 –

Germany has implemented the Vienna and Palermo Conventions. Since the last assessment, Germany has also ratified and implemented the Merida Convention. However, some deficiencies remain with respect to the implementation of the TF Convention and the criminalisation of TF (see R.5).

## Weighting and Conclusion

Germany has implemented the Vienna, Palermo and Merida Conventions. Germany has largely implemented the TF Convention however some issues were identified with respect to its implementation of the TF Convention.

**Recommendation 36 is rated largely compliant.**

## Recommendation 37 - Mutual legal assistance

In its previous MER, Germany was largely compliant with these requirements due to technical deficiencies in the scope of mutual legal assistance (MLA) provided resulting from gaps in the ML offence.

**Criterion 37.1 –** Germany has a legal basis for the provision of a wide range of MLA, including all domestically available investigative powers and tools (see c.37.8, and R.4 and R.31): search, seizure, confiscation of proceeds of crime, taking of witness statements, production orders, telecommunications surveillance and all powers available in domestic investigations (Act on International Co-operation in Criminal Matters, *Gesetz über die internationale Rechtshilfe in Strafsachen* (IRG), s.59). This assistance can be provided with respect to proceedings for ML, predicate offences and TF, regardless of the existence of a treaty on the basis of provisions in the IRG. Reciprocity is generally not a requirement for MLA, but is required for certain forms of assistance: extradition on a non-treaty basis (IRG, s.5), realization, surrender and distribution of recovered assets (IRG, s.56b) and confiscation in a foreign state (IRG, s.71a).

Germany is a party to a number of bilateral and multilateral treaties that facilitates the mutual legal assistance process including the European Convention on Mutual Assistance in Criminal Matters and the First and Second Additional Protocols. The IRG supplements bilateral or multilateral treaties, by providing guidance in situations where the treaty is silent or unclear on an issue.

For requests from EU-members, co-operation is further facilitated by a number of EU instruments including the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. Germany has also implemented Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (EU EIO Directive) (IRG, ss.91a-91j). This enables more direct communication between regional authorities requesting and executing requests, standardised forms, enhanced requirements for communication and strict timeframes for assistance.

**Criterion 37.2** – Legal assistance in criminal matters is the responsibility of the federal government (GG, art.32). The designated central authority for receiving requests for mutual legal assistance in criminal matters is the Federal Ministry of Justice (BMJ) but this has been delegated to other authorities, primarily the Federal Office for Justice in Bonn (BfJ) and to the *Länder* prosecution offices (IRG, s.74(1)). Direct communication with officials in the *Länder* is also allowed with respect to requests from some countries (IRG, s.91a). In practice, the direct channel is used primarily for requests from EU-member member states but whether the diplomatic channels or direct communication to *Länder* authorities is used ultimately depends on the bilateral arrangements in place between Germany and the requesting country.

Germany has a decentralised model for decision making on international co-operation requests. The BMJ has delegated its decision-making authority to the Federal Office of Justice in Bonn (BfJ) and to the *Länder* authorities, including regional courts and public prosecution offices (IRG, ss.74(1), 74(2)). The delegation means that in practice, decisions are mostly made by the *Länder* authorities who would be responsible for executing the request according to the location of the assistance sought.

There are clear processes for the timely prioritisation and execution of requests (Guidelines on Relations with Foreign Countries in Criminal Law Matters (*Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten*) (RiVAST). Incoming requests for assistance must be processed within the time limits that apply for domestic investigations (RiVAST, para. 22(1)). Cases are prioritised based on factors such as the nature of the case and the time sensitive nature of the assistance sought. German authorities track the progress of MLA requests using a digital case management system which is run separately by each *Länder*. For requests from EU members with an EIO, specific deadlines are further set out in the law. For example, decisions on mutual assistance requests must be made within 30 days (IRG, s.91g(1)) and requests are to be executed within 90 days (IRG, s.91g(2)).

**Criterion 37.3** – Requests for assistance are not subject to unreasonable or unduly restrictive conditions. The grounds for denying a request depend on the assistance sought, and may include: the contravention of the rule of law or human dignity, the contravention of minimum standards of elementary constitutional justice under international law, the inalienable constitutional principles of public order in Germany, or elementary requirements under international law, with particular significance placed on ensuring the rule of law and the preservation of human dignity (IRG, s.73).

**Criterion 37.4** – Germany does not refuse requests solely on the basis that the offence includes fiscal matters (IRG, s.91(b)(2)) nor on the grounds of secrecy or confidentiality requirements on FIs or DNFBPs with the valid exception of information held by lawyers and notaries in their professional capacity providing services to clients which is subject to legal professional secrecy (IRG, s.73).

**Criterion 37.5** – Authorities are required to maintain the confidentiality of mutual legal assistance requests in accordance with the relevant multilateral conventions and bilateral treaties on mutual legal assistance. Civil servants at both the federal and *Länder* level are required to keep confidential all information they obtain in the course of their professional duties (Federal Civil Service Act, *Bundesbeamtengesetz* (BBG), s.67; Civil Servants Act, *Beamtenstatusgesetz* (BeamtStG), s.37). Breaches of this duty of confidentiality can constitute a criminal offence (StGB, s.353b).

**Criterion 37.6** – Dual criminality is only required for extradition conducted on a non-treaty basis (IRG, s.3(1)), assistance with enforcement actions (IRG, s.49(1)) and requests requiring coercive powers such as matters involving the seizure and surrender of property or for other measures of a coercive nature, such as intercepting communications (IRG, ss.66, 67, 91b(4)).

**Criterion 37.7** – Germany takes a conduct-based approach to dual criminality when it is required (see c.37.6). To satisfy the requirement, the foreign country's offence provisions do not need to be identical to the equivalent offence under German law. The dual criminality requirement is satisfied if the conduct constituting the offence is considered a crime had it occurred in Germany (e.g., IRG, s.3(1) for extraditions).

**Criterion 37.8** – Germany can utilise all the powers specified under R.31 which are available to domestic authorities in executing MLA requests. This includes:

- (a) The production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other natural or legal persons and the taking of witness statements (IRG, s.59); and
- (b) A broad range of other powers and investigative techniques such as communication surveillance and intercept.

### **Weighting and Conclusion**

All criteria are met.

**Recommendation 37 is rated compliant.**

### **Recommendation 38 – Mutual legal assistance: freezing and confiscation**

In its previous MER, Germany was largely compliant with these requirements due to technical limitations in the scope of MLA provided resulting from gaps in the ML offence and the inability to provide assistance with respect to non-conviction based confiscation orders. In 2017, Germany introduced a domestic non-conviction based asset confiscation regime that enables it to provide greater assistance with respect to foreign non-conviction based confiscation orders (see R.4).

**Criterion 38.1** – Germany has the authority to take expeditious action in response to foreign requests for assistance to identify, freeze, seize and confiscate criminal assets:

- (a) Laundered property can be identified on behalf of a requesting country using all the general powers available to German authorities' domestic cases including search,

seizure and production of information documents or evidence including financial records and taking of witness statements (IRG, ss.59, 66, 67).

Requests received from EU-countries are subject to time limits imposed by EU Regulation 2018/1805 and Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence and Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition of confiscation orders (IRG, ss. 88-90, 94). As of 19 December 2020, under the Regulation 2018/1805 scheme, if the issuing authority has stated that immediate freezing is necessary requests for freezing shall be accepted or rejected within 48 hours of receipt of the freezing certificate and the concrete measures necessary to execute the order be taken within 48 hours after such a decision has been taken. Requests for confiscation shall be accepted or rejected within 45 days of receipt of the confiscation certificate (Regulation 2018/1805, Articles 9(3) and 20(1)). Under the Council Framework Decision 2003/577/JHA scheme, requests for freezing shall be accepted or rejected within 24 hours of receipt of the freezing order (Council Framework Decision 2003/577/JHA, Article 5(3)).

**(b)** proceeds of crime **(c)** instrumentalities used in, or **(d)** instrumentalities intended for use in, ML, predicate offences or TF, or **(e)** property of corresponding value; can be identified, seized and restrained using the same mechanisms as set out in criterion 38.1(a).

**Criterion 38.2** – In 2017, Germany enacted legal reforms to allow for non-conviction based confiscation in German domestic matters. Using these new provisions, Germany can provide assistance to foreign countries in non-conviction based confiscation matters (IRG, s.48 and StGB, s.76a).

**Criterion 38.3** – German police forces (BKA and LKAs) co-ordinate on seizure and confiscation with requesting states via police-to-police arrangements and multilateral arrangements.<sup>121</sup> At the EU-level, Germany participates in the European Judicial Network and the EU Network of Asset Recovery Offices (AROs) to facilitate co-operation in cross-border asset recovery cases.

The management and disposal of seized and confiscated assets is handled at the *Länder* level by the public prosecution office but the responsibility can also be delegated to investigators, a bailiff or another appropriate person (StPO, ss.111k, 111m, 111p).

**Criterion 38.4** – Confiscated assets can be shared with other EU countries (IRG, s.88 and 56(b) and with non-EU countries under bilateral MLA treaties.)

### Weighting and Conclusion

All criteria are met.

**Recommendation 38 is rated compliant.**

<sup>121</sup> Germany is a member of the Camden Asset Recovery Network (CARIN) and the Stolen Assets Recovery Initiative (StAR)

## Recommendation 39 – Extradition

In its previous MER, Germany was rated largely compliant with these requirements due to technical limitations in the scope of cooperation provided in extradition matters resulting from gaps in the ML offence.

**Criterion 39.1** – Germany can execute extradition requests in relation to ML/TF without undue delay on the basis of a number of bilateral and multilateral treaties, or under the IRG in the absence of a treaty. EU requests are conducted under the European Convention on Extradition and European Arrest Warrant (EAW) regime which allows for a more streamlined extradition process.

**(a)** Both ML and TF are extraditable offences (IRG, s.3(2) and EAW Framework Decision, art.2(2)).

**(b)** A case management system exists at the *Länder*-level and clear processes are in place to facilitate the timely execution of extradition requests including the prioritisation of requests, for both EU and non-EU countries (see c.37.2).

**(c)** Germany does not place unreasonable to unduly restrictive conditions on the execution of requests (see c.37.3).

**Criterion 39.2** – Germany cannot extradite its nationals to non-EU countries (GG, art.16(2)). However, German nationals can be extradited to an EU member state provided that the requesting country returns the person to Germany to serve their sentence (IRG, s.80) in certain circumstances. In addition, German nationals can be extradited to an international criminal court (GG, art.16(2) IRG, s.9a), provided that the principles of the rule of law are observed.

In situations where a person cannot be extradited for reasons of nationality, German authorities are required to commence an investigation on any indictable offence (StPO, ss.152(2), 160, 163) and the prosecution proceeds under German law as if the offence occurred in Germany (StGB, s.7(2)).

**Criterion 39.3** – For requests within the EU, dual criminality is not a requirement if the alleged offence carries a maximum penalty of at least three years' imprisonment in the requesting country and is a listed offence under article 2 of the EAW Framework Decision.

While dual criminality is a mandatory requirement for extradition with non-EU countries, Germany takes a conduct-based approach and the only requirement is for the offence to also constitute an unlawful act under German law (IRG, s.3(1) – see c.37.7).

**Criterion 39.4** – German law provides for a simplified extradition procedure when the requested person consents to surrender (IRG, ss.78(1), 83(c)). For EU-level requests, the final extradition must be made within 10 days after the requested person consents to a simplified extradition process (IRG, ss.78(1), 83c).

## Weighting and Conclusion

All criteria are met.

**Recommendation 39 is rated compliant.**

## Recommendation 40 – Other forms of international co-operation

In its previous MER, Germany was largely compliant with these requirements due to deficiencies in the ML offence limiting the range of assistance that could be provided and limitations on the scope of assistance that could be provided due to professional secrecy obligations for some categories of DNFBPs.

**Criterion 40.1** – Competent authorities in Germany (the FIU, Federal Criminal Police Office (BKA), *Länder* Police Offices, Customs and tax authorities, BaFin and *Länder*-level supervisors are able to provide a wide range of assistance in international cases. Co-operation can be provided both spontaneously and upon request (Federal Criminal Police Office Act, *Bundeskriminalamtgesetz* (BKAG), ss.2, 3; GwG, ss.33, 34, 35, 55(1), 54(4)); Customs Investigation Service Act, *Zollfahndungsdienstgesetz* (ZFdG) ss.11, 11a, 34, 34a); Act on International Co-operation in Criminal Matters, IRG, ss.59, 74, 91, 92, 92a, 92b and 92c).

Co-operation between supervisory authorities is enabled under the Money Laundering Act (GwG) and allows authorities to co-operate with each other and also with foreign authorities as long as the co-operation is in line with German laws on privacy and data protection (GwG, s.54(3), 54(4), 55(1)).

While most international co-operation falling under this recommendation is co-ordinated at the federal level, laws at the *Länder*-level are in place to allow for direct law enforcement co-operation and information sharing between law enforcement agencies in the various *Länder* and their foreign counterparts (e.g., Police Act, *Polizeigesetz des Landes Nordrhein-Westfalen*, ss.28, 29 and the Bavarian Police Regulations Act, *Bayerisches Polizeiaufgabengesetz* (BayPAG), ss.57, 58).

### Criterion 40.2 –

**(a)** Competent authorities have a lawful basis for providing co-operation– see c.40.1 above;

**(b)** There does not appear to be any barriers to competent authorities (police prosecutors, FIU, Customs, BaFin and *Länder*-level supervisors) co-operating with foreign counterparts.

**(c)** Competent authorities have clear and secure gateways, mechanisms or channels to facilitate, transmit and execute requests for assistance. Co-operation occurs largely through: EU mechanisms (e.g. EUROPOL’s SIENA Platform, FIU.Net, and AFIS (Automated Fingerprint Identification System)); and international mechanisms: Interpol and the Egmont Secure Web. German competent authorities also work with a network of BKA liaison officers posted around the world who have their own system for information transmission to facilitate co-operation.

**(d)** Competent authorities with high volumes of international co-operation activity (BaFin, FIU, BKA and Customs), have established processes for prioritising requests. Other competent authorities, especially *Länder* level supervisors with very low volume of international co-operation activity process all requests as top priority.

**(e)** Competent authorities have clear processes for safeguarding information received. Provisions in the BKAG combine with the general provisions on data protection and to prevent unauthorised access and disclosures of sensitive government information. (Federal Data Protection Act, *Bundesdatenschutzgesetz* (BDSG), s.71; Federal Civil Service Act, *Bundesbeamtengesetz* (BBG), s.67).

**Criterion 40.3** – Some competent authorities (BaFin and the FIU) have a range of bilateral and multilateral agreements and MOUs to facilitate co-operation with foreign counterparts. Such agreements are not conducted by *Länder*-level supervisors as it is not necessary for providing assistance but can be established promptly if required by foreign authorities. However, it is not clear that all competent authorities (particularly *Länder*-level supervisors) have this capacity to act to pursue MOUs with foreign counterparts.

**Criterion 40.4** – Competent authorities are able to provide timely feedback to foreign authorities upon request.

**Criterion 40.5** – Germany does not prohibit or place unreasonably or unduly restrictive conditions on the provision of information or assistance when assistance is provided through MLA under the IRG or on an FIU to FIU basis. However, it is not clear that this would also apply in cases of international co-operation involving other competent authorities in Germany.

**Criterion 40.6** – Police and Customs authorities in Germany are required to use information obtained from foreign counterparts for the purposes for which the information was sought or provided (BKAG, s.27(7); ZFdG, s.34(4)). Financial intelligence is also protected under the same requirements (GwG, s.35(2) and (5)) as is information received by BaFin (KWG, s.9, VAG, s.309, Securities Trading Act, *Wertpapierhandelsgesetz*, s.21).

**Criterion 40.7** – Competent authorities are required to maintain appropriate confidentiality consistent with domestic requirements on privacy and data protection (Federal Data Protection Act, *Bundesdatenschutzgesetz* (BDSG), ss.78-81).

**Criterion 40.8** – Competent authorities (police, prosecutors, FIU and Customs) can conduct inquiries on behalf of foreign counterparts and exchange information obtained as a result: this includes LEAs (IRG, ss.59, 74; RiVSt, no.123(1) sentence 31) and the FIU (GwG, s.35(2)). Supervisory co-operation with other members of the EU is established in line with EU Directive 2015/849 and EU Regulation No.1093/2010 (GwG, s.55(6)). BaFin and other supervisory authorities can also conduct inquiries on behalf of non-EU counterpart supervisors subject to the establishment of a bilateral agreement and reciprocity (GwG, s.55(8)).

**Criterion 40.9** – The FIU has an adequate legal basis for providing co-operation in relation to ML, TF and predicate offences regardless of whether their counterpart FIU is administrative, law enforcement, judicial or other in nature (GwG, ss.33-35).

**Criterion 40.10** – The FIU can provide feedback to foreign counterparts, routinely and on request, including on the use of information shared and the outcome of any analysis conducted, but there is no requirement or clear processes ensuring this occurs in every case.

**Criterion 40.11** – The FIU is able to exchange (a) information which it can access or obtain directly or indirectly as required by R.29, and (b) any other information which it can obtain or access, directly or indirectly, at the domestic level (GwG, s.35(2)). Where the exchange involves information from other domestic authorities the FIU must seek the competent authorities' approval prior to sharing it.

**Criterion 40.12** – BaFin and other financial supervisors, have a legal basis for co-operating with their foreign counterparts (GwG, ss.50, 54, 55). BaFin is the main financial supervisor and has responsibility for supervising all FIs with the exception

of the insurance sector where *Länder* authorities also play a role in supervising insurance undertakings.

**Criterion 40.13** – Financial supervisors are able to exchange domestically available information with foreign counterparts, including information held by financial institutions subject to complying with conditions on data protection and confidentiality and the conclusion of a bilateral agreement (for co-operation with non-EU countries) (GwG, ss.54, 55).

**Criterion 40.14** – Financial supervisors can exchange any regulatory, prudential and AML/CFT information they hold, to the extent outlined in c.40.12 above and pursuant to the following legal provisions: GwG, ss.54, 55; VAG, s.309(5)(2); KWG, s.9(1)).

**Criterion 40.15** – Financial supervisors are able to exercise domestic powers and conduct inquiries on behalf of overseas regulators, including conducting investigations and obtaining information or documents (GwG, s.55). However, for non-EU countries, co-operation is contingent on reciprocity and the conclusion of a bilateral agreement (GwG, s.55(8)).

**Criterion 40.16** – Financial supervisors must obtain the authorisation of the foreign supervisory authority to disclose confidential information received from the foreign counterpart (GwG, s.54(4)).

**Criterion 40.17** – Law enforcement authorities (police, prosecutors, courts, customs and tax and revenue collection agencies) are able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to ML, TF and predicate offending, including the identification and tracing of proceeds and instrumentalities of crime (IRG, ss.61a, 92, 92c).

**Criterion 40.18** – Law enforcement authorities are able to conduct inquiries and use domestically available coercive and non-coercive powers in support of a request from a foreign counterpart. Germany is part of the European Judicial Network in criminal matters, CARIN, the network of EU asset recovery offices (AROs), Eurojust, Europol and Interpol and uses these frameworks as the basis for co-operation.

**Criterion 40.19** – Law enforcement authorities in Germany are able to form joint investigative teams (JITs) for the purpose of conducting a criminal investigation under domestic legal provisions (IRG, ss.61b, 93, RiVSt, para. 142c) and several multilateral treaties including the Vienna, Palermo and Merida Conventions.

**Criterion 40.20** – Most authorities in Germany (Financial Intelligence Unit, police, Customs, BaFin and other supervisors) can exchange information indirectly with non-counterparts on a domestic and international level for specified purposes (GwG ss.35, 54, 55; BKAG, s.3, ZFdG, ss.34, 34a).

### *Weighting and Conclusion*

International co-operation arrangements are in place in Germany and the FIU, law enforcement agencies and BaFin can provide a wide range of assistance in international cases. However, minor deficiencies remain: apart from the FIU and BaFin there is also no clear authority for other agencies to enter into MOUs when required and apart from the FIU or under MLA, there are no legal provisions to ensure competent authorities do not prohibit or place unreasonably or unduly restrictive conditions on the provision of assistance.

**Recommendation 40 is rated largely compliant.**

## Annex A. Länder supervisors of DNFBPs

Sector	<i>Länder</i>	Designated competent authority	Relevant legislative reference
Real estate agents	Baden-Württemberg	4 District Governments (Stuttgart, Karlsruhe, Freiburg, Tübingen)	Verordnung des Innenministeriums über Zuständigkeiten nach dem Geldwäschegesetz vom 7. Januar 2010
	Bavaria	2 District Governments (Niederbayern, Mittelfranken)	Zuständigkeitsverordnung (ZustV) vom 16. Juni 2015 (GVBl. S. 184, BayRS 2015-1-1-V),
	Berlin	Senate Department for Economics, Energy and Public Enterprises Berlin	Gesetz über die Zuständigkeiten in der Allgemeinen Berliner Verwaltung (Allgemeines Zuständigkeitsgesetz - AZG) in der Fassung vom 22. Juli 1996
	Brandenburg	Ministry for Economic Affairs, Labour and Energy Brandenburg	Geldwäschezuständigkeitsverordnung vom 13. August 2012 (GVBl. II Nr. 71)
	Bremen	Senator for Economy, Labour and Europe Bremen	Bekanntmachung über die nach dem Geldwäschegesetz zuständigen Behörden
	Hamburg	Authority for Economy and Innovation Hamburg	Anordnung zur Durchführung des Geldwäschegesetzes vom 23. Juni 2017
	Hesse	3 District Governments (Regierungspräsidien Darmstadt, Gießen, Kassel)	Zuständigkeiten nach dem Geldwäschegesetz vom 2. Dezember 2014 (GVBl. 2014, S. 330)
	Lower Saxony	Counties/independent cities	Verordnung über Zuständigkeiten auf dem Gebiet des Wirtschaftsrechts sowie in anderen Rechtsgebieten (ZustVO-Wirtschaft) vom 18. November 2004
	Mecklenburg Western-Pomerania	Ministry of Economics, Employment and Health Mecklenburg-West Pomerania	Landesverordnung zur Übertragung der Zuständigkeiten nach dem Geldwäschegesetz (GwGZust-LVO) vom 22. Februar 2011
	Nord Rhine-Westphalia	5 District Governments (Bezirksregierungen Arnsberg, Detmold, Düsseldorf, Köln, Münster)	Verordnung zur Übertragung von Ermächtigungen, zur Regelung von Zuständigkeiten und Festlegungen auf dem Gebiet des Gewerberechts (Gewerberechtsverordnung - GewRV NRW)
	Rhineland Palatinate	Counties/independent cities	Landesverordnung über Zuständigkeiten nach dem Geldwäschegesetz (GwGZuVO) vom 4. Mai 2011
	Saarland	State Office (Landesverwaltungsamt Saarland)	Verordnung über Zuständigkeiten nach dem Geldwäschegesetz vom 11. September 2019
	Saxony	State Office (Landesverwaltungsamt Sachsen)	Verordnung des Sächsischen Staatsministeriums für Wirtschaft, Arbeit und Verkehr zur Bestimmung von Zuständigkeiten nach dem Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Sächsische Geldwäschegesetz-Zuständigkeitsverordnung – SächsGwGZustVO)
	Saxony-Anhalt	State Office (Landesverwaltungsamt Saxony-Anhalt)	Verordnung über die Regelung von Zuständigkeiten im Immissionsschutz-, Gewerbe- und Arbeitsschutzrecht sowie in anderen Rechtsgebieten

	Schleswig Holstein	Ministry of Finance Schleswig-Holstein	Landesverordnung zur Bestimmung der für die Durchführung des Geldwäschegesetzes zuständigen Behörde für bestimmte Verpflichtete
	Thuringia	State Office (Thüringer Landesverwaltungsamt)	Thüringer Zuständigkeitsermächtigungsverordnung Gewerbe - ThürZustErmGeVO
Dealers in goods (including precious metals and stones)	Baden-Württemberg	4 District Governments (Stuttgart, Karlsruhe, Freiburg, Tübingen)	Verordnung des Innenministeriums über Zuständigkeiten nach dem Geldwäschegesetz vom 7. Januar 2010
	Bavaria	2 District Governments (Niederbayern, Mittelfranken)	Zuständigkeitsverordnung (ZustV) vom 16. Juni 2015 (GVBl. S. 184, BayRS 2015-1-1-V),
	Berlin	Senate Department for Economics, Energy and Public Enterprises Berlin	Gesetz über die Zuständigkeiten in der Allgemeinen Berliner Verwaltung (Allgemeines Zuständigkeitsgesetz - AZG) in der Fassung vom 22. Juli 1996
	Brandenburg	Ministry for Economic Affairs, Labour and Energy Brandenburg	Geldwäschezuständigkeitsverordnung vom 13. August 2012 (GVBl. II Nr. 71)
	Bremen	Senator for Economy, Labour and Europe Bremen	Bekanntmachung über die nach dem Geldwäschegesetz zuständigen Behörden
	Hamburg	Authority for Economy and Innovation Hamburg	Anordnung zur Durchführung des Geldwäschegesetzes vom 23. Juni 2017
	Hesse	3 District Governments (Regierungspräsidien Darmstadt, Gießen, Kassel)	Zuständigkeiten nach dem Geldwäschegesetz vom 2. Dezember 2014 (GVBl. 2014, S. 330)
	Lower Saxony	Counties and independent cities (Landkreise und kreisfrei Städte)	Verordnung über Zuständigkeiten auf dem Gebiet des Wirtschaftsrechts sowie in anderen Rechtsgebieten (ZustVO-Wirtschaft) vom 18. November 2004
	Mecklenburg Western-Pomerania	Ministry of Economics, Employment and Health Mecklenburg-West Pomerania	Landesverordnung zur Übertragung der Zuständigkeiten nach dem Geldwäschegesetz (GwGZust-LVO) vom 22. Februar 2011
	Nord Rhine-Westphalia	5 District Governments (Bezirksregierungen Arnsberg, Detmold, Düsseldorf, Köln, Münster)	Verordnung zur Übertragung von Ermächtigungen, zur Regelung von Zuständigkeiten und Festlegungen auf dem Gebiet des Gewerberechts (Gewerberechtsverordnung - GewRV NRW)
	Rhineland Palatinate	Counties and independent cities (Landkreise und kreisfrei Städte)	Landesverordnung über Zuständigkeiten nach dem Geldwäschegesetz (GwGZuVO) Vom 4. Mai 2011
	Saarland	State Office (Landesverwaltungsamt Saarland)	Verordnung über Zuständigkeiten nach dem Geldwäschegesetz vom 11. September 2019
	Saxony	State Office (Landesverwaltungsamt Sachsen)	Verordnung des Sächsischen Staatsministeriums für Wirtschaft, Arbeit und Verkehr zur Bestimmung von Zuständigkeiten nach dem Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Sächsische Geldwäschegesetz-Zuständigkeitsverordnung - SächsGwGZustVO)
	Saxony-Anhalt	State Office (Landesverwaltungsamt Saxony-Anhalt)	Verordnung über die Regelung von Zuständigkeiten im Immissionsschutz-, Gewerbe- und Arbeitsschutzrecht sowie in anderen Rechtsgebieten
Schleswig Holstein	Ministry of Finance Schleswig-Holstein	Landesverordnung zur Bestimmung der für die Durchführung des Geldwäschegesetzes zuständigen Behörde für bestimmte Verpflichtete	
Thuringia	State Office (Thüringer Landesverwaltungsamt)	Thüringer Zuständigkeitsermächtigungsverordnung Gewerbe - ThürZustErmGeVO	

Legal profession (lawyers and tax advisors)	Baden-Württemberg	4 bar associations and 3 chambers of tax advisors	GwG, s.50, no.3 and 4
	Bavaria	3 bar associations and 2 chambers of tax advisors	
	Berlin	Bar Association Berlin and Chamber of Tax Advisors Berlin	
	Brandenburg	Bar Association Brandenburg and Chamber of Tax Advisors Brandenburg	
	Bremen	Bar Association Bremen and Chamber of Tax Advisors Bremen	
	Hamburg	Bar Association Hamburg and Chamber of Tax Advisors Hamburg	
	Hesse	2 bar associations and Chamber of Tax Advisors Hesse	
	Lower Saxony	3 bar associations and Chamber of Tax Advisors Lower Saxony	
	Mecklenburg Western-Pomerania	Mecklenburg Western Pomerania Bar Association and Mecklenburg Western Pomerania Chamber of Tax Advisors	
	Nord Rhine-Westphalia	3 bar associations and 3 chambers of tax advisors	
	Rhineland Palatinate	2 bar associations and chamber of tax advisors Rhineland Palatinate	
	Saarland	Saarland Bar Association and Saarland Chamber of Tax Advisors	
	Saxony	Saxony Bar Association and Saxony Chamber of Tax Advisors	
	Saxony-Anhalt	Saxony-Anhalt Bar Association and Saxony-Anhalt Chamber of Tax Advisors	
Schleswig Holstein	Schleswig Holstein Bar Association and Schleswig Holstein Chamber of tax Advisors		
Thuringia	Thuringia Bar Association and Thuringia Chamber of Tax Advisors		
Notaries	Baden-Württemberg	17 regional courts	GwG, s.50, no.5
	Bavaria	22 regional courts	
	Berlin	Berlin Regional Court	
	Brandenburg	4 regional courts	
	Bremen	Bremen Regional Court	
	Hamburg	Hamburg Regional Court	

	Hesse	9 regional courts	
	Lower Saxony	11 regional courts	
	Mecklenburg Western-Pomerania	4 regional courts	
	Nord Rhine-Westphalia	19 regional courts	
	Rhineland Palatinate	8 regional courts	
	Saarland	Saarland Regional Court	
	Saxony	5 regional courts	
	Saxony-Anhalt	4 regional courts	
	Schleswig Holstein	4 regional courts	
	Thuringia	4 regional courts	
Accountants	Baden-Württemberg	Federal Chamber of Accountants	GwG, s.50, no.6
	Bavaria		
	Berlin		
	Brandenburg		
	Bremen		
	Hamburg		
	Hesse		
	Lower Saxony		
	Mecklenburg Western-Pomerania		
	Nord Rhine-Westphalia		
	Rhineland Palatinate		
	Saarland		
	Saxony		
	Saxony-Anhalt		
	Schleswig Holstein		
	Thuringia		
TCSPs (not covered as lawyers, tax advisors, or accountants)	Baden-Württemberg	4 District Governments (Stuttgart, Karlsruhe, Freiburg, Tübingen)	Verordnung des Innenministeriums über Zuständigkeiten nach dem Geldwäschegesetz vom 7. Januar 2010
	Bavaria	2 District Governments (Niederbayern, Mittelfranken)	Zuständigkeitsverordnung (ZustV) vom 16. Juni 2015 (GVBl. S. 184, BayRS 2015-1-1-V),
	Berlin	Senate Department for Economics, Energy and Public Enterprises Berlin	Gesetz über die Zuständigkeiten in der Allgemeinen Berliner Verwaltung (Allgemeines Zuständigkeitsgesetz - AZG) in der Fassung vom 22. Juli 1996
	Brandenburg	Ministry for Economic Affairs, Labour and Energy Brandenburg	Geldwäschezuständigkeitsverordnung vom 13. August 2012 (GVBl. II Nr. 71)
	Bremen	Senator for Economy, Labour and Europe Bremen	Bekanntmachung über die nach dem Geldwäschegesetz zuständigen Behörden
	Hamburg	Authority for Economy and Innovation	Anordnung zur Durchführung des Geldwäschegesetzes vom

		Hamburg	23. Juni 2017
	Hesse	3 District Governments (Regierungspräsidien Darmstadt, Gießen, Kassel)	Zuständigkeiten nach dem Geldwäschegesetz vom 2. Dezember 2014 (GVBl. 2014, S. 330)
	Lower Saxony	Counties and independent cities	Verordnung über Zuständigkeiten auf dem Gebiet des Wirtschaftsrechts sowie in anderen Rechtsgebieten (ZustVO-Wirtschaft) vom 18. November 2004
	Mecklenburg Western-Pomerania	Ministry of Economics, Employment and Health Mecklenburg-West Pomerania	Landesverordnung zur Übertragung der Zuständigkeiten nach dem Geldwäschegesetz (GwGZust-LVO) vom 22. Februar 2011
	Nord Rhine-Westphalia	5 District Governments (Bezirksregierungen Arnsberg, Detmold, Düsseldorf, Köln, Münster)	Verordnung zur Übertragung von Ermächtigungen, zur Regelung von Zuständigkeiten und Festlegungen auf dem Gebiet des Gewerberechts (Gewerberechtsverordnung - GewRV NRW)
	Rhineland Palatinate	State Office (Aufsichts und Dienstleistungsdirektion Trier)	Landesverordnung über Zuständigkeiten nach dem Geldwäschegesetz (GwGZuVO) vom 4. Mai 2011
	Saarland	State Office (Landesverwaltungsamt Saarland)	Verordnung über Zuständigkeiten nach dem Geldwäschegesetz vom 11. September 2019
	Saxony	State Office (Landesverwaltungsamt Sachsen)	Verordnung des Sächsischen Staatsministeriums für Wirtschaft, Arbeit und Verkehr zur Bestimmung von Zuständigkeiten nach dem Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Sächsische Geldwäschegesetz-Zuständigkeitsverordnung - SächsGwGZustVO)
	Saxony-Anhalt	State Office (Landesverwaltungsamt Saxony-Anhalt)	Verordnung über die Regelung von Zuständigkeiten im Immissionsschutz-, Gewerbe- und Arbeitsschutzrecht sowie in anderen Rechtsgebieten
	Schleswig Holstein	Ministry of Finance Schleswig-Holstein	Landesverordnung zur Bestimmung der für die Durchführung des Geldwäschegesetzes zuständigen Behörde für bestimmte Verpflichtete
	Thuringia	State Office (Thüringer Landesverwaltungsamt)	Thüringer Zuständigkeitsermächtigungsverordnung Gewerbe - ThürZustErmGeVO
Casinos	Baden-Württemberg	District Government (Regierungspräsidium Karlsruhe)	GwG, s.50, no.8
	Bavaria	Bavarian State Ministry of the Interior, for Sport and Integration	
	Berlin	Senate Administration for the Interior and Sports Berlin	
	Brandenburg	Ministry of the Interior Brandenburg	
	Bremen	Senator of the Interior Bremen	
	Hamburg	Authority of the Interior and Sports Hamburg	
	Hesse	Ministry of the Interior Hesse	
	Lower Saxony	Ministry of Finance Lower Saxony	
	Mecklenburg Western-Pomerania	Ministry of the Interior Mecklenburg-Western Pomerania	
	Nord Rhine-	District Governments	

Westphalia	(Bezirksregierungen Arnsberg, Düsseldorf, Köln, Münster, Detmold)
Rhineland Palatinate	State Office (Aufsichts und Dienstleistungsdirektion Trier)
Saarland	Ministry of the Interior Saarland
Saxony	State Office (Landesverwaltungsamt Sachsen)
Saxony- Anhalt	State Office (Landesverwaltungsamt Saxony-Anhalt)
Schleswig Holstein	Ministry of the Interior Schleswig-Holstein
Thuringia	Ministry of the Interior Thuringia

## Annex B. Overview of Germany's obliged non-financial sector

Type of DNFBP	Number of obliged entities
Lawyers (2020)	Approx. 36 791*
Notaries (2020)	6 912
Tax advisors (2020)	86 625
Accountants (2020)	14 758
Gambling provider (2020)	19 168
Land-based casinos	28
State-owned Land lottery company	14 259
Land-based sports betting	4 394
Land-based horse betting	63
Online horse betting	7
Online sports betting	137
Illegal online gambling	226
Online sports betting Schleswig-Holstein	7
Online gambling Schleswig-Holstein	11
Real estate agents (2017)	30 324
All traders in goods (2017)	Approx. 800 000
Traders in goods boats and yachts	467
Traders in goods motor vehicles	42 829
Traders in goods watches/ jewellery/precious metals (include DPMS)	7 993
Traders in goods art and antiques	8 327
TCSPs	Unknown

Note: \* Lawyers are obliged entities only where conducting certain transactions and the number changes in any given year. The number of obliged entity lawyers for 2020 is based on an estimate by legal supervisors that 22% of all lawyers conduct such transactions.

## Summary of Technical Compliance – Key Deficiencies

### Compliance with FATF Recommendations

Recommendation	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	LC	<ul style="list-style-type: none"> <li>It is not clear that there is a whole-of-government approach or if authorities at the <i>Länder</i>-level allocate resources and implement measures to prevent and mitigate ML/TF (c.1.5).</li> <li>Certain VASPs are temporarily exempt from requirements relating to virtual asset transfers for pragmatic, rather than risk-based reasons (c.1.6).</li> <li>The list of low-risk factors that FIs and DNFBPs should consider in applying simplified due diligence includes factors that are not based on an assessment of risk (c.1.8).</li> <li>There are some limitations in the risk-based approach applied by <i>Länder</i>-level supervisors (c.1.9 &amp; c.1.12).</li> </ul>
2. National co-operation and coordination	LC	<ul style="list-style-type: none"> <li>The Steering Committee for Combating ML/TF (RÜST GW/TF) does not include all stakeholders that are responsible for implementation of AML/CFT measures (as only two <i>Länder</i> representatives participate) and does not have binding authority (c.2.2).</li> <li>Operational and policy co-ordination mechanisms exist, but do not include all relevant stakeholders (notably the FIU) (c.2.3).</li> <li>There are no formal mechanisms for law enforcement co-ordination on ML (c.2.3).</li> <li>Supervisory co-operation mechanisms do not always include all relevant supervisors, and DNFBP supervisors of some sectors have no co-ordination mechanisms (c.2.3).</li> <li>Mechanisms for PF co-operation are focused on TFS, rather than broader PF issues (c.2.4).</li> </ul>
3. Money laundering offences	C	All criteria are met.
4. Confiscation and provisional measures	C	All criteria are met.
5. Terrorist financing offence	LC	<ul style="list-style-type: none"> <li>Germany's TF offences an intention to "seriously intimidate the public" which is not permitted for the Convention's annex offences (c.5.1).</li> <li>Germany's TF offences do not extend to cover financing of an individual terrorist for any purpose because the offender must know or intend for the funds to be used for an offence (c.5.2 and c.5.4).</li> </ul>
6. Targeted financial sanctions related to terrorism & TF	PC	<ul style="list-style-type: none"> <li>The process for identifying and proposing targets for designation is not documented (c.6.1(b) &amp; c.6.2(b)).</li> <li>There is no requirement or process to ensure prompt determination of requests for designation received by Germany or the EU (c.6.2(c)).</li> <li>There is no EU or national procedure for requesting non-EU countries to give effect to EU designations or domestic freezing/prohibition orders under the AWG (c.6.2(e)).</li> <li>There is no legal authority or domestic framework that entitles the Ressortkreis to solicit the necessary information to identify potential targets for designation (c.6.3(a)).</li> <li>As AWG orders cannot be issued on weekends or holidays, there will be a delay in implementation of UNSCR 1267 designations issued immediately prior to weekends or holidays (c.6.4).</li> <li>For EU 1373 regime does not require the freezing of assets of "EU internals" and the national framework is limited in application (c.6.5(a)).</li> <li>At the EU level, the definition of assets does not explicitly cover jointly-owned assets or funds or assets controlled by, indirectly owned by, derived from assets owned by, or owned by a person acting at the direction of a designated person or entity (c.6.5(b)).</li> <li>Mechanisms to immediately communicate new listings or de-listings do not apply to all FIs or DNFBPs (c.6.5(d) &amp; c.6.5(g)).</li> <li>There is no obligation for FIs and DNFBPs to report assets frozen in accordance with orders under the AWG (c.6.5(e)).</li> </ul>

7. Targeted financial sanctions related to proliferation	PC	<ul style="list-style-type: none"> <li>As AWG orders cannot be issued on weekends or holidays, there will be a delay in implementation of proliferation-related TFS designations issued immediately prior to weekends or holidays (c.7.1).</li> <li>At the EU level, the definition of assets does not explicitly cover jointly-owned assets or funds or assets of persons acting on behalf or at the direction of a designated person or entity (c.7.2(b)).</li> <li>Mechanisms to immediately communicate new listings or de-listings do not apply to all FIs or DNFBPs (c.7.2(d) &amp; c.7.4(d)).</li> <li>There is no obligation for FIs and DNFBPs to report assets frozen in accordance with orders under the AWG (c.7.2(e)).</li> </ul>
8. Non-profit organisations	LC	<ul style="list-style-type: none"> <li>Germany has not worked with NPOs to develop best practices to address identified TF risks and vulnerabilities (c.8.2(c)).</li> <li>Germany has not encouraged NPOs to conduct transactions via regulated financial channels (c.8.2(d)).</li> <li>Measures for associations that do not seek non-profit status are not fully in line with risks (c.8.3).</li> <li>There is a very minor gap in oversight for associations that do not seek non-profit status where there is no indication of extremism (c.8.4(a)).</li> <li>Administrative sanctions do not apply to all those acting on behalf of an NPO (c.8.4(b)).</li> <li>Information-sharing mechanisms do not always include the FIU or administrative monitoring bodies (such as registrars) (c.8.5(a)).</li> <li>There is no formal mechanism or established reporting channel for registrars to share suspicions with law enforcement (c.8.5(d)).</li> </ul>
9. Financial institution secrecy laws	C	All criteria are met.
10. Customer due diligence	LC	<ul style="list-style-type: none"> <li>There is no requirement that verification of the beneficial owner must use information or data from a reliable source and there is a limited requirement that identification and verification processes are sufficient to satisfy the FI that it knows who the BO is (c.10.5).</li> <li>The requirement to take adequate measures to understand the customer's ownership and control structure does not apply to legal arrangements (c.10.8).</li> <li>FIs are not required to obtain the information set out in c.10.9 for legal arrangements, and, for legal persons, there is no explicit obligation to obtain the names of senior managers or the address of the principal place of business (where different to the head office) (c.10.9).</li> <li>Insurance intermediaries are not required to obtain information on the characteristics or categories used to designate beneficiaries for beneficiaries designated by characteristics/class, and there is no requirement that verification of identity occur no later than the time of payout (c.10.12).</li> <li>There is no specific requirement for FIs to include the beneficiary of a life insurance policy as a relevant risk factor for enhanced due diligence and insurance intermediaries are not subject to all of the insurance-specific CDD requirements (c.10.13).</li> <li>When applying CDD to existing customers, there is no explicit obligation to take into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained (c.10.16).</li> <li>The list of low-risk factors that FIs must consider in applying simplified due diligence includes factors that are not based on an assessment of risk (c.10.18).</li> <li>Where CDD cannot be completed, the requirement to consider filing a STR is in non-binding guidance (c.10.19).</li> <li>There is no explicit provision allowing entities to omit CDD and file a STR where they believe that the CDD process would tip-off the customer (c.10.20).</li> </ul>
11. Record keeping	C	All criteria are met.
12. Politically exposed persons	LC	<ul style="list-style-type: none"> <li>The requirement to establish source of funds would not always cover source of wealth (c.12.1).</li> <li>It is not clear that PEPs requirements apply to extended family members or close social associates (c.12.3).</li> <li>Insurance intermediaries are not subject to the life insurance-specific obligations where their customer is a PEP (c.12.4).</li> </ul>
13. Correspondent banking	PC	<ul style="list-style-type: none"> <li>There is no obligation for FIs to determine and document all AML/CFT responsibilities of third-country respondent institution (e.g., record-keeping, suspicious transaction reporting) (c.13.1).</li> <li>Mandatory enhanced due diligence measures for correspondent banking relationships apply only to respondent institutions outside the EEA (c.13.1).</li> </ul>

14. Money or value transfer services	LC	<ul style="list-style-type: none"> <li>There is no specific obligation to include agents in the principle's AML/CFT programme or to monitor their ongoing compliance (c.14.5).</li> </ul>
15. New technologies	LC	<ul style="list-style-type: none"> <li>It is not explicit that an FI's update of its risk assessment must occur prior to the launch or use of new products, practices and technologies (c.15.2(a)).</li> <li>Germany's risk assessment of VASPs is not yet fully comprehensive, which limits its ability to counter misuse (c.15.3).</li> <li>AML/CFT guidance specific to VASPs is somewhat limited (c.15.7).</li> <li>Sanctions may not always apply to VASP's directors and senior management (c.15.8(b)).</li> <li>Certain VASPs are exempted from the travel rule during a transitional period (c.15.9(b)).</li> </ul>
16. Wire transfers	C	All criteria are met.
17. Reliance on third parties	LC	<ul style="list-style-type: none"> <li>There is no specific requirement that an FI must satisfy itself that a third party is regulated, supervised, and has measures in place for compliance with R.10 and 11, nor is there clear guidance on this (c.17.1).</li> <li>Reliance on third-parties that are established in an EU Member State is not based on an assessment of the level of country risk (c.17.2 &amp; c.17.3).</li> </ul>
18. Internal controls and foreign branches and subsidiaries	LC	<ul style="list-style-type: none"> <li>Insurance intermediaries are not always required to include an internal audit in their ML/TF risk management systems (c.18.1).</li> </ul>
19. Higher-risk countries	C	All criteria are met.
20. Reporting of suspicious transaction	C	All criteria are met.
21. Tipping-off and confidentiality	C	All criteria are met.
22. DNFBNs: Customer due diligence	LC	<ul style="list-style-type: none"> <li>Minor deficiencies identified in R.12, 15 and 17 apply equally to DNFBNs (c.22.3, c.22.4 &amp; c.22.5).</li> </ul>
23. DNFBNs: Other measures	C	All criteria are met.
24. Transparency and beneficial ownership of legal persons	PC	<ul style="list-style-type: none"> <li>The risk assessment does not fully assess the risks associated with legal persons created in Germany and there was limited input from operational authorities (c.24.2).</li> <li>Not all legal persons are required to register basic information, information collected across different registers is inconsistent and not all information is made publicly available (c.24.3).</li> <li>Not all legal persons are required to collect and maintain information on shareholders or BO or records (c.24.4, c.24.6 &amp; c.24.9).</li> <li>No obligation to provide accurate and timely updates to basic and BO information (c.24.5 &amp; c.24.7)</li> <li>There are no specific measures requiring a natural person resident in the country to be accountable to competent authorities for providing basic or beneficial ownership information for legal persons (c.24.8).</li> <li>LEAs do not have direct access to BO information through the Electronic Account Retrieval System which can cause delays in getting access to information (c.24.10).</li> <li>Nominee shares and nominee directors are not prohibited and there are only partial measures in place to ensure they are not misused (c.24.12).</li> <li>There are sanctions in place for non-compliance with obligations with respect to the Transparency Register but no similar sanctions apply for compliance with the directory of foundations (c.24.13).</li> <li>There is no centralized system for monitoring international cooperation requests and formal MLA requests are required to obtain a significant amount of basic and BO information (c.24.14 &amp; 24.15).</li> </ul>
25. Transparency and beneficial ownership of legal arrangements	LC	<ul style="list-style-type: none"> <li>The regulatory regime does not extend to trust-like structures (c.25.1).</li> <li>There is an obligation to update information on the Transparency Register without delay but there is no guidance on what this means and there is only ad hoc verification of information filed on the Register (c.25.2).</li> <li>Information held on the Transparency Register can only be shared with foreign countries via a mutual legal assistance request which can impeded the provision of rapid assistance (c.25.6).</li> </ul>
26. Regulation and supervision of financial institutions	LC	<ul style="list-style-type: none"> <li><i>Länder</i> supervisors (of insurance companies and intermediaries) are not required to take into account the factors specified in c.26.5 in applying a risk-based approach (c.26.5).</li> </ul>
27. Powers of supervisors	C	All criteria are met.
28. Regulation and supervision of DNFBNs	LC	<ul style="list-style-type: none"> <li>Measures to prevent criminals or their associates from being professionally accredited generally focus on the applicant, operator and/or manager of the entity; there are limited proactive checks for TCSPs; and limited measures for criminals' associates c.28.4(b).</li> </ul>

		<ul style="list-style-type: none"> <li>Supervisory activity (outside of inspections) does not explicitly need to be based on risk profile and there is no model guidance or similar document to ensure a consistent risk-based approach across all DNFBP supervisors (c.28.5).</li> </ul>
29. Financial intelligence units	C	All criteria are met.
30. Responsibilities of law enforcement and investigative authorities	C	All criteria are met.
31. Powers of law enforcement and investigative authorities	C	All criteria are met.
32. Cash couriers	C	All criteria are met.
33. Statistics	PC	<ul style="list-style-type: none"> <li>There are no clear ML investigation statistics and ML is not always recorded in prosecution statistics. TF investigations and prosecutions are not counted distinct from terrorism offences (c.33.1(b)).</li> <li>Data and statistics on asset confiscation do not capture information on asset repatriation or the predicate offence generating the proceeds (c.33.1(c)).</li> <li>There is no central data or uniform statistics kept on mutual legal assistance cases (c.33.1(d)).</li> </ul>
34. Guidance and feedback	LC	<ul style="list-style-type: none"> <li>It is not clear that sufficient guidance and feedback is provided to FIs not supervised by BaFin (certain insurance undertakings and insurance intermediaries).</li> </ul>
35. Sanctions	LC	<ul style="list-style-type: none"> <li>Sanctions for natural persons related to breaches of requirements by NPOs are limited (c.35.1).</li> <li>There may be situations where sanctions cannot be applied to FI or DNFBP directors or senior managers (c.35.2).</li> </ul>
36. International instruments	LC	<ul style="list-style-type: none"> <li>Some issues were identified with respect to its implementation of the TF Convention (c.36.2).</li> </ul>
37. Mutual legal assistance	C	All criteria are met.
38. Mutual legal assistance: freezing and confiscation	C	All criteria are met.
39. Extradition	C	All criteria are met.
40. Other forms of international cooperation	LC	<ul style="list-style-type: none"> <li>Apart from the FIU and BaFin, there is also no clear authority for other agencies to enter into MOUs with foreign counterparts when required (c.40.3).</li> <li>Apart from the FIU or under MLA, there are no legal provisions to ensure competent authorities do not prohibit or place unreasonably or unduly restrictive conditions on the provision of assistance (c.40.5).</li> </ul>

## Glossary of Acronyms<sup>122</sup>

AA	Federal Foreign Office
AFCA	Anti Financial Crime Alliance
AFIS	Automated Fingerprint Identification System
AG	Stock corporations, <i>Aktiengesellschaft</i>
AktG	Stock Corporation Act, <i>Aktiengesetz</i>
AMLD	EU AML Directive
AMSLC	European Supervisory Authorities' Joint Committee Sub-Committee on Anti-Money Laundering
AO	Fiscal Code, <i>Abgabenordnung</i>
AWG	Foreign Trade and Payments Act, <i>Außenwirtschaftsgesetz</i>
BAKIS	BaFin risk assessment system
BBG	Federal Civil Service Act, <i>Bundesbeamtengesetz</i>
BDSG	Federal Data Protection Act, <i>Bundesdatenschutzgesetz</i>
BfJ	Federal Office of Justice
BfV	Federal Office for the Protection of the Constitution
BGB	Civil Code, <i>Bürgerliches Gesetzbuch</i>
BKA	Federal Criminal Police Office
BKAG	Federal Criminal Police Office Act, <i>Bundeskriminalamtgesetz</i>
BLA	Federal-Länder Working Group for supervisors, <i>Bund-Länder-Arbeitskreis</i>
BMF	Federal Ministry of Finance, <i>Bundesministerium der Finanzen</i>
BMI	Federal Ministry of the Interior and Community
BMJ	Federal Ministry of Justice
BMWK	Federal Ministry for Economic Affairs and Climate Action
BND	Federal Intelligence Service
BO	Beneficial ownership
CARIN	Camden Asset Recovery Network
COMET	EU Council's Working Party on the Application of Specific Measures to Combat Terrorism
CP	Common Position
DHKP	Devrimci Halk Kurtulus Partisi-Cephesi – the Revolutionary People's Liberation Party/Front
DPMS	Dealers in precious metals and stones
DPRK	Democratic People's Republic of Korea
DZI	German Central Institute for Social Issues, <i>Deutsches Zentralinstitut für soziale Fragen</i>
EAW	European Arrest Warrant
EC	European Council
EDD	Enhanced due diligence
EEA	European Economic Area
EIO	European Investigation Order
EU	European Union
EUR	Euro
FamFG	Act on the Procedure in Family Matters and in Matters of Non-contentious Jurisdiction, <i>Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit</i>

<sup>122</sup> Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

FCA	Financial Conduct Authority
FI	Financial institution
FSAP	IMF Financial Sector Assessment Program
FSRB	FATF-style regional bodies
FTE	Full time equivalent
GBA	Federal Prosecutor General
GBP	Pound sterling
GbR	Civil law partnerships, <i>Gesellschaft bürgerlichen Rechts</i>
GDP	Gross domestic product
GenG	Cooperatives Act, <i>Genossenschaftsgesetz</i>
GETZ	Joint Centre for Extremism and Terrorism
GewO	Trade Regulation Code, <i>Gewerbeordnung</i>
GFG	Joint Financial Investigation Group
GG	Basic Law, <i>Grundgesetz</i>
GmbH	Limited liability companies, <i>Gesellschaft mit beschränkter Haftung</i>
GmbHG	Limited Liability Companies Act, <i>Gesetz betreffend die Gesellschaften mit beschränkter Haftung</i>
GTAZ	Joint Counter-Terrorism Centre
GwG	Money Laundering Act, <i>Geldwäschegesetz</i>
GZD	General Customs Authority
IFSD	BaFin Integrity of Financial Systems Directorate
INPOL	Federal police information database
IP address	Internet protocol address
IRG	Act on International Co-operation in Criminal Matters, <i>Gesetz über die internationale Rechtshilfe in Strafsachen</i>
ISIL	Islamic State of Iraq and the Levant
IT	Information technology
JCPOA	Joint Comprehensive Plan of Action
JIT	Joint investigation team
KAGB	Investment Code, <i>Kapitalanlagegesetzbuch</i>
KG	Limited partnership, <i>Kommanditgesellschaft</i>
KGaA	Partnerships limited by shares, <i>Kommanditgesellschaft auf Aktien</i>
KWG	Banking Act, <i>Gesetz über das Kreditwesen</i>
LEA	Law enforcement authority
LfV	<i>Länder</i> -level intelligence agencies
LKA	<i>Länder</i> criminal police offices
MER	Mutual evaluation report
MLA	Mutual legal assistance
MLRO	Money Laundering Reporting Officer
MOU	Memorandum of understanding
NFS	Non-financial sector
NRA	National risk assessment
NRW	North Rhine Westphalia
OWiG	Administrative Offences Act, <i>Gesetz über Ordnungswidrigkeiten</i>
PartG	Partnership company, <i>Partnerschaftsgesellschaft</i>
PF	Proliferation financing
PKK	Kurdistan Workers' Party
REA	Real estate agent
RÜST GW/TF	Steering Committee for Combating ML/TF
SNRA	Supra-national EU risk assessment
SRA	Sub-National Risk Assessment
StGB	German Criminal Code, <i>Strafgesetzbuch</i>
StPO	Code of Criminal Procedure, <i>Strafprozessordnung</i>
TFS	Targeted financial sanctions

TKP/ML	Communist Party of Türkiye /Marxist-Leninist
UG	Entrepreneurial company, <i>Unternehmergeellschaft haftungsbeschränkt</i>
UK	United Kingdom
US	United States
USD	US Dollars
VAG	Insurance Supervision Act, <i>Versicherungsaufsichtsgesetz</i>
ZAG	Payment Services Supervision Act, <i>Zahlungsdiensteaufsichtsgesetz</i>
ZFdG	Customs Investigation Service Act, <i>Zollfahndungsdienstgesetz</i>
ZKA	Central Office of the German Customs Investigation Service





© FATF

[www.fatf-gafi.org](http://www.fatf-gafi.org)

August 2022

## **Anti-money laundering and counter-terrorist financing measures - Germany**

### ***Fourth Round Mutual Evaluation Report***

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in Germany as at the time of the on-site visit from 1-19 November 2021.

The report analyses the level of effectiveness of Germany's AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.