FATF

Anti-money laundering and counter-terrorist financing measures

United Kingdom

Mutual Evaluation Report

December 2018

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.**

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 October 2018 Plenary meeting.

Citing reference:

FATF (2018), *Anti-money laundering and counter-terrorist financing measures – United Kingdom,* Fourth Round Mutual Evaluation Report, FATF, Paris
http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.html

Table of contents

Executive Summary

1. This report summarises the anti-money laundering and counter-terrorist financing (AML/CFT) measures in place in the United Kingdom of Great Britain and Northern Ireland (UK) as at the date of the on-site visit from 5 to 23 March 2018. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the UK's AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

a) The UK has a robust understanding of its ML/TF risks which is reflected in its public national risk assessments (NRAs). National AML/CFT policies, strategies and activities seek to address the risks identified in the NRAs. National co-ordination and co-operation on AML/CFT issues at both the policy and operational levels has improved significantly since the last evaluation.

b) The UK proactively investigates, prosecutes and convicts a range of TF activity, in line with its identified risks in this area. A particularly positive feature of the system is the strong public/private partnership on TF matters. This is facilitated by the Joint Money Laundering Intelligence Task Force (JMLIT) which facilitates public/private information sharing including on TF and ML investigations.

c) The UK routinely and aggressively identifies, pursues and prioritises ML investigations and prosecutions. It achieves around 7 900 investigations, 2 000 prosecutions and 1 400 convictions annually for standalone ML or where ML is the principal offence. The UK investigates and prosecutes a wide range of ML activity. Investigations of high-end ML (a long-standing risk area for the UK) have increased since being prioritised in 2014. These cases generally take years to progress to prosecution and conviction and limited statistics are available on high-end ML investigations, prosecutions and convictions prior to its prioritisation in 2014. As a result, it is not yet clear whether the level prosecutions and convictions of high-end ML is fully consistent with the UK's threats, risk profile and national AML/CFT policies.

d) Another strong point of the system is that all entities within the FATF definition of *financial institutions* and all DNFBPs are subject to comprehensive AML/CFT requirements and subject to supervision. Supervisors' outreach activities, and fitness and proprietary controls are generally strong. Each supervisor takes a slightly different approach to risk-based supervision. However, while positive steps have been taken, there are weaknesses in the risk-based approach to supervision even among the statutory supervisors.

e) The UK has been a leader in designating terrorists at the UN and EU level, and takes a leading role promoting effective global implementation of proliferation-related TFS. The UK has frozen assets and other funds pursuant to its proliferation financing sanctions program and taken steps to increase the overall effectiveness of its targeted financial sanctions (TFS) regime, including through the creation of the Office of Financial Sanctions Implementation and the strengthening of penalties for breaching TFS. However, minor improvements are required in relation to applying penalties for sanctions breaches, ensuring consistent application of TFS and communicating designations immediately. The UK has a good understanding of the TF risks associated with NPOs and has been effective in taking action to protect the sector from abuse. The UK also has a robust confiscation regime through which it can and does deprive terrorists of assets.

f) Available financial intelligence and analysis is regularly used by a wide range of competent authorities to support investigations of ML/TF and related predicate offences, trace assets, enforce confiscation orders and identify risks. However, the UK has made a deliberate policy decision to limit the role of the UK Financial Intelligence Unit (UKFIU) in undertaking operational and strategic analysis which calls into question whether suspicious activity report (SAR) data is being fully exploited in a systematic and holistic way and providing adequate support to investigators. Additionally, while reports of a high quality are being received, the SAR regime requires a significant overhaul to improve the quality of financial intelligence available to the competent authorities.

g) The UK is a global leader in promoting corporate transparency and has a good understanding of the ML/TF risks posed by legal persons and arrangements. The UK has a comprehensive legal framework requiring all financial institutions and all DNFBPs to conduct customer due diligence and obtain and maintain beneficial ownership information in a manner that is generally in line with the FATF requirements. Beneficial information on trusts is available to the competent authorities through a registry of trusts with tax consequences in the UK. The information in the trust register is verified for accuracy, but the register itself is not yet fully populated. For legal persons, basic and beneficial ownership information is freely and immediately available to the public and all competent authorities through a central public register. This information is not verified for accuracy which limits its reliability. Authorities confirmed that beneficial ownership information, where held in the UK, was obtainable for investigative purposes in a timely manner via available informal and formal investigative tools, including JMLIT and the NCA s.7 gateway.

Risks and General Situation

2. The UK faces significant ML risks from overseas, in particular from other financial centres (including some of its Overseas Territories and Crown Dependencies), due to its position as a major global financial centre and the world's largest centre for cross-border banking. In particular, the UK is vulnerable and at risk of being used as a destination or transit location for criminal proceeds. Criminal activity in the UK also generates a significant amount of proceeds although domestic crime levels have continued to decrease over the past 20 years. The main money laundering (ML) risks include high-end ML, cash-based ML, and the laundering of proceeds from fraud and tax offences, drug offending and human trafficking, and organised crime. The UK also faces particular and significant risks from laundering the proceeds of foreign predicate crimes, including transnational organised crime and overseas corruption

3. The UK faces severe threats from international terrorism. Terrorist financing activity in the UK is usually low-level, involving small amounts of funds raised by UK-based individuals to fund their own travel to join terrorist groups, to send to terrorist associates, or to finance their own terrorist attack plans. The UK also faces threats from Northern Ireland-related terrorism which are rated severe in Northern Ireland and substantial in Great Britain. The nature of the Northern Ireland-related terrorism threat has evolved with paramilitaries and terrorist groups focusing on forms of organised crime which are not all specifically intended to raise funds for terrorism.

Overall Level of Compliance and Effectiveness

4. The UK has implemented an AML/CFT system that is effective in many respects. Particularly good results are being achieved in the areas of investigation and prosecution of ML/TF, confiscation, the implementation of targeted financial sanctions related to terrorism and proliferation, protecting the non-profit sector from terrorist abuse, understanding the ML/TF risks facing the country, preventing misuse of legal structures and co-operating domestically and internationally to address them. However, major improvements are needed to strengthen supervision and implementation of preventive measures, and ensure that financial intelligence is fully exploited.

5. In terms of technical compliance, the legal framework is particularly strong with only two areas in need of significant improvements—measures related to correspondent banking and the UKFIU.

6. The UK has significantly strengthened its AML/CFT framework since its last evaluation particularly in relation to operational co-ordination among law enforcement agencies, stronger investigative tools, mechanisms to facilitate public/private information sharing, and the creation of an authority to address inconsistencies in the supervision of lawyers and accountants. One important issue which is outstanding from the previous assessment is the need to enhance the resources and capabilities available to the UKFIU.

Assessment of risk, co-ordination and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)

7. Overall, the UK has a robust understanding of its ML/TF risks. This is reflected in the National Risk Assessments (NRA) which are public documents. National

AML/CFT policies, strategies and activities seek to address the risks identified in the NRA. For example: new investigative tools and powers were introduced to enhance the ability to investigate and prosecute ML and TF; the Joint Money Laundering Intelligence Task Force (JMLIT) was made permanent to enhance public/private information sharing; international liaison officers were posted abroad to enhance the UK's ability to provide international co-operation; Office for Professional Body Anti-Money Laundering Supervision (OPBAS) was created to address identified inconsistencies in the supervision of lawyers and accountants; and a public registry of beneficial ownership information was established to increase transparency.

8. National co-ordination and co-operation on AML/CFT issues at the policy and operational levels has improved significantly since the last evaluation. This is particularly evident in relation to operational level co-ordination among law enforcement agencies (LEAs) across all jurisdictions in the UK.

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

Use of financial intelligence (Immediate Outcome 6)

9. The competent authorities, including LEAs at the national, regional and local levels, all have access to and regularly use a broad range of financial intelligence and other relevant information to investigate ML/TF and predicate offences, and trace criminal proceeds. Even the smaller police forces have specialist financial investigators which enhances their ability to use financial intelligence in investigations. A particularly strong feature is JMLIT. JMLIT is an innovative model for public/private information sharing that has generated very positive results since its inception in 2015 and is considered to be an example of best practice.

10. The UK has pursued a deliberate policy decision to limit the role of the UKFIU in undertaking operational and strategic analysis. The UKFIU suffers from a lack of available resources (human and IT) and analytical capability which is a serious concern considering similar issues were raised over a decade ago in the UK's previous FATF mutual evaluation. The limited role of the UKFIU calls into question the quality of financial intelligence available to investigators. This is somewhat mitigated by the direct access that law enforcement agencies (LEAs) and supervisory authorities have to the UKFIU database, enabling them to apply their own resources to analysing the financial intelligence from SARs, in line with their own operational needs. However, the assessment team was not convinced that the gaps in the UKFIU are being adequately filled by other agencies such that financial intelligence is fully exploited in the context of the significant ML/TF risks faced by the UK. The limited role of the UKFIU also undercuts its ability to effectively share information with foreign FIUs.

11. While a significant number of high-quality SARs are received, the SAR regime needs a significant overhaul which would improve the financial intelligence available to the competent authorities (see also Chapter 5 on IO.4). While the full range of financial institutions (FIs) and designated non-financial businesses and professions (DNFBPs) are required to report SARs, there remains an underreporting of suspicious transactions by higher risk sectors such as trust and company service providers (TCSPs), lawyers, and accountants.

ML offence (Immediate Outcome 7)

12. The UK routinely and aggressively pursues money laundering investigations. Over 2 000 prosecutions and 1 400 convictions are achieved annually in cases of standalone ML or where ML was the primary offence. All relevant law enforcement authorities prioritise ML and financial investigations, including at the regional and local level. Investigative tools and information-sharing gateways are robust, and resources are applied flexibly both within and across enforcement agencies to respond to investigative needs. Case studies show that the UK is able to investigate and successfully prosecute a wide range of ML activity in line with the risks identified in the NRA. Where a ML conviction is obtained, the sentences appear to be effective, proportionate, and dissuasive. Where prosecution is not possible, the UK actively uses a wide array of other alternative measures to disrupt offenders, including pursuing the predicate offence, seeking civil recovery, taking action for tax offences, or obtaining serious crime prevention orders to restrict behaviour.

13. The UK's focus on pursuing high-end ML is relatively new (dating from December 2014), although high-end ML was pursued to a lesser extent prior to this date as part of LEAs' focus on other complex offending. Since being prioritised by law enforcement in December 2014, the number of high-end ML investigations has risen. However, because such cases are complex and generally take years to complete and statistics in this area are not comprehensive, the UK is not yet able to demonstrate that its level of prosecutions and convictions of high-end ML is fully consistent with its threats, risk profile and national AML/CFT policies.

Confiscation (Immediate Outcome 8)

14. The UK pursues confiscation as a policy objective. It has restrained 1.3 billion and recovered 1 billion since 2014 using POCA, civil recovery, and agency-specific disgorgement mechanisms. HMRC has recovered a further GBP 3.4 billion since 2016 using its tax powers. The UK has demonstrated its ability to recover assets in a range of ML and TF cases. LEAs routinely pursue financial investigations to identify assets for the purpose of recovery and there are many examples of specialised asset recovery units at the national and regional levels.

15. Once assets are identified, a variety of tools are available to the UK authorities including criminal restraint and confiscation, civil forfeiture, cash forfeiture, unexplained wealth orders, and a novel hybrid approach of combining civil recovery with tax powers which permits the UK to recover assets from entities and individuals with tax liabilities in the UK. Where another jurisdiction is involved and depending on the circumstances, the UK is willing to pursue asset sharing or repatriation.

16. Cash is seized at the border and the authorities proactively target high-risk ports. Increasing threats posed by cash in freight have been identified and cases were provided which show that the border authorities are working to improve detection and seizure in this area.

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

TF offence (Immediate Outcome 9)

17. The UK proactively and systematically investigates TF alongside terrorism-related investigations. Case studies demonstrate that a range of TF activity is pursued, and that TF is prosecuted as a distinct criminal activity. TF investigations are well-integrated into broader counter-terrorism strategies, and agencies co-ordinate and co-operate well across jurisdictions, regions, and sectors. Notably, counter-terrorism financing authorities have a close and fruitful relationship with both financial institutions and the non-profit organisation (NPO) sector. All TF convictions are subject to an expectation of imprisonment. The UK has demonstrated its ability and willingness to use all available measures to disrupt TF, including freezing, seizure, and confiscation, as well as the removal of legitimate benefits and entitlements, orders to restrict activity and movement, and new powers which permit the seizure of funds in bank accounts. For example, LEAs in Northern Ireland have adapted to the changing and very specific nature of TF in their jurisdiction by pursuing alternative offences, particularly relating to organised crime, to investigate and prosecute potential TF activities.

Preventing terrorists from raising, moving and using funds (Immediate Outcome 10)

18. Working closely with other countries, the UK actively proposes and co-sponsors individuals and entities for designation pursuant to UNSCR 1267/1988, 1989 and their successor resolutions. It has also implemented domestic measures for the purposes of UNSCRs 1267 and 1373 to remove the delay which currently exists under the EU sanctions regime. The UK proactively makes national designations pursuant to UNSCR 1373 and requests other countries to take freezing action as appropriate. It implements targeted financial sanctions (TFS) without delay and has successfully frozen terrorist-related assets pursuant to both UNSCR regimes. TFS designations are effective without delay in the UK. They are communicated within one business day, although this can sometimes take up to three or four calendar days.

19. The Office of Financial Sanctions Implementation (OFSI) was established in 2016 and has undertaken a great deal of communication with the industry to increase awareness of their TFS obligations. However, outside of the larger banks and MSBs, and particularly amongst DNFBPs, there is uneven understanding and application of TFS. There are also weaknesses in supervision (see IO.3) and the application of sanctions where breaches of these requirements are found, although several investigations are underway.

20. The UK has a good understanding of the TF risks associated with NPOs and applies a targeted risk-based approach to mitigating those risks. The three national charities regulators and OFSI engage regularly with the sector on these issues, have conducted extensive outreach and issued useful guidance. As centralised points of contact, the national charities regulators facilitate the ability of LEAs to investigate NPOs suspected of being abused by terrorist financiers, and provide international co-operation in such cases. There are cases demonstrating the UK's success in helping to protect the sector from such abuse. The UK also has a robust confiscation regime through which it applies both criminal and civil measures to deprive terrorists of their assets. Overall, the UK's measures are generally consistent with its overall risk profile.

Proliferation financing (Immediate Outcome 11)

21. The UK takes a leading role promoting effective global implementation of proliferation-related TFS, has designating entities under the UN and EU proliferation financing (PF) sanctions regimes and has frozen assets under both the Iran and DPRK sanctions regimes. Countering proliferation financing is a strategic priority for the UK and it has implemented national measures to close the gaps in the EU system to implement proliferation-related TFS without delay. TFS designations are effective without delay in the UK. They are communicated within one business day, although this can sometimes take up to three or four calendar days.

22. The UK has a range of mechanisms for addressing proliferation financing in a co-ordinated fashion, including OFSI which was recently created to increase the focus on these issues. OFSI's outreach has improved financial institutions' understanding of their obligation to implement TFS, particularly in the banking sector, where proliferation-related assets are most likely to be found. However, other sectors show less awareness and the issues identified in IO.10 in relation to weaknesses in supervision and the application of sanctions for breaches of these requirements by the NCA and OSFI apply equally here.

Preventive measures (Chapter 5; IO.4; R.9–23)

23. The UK has extremely large and diverse financial and DNFBP sectors. The level and types of ML/TF risks affecting individual FIs and DNFBPs vary, as do the ML/TF risks facing particular sectors. All of the entities performing activities covered by the FATF Standards are required to apply a range of AML/CFT preventive measures under the Money Laundering Regulations 2017. These requirements are comprehensive and consistent across all sectors.

24. AML/CFT compliance is not consistent across different categories of financial institutions. While SARs of a high quality are being received, there are concerns about the low level of SAR reporting in many sectors, including some identified as being at high risk, and the large number of poor quality SARs being filed even among banks which submit 85% of SARs filed. The banking sector plays a predominant role in the UK and the international financial system. Overall, the understanding of ML/TF risks and obligations and implementation of AML/CFT measures appears most developed among the banks which demonstrated awareness of their AML/CFT risks in line with the NRA. Other large FIs (MSBs, insurance providers, investment firms and wealth managers) display a good understanding of risks and AML/CFT compliance requirements in their sectors; however, both banks and MSBs, particularly smaller firms, have a mixed understanding of risk.

25. The understanding of ML/TF risk is much less developed among DNFBPs as the requirement for these entities to undertake a written risk assessment is fairly recent. While larger legal, accountancy and TCSP firms understand their ML risks and have the resources to mitigate them, the understanding is uneven in these sectors. The multiplicity of supervisors in these sectors does not aid a consistent approach, although the UK has created OPBAS to specifically address these issues. Casinos appear to have a good understanding of industry-specific risks, although the degree of understanding varies across the industry. High value dealers are less aware of their ML/TF risks and receive little guidance or supervision. Real estate agents play a minor role in the

financial aspect of property transactions in the UK and their industry's understanding of risk is likely highly variable.

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

26. All of the regulated activities under the FATF Standards are supervised for AML/CFT compliance under the UK regime. Generally, there are strong systems in place for doing background checks and looking at the fitness and propriety of persons owning or controlling regulated activities.

27. The FCA and Revenue and Customs (HMRC) have a good understanding of ML/TF risks which is in line with the NRA. Their sectoral risk understanding is also strong, but they did not demonstrate the ability to develop an accurate picture of risks at the firm-specific level. While the main legal sector supervisor displayed a good understanding of risks facing their sector, there is a mixed understanding of risks amongst the other self-regulatory bodies (SRBs), particularly the smaller ones. The Gambling Commission displayed a very strong understanding of risks both at a sector and firm-specific level.

28. A risk-based approach to supervision is mandated under the 2017 Money Laundering Regulations and each supervisor takes a slightly different approach. The FCA's supervision model focuses on the 14 largest retail and investment banks and an additional 156 smaller firms assessed as higher risk. It is positive that the FCA has recently expanded its supervisory focus (including through the Risk Assurance Reviews and the Annual Data Return). However, the FCA should consider how to ensure appropriate intensity of supervision for all the different categories of its supervisory population from low risk to high risk considering that the FCA has a supervisory population of over 19 600 and that, outside of the 170 firms covered by its systematic and proactive supervision programs, there are a significant number of firms undertaking high and medium risk activities falling outside its regular, cyclical supervisory attention. HMRC develops tactical plans rather than having a cyclical inspection cycle and the risk tool it uses to assess firms individually has only recently been introduced and should be reviewed to ensure it is sufficiently ML/TF focused and effective. While positive steps have been taken, some other supervisors tend to focus on the largest firms in their supervisory pool rather than taking a more comprehensively risk-based approach.

29. The FCA and HMRC have taken remedial actions and levied sanctions against both firms and individuals. The introduction of the Senior Managers and Certification Regime with the designation of Money Laundering Reporting Officer (MLRO) as a senior management function is also a positive development that many firms highlighted as encouraging a stronger compliance culture. There is an increasing trend in FCA and HMRC levying penalties for serious failings. For the accountancy and legal sectors, while remedial actions have been taken, and sanctions levied against both firms and individuals, the scope to enhance sanctions has been identified as an issue by the government. Supervisors have taken concrete steps to promote a clear understanding of AML/CFT obligations. In many cases, guidance is developed with the regulated sector clearly demonstrating the supervisors' willingness to work with the sectors they supervise and their commitment to improve understanding of ML/TF risks.

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

30. The UK has acted as a global leader in this space, promoting the use of public registers of beneficial ownership and using a variety of fora to encourage transparency in this area. The UK has a good understanding of the ML/TF risks posed by legal persons and arrangements. This understanding is shared by relevant LEAs and policy bodies and was reflected in the 2017 NRAs. The UK acknowledges the risks posed by UK corporate structures and Scottish Limited Partnerships, and is taking steps to mitigate these risks. This includes its recent establishment of the People with Significant Control (PSC) register which is fully public and highly transparent and the development of HMRC's register of trusts with UK tax consequences which is accessible by LEAs upon request. The UK has also implemented a comprehensive legal framework which requires all financial institutions and all DNFBPs to obtain and maintain beneficial ownership (BO) information in a manner which is in line with the FATF requirements and entities appear to comply with these requirements.

31. LEAs can access accurate and up-to-date beneficial ownership information from financial institutions and DNFBP in a timely fashion through a range of available informal and formal investigative tools, including JMLIT and the NCA's s.7 gateway. The process is more complicated and less timely where the company holds accounts abroad. Accessing the PSC register on-line is quick and easy, however, while the information in the register is subject to basic checks it remains largely unverified. Individuals and entities are not screened against targeted financial sanctions lists when registering companies. Financial institutions and DNFBPs (which use the register as one aspect of customer due diligence (CDD) information) and LEAs confirmed that the register information is sometimes inaccurate. Although such inaccuracies may be reported to Companies House for correction, there is not yet an obligation to do so and this does not always happen in practice. A legal requirement on FIs and DNFBPs to report inaccuracies will come into force in January 2020. When notified of an inaccuracy, Companies House follows up with the company concerned to encourage compliance. Sanctions are used as a last resort where compliance is not achieved prior to prosecution.

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

32. In general, the UK provides a broad range of constructive mutual legal assistance and extradition. Informal co-operation amongst LEA and prosecutorial authorities is facilitated through an extensive overseas criminal justice network, including intelligence officials, investigators, and prosecutors, who are posted to jurisdictions in a targeted fashion which is in line with the UK's identification of risk. Another particularly strong feature of the system is the public/private information sharing through JMLIT to which foreign counterparts may submit requests for consideration. International co-operation with other EU member states is facilitated by a wide range of regional co-operation tools and information-sharing gateways that streamline and speed up the process. This is an important feature as an overwhelming majority of the UK's international co-operation, including 80% of incoming MLA requests, is with other EU member states.

33. However, there remains room for improvement. Formal international co-operation would benefit from better co-ordination for requests routed through the Home Office UK Central Authority (UKCA) to ensure timely assistance is provided. The

limitations of the UKFIU (see Chapter 3 under IO.6) impact its ability to provide co-operation and the scope of assistance it is expected to provide to requesting FIUs. Although, in theory, the public PSC register should facilitate the UK's ability to respond to international requests for beneficial ownership information on legal persons, international counterparts are usually referred to the registry without being alerted to the issues concerning the accuracy of the information.

Priority Actions

a) Substantially increase the human resources available to the UKFIU and review the UKFIU's role to ensure that financial intelligence is fully exploited in the context of the significant ML/TF risks faced by the UK and so it is better able to co-operate with foreign FIUs. Substantially increase the UKFIU's IT capacity, including by updating analysis software, ensuring sophisticated screening of SARs and allowing automatic checks against multiple databases.

b) Prioritise reform of the SAR regime, including by modernising reporting mechanisms so they are fit-for-purpose for the whole range of reporting entities and making the on-line SAR form (or its replacement) more user-friendly.

c) Continue to improve the quality of information available on the PSC register to ensure that the information is accurate and up-to-date by: pursuing planned work with OFSI to screen information against sanctions lists and share this information as appropriate; ensuring that FIs, DNFBPs and LEAs report identified discrepancies to Companies House; continuing to improve the register's functionality (facilitate searching); where appropriate, clearly flagging in the register any discrepancies reported by FIs, DNFBPs, or LEAs; and ensuring Companies House continues to report suspicions to relevant authorities, including by filing a SAR as appropriate.

d) The FCA should consider how to ensure appropriate intensity of supervision for all the different categories of its supervisory population from low risk to high risk. .HMRC should consider how to ensure appropriate intensity of supervision for all the different categories of its supervisory population from low risk to high risk. HMRC should ensure that it properly takes into account ML/TF when risk rating firms subject to their supervision. Supervisors should continue to ensure, in accordance with the increased trend for levying penalties, that proportionate, dissuasive and effective sanctions are applied for violations of AML/CFT and sanctions obligations.

e) Continue its efforts to address the significant weaknesses in supervision by the 22 legal and accountancy sector supervisors through: ensuring consistency in ML/TF risk understanding; taking a risk-based approach to supervision; and ensuring that effective and dissuasive sanctions apply. The UK should closely monitor the impact of the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) in undertaking this work.

f) Ensure the UKFIU provides assistance to a larger extent to international partners.

g) To the extent possible, work with international partners to endeavour to ensure that the UK continues to use and access regional co-operation tools and information-sharing gateways comparable to those available to the UK under the EU framework.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings (High, Substantial, Moderate, Low)

IO.1 - Risk, policy and coordination	IO.2 International cooperation	IO.3 - Supervision	IO.4 - Preventive measures	IO.5 - Legal persons and arrangements	IO.6 - Financial intelligence
High	**Substantial**	**Moderate**	**Moderate**	**Substantial**	**Moderate**
IO.7 - ML investigation & prosecution	**IO.8 - Confiscation**	**IO.9 - TF investigation & prosecution**	**IO.10 - TF preventive measures & financial sanctions**	**IO.11 - PF financial sanctions**	
Substantial	**Substantial**	**High**	**High**	**High**	

Technical Compliance Ratings (Technical Compliance Ratings (C - compliant, LC – largely compliant, PC – partially compliant, NC – non compliant)

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

MUTUAL EVALUATION REPORT

Preface

This report summarises the AML/CFT measures in place as at the date of the on-site visit. 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 the country, and information obtained by the evaluation team during its on-site visit to the country from 5 to 23 March 2018.

The evaluation was conducted by an assessment team consisting of:

- Ms Havva Börekci Şahan, MASAK (FIU of Turkey) (FIU expert)
- Mr. Damian Brennan, Central Bank of Ireland (financial expert)
- Mr. Jimmy Everitt, The Swedish Companies Registration Office (SCRO) (legal expert)
- Mr. Nikolas Hecht, Federal Ministry of Justice and for Consumer Protection of Germany (legal expert)
- Ms. Anthea Li Suk Kwan, Department of Justice, Hong Kong, China (legal expert), and
- Mr. Scott Rembrandt, United States Department of Treasury (financial expert)

with the support of

- Ms. Valerie Schilling, Ms. Shana Krishnan and Ms. Liz Owen, Policy Analysts, FATF Secretariat.

The report was reviewed by: Mr. Claude LeFrançois, Department of Justice of Canada; Mr. Phineas R. Moloto, Financial Intelligence Centre of South Africa; and Mr. Tomoki Tanemura, Ministry of Finance of Japan.

The UK previously underwent a FATF Mutual Evaluation in 2007, conducted according to the 2004 FATF Methodology. The 2007 evaluation and the 2009 follow-up report have been published and are available at www.fatf-gafi.org/countries/#United Kingdom.

That Mutual Evaluation concluded that the country was: compliant with 31 Recommendations; largely compliant with 5; partially compliant with 10; and non-compliant with three. The UK was rated compliant or largely compliant with 15 of the 16 Core and Key Recommendations. The UK was placed on the regular follow-up process immediately after the adoption of its 3rd round mutual evaluation report. In

October 2009, the UK exited the follow-up process on the basis that it had reached a satisfactory level of compliance with all Core and Key Recommendations.

CHAPTER 1. ML/TF RISKS AND CONTEXT

34. The UK is a sovereign state situated off the north-west coast of mainland Europe. It is a political union made up of four constituent nations: England, Scotland and Wales on the island of Great Britain, and Northern Ireland which shares a land border with the Republic of Ireland[1]. The UK has the third largest population in the European Union (EU) (65.6 million[2] in 2016) with 84.2% living in England, 8.2% in Scotland, 4.7% in Wales and 2.8% in Northern Ireland. Over 15% of the population (about 10.3 million) live in the Metropolitan London area.

35. The UK is a constitutional monarchy headed by The Queen. Executive power is exercised by a democratically elected Government headed by a Prime Minister. Departments of state are headed by other Cabinet Ministers who are drawn from and responsible to the UK Parliament in Westminster. Parliament is the legislative body consisting of one entirely elected chamber (the House of Commons) and one part-hereditary, part-appointed chamber (the House of Lords). Since 1998, some power previously held at Westminster has been devolved to the legislatures of Scotland, Wales and Northern Ireland each of which is represented in Cabinet by a territorial secretary of state. The three devolution arrangements operate in different ways, but, several areas of law-making remain reserved for the UK Parliament and the UK government including all legislation on money laundering (ML) and terrorist financing (TF).

36. The main sources of law in the UK are statutes passed by Parliament, the Common Law which includes case law, and EU law. Where EU law conflicts with national law, the courts must uphold EU law. The UK does not have a codified constitution, relying instead on a mix of common law (derived from custom and judicial precedent rather than statute) and separate pieces of constitutional legislation. In relation to devolved issues, the main sources of law are the statutes passed by the Scottish Parliament in Scotland and the Northern Ireland Assembly in Northern Ireland.

37. The UK has three distinct legal jurisdictions—two of which are based on common law principles (England and Wales, and Northern Ireland) and Scotland which is a hybrid system based on both common law and civil law principles. The

1 There are 14 British overseas territories and three Crown Dependencies (the Bailiwick of Jersey, the Bailiwick of Guernsey, and the Isle of Man) which do not form part of the UK itself and are therefore not covered by this evaluation.

2 Office for National Statistics, National Records of Scotland, Northern Ireland Statistics and Research Agency.

1

Supreme Court of the UK is the court of last resort and the highest appellate court in all matters under English and Welsh law, Northern Ireland law and Scottish civil law.

The High Court of Justiciary remains the court of last resort for criminal law in Scotland..

ML/TF Risks and Scoping of Higher Risk Issues

Overview of ML/TF Risks

38. The UK faces significant ML risks from overseas, in particular from other global financial centres (including some of its Overseas Territories and Crown Dependencies), due to its position as a major global financial centre and the world's largest centre for cross-border banking. In particular, the UK is vulnerable and at risk of being used as a destination or transit location for criminal proceeds. Criminal activity in the UK also generates a significant amount of proceeds although domestic crime levels have continued to decrease over the past 20 years.

39. The UK has estimated the social and economic costs of the most serious and organised crime to total GBP 24 billion per year with most of this relating to drugs and fraud (around GBP 10.7 and GBP 8.9 billion respectively). The illicit drugs market was estimated to be GBP 3.7 billion in 2010. Financial Fraud Action UK estimated financial fraud losses to total over GBP 768 million in 2016, while tax evasion was estimated to cost GBP 5.2 billion in 2014/15.

40. The UK faces severe threats from international terrorism, but the majority of terrorist attack plots in the UK have been planned by British residents, with an increase in low complexity attacks by lone actor UK-based extremists. Although terrorist financing activity in the UK is varied, it is usually low-level, involving small amounts of funds raised by UK-based individuals to fund their own travel to join terrorist groups, to send to terrorist associates, or to finance their own terrorist attack plans.

41. The UK also faces threats from Northern Ireland-related terrorism which are rated severe in Northern Ireland and substantial in Great Britain. The terrorist financing threat in Northern Ireland is focused around the internal threat from Dissident Republicans. Since the signing of the 1998 Belfast Agreement, the nature of the TF threat has evolved with paramilitaries and terrorist groups focusing on forms of organised crime which are not all specifically intended to raise funds for terrorism.

Country's Risk Assessment & Scoping of Higher Risk Issues

42. In 2017, the UK published its second national ML/TF risk assessment, the National Risk Assessment of Money Laundering and Terrorist Financing 2017 (NRA), which follows up from its 2015 UK National Risk Assessment of Money Laundering and Terrorist Financing (2015 NRA). Both national risk assessments were prepared by Her Majesty's Treasury (HMT) and the Home Office in consultation with a wide range of other relevant competent authorities and key stakeholders including law enforcement agencies (LEAs), government departments, supervisors, regulated entities from the private sector and non-governmental organisations. Both national risk assessments also used terminology and a methodology based on the 2013 FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment.

43. The NRA evaluates the relative exposure of each sector to risk, ranking it against a number of risk factors to establish ML/TF risk rankings for each area. These risk ratings evaluate inherent risk, based on vulnerabilities and their likelihood of being exploited by criminals or terrorists, followed by an evaluation of the relevant mitigating factors to calculate the net risk in a particular area. The risk rating is relative, meaning that a rating of low risk does not mean that there is no risk within a sector. All sectors are exposed to some level of risk and ML/TF may still occur at a significant level through low risk areas: NRA p.83-84.

44. The NRA identifies the highest risks as those from cash-based ML and high-end ML (meaning the laundering of large amounts of criminal funds through the UK by, for example, transferring those funds through complex corporate vehicles and offshore jurisdictions). Major predicate offences include fraud and tax offences, drug offences, cybercrime and overseas corruption. The NRA identifies a high risk of criminals abusing companies and LLPs for ML purposes, often with the aid of professional facilitators such as lawyers and accountants, including those providing trust and company services. The NRA also identifies a high ML risk in relation to super-prime property in London, particularly relating to the laundering of proceeds from foreign predicate offences. The UK identified the abuse of property as a medium risk for ML overall with estate agent services posing a low risk but conveyancing posing a high risk.

45. The NRA identifies the UK as being under severe threat from international terrorism, but notes that terrorist financing in the UK is generally low-level, albeit varied. Small amounts are raised by UK-based individuals to fund their own terrorist attack plans, their travel to join terrorist groups, or to send to associates located with terrorist groups abroad. Typically, large scale co-ordinated fundraising for terrorist groups is not seen in the UK. The threat from Northern Ireland-related terrorism is severe in Northern Ireland and substantial in Great Britain. The terrorist financing threat in Northern Ireland is focused around Dissident Republicans who generally finance their activities through organised crime activities including cigarette smuggling, fuel laundering, extortion and robbery, benefit fraud, legitimate or semi-legitimate business activity and some overt fundraising.

46. In addition to the NRA, a wide range of other risk and threat assessments (some public and some restricted or classified) have been undertaken by the key LEAs and regulators, including the authorities in Scotland and Northern Ireland. These risk and threat assessments appear to be in line with the conclusions of the NRA.

47. In deciding what issues to prioritise for increased focus, the assessors reviewed material provided by the UK on their national ML/TF risks (as outlined above), and information from reliable third party sources (e.g. reports of other international organisations). The assessors focused on the following priority issues which are broadly consistent with the issues identified in the NRA:

a) ***International ML/TF risk, including foreign predicates:*** how effectively the UK mitigates its risk of being used as a destination or transit location for criminal proceeds given its role as a global financial centre; the extent to which it prioritises the investigation and prosecution of ML cases involving foreign predicates, and related international co-operation and asset recovery; how

effectively financial institutions mitigate the ML/TF risks of correspondent banking services; and the effectiveness of supervision of group-wide AML/CFT compliance programs and internal controls in foreign branches and subsidiaries.

b) ***Terrorist financing including:*** how effectively the UK investigates and prosecutes TF, including inter-agency co-operation and co-ordination and the use of financial intelligence; the UK's assessment of TF risk for foreign terrorist fighters and NPOs; supervision of the money or value transfer services (MVTS) sector which was identified as high risk for TF; the level of awareness of TF risk in the NPO sector; and the UK's efforts to prevent the misuse of NPOs.

c) ***ML related to major predicate offences including:*** the extent to which the UK is investigating and prosecuting the laundering of proceeds from drug offences, fraud and tax evasion; how effectively it is pursuing related confiscation; and other measures are being undertaken to combat ML/TF related to these predicates.

d) ***Complex ML schemes*** including the authorities' understanding and response.

e) ***Financial intelligence and investigations including:*** the UKFIU's priorities in respect of its core functions and how it manages its resources; how the FIU manages the 'consent regime' as part of the SAR reporting regime; the utility of the support provided by the UKFIU to competent agencies and international partners in respect of combating high risk ML/TF; the sources, nature and extent of transactions reports filed and the extent to which they are transformed into financial intelligence for use by competent agencies to identify potential high risk or complex cases for referral to investigators and asset recovery; the extent to which financial intelligence is accessed and used in investigations, including by LEAs; and what actions have been taken to ensure that relevant LEAs are adequately equipped to investigate ML/TF, including mechanisms to improve interagency co-operation and information sharing.

f) ***Misuse of corporate vehicles including:*** the extent to which the UK is successful in preventing criminal misuse of corporate vehicles, legal persons and arrangements; and the ease with which competent authorities can access and share accurate and up-to-date beneficial ownership information, including through international co-operation and information-exchange.

g) ***Supervision of professional service providers*** including how OPBAS and other mechanisms are addressing the current risks.

h) ***Real estate including:*** the application of CDD and preventative measures in real estate transactions (particularly transactions involving PEPs, steps taken to verify the source of funds, and the identification of beneficial owners); the effectiveness of supervision of the sector and the associated legal professionals (including solicitors); and the tools available to investigators to identify property interests and relevant asset recovery action.

48. Through the scoping note exercise, two areas were identified for lesser focus:

a) ***Notaries*** as they have a limited role in the UK. They are primarily concerned with the authentication and certification of signatures, authority and capacity for documents for use abroad or the taking of oaths. They rarely perform the activities listed in Recommendations 22 and 23, although they are capable of conducting general legal practice such as conveyancing or probate. Given their

limited functions, the assessors restricted their focus on notaries to instances where they are combining their notarial role with another relevant function, such as that of a lawyer.

b) ***Barristers*** as they are prohibited from conducting the sorts of activities that bring lawyers within the FATF Recommendations (e.g. executing transactions, conducting conveyancing and offering client account services). In addition to this, they are either barred from direct public engagement or can only engage with the public after a strict authorisation process.

Materiality

49. The UK has the fifth largest economy in the world and the second largest in Europe, with an estimated annual gross domestic product (GDP) of over $3 trillion United States dollars. The UK economy is driven primarily by the service sector (80% of GDP), with the financial services industry being particularly important. In 2015, financial services, taken together with professional services, accounted for almost 15% of total economic output. Other major industries are aerospace, pharmaceuticals and North Sea oil and gas production. Overall, the UK has one of the most globalised economies in the world.

50. The UK is the world's largest net exporter of financial services ($41 billion) accounting for 17% of the total value of international bank lending and 41% of foreign exchange trading. The UK is the leading foreign exchange market with nearly twice as many U.S. dollars being traded in the UK as in the United States, and more than twice as many Euros being traded in the UK than within the Eurozone itself. Its legal services sector is the second largest in the world (largest in Europe) accounting for 7% of global legal services fee revenue (between $580 billion and $640 billion). The UK has the largest insurance sector in Europe (fourth largest in the world) accounting for 6.4% of global insurance premiums. About $11 trillion assets are under management in the UK. The country also attracts significant investment, ranking first in Europe for foreign direct investment projects in 2016.

51. London is the world's largest financial centre. It is the leading centre for international bank lending, derivatives markets, money markets, international insurance, the issuance of international debt securities and trading in gold, silver and base metals through the London bullion Market and the London Metal exchange.

Structural Elements

52. The UK 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 Bar and judiciary.

Background and Other Contextual Factors

53. The UK has a very mature and sophisticated AML/CFT system. Financial exclusion is not a widespread issue and the UK is ranked ninth in the world in terms of banking inclusion, according to statistics published by the World Bank. Only a very small percentage of the UK population remains unbanked (around 0.02%) according

1

to the UK Financial Inclusion Commission. In 2016, migrant remittance outflows and inflows totalled just over $10 billion and $6.6 billion respectively.

54. The UK has prioritised the fight against corruption and has a robust legal framework in place through the Bribery Act. Building on its 2014 Anti-Corruption Plan, the UK has a comprehensive strategy to combat corruption as set out in the UK Anti-Corruption Strategy 2017-2022. The UK is a world leader in promoting transparency and hosted the world's first leaders' Anti-Corruption Summit in 2016. The UK recently ranked as the eighth least corrupt country in the world. The OECD Working Group on Bribery in International Business Transactions completed its Phase 4 evaluation of the UK in 2017, describing it as one of the major enforcers of foreign bribery offences and citing several good practices and positive achievements by the UK in this area.

AML/CFT strategy

55. The 2015 National Security Strategy and Strategic Defence and Security Review (NSS and SDSR) is the main strategic mechanism for reviewing the threats to the UK and allocating resources to the national security apparatus. They set out the UK's approach to national security and its implementation strategy for the next five years.

56. The NSS and SDSR identified that ML and TF undermine the integrity of the UK's financial institutions and markets, enable criminals to hide, store and benefit from the proceeds of their crime, and enable terrorist groups to function, recruit and commit terrorist acts. They categorised terrorism as a Tier One threat to the UK. Recognising the increasing global threat posed by terrorism, extremism and instability, and the increased threat from Islamist terror groups to the UK, the SDSR protected in real-terms funding for counter-terrorism policing and provided an uplift for the UK Intelligence Community. This was followed by a further funding uplift for counter-terrorism policing in light of the 2017 terrorist attacks. Serious and Organised Crime were recognised as a Tier Two threat to the UK. As part of a comprehensive response to tackling serious and organised crime, the SDSR introduced new measures to make the UK a more hostile place for those seeking to launder money or evade sanctions. This was followed up with publication of a comprehensive Anti-Money Laundering and Counter Terrorist Financing Action Plan in April 2016. The Action Plan has driven work to tackle the vulnerabilities identified in the NRA at a national level and is described in more detail below in section 2.2.2.

57. The SDSR also committed the UK to establish a cross government unit specialising in counter-proliferation activity—the Counter Proliferation and Arms Control Centre (CPACC)—which became operational in July 2016 and is the co-ordinating body for the government's counter proliferation and arms control activity, including proliferation finance. Additionally, the Cross-Whitehall Sanctions Group (Director Level) has responsibility for providing direction, prioritisation and strategic coherence on sanctions policy in line with the government's Sanctions Strategy.

Legal & institutional framework

58. The legal framework of AML/CFT measures applies equally across all jurisdictions of the UK. Preventive measures are contained mainly in the Money

Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) which, alongside other legislation, transpose the Fourth Money Laundering Directive (EU) 2015/849 into UK law. Criminal justice measures are found mainly in the Proceeds of Crime Act 2002 (POCA), the Terrorism Act 2000, the Anti-Terrorism, Crime and Security Act 2001 (ATCSA), the Serious Crime Act 2015 and the Criminal Finances Act 2017 (CFA).

59. The institutional framework for AML/CFT is broad, involving a range of authorities. At the policy level, the Home Office is responsible for the criminal justice aspects of the AML/CFT system, including national security and counter-terrorism policy, while (HMT) is responsible for the regulatory aspects and financial sanctions implementation. Oversight of the UK's AML and counter-proliferation policy is undertaken at the Ministerial-level by the Criminal Finances Board and at the working-level by two sub-groups: the ML Working Group (central government and LEAs) and the ML Advisory Committee (central government, LEAs, supervisors and the private sector). Similarly, Ministerial oversight of UK's TF policy is undertaken by the Terrorist Finance Board which is supported by a working-level shadow group. Various other government departments and agencies are also involved in AML/CFT policy development:

a) The Department for Business, Energy and Industrial Strategy (BEIS) is responsible for business, including the creation of legal persons. Companies House (which incorporates, dissolves, and registers legal persons in the UK) is an executive agency sponsored by BEIS, as is the Insolvency Service which administers bankruptcies.
b) HMRC implements tax and customs policy.
c) The Department for International Development is the UK's lead department responsible for international development policy and administering official development assistance.

60. At the operational level, a range of agencies are involved in overseeing the criminal justice response to ML/TF. The National Crime Agency (NCA) leads and co-ordinates the response to serious and organised crime in England and Wales. As serious and organised crime is devolved, the NCA works closely with Police Scotland and the Police Service of Northern Ireland (PSNI) as the lead agencies for serious and organised crime in those jurisdictions. Within the devolved administrations, the devolved criminal justice functions are overseen by the Justice and Safer Communities Directorates of the Scottish Government and the Department of Justice in Northern Ireland.

61. The following agencies do ML/TF-related intelligence-gathering and analysis:

a) The **UKFIU** is housed within the NCA and is responsible for receiving and disseminating suspicious activity reports and conducting some analysis in line with its statutory mandate (see chapter 3 under IO.6).
b) The **NCA National Intelligence Hub** identifies priority targets and develops intelligence against them using sensitive and non-sensitive material, including SARs and financial intelligence, with a focus on the NCA's priorities of high-end and cash-based ML.
c) **HMRC's Risk Intelligence Service** develops strategic and tactical understanding of the risks related to serious tax fraud and related ML as well as cross-border cash movement.

d) The **Serious Fraud Office**'s Intelligence Unit analyses, develops and disseminates intelligence concerning serious or complex fraud, bribery & corruption and associated ML.
e) The **Financial Conduct Authority (FCA)** gathers strategic and tactical intelligence on ML to drive its regulatory and enforcement activities.
f) The **police** collect and analyse significant levels of ML intelligence. Analysis is mainly conducted at a regional level, with some of the larger forces having specialist analytical teams.
g) The **Joint Money Laundering Intelligence Taskforce (JMLIT)** is a public/private partnership with the financial sector. In addition to sharing intelligence and information to support operational work, JMLIT produces strategic intelligence and products to increase private sector understanding of risk. JMLIT started as a pilot programme in 2015, but was made permanent in April 2016.
h) The **Joint Financial Analysis Centre** is a cross-agency taskforce led by the NCA and HMRC. Originally established to mine data from the Panama Papers leak, it pools data and intelligence to develop an understanding of ML methodologies, vulnerabilities and risks.
i) The **Security Service** (**MI5**) is the UK's national security agency and part of the UK's broader intelligence framework.

62. The following agencies investigate and prosecute ML and TF:

a) The **NCA** pursues high-end and complex ML cases and related asset recovery across England, Wales and (with the approval of the PSNI) Northern Ireland. It particularly focuses on cases with an international dimension.
b) The **Serious Fraud Office (SFO)** is responsible for investigating and prosecuting ML relating to serious or complex fraud, bribery and corruption across England, Wales and Northern Ireland. The SFO's Proceeds of Crime division recovers proceeds of those crimes and investigates and prosecutes standalone ML cases.
c) **HMRC Fraud Investigation Service** primarily investigates ML arising from tax offences and breaches of the MLRs by businesses supervised by HMRC, across all UK jurisdictions. It pursues cash recovery inland and at the border and, where applicable, uses tax powers to target and tackle suspected ML and assists others with TF investigations.
d) The **FCA** investigates and prosecutes ML which is ancillary to offences that it is responsible for under its statutory objectives, including market manipulation, insider dealing and unauthorised business activity such as boiler room frauds.
e) At the regional policing level, nine **Regional Organised Crime Units (ROCUs)** operate across England and Wales to investigate cases relating to serious and organised crime that do not meet the criteria for investigation by one of the specialised agencies. These units also house specialised **Regional Asset Recovery Teams (RARTs)** which investigate ML or provide financial investigative skills, and **Asset Confiscation Enforcement (ACE) teams** which focus on asset recovery.
f) At the local policing level, there are 43 forces in England and Wales which investigate primarily ML linked to predicate offending. The Metropolitan

Police Service and the City of London Police in particular have dedicated teams in place to combat ML and other economic crimes and also provide an operational arm for other LEAs.

g) The **Crown Prosecution Service (CPS)** in England and Wales is responsible for prosecuting all offending in these jurisdictions, except where this function is performed by the investigative agency (e.g. in the case of the SFO and the FCA).

h) In Northern Ireland, the **Economic Crime Unit of the PSNI** leads and co-ordinates financial crime investigations in Northern Ireland which are not investigated by a specialised agency (such as the NCA or SFO). These cases are then prosecuted by the **Public Prosecution Service of Northern Ireland**.

i) Scotland has a single national police service, Police Scotland, within which the **Economic Crime and Financial Investigation Unit** investigates economic crime in Scotland. Cases are then prosecuted by the **Crown Office and Procurator Fiscal Service (COPFS)**. Civil recovery actions are pursued by the **Civil Recovery Unit**.

63. In addition to these agencies, others have a specific focus on CFT:

a) The **Joint Terrorism Analysis Centre (JTAC)** analyses and assesses all available intelligence relating to international terrorism at home and overseas. It sets threat levels and issues warnings of threats and other terrorist-related subjects for customers from a wide range of government departments and agencies. It also produces more in-depth reports on trends, terrorist networks and capabilities.

b) **Counter Terrorism Policing** is an alliance of UK police forces working with intelligence agencies to prevent, detect and investigate terrorist activity. This is supported by 11 regional counter-terrorism investigative and intelligence police units.

c) The **National Terrorist Financial Investigation Unit (NTFIU)** within the **Special Operations 15 (SO15)** of the Metropolitan Police is the strategic lead for the UK's counter-terrorism policing.

64. The following authorities manage targeted financial sanctions and asset-freezing:

a) The **Foreign and Commonwealth Office** has overall responsibility for the UK's policy on international sanctions.

b) The **Office of Financial Sanction Implementation (OFSI)** within HMT leads the UK's implementation of financial sanctions and terrorist asset freezing.

65. The main AML/CFT supervisory bodies are described below:

a) The **Financial Conduct Authority (FCA)** supervises financial institutions.

b) **Her Majesty's Revenue and Customs (HMRC)** supervises money service businesses not otherwise supervised by the FCA, estate agent businesses, high value dealers and accountants and trust and company service providers who are not members of and supervised by an approved professional body or otherwise supervised by the FCA.

1

c) **22 approved professional body supervisors** are responsible for supervising the legal and accountancy sectors. For accountants, the largest supervisor by far is the Institute of Chartered Accountants in England and Wales (ICAEW) which supervises over 50% of the UK's accountancy sector. For lawyers, the largest supervisor by far is the Law Society of England and Wales (LSEW) which regulates its members through the Solicitors Regulation Authority (SRA) and supervises over 80% of the UK's legal sector.
d) **Office for Professional Body AML Supervision (OPBAS)** is an oversight body for the legal and accountancy sectors. It was created to address the weaknesses in AML/CFT supervision in the legal and accounting sectors identified in the 2015 NRA. It has a focus on improving application of the risk-based approach and ensuring that effective, proportionate and dissuasive sanctions are applied.
e) The **Gambling Commission** is the regulator for all gambling service providers in the UK. It supervises casinos (land-based and remote) for AML/CFT purposes and a diverse range of other gambling service providers (betting, arcades, lotteries, and land based and online gaming).

Financial sector and DNFBPs

66. This section gives general information on the size and make-up of the financial and DNFBP sectors which are extremely large and diverse in the UK. Not all of the financial and DNFBP sectors are of equal importance, given the specific risks and context of the UK system. The level and types of ML/TF risks affecting individual financial institutions (FIs) and DNFBPs vary greatly, as do the ML/TF risks facing particular sectors.

67. The assessors ranked the sectors on the basis of their relative importance in the UK context given their respective materiality and level of ML/TF risks. The assessors used these rankings to inform their conclusions throughout this report, weighting positive and negative implementation issues more heavily for important sectors than for less important sectors. This approach applies throughout the report, but is most evident in Chapter 6 on IO.3 and Chapter 5 on IO.4:

a) The **banking sector** is weighted as being the most important in the UK context based on its materiality and risks. The banking sector plays a predominant role in the UK and the international financial system and is, therefore, materially significant. With 19 620 financial, credit, payment and e-money institutions operating in the UK, the banking sector is nevertheless highly consolidated with six banks accounting for 87.5% of the total market share (current accounts). The NRA identified the banking sector as being at high risk for ML as its relative size and openness makes it attractive to criminals seeking to hide the proceeds of crime among the huge volumes of legitimate business. The retail banking sector was identified as high risk for TF, with other parts of the banking sector identified as lower risk for TF.
b) Money service businesses (MSBs), lawyers, accountants, and trust and company service providers (TCSPs) are weighted as being highly important based on their materiality and risks:
   i. **MSBs:** There are approximately 1 800 principal MSBs registered with HMRC, including over 1 100 firms providing currency exchange, 1 000 firms providing money transmission and 300 firms providing cheque

cashing services. This sector is highly diverse with over 43 000 premises offering MSB services through principals and their agents; with the largest 11 MSBs covering 83% of UK agents. The NRA identifies MSBs as being at high risk for both ML and TF in part due to their role in moving funds in and out of the UK, including to high-risk jurisdictions.

ii. ***Lawyers:*** There are 18 600 registered legal service providers, including 14 000 firms of which 72% employ less than 10 employees. The NRA identifies legal services as being at high risk of money laundering (with certain services identified as higher or lower risk), particularly high-end ML with some instances of complicity having been noted. The TF risk associated with legal services is judged to be low with no specific evidence of legal services having been abused for this purpose.

iii. ***Accountants:*** There is a large accountancy sector which comprises 48 000 entities. The term accountant covers a wide range of activities and these entities range from large firms offering multi-national businesses to much smaller book-keeping businesses. Similar to the legal sector, the NRA identifies accountancy services as being at high risk of ML (with certain services identified as higher or lower risk) and at low risk of TF.

iv. ***TCSPs:*** The TCSP sector comprises 22 626 entities, including lawyers and accountants who also provide these services.[3] The NRA notes that trust and company services pose higher risks when offered by accountants (it is estimated that 25% of supervised accountancy firms provide such services) or lawyers than by specialised company formation agents, as criminals may also exploit the accountant's or lawyer's wider services.

c) ***The securities sector*** is weighted as being of medium importance given its materiality and relative ML/TF risks. The UK is the global centre for the issuance of securities with 5 676 registered retail investment firms. The NRA identifies a significant emerging risk of ML through capital markets, particularly through high-end ML schemes involving substantial amounts of proceeds. Although the NRA notes the possibility of international terrorist funds transiting through the UK capital markets, no specific incidents of this have been identified and, on that basis, the TF risks in this sector are considered to be low.

d) The insurance sector, casinos, estate agent businesses (EABs) and high value dealers (HVDs) are weighted as being of relatively low importance:

i. ***Insurance:*** The UK has the world's fourth largest insurance sector comprised of 656 general insurance firms, and 234 pensions and income retirement firms The NRA notes that, relative to other sectors, the insurance sector in the UK is at low risk for both ML and TF. This is on the basis that, although the global nature of the London market does expose the sector to risks, firms have suitable controls to deal with them and instances of abuse have been limited.

ii. ***Casinos:*** There are 325 casinos registered in the UK. The gambling sector consists of remote and non-remote licensed casinos, remote and on and

3 The UK had difficulty in providing accurate statistics on the numbers of entities undertaking TCSP activities due to the fact that the requirement for all TCSPs to register with either HMRC or the FCA was only introduced in June 2017 and supervisors do not keep consistent statistics on TCSP activities.

1

off-course betting, remote and non-remote bingo and lotteries, and arcades. The NRA identifies varying levels of ML and TF risks across gambling sectors. However, most ML consists of criminals spending criminal proceeds (including acquisitive crime and the sale of illicit commodities) for leisure rather than for the purpose of laundering their funds. Overall, the ML and TF risks in the gambling sector are judged to be low.

iii. ***Estate agent businesses (EABs):*** There are 10 143 registered EABs of which 77 are large firms and the rest are small businesses. Estate agents are key facilitators of property transactions, and have a relationship with both the buyer and the seller at an early stage in the transaction. Overall the NRA assesses EABs as low risk and real estate medium risk.

iv. ***High value dealers (HVD):*** There are 737 HVD registered with the HMRC, not all of which fall into the FATF definition of *dealers in precious metals and stones.* Of the 25 categories of HVD, the three at highest risk are motor vehicles, jewellery and alcohol which comprise 55% of registered businesses. Overall, the NRA identifies the ML risks of this sector to be low relative to other sectors due to the limited ability for criminals to use HVDs to launder large sums of money or move terrorist funds.

Preventive measures

68. All of the UK's preventative measures are set out in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the 2017 MLRs). The 2017 MLRs came into force on 26 June 2017, and along with other legislation, transpose the EU's Fourth Money Laundering Directive into UK law. The 2017 MLRs place requirements on regulated entities to undertake risk assessments, know their customer and take enhanced measures in situations of higher-risk. EU Regulation 2015/847 (the Fund Transfer Regulation) updates the rules in relation to the information that must accompany transfers of funds and also came into force in the UK on 26 June 2017.

69. The 2017 MLRs cover all the financial institutions and DNFBPs required by the FATF Standards. The MLRs also cover a range of high value dealers that are not required under the FATF Standards. The 2017 MLRs set out the exclusions for certain low risk activities, including in relation to e-money, which are in line with the UK's national risk assessment (see Chapter 2 on IO.1).

Legal persons and arrangements

70. Since 2006, private limited companies have consistently accounted for over 96% of all corporate body types registered at Companies House. In the 2016/2017 fiscal year, Companies House registered 644 750 new incorporations and dissolved 436 526 companies.

Table 0. **Types of Legal Persons in the UK as of 31 March 2017**

Description	Number	Basic characteristics and significance
Register size	3 896 755	Almost 96% of the companies registered in Companies House are private companies limited by shares.
Private company limited by shares	3 737 487	Separate legal personality with shareholders and may keep any profits it makes after paying tax. May be incorporated or dissolved at low cost and with relative ease. Financial statements must be published at Companies House. Used for a wide range of legitimate business purposes.
Private company limited by guarantee	105 429	Separate legal personality with members who act as guarantors. Profits may be distributed to its members. Used primarily for incorporating multi-stakeholder organisations.
Private Limited by Guarantee/No Share Capital/(Exempt from using 'Ltd')	42 482	Separate legal personality with members who act as guarantors. Profits may not be distributed to its members. Used primarily for non-profit organisations requiring legal personality.
Private unlimited company	4 420	Hybrid company incorporated with or without share capital where the legal liability of its members is not limited. Used when secrecy concerning financial affairs is desired as financial statements do not need to be published.
Public limited company	6 939	Public company whose shares are publicly traded on a stock exchange or privately held with a minimum share capital of GBP 50 000.
Limited Liability Partnership	60 778	Same characteristics as a normal partnership in terms of tax liability, but provides reduced financial liability to each partner. Used primarily for professions that normally operate as a traditional partnership such as solicitors and accountancy firms.
Limited Partnership	45 250	Partnerships with general partners (who are liable for its debts and obligations) and limited partners (who contribute capital at a statement amount and are not liable beyond the amount contributed).
Scottish Limited Partnerships	31 574	A subset of limited partnerships which represent around 1% of UK corporates. They have a distinct legal personality, separate from the partners and are subject to less reporting and transparency obligations than most other corporate forms. Used primarily for financial and pension structures.
Other corporate body types	3 940	For example, European Union-wide companies structures (Societas Europaea) (SEs) or European economic interest groupings (EEIGs)
Other corporate bodies administered at Companies House	12 709	For example, companies incorporated by Royal Charter

Source: Companies House Register

71. Express trusts established under UK law are used for a range of purposes including: controlling and protecting family assets; passing on assets before or after death; or managing the assets of someone who is incapacitated or too young. It is not known how many express trusts have been established in the UK, although the number could be as high as 1.5 to 2 million (2015 NRA estimate). In the 2015/2016 fiscal year, 158 500 trusts submitted tax returns to HMRC. This statistic includes non-UK-resident trusts that generate income within the UK and trusts required to submit a tax return despite having no actual tax to pay (either through having a nil return or being due a refund).

Supervisory arrangements

72. There are 25 AML/CFT supervisors in the UK, supervising all businesses that are required to comply with the 2017 MLRs. Supervisors have powers to effectively monitor and supervise relevant persons in their own sectors as well as take necessary measures to secure compliance under the MLRs (reg.46). The basic powers of these supervisors are set out below (and are analysed in more detail in R.27 and R.28):

a) The **FCA** derives the majority of its powers through the Financial Services and Markets Act 2000 (FSMA) which gives it a wide range of rule-making, authorisation and registration powers, investigatory and enforcement powers. It also derives specific AML/CFT supervision powers through the 2017 MLRs.
b) **HMRC** derives its AML/CFT supervisory powers through the 2017 MLRs. Under Regulation 76 of the MLRs, both the FCA and HMRC are able to impose penalties and make public statements censuring any person that has failed to comply with AML/CFT requirements.
c) The 22 **professional body supervisors** each have their own rule books or authorities for undertaking inspections, imposing disciplinary action or penalties on their members; these vary greatly.
d) The **Gambling Commission** obtains its powers through the Gambling Act 2005 which allows it to issue operating licences in Great Britain, of which AML/CFT compliance is a condition. Under the Betting, Gaming, Lotteries and Amusements (Northern Ireland) Order 1985, casinos are legally prohibited in Northern Ireland.

Table 2. **UK supervisors and their supervisory population**

Supervisor	Type of services supervised (by FATF definition)
FCA	19 620 financial institutions covering all 13 financial activities within the FATF definition of *financial institutions*, including acceptance of deposits, lending, money or value transfer services (MVTS), issuing and managing means of payment (including e-money), trading, securities and insurance. The FCA also supervises some money services businesses (MSBs) and trust and company service providers (TCSPs) where this is part of other financial services that the firm provides.
HMRC	28 357 MSBs and DNFBPs including: 1 890 MSBs not otherwise supervised by FCA 1 960 TCSPs which are not members of and supervised by an approved professional body or otherwise supervised by the FCA 10 143 estate agent businesses 737 high value dealers, including dealers in precious metals and stones 13 627 accountancy firms which are not members of and supervised by an approved professional body(also referred to as Accountancy Service Providers – ASPs)
13 approved accountancy sector supervisors	27 633 accountancy firms comprising 44 381 members
9 approved legal sectors supervisors	12 930 legal services firms (lawyers, notaries and other independent legal professionals) comprising 175 015 members
Gambling Commission	325 gambling service providers including land-based and internet-based casinos and other gambling service providers (betting, bingo, arcades, on-line gaming)

Note: The FCA and HMRC supervisory populations of FIs include not only firms authorised or licensed in the UK but also entities passporting their services into the UK that have agents or branches located in the UK.

73. **Companies House** is the registrar for UK legal persons. The following legal persons must register with Companies House: private companies limited by shares, private companies limited by guarantee, private unlimited companies, public limited companies, limited liability partnerships, and limited partnerships, including Scottish Limited Partnerships. A very small number of other companies (e.g. unregistered companies, companies incorporated by Royal Charter, non-Companies Act companies) are not required to register with Companies House but are subject to certain requirements, such as submitting basic information to Companies House.

International co-operation

74. As a global financial centre exposed to high risks from the laundering of foreign predicates, organised crime proceeds and overseas corruption, the UK is a large provider and receiver of international co-operation. The UK co-operates with many jurisdictions (over 108 in 2016), but most incoming mutual legal assistance (MLA) requests come from EU Member States (80% of incoming requests received by the UKCA in 2016). The UK has four central authorities in respect of all incoming and outgoing MLA and extradition requests:

a) the **Home Office UK Central Authority (UKCA)** for MLA and non-European Arrest Warrant (EAW) extradition requests in England, Wales and Northern Ireland
b) **Her Majesty's Revenue and Customs (HMRC)** for MLA requests in England, Wales and Northern Ireland relating to HMRC functions (generally tax and fiscal customs matters)
c) **COPFS** for MLA and extradition requests in Scotland (including devolved Scottish tax matters)
d) **NCA** for EAW extradition requests in England, Wales and Northern Ireland.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND CO-ORDINATION

Key Findings and Recommended Actions

Key Findings

a) The UK has a robust understanding of its ML/TF risks as reflected in its public NRAs and shared across UK government departments, LEAs, and regulatory agencies. Generally, financial institutions and DNFBPs appear to understand their risk as framed in the NRA and use it to inform their own risk assessments.
b) National AML/CFT policies, strategies and activities generally seek to address the risks identified in the NRA. Since its first NRA, the UK has: introduced new investigative tools and powers to enhance its ability to investigate and prosecute ML and TF; made the JMLIT permanent to enhance public-private information-sharing; posted more international liaison officers abroad to enhance its ability to provide international co-operation; created OPBAS to address identified inconsistencies in the supervision of lawyers and accountants; and established a public registry of beneficial ownership information to increase transparency.
c) National co-ordination and co-operation on AML/CFT issues at the policy and operational levels has improved significantly since the last evaluation, particularly operational level co-ordination among law enforcement agencies (LEAs) across all jurisdictions in the UK.
d) The UK's ML/TF risk assessments and understanding of risk is informed by a wide range of qualitative and quantitative data, including the experience of the relevant competent authorities and feedback from the private sector.

Recommended Actions

a) Continue to monitor the implementation of the 2016 AML Action Plan, including use of the new law enforcement tools in the Criminal Finances Act 2017 and the newly established OPBAS to ensure their effectiveness.
b) Improve the collection of more consistent, comprehensive, national statistics on all ML investigations, prosecutions and confiscations; confiscation activity; and international co-operation, to further enhance risk understanding.
c) Continue to develop an understanding of emerging risks (such as virtual currencies) and intelligence gaps, and take appropriate action.

75. 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.

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

Country's understanding of its ML/TF risks

76. The UK largely has a robust understanding of its ML/TF risks (as set out in part 1.1. above) informed by a comprehensive and ongoing risk assessment process. The assessment team based this conclusion on: a review of the available risk and threat assessments; and discussions with UK government departments, LEAs, regulatory agencies, and regulated sectors.

77. UK government departments, LEAs, and regulatory agencies share an understanding of the higher risks posed by: cash-based and high-end ML; ML from foreign predicates; the misuse of legal persons; the involvement of professional enablers; and ML from drug and fraud offending. This understanding is consistent with the UK's 2015 and 2017 NRAs and the wide range of other risk and threat assessments undertaken by both LEAs and regulators. The understanding of risk across the supervisory agencies is less consistent, with some professional body supervisors' understanding of risk departing from those expressed in the NRA. For the most part, the financial institutions and DNFBPs met at the onsite also demonstrated an understanding of risk as framed in the NRA and reported using it to inform their own risk assessments.[4]

78. UK agencies and regulators were particularly sensitive to evolving risks and new and emerging threats. The authorities acknowledged that, like all risk assessments, the 2017 NRA represents a snapshot in time which must be complemented by ongoing work to maintain an up-to-date understanding of emerging risks. For this reason, they emphasised the importance of conducting ongoing risk and threat assessments to ensure an up-to-date picture of the UK's risk profile. For example, HMRC conducted 30 such assessments into ML in 2016/17 alone, in addition to contributing to other agencies' assessments. Authorities noted that the NRA was based on the ongoing work undertaken by agencies, with its primary roles being to bring together findings from wider work to inform the national public and private sector response, and to publicise the risks and raise awareness. To this end, the NRA is public and has been widely shared.

79. The UK's understanding of TF is similarly comprehensive and consistent. Agencies consistently exhibited a shared understanding of the UK's TF risk, as illustrated in the 2017 NRA. In particular, agencies note that TF in the UK is generally low-level and involves the raising of small amounts by UK-based individuals to fund their own attack plans, their travel to join terrorist groups, or to send to FTFs abroad. Relevant authorities also demonstrated a comprehensive understanding of Northern Ireland related terrorism, including a collective recognition of the TF threat in this region due to the blurred lines between TF and organised crime.

80. While the UK's understanding of risk is based on a range of qualitative and quantitative information, its measurement of risk mitigation measures could be

4 With the exception of the banking sector (which is highly consolidated), most sectors in the UK are very large and diverse with the market being spread across numerous entities. For that reason, the assessors considered the private sector firms met with during the on-site visit to be a sampling of how the FATF Recommendations are implemented in some cases, rather than being representative of how they are implemented across each sector as a whole.

further enhanced by more consistent, comprehensive, national statistics on law enforcement activity, confiscation, and international co-operation.

National policies to address identified ML/TF risks

81. National and agency-specific AML/CFT policies, strategies and activities generally seek to address the risks identified in the NRA. The assessment team based this conclusion on: a review of available AML/CFT strategy and policy documents, including the National Security Strategy (NSS) and Strategic Defence and Security Review (SDSR) which are described above in section 1.4.1; and discussions with UK government departments, LEAs, regulatory agencies and regulated sectors.

82. A strength of the UK's system is the close co-operation and collaboration that goes into all ML/TF risk and threat assessments, including the NRAs. The UK has a good framework in place for co-operation in contributing to national and sectoral risk assessments. This happens formally through established working groups and multi-agency task forces, and informally through constructive personal relationships between individuals from relevant government departments and private sector entities. This permits close co-operation and information sharing when developing risk assessments. All relevant supervisory bodies, including charities regulators, LEAs and other relevant authorities fed into the development of the 2015 and 2017 NRAs.

83. In April 2016, the UK published its AML/CFT Action Plan which was focused on steps to address the threats and vulnerabilities identified in the 2015 NRA. This resulted in a number of identified improvements, including: making the JMLIT permanent to improve public/private information-sharing and creating OPBAS to address identified significant deficiencies in the supervision of lawyers and accountants. The Action Plan also committed to SARs reform, although this remains under development. It also published a separate CFT Strategy and Delivery Plan that resulted in concrete actions, including new powers to freeze bank accounts and improved engagement with the charitable sector.

84. The UK Government's legislative programme supports national AML/CFT policies and implements measures to address identified risks. For example, in response to the risks posed by legal persons and arrangements, the UK enacted the new register of people with significant control (PSCs) and the register of trusts with UK tax consequences. Similarly, the Criminal Finances Act 2017 was enacted in response to law enforcement calls for new investigative tools and powers to enhance the ability to investigate and prosecute ML and TF and to recover assets. The 2017 MLRs also increase the expectations of supervisors, for example, requiring them to conduct criminality tests for persons in certain sectors involving a position of trust. Having identified emerging risks associated with virtual currencies, the UK authorities advise that they are preparing regulations to extend AML/CFT requirements to this sector.

85. LEA policies also respond to the ML/TF risks identified in the NRA. International liaison officers are posted abroad to higher-risk countries to enhance the UK's ability to obtain and provide international co-operation. LEAs have co-ordinated projects to raise intelligence and improve understanding in high-risk areas, including on high-end ML, cash-based ML, ML through professional enablers, and organised crime. The UK collects a range of qualitative and quantitative information

which feed into its risk understanding and is used in policy development. This could be supplemented by consistent, comprehensive, national statistics on: all ML investigations, prosecutions, and convictions; confiscation; and international co-operation. LEAs are making progress on developing policies to address emerging risks, such as cash in freight. They should continue these efforts and develop specific, risk-based strategies as necessary in these areas.

86. The resources of LEAs and supervisory bodies are largely aligned to the risk areas identified in the NRA and the UK has demonstrated that resources can be allocated in accordance with risk. Even in the context of austerity budgets, LEAs have seen an increase in specialised resourcing for ML and TF investigations and prosecutions.

Exemptions, enhanced and simplified measures

87. The UK's legal framework for exemptions and applying enhanced measures are drawn from the EU's Fourth Anti-Money Laundering Directive (4AMLD) and its 2015 and 2017 National Risk Assessments. The UK's approximately 150 000 regulated entities are required by law to identify and assess their ML/TF risks and put in place systems and controls to manage and mitigate them. In addition, HMT approves AML/CFT guidance written by and for all of its regulated sectors. Such guidance clarifies the practical application of legal and regulatory requirements to their business or sector, including situations which might be treated as higher or lower risk.

88. In high-risk situations, regulated entities must undertake enhanced due diligence (e.g. when dealing with politically exposed persons, correspondent banking relationships and high-risk jurisdictions). While the MLRs allow FIs to treat EU correspondent banking relationships as low-risk, private sector representatives met during the on-site visit advised that such relationships are considered to be high-risk.

89. Where there is proven low risk, the UK applies limited and justified exemptions for some categories of entities when they are carrying out activities that may fall under the MLRs. This includes registered societies (when issuing withdrawable share capital or accepting deposits) and local authorities providing limited financial services (see R.1 for more details).

Objectives and activities of competent authorities

90. Supervisors' objectives and activities are generally consistent with national AML/CFT policies and the ML/TF risks identified. Supervisors use the NRA to inform their understanding of risk as required by the MLRs. Most supervisors' view of ML/TF risk is aligned to that of the NRA and supervisors generally apply more focus and resources to the areas of highest risk. However, this picture is not consistent across all supervisors. Some of the 22 legal and accountancy supervisors do not share the NRA's view that their sectors are high risk. This means that their supervisory objectives and activities are less likely to be consistent with the national AML/CFT policies and ML/TF risks identified. The UK authorities are aware of this issue and have established OPBAS to address the inconsistent application of the risk-based approach by professional body supervisors in the legal and accountancy sectors.

91. LEA and other relevant authorities' goals and objectives are in line with the ML/TF risks identified in the NRA and consistent with national AML/CFT policies. LEAs demonstrated an understanding of risk consistent with the NRA and were also sensitive to evolving risks and new and emerging threats. LEAs activities, including prioritisation and allocation of resources, were broadly consistent with the risk areas identified. Authorities have taken steps to address areas more recently identified as higher-risk, such as high-end ML and cash movement through freight, although some of these activities will take time to result in criminal justice outcomes.

92. The authorities demonstrated a strong understanding of the unique nature of the specific risks facing sectors and jurisdictions and are responding accordingly. For example, authorities in Northern Ireland are aware of the specific risks posed by Northern Ireland-related terrorism and are targeting their activities to respond to the changing nature of this risk. Similarly, charity regulators are well-aware of the specific risks facing NPOs and undertake supervision and outreach in a manner consistent with these risks.

National co-ordination and co-operation

93. Co-operation and co-ordination between agencies on AML/CFT issues is a strength of the UK system and a significant improvement since the UK's last evaluation. All relevant agencies work well together at a policy and operational level. This is facilitated by strong personal relationships and multi-agency task forces, or working groups in cases where more formal co-ordination is required. The assessment team based these conclusions on: a review of information provided by the UK on various co-ordinating bodies and groups; and discussions with UK government departments, LEAs, regulatory agencies and regulated sectors.

94. National oversight and co-ordination of the UK's AML/CFT policies occurs through the weekly National Security Council, which is chaired by the Prime Minister and has broad oversight of national security issues, including ML/TF. The Ministerial-level Criminal Finances Board is responsible for national AML policy development and implementation. It brings together all relevant agencies from across all UK jurisdictions, including policy departments and LEAs.

95. At the policy level, a wide range of groups exist beneath the Criminal Finances Board and bring together working-level officials. Of these, the Money Laundering Working Group is responsible for overseeing the UK's policy response to ML and proliferation financing. Where a specific view of TF is required, the issue will be considered by the Terrorist Finance Board.

96. At the operational level, UK LEAs exhibit particularly positive co-operation across all jurisdictions in the UK. The NCA-led Criminal Finance Threat Group and Economic Crime Threat Group provide intelligence and operational co-ordination. They meet quarterly to agree the picture of threat, reach an agreed response to these risks, and identify emerging risk areas. These groups are underpinned by sub-groups focused on key risk areas identified in the 2015 and 2017 NRAs (e.g. professional enablers, cash-based ML and high-end ML).

97. The Government Agency Intelligence Network (GAIN) is an intelligence-sharing platform which brings together a range of government departments and LEAs (including the police, NCA, Companies House and others) to share information and

solve issues by submitting referrals which are disseminated to members for intelligence-gathering. Inter-agency law enforcement co-operation is further facilitated by active use of embedded law enforcement officers and co-locating different departments to facilitate collaboration. The ability and willingness of UK LEAs to provide cross-agency support and share resources allows the UK to respond effectively to changing risks and emerging trends, despite an austerity programme having been in place since 2008.

98. At the supervisory level, the AML Supervisors Forum meets quarterly to share information and best practice between supervisors, HMT, OFSI, the Home Office, the NCA, and the UKFIU. One goal of the forum is to develop a common understanding of risk. Three affinity groups for the public sector, accountancy and legal supervisors also meet regularly to exchange information on the sectors.

99. The UK also has a number of groups that bring together public and private sector representatives. JMLIT is a particularly positive example of a useful resource for ML intelligence and investigations. Agencies actively use this tool to enhance access to financial intelligence and inter-agency co-operation on specific cases, as well as to broaden their understanding of ML risks, trends, and methodologies. A Money Laundering Advisory Committee and a Financial Sector Forum also bring private sector representatives together with representatives from policy departments, LEAs, and supervisors.

Private sector's awareness of risks

100. The UK has undertaken extensive outreach to ensure that the private sector is aware of and responsive to the risks identified in the NRA, including involving the private sector in the development of the NRAs. Both the 2015 and 2017 NRAs are published on the gov.uk website. Following publication, a cross-Government and law enforcement team presented the detail of the analysis behind the findings to all supervisors at the AML Supervisors Forum. The NRAs were also disseminated through a wide range of government and supervisor mailing lists. The NRA findings were discussed in further detail at meetings and conferences with the private sector, including UK Finance's annual financial crime conference. The 2016 Action Plan for addressing the risks identified in the first NRA was opened to detailed consultation with the regulated sectors. As well, the MLRs require that all regulated sectors take the NRA into account when conducting their own risk assessments. Private sector representatives met with during the on-site visit reported using the NRA when conducting their own risk assessments.

101. Law enforcement risk assessments are also shared with the regulated sector through a variety of fora. A redacted version of the National Strategic Assessment is published by the NCA. Other LEA intelligence assessments and findings are disseminated through supervisors' outreach programmes.

Overall conclusions on IO.1

102. **The UK is rated as having a high level of effectiveness for IO.1.**

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Use of financial intelligence (Immediate Outcome 6)

a) While there are many strong features of the UK's use of financial intelligence, the deliberate policy decision to limit the role of the UKFIU and persisting issues with the SAR reporting regime cast doubt over the overall effectiveness of the exploitation and use of financial intelligence.

b) Particularly strong features of the system are that: available financial intelligence and analysis is regularly used by a wide range of competent authorities to support investigations of ML/TF and related predicate offences, trace assets, enforce confiscation orders and identify risks; direct access to the SAR database (which contains 2.3 million SARs) significantly enhances LEAs' ability to access financial intelligence in a timely manner; LEAs at the national, regional and local levels have the necessary resources, skills and expertise to use that financial intelligence in line with their operational needs; and the Joint Money Laundering Intelligence Taskforce (JMLIT) is an innovative model for public/private information sharing that has generated very positive results since its inception in 2015 and is considered to be an example of best practice.

c) The UKFIU's lack of resources (human and IT) and analytical capability is a serious concern considering the level of ML/TF risk the UK faces and in light of increasing SAR filings and DAML/DATF requests. The UK's deliberate policy decision to limit the role of the UKFIU in undertaking operational and strategic analysis calls into question whether SAR data is being fully exploited in a systematic and holistic way and providing adequate support to investigators. The assessment team were not satisfied that the analysis role envisaged to be performed by FIUs under the FATF Standards is sufficiently occurring through the NCA and in individual agencies.

d) While reports of a high quality are being received, the SAR regime requires a significant overhaul to improve the quality of financial intelligence available to the competent authorities. There is also significant underreporting by higher risk sectors such as TCSPs, lawyers and accountants. Non-bank private sector representatives consistently noted that the SAR regime is not fit for their purposes. There are also concerns about the poor quality of some SARs across all reporting sectors. These concerns are recognised by the UK, but have persisted for a number of years (see Chapter 5 on IO.4).

3

ML investigation and prosecution (Immediate Outcome 7)

a) The UK routinely and aggressively identifies, pursues and prioritises ML. Annually, the UK achieves around 7 900 investigations, 2 000 prosecutions and 1 400 convictions for cases of standalone ML or where ML was the primary offence. Prosecution and conviction figures are notably lower in Scotland. This may be due to Scotland's higher evidentiary threshold which can pose challenges in prosecuting criminal cases, particularly ML leading authorities to place a greater emphasis on general or catch-all offences.
b) Financial investigations are considered a key part of all predicate offence investigations. Local, regional and national authorities have access to specialised financial investigators and ML expertise. Agencies actively co-operate and share information and resources. This leverages and maximises resources which is positive in the context of the UK's ongoing austerity programme. JMLIT is a notable, positive example of an information-sharing and intelligence-gathering tool which has proved effective in ML investigations.
c) Case studies show that the UK investigates and successfully prosecutes a wide range of ML activity broadly in line with the risks identified in the NRA. High-end ML is a long-standing risk area for the UK and was only given specific priority in December 2014. Since 2014, investigations have increased. As these cases are complex and generally take years to complete they have not yet progressed to prosecution and conviction. The UK provided some case examples demonstrating high-end ML investigations, prosecutions and convictions before 2014, but limited statistics were available. It was therefore difficult to determine whether the level of high-end ML prosecutions and convictions is fully consistent with the UK's threats, risk profile and national AML/CFT policies.
d) The UK's ability to pursue criminal prosecutions against legal persons is limited by practical challenges in proving such cases. The UK has demonstrated its ability to take other action against legal persons involved in ML.
e) Where a ML conviction is obtained, the sentences appear to be effective, proportionate, and dissuasive. Alternative actions are pursued where a ML prosecution or conviction is not possible. The vast majority of sentences in Northern Ireland fall at the lowest end of the scale which is likely due to the types of cases and risk profile of the jurisdiction.

Confiscation (Immediate Outcome 8)

a) The UK pursues confiscation as a policy objective. Specialised asset recovery teams at the national, regional, and local level can access a range of available tools to identify, restrain and recover assets, including new unexplained wealth orders and orders to freeze and forfeit bank and building society account funds. LEAs are used to working with the UK's legal test for restraint which can be challenging to meet where assets are not restrained prior to arrest.

b) The UK demonstrated its ability to recover assets in a range of ML/TF and predicate cases consistent with its national priorities and risk profile. A particular strength of the system is active enforcement of confiscation orders through multi-agency enforcement teams and the use of automatic imprisonment sentences where individuals default on payment. Where another jurisdiction is involved, the UK is willing to pursue asset sharing or repatriation.
c) Cash is seized at the border and the authorities proactively target high-risk ports. Increasing threats posed by cash in freight have been identified and authorities are working to improve detection and seizure in this area.

Recommended Actions

Use of financial intelligence (Immediate Outcome 6)

a) Substantially increase the human resources available to the UKFIU and review the UKFIU's role to ensure that financial intelligence is fully exploited in the context of the significant ML/TF risks faced by the UK and so it is better able to co-operate with foreign FIUs.
b) Substantially increase the UKFIU's IT capacity, including by updating analysis software, ensuring sophisticated screening of SARs and allowing automatic checks against multiple databases.
c) Prioritise reform of the SAR regime, including by modernising reporting mechanisms so they are fit-for-purpose for the whole range of reporting entities and making the on-line SAR form (or its replacement) more user-friendly.
d) Give more in-depth feedback on SARs, particularly to smaller reporting entities.
e) Increase the UKFIU's profile, both domestically and internationally, and ensure that it is fully independent operationally.
f) Develop better statistics on how the SAR database is accessed by LEAs and on the UKFIU's analysis and disseminations.
g) Continue to monitor the performance of JMLIT to ensure that the UK's public-private partnership on financial intelligence has sufficient resources to meet the demands for its assistance particularly on operational information sharing.

ML investigation and prosecution (Immediate Outcome 7)

a) Improve the collection of consistent, comprehensive, national statistics on all ML investigations, prosecutions and convictions to ensure the UK has access to up-to-date, national statistics which reflect the full extent of UK LEA ML activity on which to base its policy and operational decisions.
b) Continue to prioritise high-end ML investigations and monitor the situation to ensure that ongoing cases are pursued through to prosecution and conviction as appropriate.
c) Continue to promote the investigation and prosecution of ML in Scotland despite the high evidentiary threshold.

d) Ensure that, where appropriate, the UK is able to pursue the criminal prosecution of legal persons for ML.

Confiscation (Immediate Outcome 8)

a) Monitor the use of available asset recovery tools, including the new unexplained wealth orders and orders to freeze and forfeit bank account funds, to ensure they are consistently used and understood.
b) Seek restraint of assets, where possible, before or upon the laying of a charge and ensure that where this is not possible, authorities continue to consistently employ appropriate investigative measures, such as account monitoring orders, to enable restraint and ensure assets are not dissipated.
c) Increase the use of asset sharing or repatriation where cases and international co-operation permit.
d) Continue to work with international partners to promote the recognition of civil recovery tools.
e) Continue developing the UK's understanding of the movement of cash at the border, including in freight, with a view to developing a specific strategy for pursuing these risks if necessary.
f) Given the risks it faces from cash-based ML and the recent success of Operation Enfatico, the UK should: increase joint working and intelligence-sharing; ensure continued professional development for officers from relevant agencies; and consider adopting multi-agency taskforces with financial investigation capabilities at ports with a high risk for cash movements.
g) Improve the collection of consistent, comprehensive, national statistics on the restraint and recovery of ML/TF proceeds and instrumentalities across different authorities and agencies.

103. 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.3, R.4 and R.29-32.

Immediate Outcome 6 (Financial Intelligence ML/TF)

Use of financial intelligence and other information

104. The UK authorities at the national, regional and local levels make regular use of financial intelligence and other relevant information to identify investigative leads, develop evidence in support of investigations and trace criminal proceeds related to ML/TF and associated predicate offences. This is primarily achieved through the direct access that LEAs have to the UKFIU's SARs database, access to a wide range of other sources of information, a broad network of specialist financial investigators, and the powerful JMLIT mechanism.

105. The assessment team based its conclusions on a variety of information including: statistics on the SAR data collected by the UKFIU and accessed by LEAs; discussions with a wide range of LEAs at the national/regional/local levels; discussions with sources of financial intelligence and other information (e.g. JMLIT, Companies House, reporting entities); and the team's review of numerous cases

demonstrating that such information and intelligence is used in practice to support investigations and trace assets.

106. The authorities use financial intelligence and other information from a wide range of diverse sources. One of the largest sources of financial intelligence is the SARs database which contains over 2.3 million SARs, including Defence Against Money Laundering (DAML) SARs and Defence Against Terrorist Financing (DATF) SARs. The SARs database is maintained by the UKFIU housed in the NCA's Economic Crime Command.

107. The SARs database is made available to 4 825 accredited end-users (financial investigators or administrators) in 77 end user organisations within seven to nine days. This distributed model of SARs dissemination enables LEAs to access SARs directly and apply their own resources to their analysis without waiting for a dissemination from the UKFIU. It also means that LEAs consider reviewing SARs to be a routine part of their investigative process (not something referenced only in response to dissemination by the UKFIU).

Table 0**. Access to SARs**

Access Gateway	What	When	Who
Elmer	All SARs and requests from foreign FIUs	Immediately	UKFIU officers only
Money-web	All non-sensitive SARs (99.6% of SARs)	7 calendar days from receipt	3 076 accredited end-users*
Arena	All non-sensitive SARs (99.6% of SARs)	7 calendar days from receipt	1 457 accredited end-users*
Discover	All non-sensitive SARs and NCA intelligence	7 calendar days from receipt	900 NCA accredited end-users
Email direct to end-user	DAML, sensitive and priority SARs	Immediately, DAML SARs then available on Money-web prior to day 7 for specific end user	Contact point designated by UKFIU
Requests	Sanitised intelligence reports or packages derived from analysis of all non-sensitive SARs	After request from FIU	Non-accredited competent authorities or accredited end-users without direct access to Money-web or Arena.

Note: Money-web can be used to access non-sensitive SARs and live DAML cases. It also enables users to submit feedback on SARs and add interest markers. Arena uses similar DataLab tools to analyse and visualise data, but only has one dataset – the non-sensitive SARs. Discover uses similar underlying tools to analyse and visualise the data, but has 10 datasets alongside the non-sensitive SARs.
*There were 4 825 unique users in 2017. There are 608 people who have access to both Money-web and Arena.

108. In the context of a distributed model of SARs dissemination, the authorities do not collect specific comprehensive statistics on the results obtained using this intelligence. Nevertheless, numerous cases were provided which demonstrate that financial intelligence and other relevant information are being used to successfully identify new targets (including money launderers and terrorist financiers), dismantle criminal networks, and trace assets.

109. Law enforcement agencies seek financial intelligence from a wide variety of sources throughout the lifetime of an investigation. For example:

a) The Police National Database (PND) is populated by local force intelligence systems and provides an overview of intelligence held by all forces. It contains

details of persons, addresses, vehicles, organisations, phone numbers, associations, modus operandi, financial activity and assets.

b) The Police National Computer (PNC) provides arrest, conviction, descriptive details, information markers and asset recovery markers against individuals. PNC also holds data regarding vehicles and licensing which can be used for the purposes of asset recovery.
c) Police databases maintained by the Scottish Police and the Police Service of Northern Ireland (PSNI) are directly available to the LEAs in these jurisdictions, and available upon request to LEAs of the UK's other constituent nations.
d) The Joint Asset Recovery Database holds records of confiscation and restraint orders, civil recovery, and cash seizures in England, Wales and Northern Ireland. In Scotland, this information is held on internal databases maintained within Police Scotland's Reactive Financial Investigation Unit.
e) Companies House is a public register of legal and beneficial ownership information and also includes details about disqualified directors.
f) Supervisory data held by the FCA and HMRC may be accessed directly by their respective enforcement arms and is available to other LEAs upon request. Supervisory data held by the Gambling Commission and other professional body supervisors is also available to LEAs upon request.
g) HMRC databases, including the register of trusts with UK tax consequences (Trust Registration Service), tax information, and information on UK citizens with overseas bank accounts may be accessed directly by the HMRC's law enforcement arm and are available to other LEAs upon request.
h) The Cash Declaration Database contains all declarations filed with respect to cross-border transportations of cash or bearer negotiable instruments exceeding EUR 10 000 which are entering or leaving the EU. Since February 2018, HMRC submits this data monthly to the NCA in line with an MOU. This information can then be provided to the UKFIU. There are some limitations as to the information that can be stored due to data protection legislation.
i) The Customs Handling of Import & Export Freight database contains all declarations related to incoming and outgoing freight.
j) Records held by financial institutions and DNFBPs may be provided either through compulsory production orders made to individual institutions or under section 7 of the Crime and Courts Act 2013 which provides a broad gateway for entities to voluntarily share information with the NCA ("the s.7 gateway").
k) Records held by certain larger banks may be obtained by requests to multiple FIs through the JMLIT which also uses the s.7 gateway.
l) Experian, Equifax and Call Credit which are credit reference agency databases.
m) World Check and GBG Connexus which are commercial intelligence databases.
n) KYC6, KYCC360 and Dow Jones which are due diligence proprietary databases used by the FCA.
o) The Land Registry and Motor Vehicle Registry record property and vehicle ownership respectively.
p) Covert sources, public hotlines, whistle-blowers and consumer complaints, and open source research are additional sources of information.
q) Information and records held abroad may be requested through the Egmont Group of FIUs, Europol, Interpol, the EU network of National Asset Recovery

Offices (ARO), the EU's Camden Asset Recovery Inter-Agency Network (CARIN), and bilateral channels with international counterparts.

110. A particularly strong feature is that all LEAs employ specialist financial investigative personnel to aid in the pursuit and interpretation of financial intelligence. Over 3,500 practitioners in England, Wales and Northern Ireland have taken the NCA's financial investigation course. In Scotland, financial intelligence training is delivered by Police Scotland.

111. Financial intelligence is used most extensively at the national level by the NCA, HMRC, the SFO, and the FCA, for example:

a) The NCA's National Intelligence Hub (NIH) includes two ML intelligence units. It uses SARs and a range of other intelligence to develop financial profiles of subjects and entities and identifies key priority targets for investigative teams to take action on. The NCA personnel include 114 specialist financial intelligence officers and 62 financial investigators. The NCA has access to highly sensitive intelligence, including information from investigations and covert sources, which it combines and cross-checks with SARs, other information obtained from financial institutions and partner agencies, and open source information. NCA's investigations on high-end ML facilitated by professional enablers are complex, lengthy and utilise very large amounts of financial intelligence (see box 1 below). The SARs databases is also used by all areas of the NCA, particularly those focusing on corruption, fraud, firearms and drug trafficking.
b) HMRC has dedicated Intelligence Development Teams and Operational Support teams making extensive use of SARs and the extensive amount of information available to the agency. HMRC's central database has access to 31 datasets and 22 billion records, including tax records for individuals and companies, import/export records, cash declarations and seizure information. In 2016-17, the Proceeds of Crime Operational Support team produced 237 financial profiles and conducted 1 452 other financial profiling related tasks. HMRC has 131 financial intelligence officers, 185 financial investigators and 114 financial intelligence administrators. Two HMRC officers are seconded to the UKFIU on a full-time basis to assist with tax and revenue functions with an additional two officers providing support at HMRC.
c) The SFO uses financial intelligence to investigate high-end fraud, corruption and bribery, and related ML, and employs 21 financial investigators. The SFO uses SARs at the outset and in ongoing investigations and also obtains financial intelligence from its ability to compel individuals, financial institutions, accountants and other professionals to provide it with information on an investigation.[5]
d) FCA's Intelligence Department uses SARs and information from supervision activity and enforcement actions, whistle-blowers, partner and international agencies to target ML, market abuse, insider dealing, bribery and corruption. FCA staff includes 10 financial investigators, 39 financial intelligence officers and eight financial intelligence administrators. FCA uses SARs, in addition to

5 Criminal Justice Act 1987, s.2.

the Shared Intelligence Service (SIS) to prevent criminals from controlling financial institutions (see Chapter 6 on IO.3).

e) JFAC, a multi-agency taskforce focusing on professional enablers, is extracting financial intelligence from large data sets such as the recent 'Panama Papers'. It cross-checks SARs data to identify intelligence contained within other data sets that could otherwise be dismissed as information only.

Box 1. **The use of financial intelligence by the NCA**

A UK bank became aware that one of its accounts had received an unauthorised transfer via malware. It subsequently identified a fraud totalling GBP 3.5 million across linked accounts. The fraud was aided by a bank insider acting as a professional enabler. The bank reported the malware to the NCA which opened an investigation leading to two professional launderers. Financial intelligence was obtained from a wide range of sources: the reporting bank, and other banks affected by the malware, which provided significant financial intelligence and evidence; SARs linked to the accounts and individuals involved; Cifas, a non-profit fraud reporting agency, provided intelligence on fraud reports against 200 accounts; and JMLIT which provided available intelligence from financial institutions and other LEAs. The investigation resulted in the prosecution and conviction of the two professional launderers who were sentenced to 5 years 8 months and 7 years imprisonment respectively. The bank insider was subsequently sentenced to 6 years 4 months.

112. At the regional level, all nine Regional Organised Crime Units (ROCUs) have dedicated criminal finance intelligence teams making extensive use of financial intelligence and other relevant information in predicate offence and ML investigations. The ROCUs also have asset recovery and confiscation enforcement teams actively using financial intelligence to trace assets. Financial intelligence officers have been recruited into confidential units within the ROCUs to provide real-time financial intelligence to live investigations including active surveillance and enforcement activities.

113. Scotland and Northern Ireland Police also actively utilising financial intelligence, including SARs, and other relevant information as indicated below.

Table 4**. Use of SARs in Northern Irish investigations (2012 – 2017)**

Year	SARS	DAML
2012/13	5420	164
2013/14	5536	105
2014/15	6131	98
2015/16	6446	77
2016/17	7109	88

Table 5. **Use of SARs in Scottish investigations (April 2013 – April 2017)**

Year	SARs reviewed	SARs developed for information and further investigation
2013-2014	13,795	1,401
2014-2015	13,137	1,572
2015-2016	15,981	1,273
2016-2017	21,900	1,900

114. Local police forces have specific roles or dedicated teams to receive and assess SARs. For example, the City of London Police has a dedicated SARs unit. The Metropolitan Police Service (MPS) has a Financial Intelligence Development Unit. Even smaller police forces have specialist financial investigators which enhance their ability to use financial intelligence effectively. Policing units can cross-check SARs against the Police National Database and Police National Computer, and reports from public and international partners.

115. Another particularly strong financial intelligence development feature is the Joint Money Laundering Intelligence Taskforce (JMLIT). JMLIT is an innovative model for public/private information sharing that has generated very positive results since its inception in 2015 and is considered to be an example of best practice (see box 2 below). JMLIT brings together selected private sector participants and competent authorities, including LEAs, supervisors and the UKFIU, via the NCA to undertake a collaborative, intelligence-led approach to identifying ML/TF. It allows authorities to proactively seek information from selected private sector firms conducting a large proportion of financial activity in the UK (89% of the volume of UK Personal Current Accounts). It also provides a mechanism for information sharing within the private sector.

Box 2. **Public/private sector information sharing – JMLIT**

JMLIT is comprised of an Operations Group and Expert Groups aligned to each of its core priorities. The Operations Group facilitates weekly meetings between its member LEAs and vetted bank representatives, supporting live requests for intelligence law enforcement investigations. Private sector members of JMLIT are encouraged to refer cases to the Operations Group using an information sharing gateway which complements, but does not interfere with, the mandatory obligations imposed by the UKs SARs regime.

Expert Groups operate along thematic lines to identify typologies and emerging risks and transmit this information to the wider financial sector in an accessible way. The key areas of focus for the Expert Groups are based on threats identified in the NRA and key serious and organised crime priorities (e.g. trade-based ML, ML through capital markets, human trafficking and organised immigration crime, proceeds of corruption, TF and future threats).

The work of the Expert Groups has resulted in 33 alerts for the financial sector.

The Operations Group deals with live investigations. It is briefed on an average of three cases per week by relevant LEAs, some of which may have originated as referrals from JMLIT's private sector members. Members provide information to the NCA in response to the requests on an ongoing basis to aid in the investigations. The Operations Group has accepted and developed 443 cases from law enforcement. Since inception and as a direct consequence of JMLIT activity, approximately GBP 9 million suspected to represent criminal proceeds has been seized or is under restraint, 105 arrests have been made, 3 369 accounts have been identified that were not previously known to law enforcement, 3 301 bank-led investigations were begun and over 1 563 accounts have been subject to closure.

Reports received and requested by competent authorities

116. Case studies demonstrate that SARs contain relevant information which advances investigations. LEAs interviewed on-site also advocated the benefits of the distributed-SAR model in the UK context. While some variance in reporting is expected given the high volume of reports and the range of reporting entities in the UK, concerns remain about the extent to which accurate financial intelligence is available through SARs because of the low level of SAR reporting in some sectors and general concerns about the poor quality of SARs. Given the high volumes flowing through many sectors in the UK financial system, this is a serious issue. The UKFIU has increased outreach efforts to reporting entities in an attempt to address these issues, but the results are yet to be seen. This issue is somewhat mitigated by the JMLIT which has significantly increased the quality of SARs in some areas but is limited to the largest financial institutions.

117. Since February 2018, HMRC has shared cross-border cash reports with the NCA on a monthly basis and both agencies use this intelligence to inform operation activity. Joint investigative teams provide an opportunity for HMRC to share cross-border cash declarations with other LEAs. However, beyond this mechanism, it is not clear to what extent cross-border cash declarations are used by other UK LEAs (e.g. the Police, the SFO and the FCA) for intelligence or investigative purposes.

118. The assessment team bases its conclusions on a variety of information including: interviews with competent authorities, statistics on SARs and cross-border cash reports and reviews of classified strategic assessments. Due to its all-crimes approach, the UK does not keep statistics on SAR reporting by predicate offence and was unable to provide comprehensive statistics on use of SARs by authorities.

119. LEAs at the national, regional and local levels integrate the use of SARs and other financial intelligence into their standard practice. Investigators can view and use all non-sensitive SARs on Money-web or Arena (99.6% of SARs held in the database). In 2017, agencies accessed SARs by Money-web and Arena over 1.5 million

times. From 2014 to 2016, SARs were viewed by end-users over 4 million times (3 416 170 times on Money-web/Discover and 194 941 times on Arena). While the number of views is somewhat lower than other FATF countries with distributed SARs models, case studies and discussions with LEAs demonstrated that the SARs databases were accessed regularly and in a high number of cases. Both the number of users and the number of times SARs are being accessed on Arena and Money-web is increasing. LEAs at all levels confirmed that they regularly use financial intelligence to develop and progress their investigations (e.g. by linking individuals to bank accounts, transactions, companies, assets, associates and telephone numbers).

120. In addition to ordinary SARs, the SARs database contains DAML or DATF SARs. The UK model for reporting suspicious activity is based on criminalising the failure to report suspicious activity, subject to defences being available where certain conditions are met. The defence regime applies where a reporting entity has a suspicion of ML/TF and freezes the transaction while seeking a 'defence' from the UKFIU for carrying it out. The reporting entity seeks a defence by filing a DAML or DATF with the UKFIU after which the NCA (through the UKFIU) has a strict time limit within which to respond. The UK changed the terminology relating to DAML and DATF SARs. Previously known as 'consent' SARs, the UKFIU found that this resulted in a large number of irrelevant reports as it was too often misinterpreted as the act of seeking permission or using the regime as part of a risk-based approach to permit a transaction to continue.

Table 6. **Numbers of SARs received by the UKFIU**

Year	2011/12	2012/13	2013/14	2014/15	2015/16	2016/2017
Total SARs	278,665	316,527	354,186	381,882	419,451	441,953
Consent SARs		14,103	14,155	–	–	
Consent SARs refused (and %)	1,229 (9.5%)	1,387 (9.8%)	1,632 (11.5%)			
DAML requests*	–	–	–	14,465	17,909	19,445
DATF requests	–	–	–	207	289	317
DAML requests refused (and %)	–	–	–	1,356 (9.37%)	1,242 (6.94%)	1,301 (6.4%)
DATF requests refused (and %)	–	–	–	18 (8.7%)	19 (6.57%)	24 (7.57%)
Breaches of confidentiality		2	2	3	2	1

Note: *The consent SAR regime was reformed in 2014 and are now referred to as the Defence Against Money Laundering or Defence Against Terrorist Financing requests.

121. DAML and DATF requests (roughly 4% of SARs) are a useful type of financial intelligence, particularly in ML/TF prevention. The majority of cases where SARs trigger an investigation in the UK are in response to DAMLs (in part due to the legal obligation to investigate these requests within a set time period). In 2016-2017, as a result of DAMLs, GBP 46 281 214 was restrained, GBP 17 142 640 in cash was seized, GBP 6 470 595 of funds was disrupted and 29 arrests were made. In 2017/18, as a result of 423 DATF SARs, over GBP 300 000 was frozen relating to suspected TF.[6] This is a significant amount which illustrates the utility of this mechanism, given the

6 The UK only captures data relating to the freezing action in relation to DATF requests and does not collect further data on ongoing action.

nature of the UK's TF risks (often low value, self-funded and derived from legitimate sources). The number of SARs, DAMLs and DATFs being filed is increasing annually. The FIU and relevant police services expend significant resources in responding to DAML and DATF requests. There are clear operational benefits of this system, particularly in the context of restraining and/or confiscating assets and in triggering ML investigations (see also the case study below). However, it was not clear to the assessment team if this reactive process and the resources allocated to it, clearly aligned to combat the highest priority ML/TF risks facing the UK.

Box 3. **Example of DAML SAR enabling law enforcement action**

In 2017, the UKFIU received a DAML SAR from a reporter, regarding a USD 500 million transaction. On receipt of the SAR, the UKFIU analysed it and identified PEP links and so referred it to the NCA's International Corruption Unit (ICU) for advice. This resulted in consent being refused and an NCA operation being tasked. Enquiries suggested the transaction appeared to be embezzlement and grand corruption, likely designed to steal the funds from another country.

In order to ensure the monies were returned safely, NCA needed to make enquiries of the country's authorities which would take longer that the 31 day moratorium period for DAML SARs. Therefore, it was decided to approach the court to apply to the court for the first ever extension of the moratorium period, a new power under Criminal Finances Act 2017.

UKFIU worked closely with the officer in respect of the information that could be disclosed to court. The judge agreed to extend the moratorium period, and on the same day the UKFIU decided to maintain its refusal to give consent to proceed. A further extension and UKFIU refusal took place subsequently in order to allow the ICU to continue its enquiries. Following the receipt of a number of assurances safeguarding the account, it was agreed that the funds could be safely remitted. The UKFIU made a decision to grant consent accordingly, allowing the monies to be returned. The USD 500 million has now been transferred safely back to the originating account.

122. The NTFIU analyses TF SARs which are prioritised and screened by the UKFIU. The NTFIU has an officer embedded in the UKFIU to quicken the flow of information. It also has a dedicated Financial Intelligence Development team with an independent work stream dedicated to managing SARs. The NTFIU uses a range of open source and classified intelligence products, alongside LEA and commercial databases, to investigate TF, detect whether SARs are linked to terrorism and build financial profiles. Classified intelligence is received from 11 local counter-terrorism and intelligence units and the UK intelligence community (principally the Security Service). The number of TF SARs and the disseminations to counter-terrorism units is increasing. The NTFIU provides feedback to firms' Money Laundering Reporting Officers (MLROs) on TF SARs biannually.

Table 7. **Terrorist financing SARs and disseminations**

	2013	2014	2015	Total
Total TF SARs received	318	756	1 082	2 156
TF-related SARs disseminated to Counter Terrorism Units	856	1 342	1 899	4 792
Increase in SARs disseminated from previous year	23%	57%	42%	

123. The requirement to report SARs applies to all financial institutions and DNFBPs as required by the FATF. Ordinarily, this should ensure that financial intelligence from all of the sectors covered by the FATF Recommendations is available, but the low level of reporting in many sectors and the poor quality of many SARs negatively impacts the quality and usefulness of the financial intelligence available to the competent authorities (see Chapter 5 on IO.4).

124. The UKFIU has taken steps to improve the SARs regime. The UKFIU contributes to SARs Affinity Groups for the legal and accountancy sectors and SARs Supervisor Forum to assist in improving the quality of SARs. It also produces a SARs Annual Report and engages at conferences and events with reporting entities. It has also undertaken some limited analysis of SARs to increase the quality of SARs intelligence from reporting entities. In 2016, it focussed on the legal and accountancy sectors, but the analysis is largely quantitative and does not reflect a strong understanding of the sector risks. Additionally, in 2016, the UKFIU changed the terminology relating to DAML and DATF SARs.

125. Important outreach is also undertaken by the supervisors. For example, HMRC cover SARs in their webinars, including one specifically on SARs which has been viewed 1 200 times.

126. Despite these outreach efforts, the vast majority of private sector participants interviewed showed little awareness of the UKFIU's guidance products and suggested that they get no feedback on the SARs they file (although some noted that they were asked for additional information on DAMLs). This may be in part to the limited resources dedicated to this function (four staff undertaking strategic analysis and an additional four staff undertaking engagement activities with reporting entities and end-users - see figure 1). In addition to this, the UK recognises that there is underreporting from DNFBPs, in particular from the legal and accountancy sectors which the NRA identifies as being at high risk. This may also be a result of lacking and inconsistent supervision of these sectors (see Chapter 6 on IO.3). There are also serious concerns about the 'SAR online' reporting tool which is not adapted for non-banks and inhibits reporting entities from providing input in a useful format (see Chapter 5 on IO.4). The UK has recognised these issues for some time and is currently discussing SARs reform.

127. Through the JMLIT, LEAs can, with one request, obtain information from multiple institutions, which is an efficient means to develop a comprehensive intelligence picture. When participating institutions develop a suspicion of ML/TF in a JMLIT case, they are obliged to submit SARs to the UKFIU. Such SARs are considered to be of a very high standard. While the JMLIT provides an excellent resource to competent authorities in accessing information held by the largest institutions in relation to high priority cases, it is not an appropriate avenue for the majority of cases and only provides access to a limited number of the biggest financial institutions. That

said, there are flow-on benefits for other reporting entities. JMLIT has developed alerts that are distributed to a wider audience and non-JMLIT banks have filed SARs based on the information learnt from these alerts.

128. In addition to JMLIT, other channels enable competent authorities to obtain information. LEAs frequently use production orders, account monitoring orders, customer information orders and disclosure orders to seek information directly from entities. A streamlined process allows production orders to be sought and granted electronically, reducing court time. Disclosure orders are a particularly useful tool as they last throughout the lifetime of an investigation. Recognising their utility, the Criminal Finances Act 2017 now permits disclosure orders to be used in ML investigations by the FCA, HMRC and other LEAs. The s.7 gateway allows the NCA, including the UKFIU, to ask reporting entities to voluntarily provide information. The Criminal Finances Act 2017 also grants the UKFIU a new power to obtain a further information order to compel information relating to a SAR from reporting entities, but it remains to be seen whether this will be actively used.

129. In addition to SARs, the UK also collects cross-border cash reports (see table 8 below) and import and export declarations which are stored in databases maintained by HMRC. From February 2018, the NCA has had regular access to these databases under a MOU between the NCA and HMRC. This data is used to inform operational activity, but the recency of the MOU means it is not clear if these databases are systematically cross-checked against STRs and other financial intelligence. Other LEAs have access to HMRC databases primarily through joint investigative teams or embedded HMRC officers. Joint investigative efforts have proved successful in pursuing specific cross-agency projects with a focus on cross-border cash movements (see chapter 3 under IO.8 below). Outside these projects, cross-border cash and customs declarations can be accessed by HMRC officers and provided to LEAs for operational or intelligence purposes. This is facilitated where HMRC officers are embedded within the relevant LEA unit, as is the case in the NCA and in the intelligence teams that service the ROCUs. For other LEAs, the extent to and ease with which HMRC data is accessed for intelligence or investigative purposes is not clear.

Table 8. **Number of Cross-border Cash Declarations Received and Amount Declared**

	2014	2015	2016
Cash declarations received	2 317	4 789	3 747
Amount declared (EUR)	110 522 296	372 673 582	466 430 404

Operational needs supported by FIU analysis and dissemination

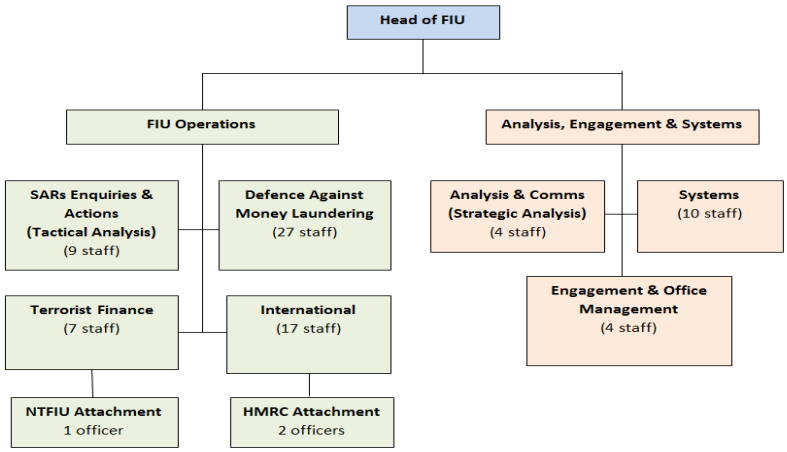
130. The UK has made a deliberate policy decision to limit the role of UKFIU in performing operational and strategic analysis. Compared to other FIUs which do have the mandate to analyse and disseminate reports, the UKFIU lacks both IT and human resources to perform these functions, particularly in light of increasing SAR filings and DAML/DATF requests. Under the UK's distributed model, all agencies are responsible for undertaking their own financial analysis of SARs. While financial intelligence is accessed by LEAs on a routine basis and strategic analysis does occur, in line with its limited role, the UKFIU does not play a sufficient role in supporting the operational needs of agencies through its analysis and dissemination function. By not

taking full advantage of its position, the UKFIU misses the opportunity to search for criminal activity that might otherwise be missed by LEAs which mine the SARs database for issues linked to their own geographical or operational remits.

131. The assessment team based its conclusions on: material and interviews with the UKFIU and other LEAs (including classified assessments); a visit to the UKFIU and demonstrations of its systems; and a review of case studies and examples of strategic analysis undertaken by the FIU.

132. The volume of SARs received by the UKFIU is significant and continues to rise. In 2015-2016, the UKFIU received 419 451 SARs, representing approximately half of all STRs reported across the EU in the same time period. However, the staff available to the UKFIU is inadequate with approximately 84 staff (currently around 80 full-time equivalent staff). At the time of the 2007 mutual evaluation, the UKFIU had 97 staff and expected an increase to 200 but it appears this surge did not occur. Only nine staff perform tactical analysis which is inadequate considering the increasing volume of SARs. The level of resources available for strategic analysis and international co-operation are also inadequate. The UKFIU uses a significant amount of its resources responding to DAML requests (27 staff), but there is a question about whether this is an efficient use of resources. Additionally, the UKFIU does not appear to have access to specialist skills such as forensic accountants to strengthen its ability to undertake sophisticated financial analysis. This is problematic given the large and diverse ML/TF risks facing the UK. For example, private sector participants provided feedback that there was a lack of understanding of the business of the non-bank regulated sectors.

Figure 1. Structure and staffing of the FIU



Operational analysis

133. The UKFIU screens SARS before they are made available to all agencies on Arena or Money-web. The screening tool is a basic key word search to identify SARs that relate to sensitive issues (e.g. LEA corruption) and other priorities (e.g. TF, vulnerable persons, PEPs, human trafficking). The keyword search appears to be the only screening tool available to the UKFIU and is a rudimentary filter. Keyword searches utilise a set of keywords that is maintained by the relevant teams in the UKFIU and also focus on glossary codes that reporting entities use to signal suspected

types of predicate offending or ML typology. Continued development of glossary codes in line with a range of NRA priorities has resulted in the UKFIU making more targeted disseminations to LEAs concerning those areas (e.g. disseminations relating to vulnerable persons and PEPs have increased in line with the increased use of those glossary codes). However, instead of focusing on the priorities of a single agency (the NCA), the UKFIU should focus on high-end ML and cash-based ML which are the highest risk ML threats facing the UK overall.

134. Where a search reveals a positive hit on a keyword and/or glossary code, the SAR is prioritised. All priority SARS are reviewed by a UKFIU officer and fast-tracked to the relevant LEA if prioritisation criteria are met. Roughly 13% of all SARs received in 2015-2016 (about 55 000) met the priority criteria and were reviewed by a UKFIU officer. Roughly 10% of SARs received in 2017 (again, about 55 000) were reviewed by the UKFIU as a result of positive hits through keyword screening. As the UKFIU has limited tools to undertake complex financial analysis, all database checks are undertaken manually by UKFIU officers on the prioritised cases before being disseminated to the relevant LEA based on crime type (NCA, SFO, HMRC) and/or location (regional or local police units based on any geographical links in the SAR). All TF SARs are prioritised and screened by the UKFIU, but are further analysed by the NTFIU and/or other relevant CTUs.

135. The UKFIU undertakes a preliminary review of DAML requests to identify which LEA should advise on the request and whether it relates to an ongoing investigation. All DATF requests are forwarded to the relevant CT units. LEAs consistently reported that the UKFIU undertakes only limited analysis and they analyse DAMLs and DATFs themselves. While the UKFIU does seek additional information to clarify the information in DAMLs and DATFs, there was no evidence that the UKFIU seeks additional information on normal SARs or in relation to other analysis or requests where no SARs were filed. This negatively impacts the ability of the UKFIU to follow the transaction trail, determine links between targets, and identify further proceeds of crime.

136. Statistics are not kept on the number of SARs directly disseminated by the UKFIU to LEAs for further action. However, the UKFIU's system for prioritising SARs for review appears to be simplistic compared to the risk-modelling undertaken by other agencies. Moreover, the lack of IT sophistication risks leaving many connections undiscovered and impacts the number and usefulness of direct disseminations to LEAs.

Strategic analysis

137. Strategic analysis by the UKFIU is also limited in line with the distributed model. To some extent, this is mitigated by the dedicated teams in LEAs (such as the National Intelligence Hub in the NCA) which undertake sophisticated operational and strategic analysis on the SARs that are available to them through Money-web and Arena. In addition, HMRC and NCA can bulk download SARS for analysis purposes. The following table indicates what type of strategic analysis products are produced by each agency, including the UKFIU.

Table 9. **Strategic Analysis performed by UK agencies**

Agency/Body	Role/Priority	Example of strategic analysis products
UKFIU	▪ Maintaining the SAR database, making a decision in relation to DAML and DATF requests and providing feedback to reporting entities to improve the quality of SARs.	▪ specific reviews of the following sectors; legal, charity, accountancy, banking, non-regulated gaming, estate agents, the UK property sector, money service businesses, trust or company service providers sectors, professional enablers as well as on corruption and on levels of reporting across the regime. ▪ Alerts on specific issues to reporting entities, and input into JMLIT alerts.
NCA	▪ The NCA's National Intelligence Hub (NIH) is responsible for articulation the threat to the UK from ML and identifying key priority targets and developing intelligence against them using both sensitive and non-sensitive material, including SARs. ▪ NCA's priority is on high-end ML and cash-based ML.	▪ Annual National Strategic Assessment (the team viewed the draft assessment for 2017). ▪ NCA Quarterly ML Tactical Assessment ▪ NIH Trade-Based Money Laundering, the use of gold to launder money, the mirror trading scheme, International Controllers, and Money Service Businesses
HMRC	▪ Responsible for tackling serious tax fraud and associated money laundering and has a Risk and Intelligence Service (RIS) which is responsible for developing strategic and tactical understanding of risk, intelligence interrogation of internal and external data sets and the development of intelligence packages for case adoption.	▪ RIS has issued 75 money laundering and terrorist financing related intelligence and threat assessments from 2013-16. ▪ The team viewed two assessments on ML/TF risks related to trusts and to gambling.
SFO	▪ Uses financial intelligence to investigate fraud, corruption and bribery.	▪ Strategic Assessment 2017
JMLIT	▪ JMLIT's expert working groups produce strategic and tactical products to increase private sector awareness of certain typologies.	▪ Examples of JMLIT alerts on Money Laundering and Trade Finance, Proceeds of Corruption Indicators, Possible Displacement from the Increasing Transparency of Beneficial Ownership of Companies
JFAC	▪ Originally established as a UK response to the leaked Panama Papers, the JFAC brings together NCA, HMRC, SFO and FCA and is responsible for developing understanding of methodologies, vulnerabilities and risks related to economic crime.	▪ Methodologies, vulnerabilities and risks, initially focusing on offshore financial structures and their abuse by criminals.
FCA	▪ The FCA has a dedicated Intelligence Department which manages FCA intelligence requirements across its Authorisations, Supervision and Enforcement Divisions in line with its strategic objective to make relevant markets function well. It has a separate Strategic Assessment team that sits within that Department.	▪ A range of strategic intelligence products using all source intelligence focused on market abuse, money laundering, fraud and other economic crime threats.
JTAC	▪ JTAC analyses and assesses all available intelligence relating to international terrorism, at home and overseas. It sets threat levels and issues warnings of threats and other terrorist-related subjects for customers from a wide range of government departments and agencies, as well as producing more in-depth reports on trends, terrorist networks and capabilities.	▪ UK Terrorist Financing Update
MI5	▪ The UK's national security and counter-intelligence agency.	▪ Northern Ireland-related terrorism - TF assessment (March 2018)
NTFIU	▪ Strategic lead for UK counter-terrorism policing.	▪ Financial profiles in relation to recent terrorist attacks in the UK

138. These agencies produce useful products and have access to a wider range of information than is traditionally available to FIUs. However, as the UKFIU does not have the remit to conduct strategic analysis across the entire SARs database, there is potential for opportunities to detect ML/TF activity to be missed. The assessment team were not satisfied that these potential gaps are being effectively mitigated by the strategic and operational analysis being undertaken by individual agencies. This is a serious concern, particularly given the importance and global reach of the UK financial system.

139. While the LEAs analyse and use the financial intelligence to which they have access (noting that one percent of SARs that are deemed to be sensitive are not shared

with LEAs), they will only ever do so in line with their operational and geographical mandates. The additional analysis and intelligence being developed by different agencies does not appear to be re-captured on the SARs databases so that it could be leveraged across agencies. There is a real need to ensure that this information is brought together so that ML/TF methods and trends are analysed holistically and lessons learnt fed back to LEAs and reporting entities on an ongoing basis.

140. The UK provided information on the role of the National Assessments Centre and the National Criminal Intelligence Hub within the NCA and the interagency Criminal Finances Threat Group (which meets for roughly two hours each quarter) in co-ordinating and consolidating the range of extensive agency-level operational analysis. The assessment team were not satisfied that these units or mechanisms adequately fill the gaps left by the UKFIU.

141. In 2017, the UKFIU developed the Intelligence Development Referral process (IDR) which allows officers to examine SARs and intelligence not already exploited by the UKFIU or LEAs, including spontaneous disseminations from overseas FIUs. In 2016/17, the UKFIU generated 46 cases through this process for dissemination to the NCA for further development and allocation. This is a relatively small number given the high volume of SARs being received. Nevertheless, it demonstrated the value of having the UKFIU do broad strategic analysis across the entire SARs database. The IDR process led to: three disseminations to the NCA Project team on professional enablers; one on trade-based ML to the NCA ML threat desk; one on HEML to the International Corruption Unit (ICU); and two on modern slavery to the relevant NCA threat desk. This relatively small and recent exercise demonstrates that there is a vast amount of information to be extracted from the full SARs database that is currently overlooked.

Co-operation and exchange of information/financial intelligence

142. Competent authorities demonstrated a high degree of co-operation, co-ordination and exchange of financial intelligence which is particularly important in the UK context given the high number of LEAs (including 43 police forces in England and Wales, in addition to Police Scotland and the Police Service of Northern Ireland). The distributed SAR model is a very broad exchange of information with adequate safeguards in place to protect the confidentiality of information exchanged and used. In the absence of a strong FIU, it is not clear that there overall co-ordination on the use/exploitation of financial intelligence. However, information exchange and co-operation does occur through a number of mechanisms outlined below.

143. The assessment team based these conclusions on various sources including: discussions with different agencies at national, regional and local levels; analysis of case studies; annual reports on SAR reporting; and a visit to the FIU's premises which included a walk-through of some of the security measures in place.

144. Competent authorities in the UK co-operate and exchange information and financial intelligence on a regular basis, including internationally (see Chapter 8 on IO.2). The NCA co-ordinates high-level AML activity through the multi-agency Criminal Finances Threat Group which has sub-groups on cash-based ML (led by Metropolitan Police), non-cash based money laundering (led by NCA), and professional enablers (led by HMRC). The group meets for two hours every quarter. The NTFIU co-ordinates activity on terrorist financing. Additionally, since February

2018, the HMRC and NCA, including the UKFIU, have a Memorandum of Understanding to share the Cash Declaration Database which can be matched against the SARs database. As this MOU was fairly recent at the time of the on-site it is not clear to what extent it has been successful.

145. A strong feature of the system is the NCA's section 7 gateway which is very broad and enables any person across the public or private sector to voluntarily share information with the NCA (including UKFIU), provided that the disclosure is for the purposes of exercising any NCA function. The gateway also allows the NCA to share received information with any person. This enables it to act as an information intermediary between LEAs and reporting entities. This gateway allows the sharing of confidential information without breaching any duty of confidence owed by the person sharing the information. While no statistics are kept on the number of section 7 requests, the NCA confirmed this power is used frequently, including on behalf of other LEAs and also in the context of requesting beneficial ownership information.

146. Another strong feature of the system is the UK's multi-agency taskforce model which enables agencies to exploit the different information gateways available to the participating members. The Joint Financial Analysis Centre (JTAC) and the JMLIT (see box 2 above) are good examples of this type of information exchange. In addition to this, the UK actively and regularly uses a range of secondments to facilitate the exchange of information.

Box 4. **Example of exchange of financial intelligence – Joint Financial Analysis Centre**

The Joint Financial Analysis Centre (JFAC) is a multi-agency taskforce, formed of the NCA, HMRC, SFO and FCA. It was originally established as a UK response to the leaked Panama Papers data. JFAC is staffed by intelligence professionals from all four agencies who bring with them a range of skills, experience, knowledge, and access to their respective intelligence systems and other databases. JFAC leads law enforcement's exploitation of criminal intelligence on economic crime and bulk financial data, in order to produce tactical intelligence, identify significant targets for new investigations and develop understanding of methodologies, vulnerabilities and risks, initially focusing on offshore financial structures and their abuse by criminals. For example, JFAC has identified 25 companies that appeared in the ICIJ Panama Papers data, Land Registry and SARs. Detailed development of the targets and those associated with them identified over 30 new money laundering, professional enabler, tax evasion and corruption leads.

147. There are mechanisms to exchange financial intelligence in Northern Ireland and Scotland. For example, the Criminal Finances sub group of the Organised Crime Task Force (OCTF) in Northern Ireland OCTF brings together relevant organisations involved in AML or assets recovery work. In Scotland, the Scottish Crime Campus facilitates collaboration between the 20 law enforcement partners who operate from it to effectively reduce the threat, risk and harm to Scotland's communities from serious organised crime and terrorism.

148. The UKFIU supports partner agencies by seeking information from international FIU counterparts. For example, in 2017, 96% of requests to foreign FIUs and 54% of spontaneous disseminations were sent on behalf of other UK LEAs. The UK also regularly exchanges information with international counterparts in a variety of ways (see Chapter 8 on IO.2). However, the limited role of the UKFIU undercuts its ability to effectively share information with foreign FIUs (see IO.2).

149. The UKFIU is situated within NCA offices which are secure and site access is controlled via the NCA Security Department and site guards. There are safeguards in place to protect the confidentiality of SARs (see R.29.6). The NCA/UKFIU's SARs Annual Reports identifies and explains any breaches of SAR confidentiality. Where breaches have been detected (approximately two to three annually), the UKFIU works with end-users of SAR data to remind them of the statutory offences in the legislation and ensure that appropriate re-training is undertaken.

150. The FIU seeks feedback from LEAs each year as part of the SARs Annual Report. As explained in section 3.2.3, more could be done to ensure that LEAs provide feedback to the FIU on SARs, and their use in investigations, in a systematic fashion.

Overall conclusions on IO.6

151. **The UK is rated as having a moderate level of effectiveness for IO.6.**

Immediate Outcome 7 (ML investigation and prosecution)

ML identification and investigation

152. The UK has a robust system for identifying and investigating ML cases. All local, regional, and national agencies with investigative powers are responsible for ensuring that ML cases are identified and investigated from the earliest opportunity and consistently view ML as a priority. The UK does not collect data on ML investigations at a national level, meaning available statistics on ML investigations were patchy and difficult to compare. As a result the assessment team based its conclusions primarily on: numerous case studies provided by the UK; the limited statistics on ML investigations that were available; and discussions with LEAs and prosecution agencies from across the UK jurisdictions, including the NCA, HMRC, FCA, police, CPS, SFO, and authorities from Scotland and Northern Ireland.

153. While the UK jurisdictions do not keep consistent investigation statistics, the available data indicates that approximately 7 900 ML offences are investigated annually. Overall, the UK prosecutes approximately 2 300 persons for ML each year and secures about 1 400 convictions annually. These statistics are not fully reflective of the UK's situation as they relate only to cases in which ML was the principal offence[7] and therefore exclude cases in which ML was pursued alongside a more serious offence. Nonetheless, the number of cases pursued in Scotland appears low, particularly when compared to the figures for Northern Ireland, a significantly

7 When collecting statistics, the basis for selection of the principal offence is: (a) Where a defendant is found guilty of one offence and acquitted of another, the principal offence is the offence for which they are found guilty; or (b) where a defendant is found guilty of more than one offence, the principal offence is the one for which the heaviest sentence is imposed.

smaller jurisdiction. This may be in part due to Scotland's different legal system and higher evidentiary threshold[8] which can pose challenges in prosecuting all criminal offences, including ML resulting in a preference for pursuing general or catch-all offences as opposed to ML charges. Scottish LEAs have undertaken outreach to increase the profile of ML charges and enhance their capability to pursue ML. While it remains early days, these efforts appear to be having a positive effect in practice.

Table 10. **Number of ML charges and ML convictions**

	2013	2014	2015	2016
England and Wales				
Proceeded against	2 349	2 095	2 307	1 998
Convictions	1 269	1 143	1 336	1 435
Scotland				
Proceeded against	13	42	18	21
Convictions	5	16	11	12
Northern Ireland				
Proceeded against	156	135	133	125
Convictions	129	118	95	58
TOTAL				
Proceeded against	2 518	2 272	2 458	2 144
Convictions	1 403	1 277	1 442	1 505

Note: 'Proceeded against' means to start a legal action against an individual. Convictions may take place several years following the commencement of proceedings, so the number of convictions in any given year cannot be strictly compared to the number of proceedings in the same year.

154. LEAs identify ML through two main sources: (i) financial intelligence and analysis, such as SARs, reports from intelligence agencies, open source intelligence, or foreign intelligence; and (ii) through an ongoing investigation into predicate activity. There is a risk that investigative opportunities, particularly relating to complex criminal activity, may be missed as a result of a lack of comprehensive, cross-agency analysis of available financial intelligence and the poor quality of SARs.

155. LEAs confirmed that financial investigations are systematically included in their investigations into proceeds-generating offences. Investigators and LEA officers receive training on ML and the pursuit of proceeds of crime. Some LEAs have also implemented guidance or mechanisms to promote the pursuit of ML. For example, the HMRC Fraud Investigation Service Handbook has a dedicated section on the benefits of pursuing ML investigations and prosecutions. At the local level, the crime recording system for the England and Wales police forces automatically flags the potential for a parallel ML investigation where proceed-generating offences are recorded. In Scotland, all organised crime investigation teams include a specialist financial investigator.

8 Scotland's evidential threshold requires (1) that there be at least one source of evidence that points to the guilt of the accused, and (2) that each essential fact be corroborated by other direct or circumstantial evidence. Reforming Scot Criminal Law and Practice: The Carloway Report (2011) found that of 458 serious criminal cases which did not make it to trial in Scotland, 58.5% would have had a "reasonable prospect of conviction" in England: www.gov.scot/Topics/archive/reviews/CarlowayReview

156. Once ML is detected, various LEAs have the mandate to pursue a ML investigation. The tasking decision depends on the nature of the case with the NCA leading national LEA groups that make tasking decisions. LEAs at all levels and across all jurisdictions have access to specialised ML and financial investigative expertise.

Table 11. **Roles of LEAs with responsibility for investigating ML**

Agency	Jurisdiction (for ML purposes)	Specialist units and resource	Types of ML case pursued
NCA	England and Wales, Northern Ireland (at the request of PSNI)	Economic Crime Command: 114 financial intelligence officers and 21 trainees, 62 financial investigators, 13 specialist volunteer officers with niche expertise and skills	• ML cases at the high end of high risk • Cases with an international dimension • Lengthy and complex cases
SFO	England, Wales, and Northern Ireland	Three specialist teams for fraud, bribery, corruption and associated ML, one specialist Proceeds of Crime Team: 21 financial investigators, 31qualified forensic accountants	• ML relating to serious or complex fraud, bribery, and corruption
HMRC	England, Wales, Northern Ireland and Scotland	Fraud Investigation Service: 131 financial intelligence officers, 185 financial investigators, 47 forensic accountants (to increase by 8 in 2018/19)	• Primarily ML arising from tax offences, but can pursue wider ML offences
FCA	England, Wales, Northern Ireland and Scotland	FCA Enforcement Division: approx. 150 investigations, 39 financial intelligence officers	• ML arising from market abuse, insider dealing, unauthorised business activity, and MLR breaches
ROCUs	England and Wales	Total ROCU staffing is approx. 250 FTEs, approx. 30 of which are financial investigators or financial intelligence officers. Each RART: 19 specialist staff. Each ACE: 7 FTEs. Also Project Teams with specific financial investigators.	• ML cases relating to serious and organised crime that do not meet the criteria for investigation by national agencies but require specialist expertise which is not available in local forces
Local Police	England and Wales	Specialist economic crime teams exist within all forces. E.g. the Metropolitan Police and the City of London Police host 739 financial intelligence officers and 466 financial investigators	• ML relating to predicate offending (e.g. drugs, fraud) • Lower level ML, typically cash-based
PSNI	Northern Ireland	117 financial investigators across PSNI. Economic Crime Unit: 48 financial investigators, 1 forensic accountant	• ML in Northern Ireland, including low-level ML and ML relating to serious and organised crime where this is not investigated by national agencies
Police Scotland	Scotland	Economic Crime and Financial Investigation Unit, with approx. 65 financial investigators, 1 forensic accountant Financial investigation training provided to all officers	• All ML in Scotland, with the exception of ML investigations conducted by HMRC

157. This framework ensures that all LEAs are well-equipped to pursue ML.

Box 5. **Pursuing ML at the national and the local level**

Operation Ewing originated as a drug investigation and developed into an ongoing multi-agency investigation into an organised criminal group suspected of fraud and ML. Various investigative steps have been taken: financial investigations have been conducted into shell companies; financial intelligence obtained through JMLIT has been used to track financial flows; and searches have been conducted on the premises of professional enablers.

Operation Arylide was a Metropolitan Police investigation into an MSB in London suspected of receiving the proceeds of drug trafficking from an organised criminal group. The MSB colluded with other MSBs to launder the money before returning it to the criminal group for smuggling out of the UK. The Metropolitan Police used the full range of covert investigative sources as well as international co-operation with the cash destination countries. Nine individuals involved in the MSB were prosecuted and convicted of a range of offences, including ML. The individuals received sentences of up to six years' imprisonment.

158. The UK makes full use of inter-agency co-operation, joint investigation teams, and embedded officers to share expertise and capabilities in investigating ML. JMLIT is a particularly useful resource for ML investigations and agencies actively use this tool to facilitate access to financial intelligence and promote inter-agency co-operation. Inter-agency co-operation is further facilitated by the UK's active use of embedded officers and collocating. For example, CPS lawyers are embedded within ROCUs and co-located with the NCA. HMRC officers are embedded within the NCA. The Scottish Crime Campus at Gartcosh brings together officers from 20 LEAs including Police Scotland, COPFS, NCA, and HMRC. In Northern Ireland, officers from PSNI, the NCA and HMRC are co-located in the Paramilitary Crime Task Force to target organised criminality linked to paramilitary groups. PSNI, the NCA and HMRC also co-operate with Northern Irish LEAs to tackle organised crime through the Joint Agency Task Force.

159. The ability and willingness of UK LEAs to provide cross-agency support and share resources allows the UK to respond to changing priorities or address the need for specific capabilities. This is a particularly useful and positive tool in light of the UK's austerity programme which has been in place since 2008. Importantly, even in this context, LEAs noted that resources for ML investigations remain sufficient, despite certain LEAs facing budget cuts. In some cases (e.g. the NCA) human and/or financial resources have increased towards key risk areas, including high-end ML.

Box 6. **Inter-agency co-operation to identify and investigate ML**

Operation Tarlac was an investigation into the defrauding of 21 public bodies, including hospitals, schools and councils, and the subsequent ML of about GBP 12.6 million in proceeds. The initial fraud was relatively simple, but the ML was complex involving the funds being moved to foreign jurisdictions, false invoicing, cash withdrawals and gold trading. As a result, a co-ordinated investigation was required. The investigation was commenced by the Lincolnshire Police which first detected a fraud involving a National Health Service (NHS) Trust in its territory. The Lincolnshire Police liaised with the NHS to uncover the scale of the fraud. The police also worked with the NCA, including international liaison officers, and relevant foreign authorities. Charges of fraud and ML were laid against 15 defendants who received sentences of up to 10 years' imprisonment.

Operation Kanteen was an investigation by the South East ROCU into multiple organised criminal groups committing fraud against vulnerable victims. As the offending was committed across the jurisdiction of 13 local police forces, it was investigated by the regional ROCU. All 13 forces collaborated to obtain information and evidence for the ROCU. The case involved 55 suspects, 92 victims, and an estimated loss over GBP 3 million. As of March 2018, 43 people had been charged with ML.

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

160. The ML investigations pursued by the UK authorities are in line with the types of ML identified in the 2017 NRA and other risk assessment documents as being particularly high risk (see Chapter 2 on IO.1). Investigations are prioritised and resources are allocated in line with these risks. The UK has had success prosecuting and convicting high-end ML even before it was identified as a specific priority area for law enforcement in December 2014. LEAs are increasingly focused on combating this activity, which has led to a rise in the number of investigations. This is promising, although it is too soon to fully assess whether these investigations will result in positive outcomes in the form of prosecutions and convictions since the cases take many years to complete given their complexity.

161. The assessment team based its conclusions on: the strategy documents relating to the relevant agencies; available budget and resourcing figures; discussions with LEA representatives; and cases demonstrating LEA priorities. Based on the main risks and priorities identified by the UK, and its own scoping exercise, the assessment team placed an increased focus on how the UK was pursuing: high-end ML; cash-based ML; ML through professional enablers; and ML through MSBs. In terms of predicate offending, the assessment team focused on fraud and international corruption, and drug offending, often in the context of organised crime.

162. The UK has initiated specialised projects and multi-agency groups to enhance law enforcement activity in relation to its identified risk areas.

Box 7. **Targeted work to enhance investigation and prosecution of key risk areas**

Thematic projects

Project H was commissioned by the NCA following the 2017 NRA to fill the identified intelligence gaps around high-end ML, particularly through professional enablers and complex corporate structures. The project has resulted in significant improvements in the understanding of high-end ML, as is reflected in the 2017 NRA. This has also seen the improved identification of high-end ML cases, as seen in the increasing number of investigations.

Project A was established following engagement between HMRC and the Metropolitan Police Service on the movement of cash in freight. It focuses on ML risks associated with MSBs and cash movements around the world and has resulted in operational co-operation in key jurisdictions such as the UAE. Resulting investigations inform the UK's strategic response to cash in freight.

Project L is an NCA-led project focusing specifically on professional enablers. It co-ordinates law enforcement and supervisory activity to improve intelligence and co-operation. Project L has led the NCA to initiate or enhance more than 30 investigations, and make over 20 referrals to supervisors.

Project T is an all-of-government response to organised crime from a specific high-risk jurisdiction using intelligence from all agencies, including international liaison officers, to identify potential offenders. The project has resulted in over 350 arrests and nearly GBP 8 million in cash seized since October 2016.

Multi-agency co-ordination groups

The UK law enforcement response to serious and organised ML is co-ordinated by the NCA through the multi-agency Criminal Finances Threat Group which is underpinned by sub-groups in line with the priorities identified in the 2017 NRA. These include the:

- **Professional Enablers sub-group chaired by HMRC**. It has two main focuses: outreach and awareness-raising with professional and supervisory bodies on the ML risks posed by professional enablers; and developing intelligence against suspected professional enablers and implementing a co-operative law enforcement response.
- **Cash-based ML sub-group chaired by the Metropolitan Police**. It co-ordinates the law enforcement response to

cash-based ML, including around specific risk areas such as MSBs, high-value dealers, cash-movements and ATM abuse.

163. **High-end ML[9]:** Prior to December 2014 high-end ML was not designated as a specific threat and a strategic priority in its own right, despite the UK's position as a major global financial centre and the world's largest centre for cross-border banking. Before 2014, high-end ML was pursued to a lesser degree through relevant LEAs' focus on serious and foreign predicate offending. Case studies demonstrate that the NCA, HMRC, FCA, CPS and the SFO successfully obtained convictions in high-end ML cases, even prior to its prioritisation. In the absence of statistics, it is difficult to determine the scale of convictions pre-2014. The identification of high-end ML in December 2014 has resulted in several notable outcomes:

a) human resources for the NCA Economic Crime Command increased by 11% (15 persons)
b) the NCA created a ML and Corruption Threat Desk to mine intelligence for potential high-end ML cases resulting in the tasking of 43 intelligence packages for investigation since April 2015, and
c) the number of high-end ML cases investigated by the NCA saw a marked increase with nearly 180 cases under investigation by UK LEAs at the time of the on-site. (see table 12 below). Based on the UK's average number of investigations, this amounts to approx. 0.8% of the total annual investigative workload.

164. This is positive, however, the complex, transnational nature of these cases means that investigations can take years to bear fruit, so it remains too early to determine whether the increased investigative activity and strategic prioritisation of high-end ML will result in increases in high-end ML prosecutions and convictions consistent with the UK's threats and risk profile. The statistics provided by the UK on high-end ML are positive (see Tables 12 and 13 below), but relate to ongoing investigations which may not all proceed to prosecution and conviction.

Table 12. **High-end ML investigations commenced by the NCA, HMRC, and the SFO**

	2014	2015	2016	2017
NCA	2	5	8	20
HMRC	8	15	13	36
SFO	12	5	5	8

9 The UK defines high-end ML as the laundering of large amounts of criminal funds through the UK financial and professional services sectors, often transferring funds through complex corporate vehicles and offshore jurisdictions.

Table 13. **High-end ML ongoing caseload across UK LEAs (as at March 2018)**

LEA	Active cases
NCA	39
HMRC	71
SFO	32
FCA	6
Police – England and Wales	25
Police Scotland	4
PSNI	3
Total	*180*

165. **Cash based ML:** The majority of the UK's ML investigations and prosecutions relate to cash-based ML. Such cases are largely pursued by local police forces, by ROCUs in higher priority cases, or by HMRC where there is a link to excise fraud or customs violations. Local and regional police demonstrated a robust understanding of cash-based ML and evidence their capacity to investigate this type of offending.

166. **ML through professional enablers:** The 2015 and 2017 NRAs recognised the high risk posed by professional enablers. Understanding has significantly improved since the 2015 NRA. The authorities acknowledge the remaining intelligence gaps in this area, but note that LEAs are very sensitive to this risk and case studies show the UK's willingness to pursue professional enablers.

167. **ML through MSBs:** Risks identified with MSBs have seen LEAs place increased emphasis on reducing this risk. This is evidenced at a supervisory level (see Chapter 6 on IO.3) and in case studies provided by the UK.

168. **Fraud and international corruption:** The NCA, the SFO, HMRC and the City of London Police are well-equipped to pursue complex fraud and international corruption. In 2015, the NCA established the International Corruption Unit to investigate serious international bribery and ML. Since July 2017 the NCA has also hosted the International Anti-Corruption Co-ordination Centre which combines resources from the UK, Interpol, the United States, Canada, Australia, New Zealand and Singapore to improve intelligence-sharing on grand corruption and ML. Notably, the SFO has demonstrated its ability to pursue legal persons for fraud and corruption, which is a rarity in the UK. Local authorities also noted an increase in fraud offending by organised criminal groups which increasingly view fraud as a higher value crime.

169. **Drug offending:** The UK estimates that a majority of ML cases in the UK are based on drug offending. This is consistent with the NRA's identification of the large illegal drug market in the UK.

Box 8. **Case studies illustrating the UK's pursuit of cases in accordance with its risks**

High-end ML: Operation Concentric is an ongoing investigation by the HMRC in Northern Ireland. The case involved an Organised Criminal Group which provided a ML service using a series of shell companies and associated bank accounts to convert legitimate work into 'cash in hand' payments to avoid or reduce VAT and income tax

liability. The investigation utilised a range of investigative tools including surveillance, search warrants, and production orders.

Cash-based ML: In 2015, HMRC and the Greater Manchester Police searched a residential address and found cash totalling over GBP 400 000 and drugs worth GBP 80 000. Evidence collected in the search resulted in the conviction of the two property residents for ML and drug offences. The defendants received sentences of two years imprisonment, and 26 months' suspended imprisonment respectively.

ML through professional enablers: Operation Slive was a drugs and ML investigation by the NCA. The laundering was conducted through the use of fraudulent mortgage applications and shell companies, set up with the aid of various professional enablers, including a solicitor and a financial advisor. The investigation resulted in the conviction of 13 individuals, including the solicitor and the financial advisor who was sentenced to six years' imprisonment.

ML through MSBs: In 2009, HMRC opened an investigation into two MSBs who were exchanging large quantities of Sterling into high denomination Euro notes. The resulting financial investigation found that several customers were regularly depositing large amounts that were recorded as smaller transactions. As a result of the investigation, five individuals were convicted.

Types of ML cases pursued

170. UK authorities demonstrated their ability to prosecute and obtain convictions for a full range of ML cases, including stand-alone and self-laundering, third-party laundering and the laundering of foreign predicates. Differences in the Scottish legal system and resulting difficulties in proving criminal offences, including ML, result in lower prosecution figures in Scotland. Nonetheless, Scottish LEAs have shown that they are able to successful pursue ML. The UK's prioritisation of financial investigations and ML has had a positive impact in this area. The assessment team based these conclusions on: numerous case studies presented by the UK showing the prosecution and conviction of various types of ML; discussions with LEAs and prosecutorial authorities; and statistics provided by the UK which, while not able to be disaggregated based on the type of ML pursued, nonetheless provide an indication of the extent to which standalone ML is pursued.

171. The UK's prioritisation framework results in its active pursuit of a range of types of ML. The CPS has specific guidance on ML which explains the different types of ML to ensure they are pursued where possible. The systematic use of financial investigations by LEAs ensures that the UK is well-equipped to pursue a range of types of ML. This is demonstrated in cases, which illustrate the UK's ability and willingness to pursue standalone ML, third-party laundering, self-laundering, and the laundering of foreign predicates. The UK's prioritisation of investigations into professional enablers has been particularly useful in obtaining third party ML

convictions. Scotland's different legal system and higher evidentiary threshold presents difficulties which result in the pursuit of predicate offending as an alternative to ML in certain cases. While this may result in fewer ML prosecutions and convictions, case studies have demonstrated Scottish LEA's ability to obtain convictions for ML.

Box 9. **The ability of UK LEAs to pursue different types of ML**

Third party ML: During the course of a trial for conspiracy to supply drugs, it emerged that the principal defendant, Cawley, had also defrauded an individual out of GBP 150 000. Cawley was convicted of both offences in 2012. The financial investigation revealed that Cawley's parents had permitted the use of their bank accounts to enable the ML. Both parents were subsequently convicted of ML and sentenced to one year imprisonment.

ML based on a foreign predicate: Following the theft of GBP 12 million from a bank in Germany, an individual, assisted by others, laundered the money through a network of shell companies and the purchase of real estate. The individual was convicted of ML and sentenced to 5 years' imprisonment.

Standalone ML: The defendant in this case, Katchi, was a collector for an organised criminal group operating throughout the UK. During a traffic stop, Katchi was found to be in possession of large amounts of cash, with further quantities found at his residence upon a search. Katchi was charged with two counts of ML, and received a sentence of six years' imprisonment.

Self-laundering: An organised criminal group committed construction industry fraud and associated tax evasion and laundered GBP 8 million over two years. Twenty individuals were convicted and sentenced to imprisonment totalling almost 90 years. The group employed off-the-books subcontractors and kept the income tax and public contributions they would otherwise have to pay, as well as claiming false invoices for VAT refunds to which they were not entitled. The money was laundered through a complex system of industry business structures.

Effectiveness, proportionality and dissuasiveness of sanctions

172. The sanctions imposed for ML are broadly effective, proportionate and dissuasive. Sentencing guidelines apply to all courts in England and Wales. While most convictions result in sentences at the lower end of the scale (reflecting the nature of the offending), the courts have also demonstrated their willingness to impose the highest available penalties in the most serious and high-end cases. The assessment team based these conclusions on: statistics on the range of sanctions imposed in ML cases; and case studies demonstrating convictions and sentences against natural persons. The ability to impose effective sanctions for legal persons could not be assessed due to a lack of ML convictions in this area.

173. The maximum sentence for ML in the UK is 14 years' imprisonment which is the longest available sentence under UK law short of life imprisonment. In general, the majority of sentences fall in the range of 1 to 3 years' imprisonment. Higher sentences are particularly rare in Northern Ireland which may be a reflection of the types of cases pursued. A higher occurrence of complex and high-end ML in England and Wales is consistent with the UK's risk profile. Recent years have seen an increase in the imposition of higher sentences in England and Wales (see table 14 below) and courts have demonstrated their willingness to impose sentences at the top end of the range in the most serious cases (see box 10 below).

Table 14. **Sanctions imposed for ML in England and Wales**

England and Wales	2014	2015	2016	Total
Less than 1 year	145 36%	147 29.9%	168 32.9%	460 32.8%
1-3 years	204 50.7%	261 53.2%	250 48.9%	715 50.9%
3-5 years	35 8.7%	53 10.8%	57 11.2%	145 10.3%
5-10 years	18 4.5%	29 5.9%	34 6.7%	81 5.8%
More than 10 years	0 0%	1 0.2%	2 0.4%	3 0.2%
Northern Ireland	2014	2015	2016	Total
Less than 1 year	27 75%	18 85.7%	24 80%	69 79.3%
1-3 years	9 25%	1 4.8%	6 20%	16 18.4%
3-5 years	0 0%	2 9.5%	0 0%	2 2.3%
5-10 years	0 0%	0 0%	0 0%	0 0%
More than 10 years	0 0%	0 0%	0 0%	0 0%
Scotland	2013/14	2014/15	2015/16	Average proportion
Less than 1 year	4 36.4%	0 0%	1 20%	5 25%
1-3 years	3 27.3%	1 25%	3 60%	7 35%
3-5 years	4 36.4%	3 75%	0 0%	7 35%
5-10 years	0 0%	0 0%	1 20%	1 5%
More than 10 years	0 0%	0 0%	0 0%	0 0%

Box 10. **Examples of sentencing for ML in the UK**

The imposition of sentences at the higher end of the sentencing range

A defendant, Nobre, received the maximum sentence, **14 years' imprisonment**, for conducting a sophisticated ML scheme involving investment funds and professional enablers to launder EUR 100 million in the proceeds of fraud.

A defendant, Gill, was sentenced to **11 years' imprisonment** for laundering over GBP 35 million in proceeds from drug offending through a network of shell companies with accounts in banks and MSBs located in the UK and abroad.

The imposition of sentences in the middle of the sentencing range

An individual convicted of laundering GBP 1.8 million in drug offending proceeds over four years was sentenced to four years' imprisonment for drug trafficking charges and **two years'** for ML to be served concurrently.

Use of alternative measures

174. Where a conviction for ML cannot be obtained, UK authorities are able to utilise various tools to disrupt and sanction ML, including pursuing alternative offences, asset recovery, tax investigations, or orders to restrict activity. The assessment team based these conclusions on: statistics and data provided by the UK on disruptions and the use of alternative measures; case studies demonstrating the alternative measures available to the UK; and discussions with LEAs.

175. The NCA's disruption performance framework measures its success in disrupting serious and organised criminality. This framework is an attempt to measures the NCA's impact on a particular threat whether or not a criminal justice outcome is pursued. The NCA's data indicates that it has had good success in this regard, although it is difficult to compare numbers across years as the methodology has matured. In particular, the definitions of a major, moderate, or minor disruption continuously evolve[10].

10. The NCA's disruption reporting framework measures the impact of LEA activity on serious organised crime. The impact can be considered significant and long-term (major), noticeable and medium-term (moderate) and minimal and short-term (minor).

Table 15. **NCA disruption data for economic crime and ML**

	2013/14	2014/15	2015/16	2016/17
Major disruption	6	17	8	3
Moderate disruption	30	40	27	22
Minor disruption	52	66	97	144
Total	**88**	**123**	**132**	**169**

176. Where ML cannot be proved, UK LEAs pursue alternative criminal justice measures, including criminal confiscation or offences under the MLRs for professional enablers and regulated bodies. The UK can also pursue civil asset recovery where no conviction can be obtained (see Chapter 3 under IO.8). As well, the UK uses Serious Crime Prevention Orders (SCPO) to prevent and disrupt further offending. These orders restrict an individual's conduct and are usually obtained by a prosecutor on conviction, but can also be obtained in the absence of a conviction, provided the court is satisfied that the subject has been involved in serious crime and that the order will protect the public by preventing future crime. Breach of a SCPO is a criminal offence punishable by up to five years' imprisonment. The NCA currently has 38 such orders and HMRC has 33. HMRC is also active in using intelligence obtained in unsuccessful ML investigations to pursue potential tax offending.

Box 11. **The use of alternative measures to disrupt ML**

Serious Crime Prevention Orders: A UK national was convicted of drug trafficking in two foreign jurisdictions and sentenced to imprisonment alongside confiscation orders. The UK later applied for a SCPO to protect the public by preventing, restricting, or disrupting the individual's future involvement in serious crime given the high risk of reoffending. In 2013, the Court made a SCPO tailored to the nature of the offending (including, for example, prohibitions, restrictions and notification requirements concerning his potential communication devices).

Using a tax investigation: In 2015, following an unsuccessful prosecution for ML involving MSBs, HMRC utilised the intelligence from the investigation to develop a broader intervention project aimed at MSBs which pose a risk of potential tax evasion. The project was extended across the UK and between April 2016 and September 2017 resulted in 2 721 cases and yielded GBP 19.9 million.

177. The nature of the UK's threat and risk profile means that legal persons are often involved in ML cases. For example, this may occur through the use of: shell companies to obscure beneficial ownership; complicit entities such as MSBs or freight companies to facilitate ML; or a corporation fostering a culture which encourages predicate offending, such as fraud or bribery, and the resulting ML.

178. Where legal persons are involved in offending, the UK will wind up shell or front companies and pursue prosecution of the natural persons or civil or regulatory actions. Complicit legal persons are investigated as part of the broader investigation,

but rarely convicted. This is because the UK's ability to prosecute large legal persons for criminal ML offences under POCA and notable predicates such as fraud remains limited due to difficulties in proving criminal intent. Under the 'Identification Doctrine' established in UK case law, a criminal act can only be attributed to a legal person where the natural person committing the offence can be said to represent the "directing mind and will" of the legal person. In large companies with diffused decision-making responsibilities, proving this is extremely difficult, as was acknowledged by the NCA and the SFO. In response to this issue, the UK has made legislative changes to ease the intent requirements with respect to certain offences, including bribery and corruption and, with the enactment of the Criminal Finances Act 2017, tax evasion. The UK opened a call for evidence on making similar changes to corporate liability for economic crime offences in January 2017 and as at March 2018, was analysing the feedback.

Box 12. **The UK's ability to pursue legal persons for ML**

In 2009, the SFO opened an investigation into **Gresham Ltd** following reports from individuals and companies who had been defrauded of large sums. Gresham appeared to be a reliable, profitable business, but in reality was defrauding individuals out of GBP 4.5 million by charging fees for services never rendered. The beneficial owner of the company had set up a network of international shell companies to distance himself from the offending. In 2009, the individual perpetrator was convicted and sentenced to seven years' imprisonment. The SFO also worked with the Insolvency Service to wind up the company.

The Devon and Cornwall Police opened an investigation into two individuals who used two companies, **Denver Trading Ltd and Denver Trading AG**, to fraudulently sell GBP 8 000 000 of investments in oxides and metals. The companies were banked outside the UK and a network of brokers in London was employed to sell the 'investments' to hide the beneficial ownership and distance the perpetrators from the fraud. After the investigation, the two perpetrators, Sabin and Ridpath were convicted and sentenced to nine years' imprisonment while two complicit brokers, Start and Berkeley, received sentences of seven and four years' imprisonment respectively. The companies were taken into liquidation by the Insolvency Service.

Overall conclusions on IO.7

179. **The UK has achieved a substantial level of effectiveness for IO.7.**

Immediate Outcome 8 (Confiscation)

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

180. The UK recognises the importance of asset recovery and law enforcement agencies consistently pursue civil and criminal confiscation as a policy objective. This finding is based on: a review of law enforcement and government policies, strategies, and guidance on confiscation and asset recovery; discussions with law enforcement officials and prosecutors; and case studies illustrating the UK's commitment to confiscation.

181. UK policies have consistently emphasised the importance of confiscation. The 2013 Serious and Organised Crime Strategy highlighted the importance of improving asset recovery.[11] The 2018 Proceeds of Crime Act (POCA) Guidance states that all relevant authorities should consider financial investigation and the full range of asset recovery tools, including civil recovery and taxation action, from an early stage in all criminal cases.[12]

182. Recent legislative changes to expand asset recovery powers also demonstrate Government commitment in this area. The Criminal Finances Act 2017 built upon the UK's existing legal framework and introduced powers to seize and forfeit bank accounts, extended the ability to obtain civil recovery orders to HMRC and the FCA, and introduced unexplained wealth orders. These orders require an individual to explain the origin of their assets. Failure to provide a full response could lead to or assist a civil recovery action or criminal conviction.

183. The UK incentivises asset recovery activity by law enforcement. In England, Wales, and Northern Ireland, recovered monies are invested back into law enforcement, while in Scotland recovered assets provide funding for community initiatives.

184. Confiscation is prioritised in law enforcement policies and guidance. CPS guidance from 2014 emphasises pursing confiscation, particularly for serious and organised crime and serious economic crime.[13] Confiscation is an objective in the NCA Confiscation Framework, the FCA's Approach to Enforcement[14] and the SFO's Strategic Plan 2016-19.[15] The HMRC Fraud Investigation Service Handbook stresses the importance of gathering material to support asset recovery.

185. In practice, case management systems ensure that the NCA, SFO, and HMRC systematically consider asset recovery mechanisms. All LEAs, including the NCA, the SFO, HMRC, FCA, and the Asset Confiscation Enforcement (ACE) teams (see para. 195)

11 HM Government "Serious and Organised Crime Strategy" (October 2013).

12 Home Office and Attorney General's Office "The Proceeds of Crime Act 2002 (POCA) Guidance under section 2a: January 2018" (January 2018).

13 CPS, "CPS Asset Recovery Strategy: June 2014" (June 2014).

14 FCA, "Enforcement Strategy" (April 2016).

15 SFO, "SFO Strategic Plan (2016-2019)" (2016).

consistently emphasised their commitment to confiscation. Available data supports this. Since 2014, the UK has recovered GBP 1 billion.

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

186. The prioritisation of confiscation in nationwide and agency policies is reflected in law enforcement activity. Relevant authorities, including those involved in international co-operation, consistently and proactively pursue confiscation of the proceeds of domestic and foreign predicates. Asset repatriation has been used in a number of cases. The assessment team's findings were based on: statistics on asset recovery; discussions with LEAs and international co-operation agencies; and case studies demonstrating the consistent pursuit of confiscation.

187. Relevant authorities in the UK have a wide range of asset recovery tools at their disposal, including conviction-based confiscation, civil recovery, tax recovery and cash forfeiture. The Criminal Finance Act 2017 also introduced new asset recovery powers:

a) LEAs are now able to seek orders to freeze and forfeit the balance of bank accounts where the funds are suspected of being the proceeds of crime or of being intended for use in criminal conduct.
b) The NCA, HMRC, FCA, SFO, CPS and the Scottish Crown Office and Procurator Fiscal Service (COPFS) can obtain Unexplained Wealth Orders to investigate funds from individuals reasonably suspected of involvement or connection with serious crime where there is no reasonable explanation for their ownership of the assets.

188. In addition to these measures, the NCA is also able to use a hybrid approach, pursing civil recovery in addition to levying taxes against criminal proceeds. This allows the recovery of additional assets and the NCA reported that the addition of a tax liability incentivises respondents to repay the criminal proceeds. Authorities largely agreed that they would decide which asset recovery mechanism to use based on the particular case.

189. Some differences in statistics between the different asset recovery tools and across agencies made cross-comparison difficult, but case studies and discussions with UK LEAs confirmed their ability to use all available measures.

190. The total amounts restrained and recovered are high, amounting to GBP 1.3 billion restrained and GBP 1 billion recovered since 2014 using POCA, civil recovery, and agency-specific disgorgement mechanisms (see Table 16). HMRC has recovered a further GBP 3.4 billion since 2016 (see para. 205 below). POCA confiscation and cash forfeiture account for the largest share of assets recovered (see table 16). Civil recovery was once considered only as a secondary alternative to confiscation, but authorities confirmed this is no longer the case and civil recovery is now considered an equivalent action to pursue in first instance. This is not reflected in the statistics which show a decreasing number of civil recovery orders, with a fluctuating amount recovered (see Table 16).

Table 16. **Asset restraint and recovery in the UK 2014-17***

	2014/15		2015/16		2016/17	
	Number of orders	Amount (million GBP)	Number of orders	Amount (million GBP)	Number of orders	Amount (million GBP)
Total assets restrained	1 297	396.9	1 499	473	1 422	382.8
Total assets recovered		200.85		321.72		483.64
POCA confiscation	6 126	160.8	6 117	211.4	5 649	165.6
POCA civil and tax recovery	24	6.55	15	11.33	13	8.52
POCA cash forfeiture	3 111	33.5	3 336	40.49	3 560	42.22
SFO disgorgement	0	0	1	6.2	1	258.2
FCA disgorgement	0	0	1	52.3	1	9.1

* Note that the number of orders does not directly correspond to the amounts restrained or recovered as an order is not necessarily realised in the same year it is made.

191. The UK is active in restraining assets prior to recovery (see table 16 above). To obtain a criminal restraint order, authorities must prove to a court that there is a real risk of dissipation. The CPS will consider a range of factors, which may include previous convictions, any evidence of preparations to move or dissipate assets, the accused's capacity and capability to move or dissipate assets (e.g. access to foreign bank accounts or corporate structures) and any actual dissipation. The CPS explained that where restraint is sought prior to or concurrently with the subject's learning of the investigation, risk of dissipation can be proved relatively easily by virtue of the nature of the offending. However, in the 57% of cases where restraint is sought at the post-charge stage, if the subject has not attempted to move or conceal the unrestrained assets, it can be more difficult to show risk of dissipation and meet the threshold for restraint. In such cases, the CPS would typically have to wait until some dissipation occurs before restraint can be pursued. The UK authorities explained that they are accustomed to working with these legal requirements and did not view them as a hurdle to effective restraint. A variety of tools are available to the CPS and LEAs to monitor accounts and assets and react to any evidence of an intention to move, conceal or dissipate those assets (see box 13 below).

192. The civil equivalent of a restraint order (a property freezing order) can be obtained provided the court is satisfied that there is an arguable case that the property relates to or includes recoverable property.

Box 13. **HMRC and CPS efforts to meet the threshold for restraint and prevent dissipation of assets**

In 2015, HMRC investigated a value added tax (VAT) fraud case in which the accused received GBP 5 million in wrongful payments. The money was concealed in assets owned by the accused's family.

Prior to arresting the accused, HMRC and CPS considered restraint but concluded that there was insufficient evidence of a real risk of dissipation.

To ensure that dissipation did not occur, HMRC secured an account monitoring order for the accused's accounts prior to his arrest. Shortly after arrest, HMRC became aware from the account monitoring order that the accused was withdrawing lump sums of cash. HMRC immediately worked with CPS to gather the evidence necessary to prepare an application for restraint. A restraint order was obtained within a week of receiving this evidence. By this time, the accused had withdrawn a total of GBP 45 000. The accused was convicted of ML in 2016 and sentenced to six years' imprisonment. In May 2017, the court issued a confiscation order in the amount of almost GBP 3.4 million with a default penalty of eight years' imprisonment. As of September 2017, GBP 2.9 million had been recovered.

193. Criminal restraint and confiscation in the UK is value-based. This facilitates asset recovery as authorities are not required to identify specific illicit assets in order to pursue restraint and confiscation.

194. Confiscation is also facilitated under POCA through automatic assumptions being made in certain cases where the offender has been found to have a criminal lifestyle. The assumptions apply to many of the UK's priority offences including ML, drug trafficking, people trafficking, and terrorism. In these cases, the court will assume that any property transferred to the defendant or expenditure by the defendant in the six years preceding criminal proceedings, or any property held by the defendant after the date of conviction, is assumed to have been obtained through criminality. The value of this property is then used in calculating the benefit obtained by the defendant for the purpose of confiscation (unless the defendant can prove otherwise or there would be a serious risk of injustice if the assumption were to be made).

195. Law enforcement authorities systematically use available restraint and asset recovery measures in both major and minor cases relating to domestic and foreign offending (see Table 19 below).

196. The confiscation of instrumentalities themselves is relatively uncommon, but is possible under specific legislative schemes[16]. Instrumentalities can also be taken into account in confiscation proceeds and can be realised in order to pay a confiscation order. Statistics are not maintained on the confiscation of instrumentalities, but the UK was able to provide case studies demonstrating confiscation of instrumentalities.

16 E.g. Under the Misuse of Drugs Act 1971, Powers of the Criminal Courts (Sentencing) Act 2000 and Customs and Excise Management Act 1979.

Box 14. **The use of restraint and confiscation in a range of crimes**

Cash forfeiture in a domestic, cash-based ML case: Operation Applepie

Two individuals were stopped by UK Border Force leaving the UK in a van containing a consignment of soft drinks. Upon questioning, the individuals declared approx. GBP 900 of cash. Upon investigation, Border Force found that the soft drinks concealed GBP 325 000 in cash. This cash was forfeited immediately as UK authorities secured disclaimers from the defendants that they would not contest the hearing. Both individuals were arrested, charged, and pleaded guilty to ML. The primary individual was sentenced to three years' imprisonment while the other received a suspended sentence.

Confiscation in a high-end ML case based on foreign predicate: Operation Vista

Operation Vista involved a scheme to launder the proceeds of VAT fraud committed in a number of overseas jurisdictions. Approximately GBP 40 million was laundered over a 10 month period through UK-based MSBs using accounts of companies set up by professional enablers in Europe and the UK. Extensive international co-operation was used to investigate the full scale of the offending and to ensure co-ordinated enforcement action. Several UK individuals were involved in and benefited from the offending. The case resulted in convictions of six individuals in the UK, including three company directors and one accountant. The court issued confiscation orders totalling almost GBP 600 000.

Confiscation of benefits and instrumentalities: the Hatton Garden Burglary

The 2015 Hatton Garden Burglary was the largest burglary in recorded English history. Thieves stole up to GBP 20 million in assets from a safe deposit company. The proceeds of the burglary were then laundered. Nine defendants were found guilty of conspiracy and ML and received sentences of up to seven years' imprisonment. Taking into account the benefit obtained (estimated to be GBP 13.5 million) and the assets available from the defendants (which ranged from GBP 5 000 to 7 million), the court issued confiscation orders totalling GBP 11.9 million. In addition, the court issued a deprivation order under the Powers of the Criminal Courts (Sentencing) Act 2000 to forfeit instrumentalities seized in connection with the offending, including drilling equipment, walkie talkies, and computers.

197. Asset recovery is facilitated by the existence of specialised officers and teams. All prosecutorial agencies (the CPS, COPFS, Public Prosecution Service of Northern

Ireland, SFO and FCA) have specialised proceeds of crime teams that provide advice to law enforcement on asset recovery.

198. All LEAs, including regional police forces, have specialised proceeds of crime units which provide in-house expertise.[17] These units include POCA accredited financial investigators who receive accreditation and training from the NCA Proceeds of Crime Centre and are able to exercise POCA powers, including search, seizure, and application for restraint. Financial investigators in Police Scotland also receive accredited training. The specialist teams have proved effective. The HMRC Proceeds of Crime Intervention Team (dedicated to cash intervention) has seized GBP 13.5 million and forfeited GBP 7.5 million since it was established in April 2015, while the FCA Criminal Prosecutions Team's asset recovery sub-team had secured approximately GBP 11 million as at March 2018.

199. A strength of the UK system is its active enforcement of confiscation orders. Eleven multi-agency Asset Confiscation Enforcement (ACE) teams are located across the UK, with nine located in the ROCUs, one in the NCA, and one in HMRC. These teams help agencies to identify assets to satisfy outstanding priority confiscation orders and detect hidden assets to permit existing orders to be revisited and increased. ACE teams proactively share information with Border Force and local police on targeted individuals to help identify assets. ACE teams have been successful in both collecting outstanding amounts and having orders revisited (see table 17 below). In the 16 months following their commencement (in December 2013), ACE teams collected GBP 40 million in outstanding orders. HMRC also has an Offender Management and Enforcement Team (OMET), one function of which is to pursue recovery against high value individuals.

Table 17. **ACE collection and re-visitation of orders 2015-17 (GBP million)**

	2015/16	2016/17
Total amount collected in outstanding recovery orders	23.0	32.5
Total increase in value of orders revisited	14.3	4.6

200. To support enforcement of confiscation orders, courts will include a sentence for default to which individuals are automatically subject should they default on the order. These sentences can be extremely high (often higher than the sentence for the original offending) and provide a strong incentive for payment of confiscation orders. For sentences orders exceeding GBP 1 million, the defendant may serve up to 14 years' imprisonment (in addition to any imprisonment sentence relating to the original offending) (see box 15 below).

17. These include: the NCA Proceeds of Crime Centre; the SFO Proceeds of Crime and International Assistance Division; the HMRC Fraud Investigation Service Proceeds of Crime Team; the HMRC Proceeds of Crime Intervention Team; the FCA Criminal Prosecutions Team asset recovery sub-team; the PSNI Economic Crime Unit; and the Regional Asset Recovery Teams of the England and Wales police forces.

Box 15. **Enforcement of confiscation orders**

The use of default sentences: Johnson case

After fleeing the UK in 2014, Johnson was convicted in absentia for his role in a multi-million pound tax fraud. In March 2016, the court issued a confiscation order of GBP 109 million to be paid immediately or he would be subject to a 14 year default sentence. In July 2016, he was detained attempting to enter the UAE. UK authorities, including OMET, worked with the UAE to have him deported back to the UK. Johnson was returned to the UK, and sentenced to the 14 year default sentence for failure to make payment against his confiscation order, in addition to his original 10 year sentence.

Recalculation of confiscation order: North East ACE Team/CPS

In 2008, a defendant was found guilty of drug offences and sentenced to 11 years' imprisonment. During confiscation proceedings in 2009, the Court determined that the benefit amounted to GBP 2.8 million. However, as the defendant's assets totalled only GBP 300 000, the Court made a confiscation order for this amount to be paid by late 2010.

In 2015, the North East ACE Team identified substantial assets available to the defendant. These included new assets, in addition to properties which had been in 'negative equity' at the time of the confiscation hearing, but had since risen in value. In 2017, CPS (working with the North East ACE Team) made an application for the Court to reconsider the defendant's available assets. In April 2018, the court increased the available amount by GBP 1 865 368. The defendant was given 3 months to pay with a default sentence of 10 years being set if he failed to do so.

201. The UK is able to restrain and forfeit assets on behalf of a requesting state and can share assets through multilateral or bilateral agreements or on an ad hoc basis. As at December 2017, the CPS had GBP 254 million under restraint on behalf of foreign states. From 2014-16, the SFO has approximately GBP 43 million restrained pursuant to MLA requests. In total, the UK has repatriated GBP 47 million in assets between 2014 and 2016. GBP 29 million was repatriated on the basis of confiscation orders in three cases, with the vast majority (97%) of this sum relating to one case (see box 16 below). The remaining GBP 18 million has been repatriated in response to compensation orders or similar mechanisms.

202. The UK is also making efforts to improve confiscation of assets located abroad. The CPS's 2014 Asset Recovery Strategy recognised the importance of pursuing overseas assets. Its International Liaison Magistrates include specialist asset recovery lawyers posted to specific jurisdictions to improve and build capacity in asset recovery. A Video Teleconference project between 13 countries allows the UK to share expertise and facilitate co-operation, particularly on asset recovery. These

mechanisms have helped the CPS recover GBP 23 million from overseas jurisdictions since 2013. Notably, the UK has had success in having its civil recovery orders recognised and enforced outside the UK (see Box 16).

Box 16 **Pursuit of foreign proceeds and asset repatriation**

Landmark case for having civil recovery case orders recognised overseas

In 2008, the predecessor agency to the NCA commenced a civil recovery investigation into the UK-based assets of a subject who had been convicted in the UAE for drug trafficking and ML. In 2010, a property freezing order was obtained for six residential properties in the UK, and a number of bank accounts, including one held in Luxembourg. The UK authorities worked with the Luxembourg authorities to have the freezing order registered in Luxembourg. This was the first time an order under the civil recovery provisions of POCA had been formally recognised in any foreign jurisdiction. In September 2014, a civil recovery order was made in the UK against GBP 3.3 million in assets. In 2015, the court in Luxembourg recognised and enforced this order in respect of the bank accounts located in their jurisdiction. The case pioneered the successful use of UK civil recovery proceedings against assets held outside the UK.

Asset repatriation with Macau, China

In 2008, an individual was arrested in Macau, China and sentenced to 27 years' imprisonment for 40 counts of corruption and two counts of ML amongst other changes. Members of the individual's family were also convicted of ML. The UK had undertaken its own ML investigation and provided support to the Macau authorities throughout the case in tracing the assets located in the UK. The CPS was able to restrain the assets and later, upon conviction, enforce confiscation orders for GBP 28.7 million. These funds were realised and repatriated to Macau under the UN Convention against Corruption.

Co-operation between jurisdictions on disgorgement in a SFO deferred prosecution agreement

Following a SFO investigation, Rolls Royce entered into a deferred prosecution agreement with the SFO for 12 counts of conspiracy to corrupt, false accounting, and failure to prevent bribery spanning 3 decades and 7 jurisdictions. Throughout the investigation, the SFO co-operated with LEAs in the USA and Brazil who were also undertaking investigations relating to conduct in their jurisdictions. This culminated in Rolls Royce reaching simultaneous agreements in the three jurisdictions, totalling approximately GBP 671 million. Under the SFO deferred prosecution agreement, Rolls Royce agreed

to pay over GBP 497 million plus interest (comprising disgorgement of over GBP 258 million and financial penalties of over GBP 239 million).

203. The UK has made various legislative changes to improve its asset recovery framework. In 2014, it introduced the possibility of deferred prosecution agreements for the SFO. Under these agreements the prosecution of a company can be suspended where the company agrees to certain measures, and with the approval of the Court. The agreements can include provisions for the substantial disgorgement of profits from the alleged offending, in addition to financial penalties and compensation (see box 16 above).

204. Unexplained Wealth Orders came into effect in 2018 and provide another avenue for the UK to recover assets. LEAs expressed enthusiasm for these orders, noting that as they can be applied to politicians, officials, and associates from outside the European Economic Area, they are particularly useful for the recovery of assets from foreign predicates. The NCA has already secured two orders in one case. As the orders are new, it remains too early to determine their effectiveness and the extent to which they will be exercised.

205. Since 2016, HMRC's Fraud Investigation Service (FIS) has also been able to use civil tax powers to recover criminal proceeds related to serious tax fraud, or to support multi-agency efforts focused on particular risks (such as modern slavery and human trafficking). This work is separate to the traditional HMRC tax compliance work. Since 2016, FIS has recovered more than GBP 3 billion in criminal proceeds.

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

206. The UK clearly recognises the importance of confiscating falsely or undeclared cross-border transaction of currency and bearer negotiable instruments (BNI) as shown by its proactive law enforcement activity in this area. It also recognises the emerging risks of cash in freight and is developing a strategy to manage this risk. These findings were based on: statistics on the amounts of cash confiscated; case studies on specific operations and mechanisms used by the UK to target the illicit cross-border cash movements; and discussions with HMRC, the NCA, Border Force, and the police.

207. The LEAs including HMRC, the NCA and the police, have the authority under POCA to seize and forfeit cash of GBP 1 000 or more where it is the suspected proceeds of crime or is intended for use in unlawful conduct. The initial seizure period is 48 hours, but this can be extended to up to two years. "Cash" covers notes, coins, postal orders, cheques, bankers' drafts, and bearer bonds and (since the 2017 enactment of the Criminal Finances Act) also includes betting slips, gaming vouchers, and fixed value casino tokens. Authorities actively use their powers to seize and forfeit cash at the border (see Table 18 below). Border Force also has cash seizure powers (with the exception of counterfeit currency) and will refer the cash to a partner agency for further action.

Table 18. **Cash seizures by transportation method 2015-18(GBP million)**

	2015/16	2016/17	2017/18
Air transportation	4.3	3.6	7.7
Maritime transportation	5.3	3.1	8.2
Transportation by post	0.06	0.006	0.01
Other	0.01	0	0.78
Total cash seized at the border	9.7	6.7	16.7

208. Cash declarations in and out of the EU are recorded on the HMRC Cash Declaration Database which is used by HMRC and the NCA in operational work. HMRC has established a Memorandum of Understanding to regularly share the database with the NCA, which can in turn share it with other LEAs as appropriate. The UK recognises that cash movements within the EU carry similar risks; however, there is no declaration system in place for these movements.

209. The UK has a proactive approach to confiscating cross-border cash. HMRC, Border Force and NCA work together to target high-risk air and sea ports, transport channels, and passengers who are identified using SARs, passenger information, covert intelligence, profiling, and by identifying jurisdictions with cash based economies or limited cash restrictions. Operations are frequently based around high-risk ports or flights.

210. The particular risks posed by the Heathrow Airport led to the creation of a multi-agency taskforce which has proven very successful (see box 17 below). The NCA also posts trained financial investigators, accredited to deal with cash detection and seizure, to Heathrow and Dover. Authorities noted that the success of initiatives at Heathrow and Dover has resulted in a displacement of cash movements to other ports and airports. As a result, agencies are considering extending the multi-agency taskforce model to other locations.

Box 17. **Law enforcement activities to target cross-border cash transfers**

The success of multi-agency taskforces: the Heathrow Joint Finance Team

In September 2015, the UK established a multi-agency team comprising the NCA, Border Force, and the Metropolitan Police Service. It is stationed at Heathrow Airport. Its aim is to increase detection, seizure and forfeiture of criminal and terrorist related funds. The team was initially piloted for six months and, in that time, the UK saw a 73% increase in the amount of cash detected and seized at Heathrow. As a result of this success, the team has been made permanent and the UK is considering extending the model to other ports.

Case study: Operation Enfatico

In February 2017, Counter-Terrorism Policing, Border Force, and other agencies launched a project to intensify cash seizures over the following month. The project focused on Counter Terrorism-related

cash but included targeting all forms of cross-border cash-movement, including air, sea and rail travel. The project resulted in 97 cash seizures totalling GBP 1.2 million. The project also resulted in broader learning and recommendations, including: to increase joint working and intelligence-sharing; to ensure continued professional development for officers from relevant agencies; and to consider adopting multi-agency taskforces with financial investigation capabilities at all ports.

211. The UK has identified cash in freight as an increasing threat. Cash transported in freight is not disclosed as such for security reasons. Instead, it has a separate Customs Code, which HMRC can track via the Customs Handling of Import & Export Freight (CHIEF) system. HMRC undertakes analysis to determine the values and volumes moved and officers follow up on any concerns.

212. Discussions with LEAs and border authorities show that the UK is working to improve detection and seizure of cash in freight. HMRC is particularly active in this regard, conducting analysis of various data sources, including CHIEF and the Cash Declaration Database, as well as working with the Bank of England to understand the totality of cash importation and export. HMRC is increasingly working with the private sector to detect cash movements and identify potential red flags for those involved in the freight forwarding process. While there is no independent strategy for managing the risks of cash in freight, this work is overseen by an internal cross-HMRC governance group and is shared with the relevant sub-group of the Criminal Finances Threat Group as part of the response to the Strategic Action Plan.

Box 18. **HMRC project to identify risks relating to cash in freight**

In 2017, HMRC commenced a project with the goal of increasing the UK's understanding of risks relating to cash in freight. The project involved a strategic analysis of three years of data from the CHIEF system including cash-related customs movements. The analysis identified large-volume cash movements from MSBs to foreign countries with no obvious demand for GBP. This triggered an HMRC-wide operation, combining AML/CFT compliance work, civil tax investigations, the use of asset recovery powers, and traditional criminal investigations. HMRC also worked closely with UAE LEA to obtain intelligence about the businesses that received the freighted cash. The project and resulting operations has triggered policy responses on AML/CFT compliance, improved outreach with the private sector, and identified overlaps with other LEA activity.

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

213. The UK's confiscation results are in line with its identified risks and national policies (see Chapter 2 on IO.1). This assessment was based on: statistics provided by the UK on confiscation by predicate offence; case studies showing the consistent

pursuit of confiscation in high-risk and priority cases; and discussions with LEAs which emphasised their commitment to confiscation.

214. As set out under IO 6 above, the UK largely investigates and prosecutes ML in line with its risk profile. Authorities have had success forfeiting large amounts and varied types of assets in complex and transnational cases, and cases involving specific risk areas (e.g. cash based ML, high end ML, MSBs, and professional enablers) (see Box 14 above). Confiscation in terrorism-related cases is relatively low, in line with the UK's risk profile of TF cases involving relatively small funds (see Chapter 4 under IO 10).

215. Statistics show that the UK pursues asset recovery in a manner consistent with its identified risks and national AML policies. The 2017 NRA identifies drug offending, fraud and tax offending, acquisitive crime, and immigration crime and modern slavery as the UK's key predicate offences for ML. These findings are supported by other assessments and views from law enforcement agencies. In total, ML and key predicates typically account for more than 90% of the UK's total asset recovery (see Table 19 below).

Table 19. **Asset recovery outcomes based on key predicate offences, excluding terrorism (GBP million)**

	2014/15	2015/16	2016/17
Total value of confiscation orders	**244.5**	**454.6**	**185.1**
Offence type			
Money laundering	38.4	59.5	26.5
- as a percentage of total value	16%	13%	14%
Fraud	75.2	61.8	60.5
- as a percentage of total value	31%	14%	33%
Tax-related offending	61.1	259.7	18.6
- as a percentage of total value	25%	57%	10%
Drug offending	37.2	49.0	57.2
- as a percentage of total value	15%	11%	31%
Immigration crime	1.1	0.5	1.4
- as a percentage of total value	~0%	~0%	1%
Acquisitive crime	6.7	5.8	6.6
- as a percentage of total value	3%	1%	4%
Total (above offences)	**219.7**	**436.3**	**170.8**
- as a percentage of total value	**~90%**	**~96%**	**~92%**

216. In deciding whether to pursue asset recovery, the UK is primarily focused on output, but also takes into account the type or nature of offending involved. The NCA Confiscation Framework guides investigators on the priorities, factors and considerations in deciding to pursue confiscation. While it is not focused on specific crime types, its focus on delivering outcomes and outputs against high priority threats does encourage the pursuit of confiscation in cases involving high-end ML, organised immigration crime, and modern slavery and human trafficking. In pursuing the enforcement of confiscation orders, the CPS, the NCA, and HMRC identify priority cases based on the value of the outstanding debt as well as whether the offending involved serious and organised crime.

Overall conclusions on IO.8

217. **The UK 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

TF investigation and prosecution (Immediate Outcome 9)

a) The UK proactively investigates, prosecutes and convicts a range of TF activity. TF case studies are consistent with its identified risks from low-level funding for foreign terrorist fighters (FTFs), self-funding FTFs or self-funding UK-based attackers. TF investigations are systematically considered alongside terrorism-related investigations and are pursued as a distinct criminal activity.

b) The UK, in particular authorities in Northern Ireland, have a developed understanding of the distinct risks faced in Northern Ireland, and have adapted their approach over time to respond to the evolving risks, in particular, by focusing on organised crime as a way to disrupt potential TF activities.

c) A positive feature of the UK's system is the strong public/private partnership on TF matters. This is facilitated by the JMLIT and a close relationship between the NTFIU and UK financial institutions which has proved effective in practice.

d) TF investigations are well-integrated into broader counter-terrorism strategies. Agencies co-ordinate and co-operate well across jurisdictions, regions and sectors. Notably, counter-terrorism financing authorities have a close and fruitful relationship with both financial institutions and the NPO sector.

e) LEAs share a strategy of pursuing more serious terrorism-related charges, instead of standalone TF charges, where the evidence permits since this option can lead to a harsher sentence. While the TF offence carries a lower maximum sentence and therefore generally results in lower sanctions, a person convicted of this offence is typically also sentenced to orders restricting their movements and activities which increases the overall effectiveness, proportionality, and dissuasiveness of available sanctions. Where a conviction cannot be obtained, the UK uses a variety of available measures to disrupt TF.

4

TF preventive measures and financial sanctions (Immediate Outcome 10)

a) While larger FIs and DNFBPs appear to have effective controls with respect to sanctions, implementation is less consistent among smaller FIs and DNFBPs. This is a concern particularly in the MVTS sector which is higher risk for TF sanctions abuse. Since its creation in 2016, OFSI has worked closely with a range of FIs and DNFBPs to improve their understanding of sanctions obligations and new sanctions programs, including smaller FIs and DNFBPs.
b) The legal requirement to freeze assets applies in the UK without delay. The communication of designations by OFSI occurs within one business day, unless designations occur on Fridays, Saturdays or public holidays where it can take up to three or four calendar days. If during the designation process, OFSI becomes aware that there are relevant assets in the UK, it actively notifies entities prior to a designation to ensure the freeze will be effective. While large FIs and DNFBPs which use commercial providers of sanctions lists are unlikely to be affected by this communication delay, smaller FIs and DNFBPs, including MVTS providers, may not be notified of designations for three to four calendar days.
c) The UK has a good understanding of the TF risks associated with NPOs and applies a targeted risk-based approach to mitigating those risks. The charities regulators have conducted extensive outreach and provide largely useful guidance. Regulators co-operate well with LEAs and the banking sector. Cases demonstrate the UK's success in helping to protect the sector from such abuse.
d) The UK has a robust confiscation regime through which it can and does deprive terrorists of assets. A range of powers exist and are widely used. While overall amounts confiscated are low, this is consistent with the UK's TF risk profile.

PF financial sanctions (Immediate Outcome 11)

a) Like TF, proliferation financing (PF) is a high priority for the UK and the UK has played an active role in proposing designations under the UN and EU PF sanctions regimes and encouraging global compliance with TFS. National co-ordination and co-operation among the UK authorities is strong, at both the policy and operational levels. The UK has a cross-government approach to countering proliferation and disrupting the procurement of proliferation-sensitive goods and proliferation financing. The 2015 Strategic Defence and Security Review, the establishment of OFSI in 2016, and the strengthening of enforcement powers in 2017, highlights the priority placed on PF issues.
b) The UK has frozen a significant volume of assets and other funds pursuant to its PF sanctions programs. New UN designations are immediately effective in the UK, and new designations are communicated within one business day, unless designations occur on Fridays, Saturdays or public holidays where it can take up to three or four calendar days to be updated on OFSI's consolidated list (see key finding c in IO.10).

c) While large banks have significantly improved sanctions implementation, there is uneven implementation among smaller banks, MVTS providers and DNFBPs. The UK recently has (and is continuing) engaged in awareness-raising in these sectors. The lack of public-enforcement actions in relation to sanctions breaches reduces the incentives for compliance by smaller FIs and DNFBPs.

Recommended Actions

TF investigation and prosecution (Immediate Outcome 9)

a) Pursue all ongoing CFT efforts and continue adapting to new threats as they emerge.
b) Continue to explore ways to facilitate and promote the strong co-operation between JMLIT, the NTFIU and financial institutions.

TF preventive measures and financial sanctions (Immediate Outcome 10) and PF financial sanctions (Immediate Outcome 11)

a) UK law enforcement agencies and OFSI should ensure that they pursue public enforcement of sanctions evaders.
b) The UK should review and formalise supervisors' powers to monitor sanctions systems and controls.
c) OFSI, supervisors and law enforcement agencies, should continue to work with FIs and DNFBPs to promote effective implementation of TFS requirements, and should take dissuasive and proportionate action to address breaches or deficiencies when they occur.
d) The UK should continue to notify UK legal and natural persons of updates to the UN or the EU TF sanctions to prevent asset flight and, where practicable, reduce the time lag between designations and communications.
e) Companies House should continue to work with OFSI to screen PSC information for sanctioned entities and individuals and share this information as appropriate to enhance effective implementation of targeted financial sanctions.

218. 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.

Immediate Outcome 9 (TF investigation and prosecution)

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

219. The UK encounters different terrorism and TF risks in mainland UK from those faced in Northern Ireland. Authorities in all jurisdictions demonstrate a good understanding of their particular TF risks and the nature, scale, and number of TF cases pursued across the UK is in line with its distinct risk profile. The assessment team based these conclusions on numerous case studies demonstrating the types of

TF cases pursued; statistics; a review of the NRA and other relevant assessments; and discussions with the National Terrorist Finance Investigation Unit (NTFIU), the Crown Prosecution Service (CPS), the Police Service of Northern Ireland (PSNI), the Public Prosecution Service of Northern Ireland (PPSNI), and other LEAs.

220. While international terrorism is assessed to be a severe threat to the UK, the majority of terrorist attack plots have been low complexity, planned and executed by lone actor extremists. The 2017 NRA therefore recognises the UK's TF threat as predominantly UK-based, with the highest risks posed by: low-level, self-funded attackers; individuals providing small amounts of funding to FTFs; or individuals financing their own travel plans. As a result, MSBs, cash couriers and retail banking were considered at high risk of abuse for TF. TF risks in the NPO sector overall were considered to be low with certain parts of the sector facing significantly higher risks. The LEAs also noted a propensity for individuals to abuse benefits or commit low-level fraud to generate funds for terrorist activity. This understanding of risk was consistently shared by all relevant LEAs and prosecutorial agencies. Numerous case studies illustrate the UK's proactive investigation, prosecution and conviction of a range of TF activity, consistent with its identified risks.

Box 19. **Types of TF prosecuted and convicted in the UK**

Abuse of benefits: Operation Yawler

Two UK nationals, Ahmed and Boufassil, were under investigation by the West Midlands Counter Terrorist Unit following contact with known FTFs. Ahmed and Boufassil were believed to have provided GBP 3 000 to Mohammed Abrini who was later involved in the 2015 Paris attacks and the 2016 Brussels attack and was arrested by Belgian authorities. The money was initially provided to Ahmed and Boufassil by a FTF who had obtained it through a housing benefit. Following Abrini's arrest in Belgium, the UK co-operated with Belgian officials to obtain statements from Abrini to support the intelligence obtained throughout the UK investigation. Ahmed and Boufassil were subsequently convicted of TF and preparation of a terrorist act and sentenced to three years' and eight years' imprisonment respectively.

Use of cash couriers: Operation Benchmaker

A UK national, Wahabi, was convicted under s.17 of TACT (being involved in an arrangement which makes money or other property available to another with the knowledge or reasonable cause to suspect it may be used for terrorism). Wahabi had organised for EUR 20 000 in funding to be transferred to her husband, a UK FTF fighting in Syria, through the use of a cash courier. The NTFIU worked with the Security Services, the UK Border Force, and overseas LEAs to identify the route of the cash transfer. As a result, the NTFIU was able to intercept the cash courier at the airport and confirm that she had been paid to take money out of the UK for TF purposes using communications evidence to support this. The cash

was forfeited as terrorist property under TACT and Wahabi was sentenced to 28 months' imprisonment in 2014.

Abuse of NPOs: Aid convoy case

Two UK individuals, Hoque and Miah, were charged with providing funds to Hoque's nephew, a FTF in Syria. The UK uncovered evidence of Hoque's nephew asking Hoque for funding for a sniper rifle. Hoque was put in touch with Miah who travelled to and from Syria with an aid convoy to transport the funds to Hoque's nephew. Hoque was sentenced to five years' imprisonment for two charges of supplying GBP 4 500 in terrorist funding, while Miah was sentenced to 2.5 years' imprisonment on one count of providing GBP 1 500 to an FTF in Syria.

During the police investigation, the Charity Commission for England and Wales (CCEW) became aware of an organisation soliciting funds for charitable purposes via aid convoys, which had not registered as a charity. Following Hoque and Miah's arrest, documents were discovered in Miah's house linking Miah to charitable aid convoys. CCEW and police intervention led to the winding up of the organisation as well as a substantial reduction of aid convoys (see section 4.3.2, para.261).

221. LEAs across the UK share a cohesive strategy of pursuing the most serious available terrorism-related offence. This often results in TF being pursued as a more serious charge (e.g. preparation of a terrorist act (TACT, s.5) which carries a greater sentence) instead of or alongside a TF-specific charge (TACT, ss.15-18). Since 2012, of the 68 persons convicted of preparation of a terrorist act (TACT, s.5), one in five were also convicted of a specific TF offence (TACT, ss.15-18). The UK also pursues standalone TF charges where appropriate. Between April 2012 and March 2017, the UK prosecuted 25 persons under the TF-specific offences of the Terrorist Act 2000 (TACT, ss.15-18) resulting in 18 convictions (a 72% conviction rate) (see Table 20 below).

Table 20. **TF prosecutions and convictions in England, Wales and Scotland**

	2014/15	2015/16	2016/17
TF prosecutions			
TF-specific charges: TACT, ss.15-18	4	11	2
Other TF related TACT offences	19	23	23
TF-related prosecutions under other legislation	24	55	25
Total TF prosecutions	**47**	**89**	**50**
TF convictions			
TF-specific charges: TACT, ss.15-18	3	3	6
Other TF related TACT offences	25	11	10
TF-related convictions under other legislation	11	33	46
Total TF convictions	**39**	**47**	**22**

222. The threat of terrorism in Northern Ireland is different, and continues to be assessed as severe. However, the nature of the threat has changed as terrorist groups

move away from criminal activity engaged in for ideological reasons and towards serious organised crime committed for financial gain.[18] Terrorist funding is often derived from the proceeds of crime, including extortion, smuggling, or protection rackets. Funds are typically moved in cash, often across the border to and from the Republic of Ireland; the UK takes active steps to mitigate this risk (see box 20 below).

4

Box 20. **Disrupting TF in Northern Ireland: focus on organised crime, cross-border cash transfer, and abuse of MSBs**

Since the signing of the Belfast Agreement in 1998, the nature of TF in Northern Ireland has evolved with paramilitary and terrorist groups increasingly focusing on organised crime, not all of which is intended to raise funds for terrorism. Dissident Republican groups in Northern Ireland undertake a range of criminal activities, including cigarette smuggling, fuel laundering and smuggling, extortion and robbery. These groups operate as organised criminal groups. While some of their conduct may be committed for the purpose of funding terrorist activity, some may also be committed for personal gain. By focusing on organised crime, the Northern Irish authorities are therefore able to prosecute and disrupt potential terrorist groups engaged in potential TF activity. LEAs operating in Northern Ireland collaborate in an Organised Crime Task Force which targets organised crime in Northern Ireland. Dissident groups often move the proceeds of their organised criminal offending across the border either to or from their counterparts in the Republic of Ireland. Acknowledging the TF (and ML) risk posed by cross-border cash transfers and MSBs in Northern Ireland, the Task Force established a program to visit MSBs located close to the Irish border to understand their particular compliance challenges. The PSNI, NCA and HMRC also established a co-located Paramilitary Crime Taskforce in 2017. The program has already resulted in the financial scoping of over 40 cases of individuals linked to paramilitary crime.

223. The blurred lines between TF and organised crime are reflected in law enforcement efforts. The PSNI is focused on disrupting organised crime and paramilitary groups as a method of preventing TF. TF investigations and interventions therefore tend to result in prosecutions and convictions for the underlying criminal activity. This strategy is reflected in Northern Ireland's TF prosecution and conviction figures (see Table 21 below), but enables LEAs to pursue TF without providing evidence that finances are being raised for terrorist purposes which is difficult in Northern Ireland's current terrorism context.

18 2017 NRA and Fresh Start Panel "Report on the Disbandment of Paramilitary Groups in Northern Ireland" (May 2016).

Table 21. **TF and terrorism prosecutions and convictions in Northern Ireland 2015-17**

	2015	2016	2017
TF prosecutions (TACT, ss.15-18)	0	1	1
TF convictions (TACT, ss.15-18)	0	0	1
Terrorism-related convictions (other legislation)	13	2	0

TF identification and investigation

224. The UK successfully identifies and investigates TF through the use of financial intelligence and other information, and in the course of terrorism investigations which systematically consider a TF component. These findings were based on: statistics on the number of cases investigated, prosecuted and convicted; discussions with NTFIU, UKFIU, CPS, PSNI, PPSNI and other relevant LEAs; and various case studies.

225. The UK's ability to pursue TF investigations is aided by the availability of specialist teams and expertise. NTFIU leads TF investigations for England, Wales and Scotland from within the Counter Terrorism Command (SO15) of the London Metropolitan Police. Eleven specialist counter-terrorism units exist across the UK, each with access to Counter Terrorist Financial Investigators who are accredited and trained by the London Metropolitan Police (which has devolved responsibility to the NTFIU). This structure ensures that TF investigations are integrated into any terrorism-related investigation. As at June 2017, almost 70% of counter-terrorism investigations were receiving specialised financial investigation support (see table 4.3 below) and nearly 10% of counter-terrorism investigations were primarily financial investigations. In Northern Ireland, the Crime Operations Department leads the counter-terrorism response, including on TF. The different TF profile in Northern Ireland means that the distinction between activity pursued for criminal gain and terrorist fundraising is blurred. As a result, a lot of counter-terrorism LEA activity in Northern Ireland is integrated with the response to organised crime.

Table 22**. Counter-terrorism (CT) investigations with a financial investigation component (2017)**

	Total of CT investigations	CT investigations receiving financial investigation support	% of CT investigations receiving financial investigations support
England, Wales, and Scotland	538	364	68%
Northern Ireland	52	6	12%

Note: The data represents a snapshot in time as at 5 June 2017 for England, Wales, and Scotland and 19 September 2017 for Northern Ireland.

226. The nature of the UK's TF threat (low level, low value) makes the identification and detection of TF more difficult and renders co-operation between agencies essential. The UK has an NTFIU officer embedded within the UKFIU to facilitate the distribution of TF SARs, and DATF requests are also useful in detecting and preventing TF (see Chapter 3 on IO.6).

227. Once the financial investigation is opened, the investigating authorities have access to a broad range of investigative tools and intelligence which can be easily shared between relevant agencies through existing gateways. Investigators may also

share and obtain information from other LEAs and financial institutions through JMLIT. This public/private collaboration has had positive investigative outcomes (see box 21 below). Investigators are well equipped to use available tools and receive financial investigation training from the NCA and NTFIU. The UK's capacity for undertaking TF investigations was extended by the Criminal Finances Act 2017 which now permits the financial investigation powers in TACT to be exercised by civilian-accredited financial investigators employed by the LEAs.

Box 21 **Public-private sector collaboration on counter terrorism and TF**

The close relationship between the NTFIU and UK financial institutions is demonstrated by the proactive co-operation provided following attacks in 2017.

In the aftermath of the Westminster attack, multiple financial institutions proactively reached out to the head of the NTFIU to offer assistance in identifying the terrorist networks involved, allowing the NTFIU to more rapidly obtain a full financial picture.

After the London Bridge attack NTFIU, with UKFIU support, initiated a 24/7 response and the case was brought to JMLIT within 12 hours of the attack. Within a few hours of the briefing, financial institutions were able to provide assistance to identify the payments for van hire and establish spending patterns, allowing further investigative strategies to be identified. This assistance was crucial in allowing investigators to conclude that the attack involved only three attackers with no broader network.

TF investigation integrated with –and supportive of– national strategies

228. TF investigations are well integrated into and supportive of the UK's national counter-terrorism strategies. The assessors' conclusions were based on a review of the UK's counter-terrorism strategies and oversight bodies, and discussions with the UK Home Office, NTFIU, the Security Service, JTAC, and other law enforcement agencies.

229. The UK's counter-terrorism and TF structure is led by Home Office and overseen by the Ministerial-level, inter-agency Terrorist Finance Board. The UK's counter-TF policy, as set by the Terrorist Finance Board, is framed in the 2016 Counter-Terrorist Finance Strategy and associated Delivery Plan. The Delivery Plan identified vulnerabilities and legislative gaps through a review of ongoing and closed investigations and intelligence from relevant bodies. Several identified gaps have subsequently been addressed by the Criminal Finances Act, including improving private sector and law enforcement information-sharing and enhancing law enforcement powers to seek disclosure and freeze accounts.

230. Integrating TF with national counter terrorism strategies is facilitated by the UK's Counter-Terrorism Network which improves co-operation and information-sharing between the Security Service, NTFIU, regional Counter-Terrorism Units, and

other government departments or regulators. A particular strength in this area is strong public/private co-operation (see box 21 above). The UK also makes frequent use of embedded officers. An NTFIU officer is embedded within the UKFIU. Officers from HMRC, Department of Work and Pensions, and other relevant LEA and government personnel are embedded within the NTFIU (see box 22 below).

Box 22. **TF investigations as part of a broader strategy to fight FTFs**

UK intelligence estimates that approximately 850 UK individuals have travelled to Syria and Iraq to engage in conflicts as FTFs. The UK estimates that just over half have returned to the UK and 15% have died abroad, leaving around 300 FTFs who remain in conflict zones and may return to the UK. The UK actively pursues two TF aspects with respect to these individuals: the funding of travel to the conflict zone; and subsistence in-country potentially through the support of relatives or contacts in the UK or the abuse of legitimate benefits. Law enforcement agencies work with HMRC and the Department of Work and Pensions to suspend benefits wherever intelligence indicates a claimant has left the UK for extremist purposes. These TF aspects integrate with a broader counter-FTF policy. This includes utilising available powers to remove passport facilities, imposing travel restrictions, and depriving individuals of British citizenship. The flow of UK FTFs has steadily fallen since the start of 2015.

Effectiveness, proportionality and dissuasiveness of sanctions

231. The penalties applied by UK courts in TF cases are effective, proportionate, and dissuasive given the types of offending and how it is pursued. The assessment team based this conclusion on sentencing statistics provided by the UK, case studies on convictions and sentencing in TF cases, and discussions with the NTFIU and CPS.

232. Overall, the conviction rate in the UK is relatively high. Between 2012 and 2017, the UK charged 25 individuals with TF-specific offences and obtained 18 convictions, amounting to a 72% conviction rate. Over the same period, the UK pursued 108 individuals for preparation of a terrorist act (e.g. s.5 TACT), obtaining 68 convictions (a 63% conviction rate). No legal persons have been convicted of TF offences; however, this is in line with the UK's risk profile and the types of TF activity being undertaken in the UK context.

233. Upon conviction, TF-specific offences (TACT, ss.15-18) are punishable by 14 years' imprisonment, a fine, or both while preparation of a terrorist act (TACT, s.5) is punishable by life imprisonment. These are the highest custodial sentences available in the UK and are broadly in line with related offending (dissemination of terrorist publications is punishable by seven years' imprisonment). In practice, sentences in the UK's TF-specific cases (i.e. those pursued under TACT, ss.15-18) tend to fall at the lower end of the scale with the majority of defendants being sentenced to less than three years' imprisonment. In some cases, this is a reflection of the UK's pursuit of all TF offences, including both serious and low-level types of offending, although case

studies suggest there are higher-end cases in which the sanctions imposed have still been low (see box 23 below). The low sanctions for TF-specific offending may also reflect the UK's strategy of pursuing standalone TF-specific charges only where a more serious charge (e.g. preparation of a terrorist act under TACT, s.5) cannot be made out. The average sentence length for all potential TF offences (TACT, ss.5 and 15-18) is 15 years' imprisonment, although the majority of sentences for all terrorism-related convictions still fall between one and four years (see Table 23 below). There is an automatic assumption of imprisonment in TF cases and if either the CPS or a member of the public believes a TF sentence is unduly lenient, they can appeal to the Attorney General to lengthen the sentence. In addition, individuals convicted of TF are typically also sentenced to counter-terrorism monitoring and notification orders which restrict their movements and activities. These factors increase the effectiveness, proportionality and dissuasiveness of available sanctions.

Box 23. **Examples of sanctions in TF cases in the UK**

21 months' imprisonment for the offer to provide ballistic glasses

A UK individual entered into an agreement to make available a pair of military grade ballistic glasses to a person he knew was in Syria participating in the on-going conflict. The individual offered the glasses and asked for the person's prescription. As a result, he was found guilty of TF and sentenced to 21 months' imprisonment in addition to a Notification Order under the Counter-Terrorism Act 2008 (which included requirements to register with the Police, keep them informed on his movements, and obtain approval to travel).

27 months' imprisonment for the provision of GBP 219

Two UK individuals, Mr and Mrs A, arranged to send GBP 219 to their nephew through an MSB and via a third party country after being informed that the nephew had participated in a training camp and was fighting in Syria. Mr and Mrs A were arrested. Both pled guilty and were sentenced to 27 months' and 22 months' imprisonment respectively, in addition to terrorism notification orders.

28 months' imprisonment for the provision of EUR 20 000

A UK individual, Wahabi, arranged for a cash courier to smuggle EUR 20 000 in cash to Wahabi's husband, who was a FTF for ISIL. The cash courier was detained at the border and admitted to the attempted cash movement. The courier was found not guilty, while Wahabi was sentenced to 28 months' imprisonment (on the basis of certain mitigating circumstances) in addition to forfeiture of the EUR 20 000 and the payment of costs.

Table 23. Sentence lengths for terrorism-related convictions under TACT 2013-16

	2013/14	2014/15	2015/16	Total (%)
Under 1 year	2	1	1	4%
1 < 4 years	10	15	19	44%
4 < 10 years	7	3	16	26%
10 < 20 years	11	4	-	16%
20 years to life	3	1	3	7%
Other	-	-	3	3%
Total	**33**	**24**	**42**	**100%**

234. Convictions for terrorism-related offences, including TF, are rarely appealed successfully. Between April 2009 and March 2016, 57 appeals against terrorism convictions were heard, of which 46 (81%) were dismissed or abandoned. No appeals resulted in the conviction being quashed, although 10 appeals (18%) resulted in a reduction in sentence and one resulted in an increase in sentence.

235. In England and Wales, the judiciary-led Sentencing Council is in the process of codifying existing case-based guidance on TF and terrorism sentencing in response to recent terrorist attacks in the UK.[19] These would formalise the judges' weighting of culpability and harm in determining the appropriate sentence. Under the proposed guidelines, the sentence would be lower where there was little planning or the act was committed through coercion or intimidation, and where the funding would make "a minor contribution to furthering terrorism". These considerations appear in line those currently being applied by the courts. In Northern Ireland and Scotland, there are no formal sentencing guidelines, but there are guideline judgments from the higher courts.

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

236. The authorities make good use of alternative criminal justice, regulatory or other measures to disrupt TF activity where securing a TF conviction is not possible. Alternative measures include: pursuing other criminal charges, using broader counter-terrorism powers, financial disruptions and pursuing civil penalties. These findings were based on a review of statistics on the use of alternative offences in TF-related cases, case studies showing effective disruption and the use of alternative mechanisms, and discussions with authorities on the tools used to counter TF.

237. The LEA and prosecutorial authorities consistently pursue other offences where a TF conviction is not possible. As noted above, it is standard policy for a more serious terrorism charge to be pursued wherever possible (e.g. preparation of a terrorist act). Where a terrorism-related charge is not possible due to the circumstances of the case, the UK will actively consider and pursue alternative criminal offences. LEAs will also seek to use other relevant agencies to support prosecutions as necessary.

19 UK Parliament, Draft Sentencing Council Guideline on Terrorism (23 February 2018).

Table 24. **Common criminal alternatives to a TF prosecution**

	2013/14	2014/15	2015/16
Prosecutions			
Common law fraud offences	0	3	0
Criminal Law Act 1977 fraud offences	0	2	16
Fraud Act 2006	6	13	22
Proceeds of Crime Act 2002	10	6	17
Total alternative prosecutions	**16**	**24**	**55**
Convictions			
Common law fraud offences	2	1	0
Criminal Law Act 1977 fraud offences	0	3	10
Fraud Act 2006	12	7	7
Proceeds of Crime Act 2002	0	0	16
Total alternative convictions	**15**	**14**	**36**

238. Where criminal prosecution is not possible, the UK seeks to disrupt TF through freezing, seizing, or forfeiting terrorist funds or assets (see description under IO 10). The Home Secretary also has powers to restrict the activities of suspected terrorists where necessary for public protection by issuing a notice under the Terrorism Prevention and Investigation Measures (TPIM) Act 2011. TPIM notices can restrict the amount of cash held by the subject, access to communication devices, residency requirements, access to certain areas, association with certain persons, and can require regular reporting. TPIM notices remain in place for 2 years and can be renewed only once. TPIMs are used rarely. As of August 2017, only six individuals were subject to a TPIM notice. Given their invasive nature, this minimal use appears appropriate.

Overall conclusions on IO.9

239. **The UK has achieved a high level of effectiveness for IO.9.**

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

240. Overall, the UK has a strong system to implement targeted financial sanctions (TFS) without delay under the relevant UNSCRs. Using the legal framework described under R.6 the UK has demonstrated its ability to implement TFS within the context of: i) UN designations pursuant to UNSCRs 1267/1989 and 1988; ii) EU designations and national designations; and iii) in response to requests from third countries to take freezing action pursuant to UNSCR 1373.

241. HMT's Office of Financial Sanctions Implementation (OFSI) leads on the implementation of financial sanctions and terrorist asset freezing in the UK. The creation of OFSI in March 2016 reflects the importance that the UK attaches to financial sanctions.

242. There are minor shortcomings in relation to enforcement actions taken with respect to sanctions breaches, delays in communicating designations and inconsistent appreciation and application sanctions compliance across FIs and

DNFBPs. However, the requirements under core issue 10.1 are well-implemented in relation to the FIs facing the highest risk of providing services to and/or dealing with the assets of designated entities. The assessment team's conclusions are based on: interviews with OFSI, supervisors and private sector entities, case studies in relation to actions for non-compliance, and statistics on assets frozen.

Designation

243. The UK has a leading role in international sanctions policy and generating listings at the UN. The UK is on the UN Security Council and CFT is one of its priorities for the UNSCR 1267 Sanctions Committee. Between 2010 and the on-site visit, the UK has co-sponsored more than 41 designation proposals to the 1267 Committee and has made 8 designation proposals concerning UK nationals.

244. The UK takes a multi-agency approach to proposing sanctions designations, with the Foreign and Commonwealth Office (FCO) leading on the UK's policy on UN and EU counter-terrorism sanctions. An MOU between FCO, OFSI and operational partners was established in January 2017 and sets out how relevant agencies should work together on proposing designations. Two proposed designations were put to the UN Sanctions Committee under the MOU process and were designated at the UN in July 2017.

245. A similar process applies domestically under the UK's domestic 1373 process pursuant to the Terrorist Asset-Freezing Act 2010 (TAFA). There were 20 current designations under TAFA as of November 2017. These designations are reviewed on an annual basis. OFSI has conducted outreach to operational partners to ensure they are aware of the domestic designation processes. Below is a case study of how a foreign terrorist fighter (FTF) was proactively disrupted using targeted financial sanctions.

Box 24. **FTF disruption through domestic sanctions**

In June 2014, law enforcement approached HMT with the view to imposing an asset freeze on an individual who was assessed to have joined Da'esh and then thought to be in the Turkey-Syria border area. Information became available that he had crossed into Turkey and was attempting to access his UK bank account by withdrawing the maximum permitted cash amount every day. HMT worked closely with operational partners, applying the freeze within two weeks of initial contact from law enforcement. The disruption was successful and prevented the individual from accessing further funds whilst in the region.

Implementation of sanctions

246. In total, the UK currently has GBP 70 000 frozen under UNSCR 1267 measures (the UN ISIL (Da'esh) and Al-Qaida Regime) and GBP 9 000 frozen under UNSCR 1373 measures (under the TAFA).

247. The legal obligation to implement TF-related TFS occurs without delay. OFSI notifies UK FIs and DNFBPs of any updates within one business day (although in practice this can be three to four calendar days). The UK has addressed the delays in the EU system through the Policing and Crime Act 2017 which gives all new sanctions listings made by a UN Security Council immediate effect in the UK for 30 days. This allows time for the EU to add the new listings to an existing sanctions regulation. Therefore, UN-designated persons are immediately designated in the UK. As such, when names are added per existing UNSCRs related to Al-Qaida and ISIL individuals are immediately designated. Since April 2017, all TF-related TFS have taken direct effect in the UK without delay.

248. Listings take direct effect as soon as they are made at the UN. To publicise the listing, OFSI updates its consolidated list of financial sanctions targets within one business day of publication by the UN. OFSI also publishes notices of new additions to the list and notifies its subscriber base of approximately 22 500 people including financial institutions and other relevant organisations such as law firms. OFSI aims to communicate these listings within one business day. On rare occasions, this can be up to three or four calendar days when designations occur on Fridays, Saturdays or on public holidays, however, this is a minor deficiency. As a permanent member of the UNSC, the UK is aware of imminent listings ahead of designation and has, where appropriate and necessary, pre-notified FIs and DNFBPs of these listings.

249. Larger FIs and DNFBPs appear to have effective controls with respect to sanctions, though these controls are more varied in smaller FIs and DNFBPs. OFSI has a program of continuous engagement to raise and maintain awareness with FIs and DNFBPs of all sizes in an effort to ensure that financial sanctions are properly understood, implemented and enforced. OFSI has also developed guidance on how to implement sanctions, including for charities. These extensive outreach efforts have led to improvements in industry understanding and compliance.

250. Sanctioned persons and entities are not prevented from setting up companies in the UK. Companies House should be required to perform sanctions checks on individuals and entities prior to their registration and on an ongoing basis as changes are made to registration details.[20] However, this is considered to be a minor shortcoming as UK companies with UK bank accounts (which constitute the majority of UK companies) will be screened by UK FIs.

251. OFSI addresses non-compliance through a range of approaches including warning letters to persons suspected of breaches, requesting them to provide details of how they intend to improve compliance, and engaging firms' management to obtain information about how they will improve compliance. However, supervisory limitations to date (which have largely consisted of non-public action), the limited sanctions that FCA has imposed for sanctions violations, and the lack of any fines by OSFI may exacerbate the risks of sanctions evasion by unwitting financial institutions or DNFBPs, but this has been given less weight under IO.10.

252. Until recently, the UK's enforcement powers were limited to criminal penalties with a maximum custodial sentence of two years. The Policing and Crime Act 2017 increased the maximum custodial sentence for a breach of financial sanctions from

20 After the on-site visit, Companies House started working with OFSI to ensure it can perform these checks.

two to seven years. Also, in April 2017, OFSI was given the power to impose a non-criminal monetary penalty for breaches and the UK's Deferred Prosecution Agreement (DPA) and Serious Crime Prevention Order (SCPO) regimes were extended to cover financial sanctions offences. These new powers are yet to be used. However, the introduction of these new powers was accompanied by considerable press and professional comment in the UK and the authorities believe that it will have a substantial deterrent effect.

253. Apart from the FCA which acts under specific legislative provisions, supervisors rely on very broad powers to monitor sanctions systems and controls. Other supervisors examine whether such controls are in place, as part of their supervisory programmes and, pursuant to general provisions in their own regulatory handbooks can require legal and regulatory actions where an absence of systems and controls, or deficiencies in such controls, is identified. These powers have varying levels of legal status and may make non-compliance with sanctions obligations harder to pursue by supervisors other than the FCA. Only the FCA and HMRC have taken specific enforcement action to date in relation to deficiencies identified in sanctions systems and controls. One professional body supervisor is also working on a number of live enforcement cases.

254. OSFI has demonstrated that it uses its licensing authority effectively. Between January 2015 and November 2017, OFSI issued eight licences under the ISIL (Da'esh) & Al Qaida regime, mostly in relation to the basic needs of designated persons. OFSI works closely with operational partners to determine what amounts the designated person may have access to and requires them to report on their expenditure along with supporting evidence.

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

255. The UK has undertaken significant work to identify which NPOs are at risk of abuse for TF. The charity regulators actively work with these NPOs to promote measures to prevent abuse and proactively apply targeted and proportionate measures to at-risk NPOs, as appropriate. The assessors' conclusions were based on: risk assessments and reports provided by the UK; case studies illustrating outreach undertaken by the charity regulators; and discussions with the charity regulators, LEAs, and UK charities of varying sizes.

256. The UK's NPO sector is large and diverse (over 900 000 organisations).

Table 25. **Size and features of the UK charity sector**

	Number of registered charities	Annual income (GBP billion)	Number of charities operating abroad	Annual income (GBP billion)
CCEW	183 272	72.31	16 731*	15.94
CCNI	5 693	2.27	358	0.36
OSCR	23 098**	11.4	2 642	4.47
Total	212 063	85.98	19 731	20.77

* This figure covers all charities operating outside England and Wales, including those operating in Northern Ireland and Scotland.
** 1 049 additional charities are registered with OSCR but operate in another UK jurisdiction and are therefore primarily supervised and regulated by one of the other charity regulators.

257. Depending on their location, charities in the UK are registered with and supervised by one of three regulators: the Charity Commission for England and Wales (CCEW); the Office of the Scottish Charity Regulatory (OSCR); or the Charity Commission Northern Ireland (CCNI). Charities in Scotland and Northern Ireland must register with the relevant regulator.

258. In England and Wales, approximately 164 000 charities are exempt from registration by virtue of their income or activities. While lower income charities are identified as being at higher risk of abuse, the majority of low-income unregistered charities are local charities which have not been identified as being high-risk. Even though they are not registered, the CCEW has jurisdiction over them and case studies show that CCEW can and will intervene where there are concerns about the operations of an unregistered or informal charity (see box 25 below). The close relationship between the CCEW and counter-terrorism agencies, including the NTFIU, also ensures that any information and intelligence on unregistered and informal charities is shared to ensure oversight of the sector.

259. The charity regulators and broader UK government have undertaken extensive work to identify the risks within this sector. This work has consistently concluded that the vast majority of the NPO sector in the UK are at low risk of terrorist abuse, with the risks concentrated in a sub-sector of just under 20 000 charities which operate internationally (see Table 26 below). Within this small sub-sector, charities facing the highest risk of abuse are those: operating in high-risk countries (such as Syria and Iraq); with a low annual income; which are newly registered; and which are located in London, the Midlands, and the North-West of England. While assessments have identified charities operating abroad as facing higher risks, discussions with the charity regulators showed that they remain alert to the risk of domestic TF and ensure that this is conveyed to charities during outreach activities. In addition to the risk assessments listed in Table 26 below, the UK has also undertaken further, classified, risk assessments which were shared with the assessment team.

Table 26. **UK NPO sector specific risk assessments or reports**

Assessment/ Report	Lead Agency	Contributing Charity Regulators	Key Findings
2015 NRA	HMT, Home Office	CCEW, CCNI, OSCR	• Proven instances of terrorist abuse in the NPO sector are rare • TF risks in the charitable sector are medium-high • Key threats are: illegal fundraising; trustee abuse; looting; diversion of charitable goods; and local extortion
2016-17 annual report on Tackling Abuse and Mismanagement	CCEW		• The TF risk of the NOI sector as a whole is low, but certain parts – particularly charities working internationally in certain countries – face higher risks • Cases over 2016-17 related to: looting or theft of goods and resources by terrorist groups; and allegations against employees, agents, or partners being involved in terrorist activity.
2017 NRA	HMT, Home Office	CCEW, CCNI, OSCR	• The NPO sector is low risk for TF with certain parts of the sector facing higher risks

Assessment/ Report	Lead Agency	Contributing Charity Regulators	Key Findings
			• Risks are higher for charities operating internationally (particularly in Syria and Iraq), particularly low income charities located in London, the Midlands, and the North-West of England • Key risks relate to: charities organising or participating in aid convoys to Syria; charities operating in cash or through MSBs; newly registered charities working in high risk countries; individuals or organisations raising charitable funds for Syria outside of a charity structure; and charities or individuals of interest to law enforcement
2017 Domestic Sector Review of the UK NPO Sector	CCEW	CCNI, OSCR	• The only proven instanced of TF abuse in the NPO sector have occurred in the charity sector • The highest TF risk is within registered charities offering services internationally operating close to an active terrorist threat, although there have also been instances of domestic abuse

260. The UK has successfully taken targeted action to respond to high risk areas. For example, the risk assessments undertaken by the UK consistently identify aid convoys operating in specific regions as at higher risk of terrorist abuse. From 2012 to 2016, 66 aid convoys departed the UK involving 1 335 participants and with the participation or support of over 20 UK charities (all registered with the CCEW). The UK saw a rise in the use of aid convoys between 2012 and 2014, with 31 recorded in 2013. In light of the identified risks, the CCEW, the police, and other government agencies engaged in targeted outreach to highlight the challenges associated with aid convoys and concerns around the efficacy of this aid method. In addition to outreach, the CCEW and LEAs deployed resources and undertook investigations to stop individuals of concern traveling in aid convoys and to scrutinise participating charities to ensure all donations could be accounted for. In 2014, the CCEW also published a regulatory alert for charities organising or participating in aid convoys. As a result of this activity, the use of aid convoys decreased, with only three recorded in 2016.

261. According to the UK's risk assessments, charities with a higher risk of terrorist abuse fall under the purview of the CCEW. Consistent with the risks identified, the CCEW conducts extensive outreach on preventing terrorist abuse which is targeted at at-risk charities that: are operating internationally in high-risk areas; have an annual income of under GBP 10 000; and are newly-established. Targeting occurs through specific invitations and communications as well as proactive on-site compliance visits and meetings with charities. As charities with an annual income of under GBP 5 000 are not required to register, there is a minor risk that the CCEW is not able to identify and target them. However, the CCEW's wider activities largely mitigate this risk. Participation in targeted CCEW outreach events has proven successful. Attendees are asked to complete a pre- and post-event self-assessment which shows an average 48% increase in participants' knowledge and understanding of TF issues related to the NPO sector.

262. The CCEW, in partnership with the charity sector, has also developed an online toolkit of resources for charities containing model templates and forms and advice, including on how to move money safely. Charities spoke very positively of outreach

and guidance efforts by the CCEW. Feedback from the NPOs met at the on-site visit did, however, suggest that the toolkit could be enhanced by providing more specific, detailed guidance for charities, particularly smaller NPOs, including more practical tools (e.g. guides to use hawala in different countries or subsidised membership to sanctions list screening tools). The CCEW does conduct a range of outreach activities with smaller NPOs to provide further assistance in addition to the toolkit.

263. While the risks in Scotland and Northern Ireland are lower, both CCNI and OSCR also conduct outreach to prevent TF abuse. This covers general measures for good governance, accounting and reporting, and the use of regulated financial channels. Both regulators target charities that are higher risk. CCNI is alert to the potential risk of charitable abuse connected to Northern Ireland-specific terrorism. Of the charities registered in Northern Ireland, 20% are engaged in activities relating to 'the Troubles',[21] but assessments undertaken by the UK give no evidence to suggest that these charities are vulnerable to TF abuse and the risk of TF abuse of Northern Irish and Scottish charities is identified as low.

264. All three charity regulators have good relationships with partners. As central points of contact, the charity regulators help LEAs to investigate charities suspected of abuse and assist with international co-operation. Case studies and discussions with the charity regulators and LEAs, including counter-terrorism LEAs and intelligence agencies, show close co-operation between these entities (see Box 25 below). Information is shared between agencies to identify at-risk charities for targeting and any concerns of abuse identified by the charity regulators will be shared with law enforcement. The charity regulators also have strong relationships with the banking sector, and reported ongoing activities to improve charitable access to the banking sector and prevent wide-scale de-risking. Feedback from the banking sector is being incorporated into outreach products, including an updated CCEW compliance toolkit. Charities welcomed these efforts, but noted that charitable access to the banking system remains a global issue.

Box 25. **Co-operation between charity regulators and law enforcement to detect, prevent and sanction TF**

In March 2014, the police contacted the CCEW regarding a person of interest for TF. The police shared information with the CCEW (under a statutory gateway provided by s.54 of the Charities Act 2011) on the individual's solicitation of funds via social media. However, the CCEW was able to confirm that the individual lacked any formal involvement in any registered charity. The CCEW commenced an investigation which found that between July 2013 and April 2014, the individual had received more than GBP 12 000 in charitable donations. While some of these funds were transferred to registered charities, most could not be accounted for or were spent on items

21 The Troubles' refers to the violent 30-year conflict in Northern Ireland in the 1960s and 1970s.

with no charitable application (e.g. a night-vision scope). The CCEW used its statutory powers to remove the individual's claim to the funds; to freeze the bank account; and to direct the application of the remaining funds to another registered charity. The information obtained by the CCEW in the course of its investigation was shared with the police. In February 2016, the individual, Ul-Haq, was convicted of preparation of terrorist acts and TF and sentenced to five years' imprisonment.

Deprivation of TF assets and instrumentalities

265. The UK has effectively frozen assets and funds of terrorists under a variety of available regimes. While the volume of funds involved is not large, it is consistent with the UK's TF risk. The assessment team based its findings on: statistics provided by the UK; discussions with the NTFIU, OFSI, and LEAs; and case studies showing the UK's use of terrorist cash seizure powers.

266. The UK has frozen approximately GBP 80 000 under the TFS regime (see above).[22] The UK also has access to, and actively uses, a range of measures and mechanisms to freeze and forfeit terrorist funds:

a) The Terrorism Act 2000 (TACT) allows the court to make a forfeiture order where an individual is convicted of a TF offence for any money or property in the individual's possession or under their control which might be used for the purposes of terrorism. This power has been used to forfeit almost GBP 40 000 since 2013. While not large, this amount is in line with the UK's identification of TF risk in the UK which is low-level and low-value.
b) ATCSA allows law enforcement to seize suspected terrorist cash for 48 hours after which it can be forfeited where a court concludes on the balance of probabilities that it is terrorist cash. The Criminal Finances Act 2017 extended the definition of cash to include gaming vouchers, fixed-value casino tokens and betting receipts. Even before these changes, this power was used regularly. Between April 2012 and March 2017, police made 79 cash seizures totalling GBP 495 797. Further changes under the Criminal Finances Act 2017 enable LEAs to use ATCSA to freeze terrorist funds in bank accounts for up to two years after which forfeiture can be sought. As at March 2018, the power has been used 13 times.
c) The Terrorist Asset Freezing etc. Act 2010 (TAFA) allows HMT to indefinitely freeze assets where the subject was involved in terrorist activity and freezing is required to protect the public anywhere in the world. A TAFA order makes it an offence to deal with or make available funds or economic resources for a TAFA designated person. The orders have been used for 158 individuals since 2001 to freeze GBP 151 000. TAFA has not been used for a new designation since 2015, but the regime remains active to renew existing designations annually.

22 Approximately GBP 70 000 has been frozen under UNSCR 1267 and GBP 9 000 under UNSCR 1373.

d) Where LEAs cannot meet the criteria for using specific terrorism-related freezing and forfeiture provisions, they are able to utilise the general POCA provisions to seize and confiscate assets. The Criminal Finances Act extended LEAs' seizure powers to cover a broader range of assets, including artistic works, watches and precious stones. It also created a new administrative forfeiture power which allows LEAs to forfeit funds via an administrative process overseen by a police officer rather than a court. These powers remain new and have not yet been used.

Table 27. **Terrorist funds forfeited (GBP)**

Basis for forfeiture	2014/15	2015/16	2016/17
TACT	2 890	0	600
ATCSA	117 672	17 761	199 040
POCA (where the primary offence is terrorism-related)	1 850	16 521	15 454
Total	122 412	34 282	215 094

Consistency of measures with overall TF risk profile

267. The measures undertaken by the UK are consistent with its overall TF risk profile. These conclusions were based on: statistics provided by the UK; discussions with the NTFIU, OFSI, and LEAs; relevant risk and threat assessments; and case studies showing the UK's use of terrorist cash seizure powers.

268. The UK is extremely active on TFS which is consistent with its priorities and role as a global leader in this space. As recognised in the NRA, the TF risk is predominantly UK-based, with the highest risks posed by: low-level, self-funded attackers; individuals providing small amounts of funding to FTFs; or individuals financing their own travel plans. The UK's action in freezing terrorist funds and depriving terrorists of funding is consistent with these risks. While the vast majority of UK charities pose little or no TF risk, the UK has actively identified the at-risk parts of the sector as those charities which: operate in high-risk countries (such as Syria and Iraq); have a low annual income; are newly registered; and are located in London, the Midlands, or the North-West of England. Appropriate action is taken to engage with these charities.

Overall conclusions on IO.10

269. **The UK is rated as having a high level of effectiveness for IO.10.**

Immediate Outcome 11 (PF financial sanctions)

Implementation of targeted financial sanctions related to proliferation financing without delay

270. The UK has a long-standing commitment to counter proliferation and has been active in disrupting those seeking to finance proliferation activity in the UK and globally. It has also proposed and supported designations under the relevant UN sanctions regimes. The 2015 Strategic Defence and Security Review (SDSR) underlined the UK's commitment to remaining at the forefront of international efforts to tackle proliferation. The National Counter-Proliferation Strategy 2020 has

countering proliferation financing as an integral part. The UK bolstered its commitment to the robust implementation and enforcement of financial sanctions by establishing the Office of Financial Sanctions Implementation (OFSI) in HMT in 2016 and by adopting stronger enforcement powers to address serious breaches through the Policing and Crime Act 2017.

271. The UK maintains a whole of government approach to counter proliferation work with a focus upon co-operation and collaboration. Under the SDSR, the UK committed to developing the Counter Proliferation and Arms Control Centre (CPACC) which became operational in July 2016 and brings together 50 personnel from all relevant ministries, including the Foreign and Commonwealth Office (FCO), Ministry of Defence (MOD), Department for International Trade (DIT) and the Department for Business, Energy and Industrial Strategy (BEIS). The Centre is the co-ordinating body for counter proliferation and arms control policy and activity, including proliferation finance (PF). There are also a range of other co-ordinating mechanisms, including at cabinet, director and working level, in relation to sanctions, which include a variety of partners, such as HMT (including OFSI), HMRC, the NCA, the FCA, other export control bodies, operational partners and intelligence agencies. These groups encourage information sharing in support of enforcement and disruption activity.

272. Similar to the TF-related targeted financial sanctions (TFS), the UK takes a multi-agency approach to proposing PF sanctions designations and is able to use, as appropriate, classified intelligence in this process to improve the effectiveness of the system. In October 2017, the UK led successful proposals at the EU level for a series of designations and economic measures going beyond the UN measures in order to restrict DPRK-related PF. This included the designation of six entities and three individuals.

273. The UK has a range of staff across agencies working on sanctions policy and implementation. OFSI has around 30 full-time equivalent staff, in addition to support received from a full-time equivalent team of approximately nine legal advisors from HMT (and 5 policy staff). In CPACC, 17 people are engaged in work on sanctions. The Sanctions Unit in the FCO is staffed by around 30 officials. The NCA, and the intelligence community also have officials that work on sanctions targeting and designation. According to the authorities, in times of high demand for resources, the UK applies significantly more personnel to the tasks.

274. Similar to the TF-related TFS, the legal obligation to implement PF-related TFS occurs without delay via the Policing and Crime Act 2017 (see section 4.3 on IO.10). This addresses the gap identified in other EU MERs and the UK has confirmed that since April 2017 there have been no delays in implementation of TFS related to Iran or DPRK. As set out in IO.10 above, communication of designations on OFSI's consolidated list can take up to three to four calendar days when designations are made on Fridays, Saturdays or public holidays. Where OFSI has become aware of relevant assets in the UK, OFSI has pre-notified the entities holding the assets to ensure against asset-flight.

275. OFSI also has clear and effective processes in relation to assisting industry to identify 'false positives' and issuing of licences to allow access to frozen funds. OFSI seeks to and has dealt with requests for de-confliction within three days and has dealt with the last five de-listing requests within one day. On licencing, OFSI has issued guidance about how the UN sanctions sit alongside the EU autonomous authorisation

regime. OFSI has granted authorisation on three occasions from April 2016 to March 2017 to an international humanitarian agency to support a humanitarian programme in DPRK. OFSI has also provided licenses relating to Iran and provided evidence that licences were being refused in cases where funds would have been made available to a designated entity or individual.

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

276. FIS and DNFBPs are required to report (under European Regulations and OFSI guidance) to OSFI if they are holding the funds of a designated entity or person. OSFI also receives reports of potential sanctions breaches and of frozen funds. OFSI undertakes an annual audit to ensure that: it is informed of any freezes; freezes are maintained; and any licences are applied properly. The UK provided the assessment team with a breakdown of funds frozen under PF sanctions (including the number of bank accounts/assets frozen and the amounts of funds frozen). A significant amount of funds are currently frozen under the Iran TFS and to a lesser extent the DPRK TFS. This appears to be in line with the respective trade/financing relationships with Iran and the DPRK.

277. UK law enforcement authorities have used the JMLIT operations group to share intelligence with JMLIT members on proliferation finance cases relating to Iran and DPRK. One DPRK case is currently ongoing. During this work, JMLIT members shared relevant information with the NCA which in turn assisted NCA investigations relating to proliferation finance. The UK is currently working with G7 partners to ensure that lessons learnt from countries' domestic information sharing exercises, including this JMLIT work, can be used to inform internationally co-ordinated typologies and red flag indicators. Similar to TF-related TFS, Companies House does not currently prevent persons and entities subject to PF TFS from setting up companies in the UK (see under IO.10).[23]

FIs and DNFBPs' understanding of and compliance with obligations

278. Similar to TF-related TFS, while larger FIs and DNFBPs generally appear to have effective controls with respect to sanctions, representatives of the government, financial institutions and DNFBPs all stated that the levels of sanctions understanding differed across industry, particularly amongst some smaller or medium size firms. However, the UK has (and is continuing) a programme of continuous engagement to raise further awareness with FIs and DNFBPs of all sizes. For example, on 27 February 2018, OFSI held a meeting with maritime insurance firms to discuss DPRK proliferation finance. OFSI found that while some of these firms were small, they had a good understanding of financial sanctions due to the nature of their business.

279. Large financial institutions demonstrated more sophisticated understanding of Iran and DPRK sanctions obligations and risks, and have more complex risk management, policies and procedures in place to manage these risks. Several banks also participate in the JMLIT which has actively considered PF risks and assisted with NCA investigations relating to proliferation finance.

23 After the on-site, Companies House has begun working with OFSI to run these checks.

280. Small and medium-sized financial institutions, lawyers, accountants, TCSPs, HVDs and EABs have varying degrees of understanding of sanctions obligations (see Chapter 5 on IO.4). Lower PF-related breach reports to OFSI from many DNFBPs may be due to the lesser likelihood of their misuse by sanctions evaders (since much of the PF risk lies with entities involved in international trade). To address this, OFSI has developed sector specific plans for further engagement with the banking, insurance, export, charity and wider DNFBP sectors.

Competent authorities ensuring and monitoring compliance

281. OFSI works well with LEAs and supervisors to ensure that TFS are complied with, including by issuing warning letters. Where non-compliance has been identified, OFSI has pursued a wide range of enforcement activities, including liaising with organisations to require processes and procedures to be put in place to ensure future compliance. OFSI was recently given the power to impose non-criminal monetary penalties for breaches. OFSI has not used these powers as they were not considered to be an appropriate response in the cases thus far identified. While no public enforcement actions have been taken by OSFI and NCA, both agencies are actively investigating and assessing a number of cases where public enforcement action is being considered. If carried out, these enforcement actions will provide an additional deterrent effect for sanctions evaders or unwitting firms.

282. OFSI has identified potential sanctions breaches through reports made directly to it, datasets relating to financial sanctions and proliferation finance, from other government partners or through SARs. It passes all significant breaches of financial sanctions to the NCA for assessment and investigation and meets regularly with NCA colleagues to discuss current and potential cases. The NCA draws on a number of tools to identify PF activity such as referrals from OFSI, reporting through SARs, its own intelligence databases, specific datasets relating to financial sanctions/proliferation finance and referrals from other government partners.

283. Sanctions breaches are being detected. In 2016-2017, 109 breach cases reported to OFSI and 104 investigations were opened relating to potential values of GBP 227 million. The UK provided two examples of working with NCA to deal with such breaches which resulted in a business closing voluntarily and the improvement of a company's sanctions screening as a result of an OFSI warning letter.

284. As with TF-related TFS, OFSI administers and enforces compliance with all relevant UN and EU sanctions regimes. To complement OFSI's enforcement regime, all supervisors also examine FIs and DNFBPs for compliance with sanctions obligations as part of their supervisory programmes, and both the FCA and HMRC have taken enforcement action where an absence of systems and controls or deficiencies in these systems and controls have been identified (see box 26) and one legal sector professional body supervisor is actively working on a number of enforcement cases. As set out under IO 10, there is scope to ensure that supervisors' powers in relation to sanctions screening and controls are consistent and clearly specified in legislation, regulatory handbooks or rule books.

Box 26. **HMRC action on an MSB's failure to apply sanctions screening**

An MSB made a voluntary disclosure to HMRC of an issue with its sanctions list monitoring system (part of their AML compliance IT systems). After some routine systems update/maintenance by the MSB's IT staff, technicians had failed to turn the sanctions monitoring elements of the system back on, and this was not noticed by the business for six months. Upon identifying the issue, the MSB immediately ran all transactions for the six month period in question back through the sanctions checking software and were able to confirm and show to HMRC that no-one on the sanctions lists had been involved in any of the MSB's transactions in the period. More widely, as part of visits to 37 agent premises of this large MSB between October 2014 and April 2015, HMRC found issues relating to maintaining details of agents and training. HMRC applied civil financial sanctions under the MLRs: Regulations 20(1)(d) (internal controls), 20(1)(f) (monitoring and managing compliance with and the communication of the firms policies and procedures) and 21 (training). The penalty of GBP 180 165 was calculated using HMRC's standard framework. The penalty accounts for the sanctions monitoring system failure plus the other failings identified in relation to principle-agent issues.

285. The UK displays the characteristics of a highly effective system. There are weaknesses identified in relation to supervision, compounded by varying understanding of sanctions obligations across industry, and the lack of public enforcement actions by OSFI or the NCA, however, only minor improvements are needed. Granting OFSI civil penalty powers in 2017 is a positive step in addressing this, and investigations are ongoing by a range of agencies, but the results of these are yet to be seen.

Overall conclusions on IO.11

286. **The UK is rated as having a high level of effectiveness for IO.11.**

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

a) All entities performing activities covered by the FATF Standards are required to apply a range of AML/CFT preventive measures under the Money Laundering Regulations 2017. These requirements are comprehensive and consistent across all sectors.
b) The UK has extremely large and diverse financial and DNFBP sectors. The level and types of ML/TF risks affecting individual financial institutions (FIs) and DNFBPs vary greatly, as do the ML/TF risks facing particular sectors. The banking, MSB, legal, accounting and TCSP sectors are materially important and vulnerable to the greatest risks for ML/TF.
c) The UK publishes thematic reviews by regulators which provide examples of best and poor practices and are helpful guides to industry. Published thematic reviews indicate that AML/CFT compliance is not consistent across different categories of FIs. The lower level of supervision of smaller entities raise concerns about the risk mitigation measures that have been applied. These issues are particularly concerning in relation to smaller banks, MSBs and the legal, accountancy and TCSP sectors.
d) There are concerns about the low level of SAR reporting in many sectors, particularly the legal, accountancy and TCSP sectors. While high-quality SARs are being submitted, there remain concerns about the quality of SARs reported across sectors (even among banks which submit 85% of SARs filed).

Recommended Actions

a) The UK should continue to monitor sectors' compliance using thematic reviews, including firms which have not been subject to supervisory attention, and continue to use these activities to raise effectiveness of risk mitigation across sectors.
b) The UK should prioritise and implement SARs reform. One aspect of this should include working with the private sector to customise the SAR form to make it fit-for-purpose for the range of DNFBPs and non-bank FIs.
c) Authorities should continue to improve the feedback and guidance to reporting entities (including those that are not major reporters but are exposed to high ML/TF risks such as smaller banks, MSBs, TCSPs, lawyers, and accountants) on SAR reporting requirements and improving the quality of SAR reporting in order to raise the level of reporting in these sectors, as appropriate. Reporting entities should be encouraged to reinforce this

feedback loop into their ML/TF risk identification and the effectiveness of their AML/CFT programmes.

d) The UK should monitor how the new moratorium extension provisions for DAML requests (i.e., the extended freezing limits) are applying in practice with a view to preventing tipping off.

287. 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.

Immediate Outcome 4 (Preventive Measures)

288. For the reasons of their relative materiality and risk in the UK context, implementation issues were weighted most heavily for the banking sector, heavily for important sectors (MSBs, lawyers, accountants and in some circumstances, TCSP services[24]), moderately heavy for the securities sector, and less heavily for less important sectors (insurance, casinos, EABs, HVDs). This is explained above in Chapter 1 (under structural elements). Overall, the assessors concluded that:

a) ***Most heavily weighted:*** Large banks appear to be implementing preventive measures effectively and engaging proactively with authorities. However, it is not clear if this applies equally to smaller banks which also undertake a range of higher-risk activities and present vulnerabilities for ML/TF, although some of these smaller banks have demonstrated that they are implementing preventative measures commensurate with their risks.
b) ***Heavily weighted:*** Implementation of preventive measures in the MSB sector and among lawyers, accountants and TCSPs is mixed.
c) ***Medium weight:*** The securities sector generally appears to be implementing preventive measures effectively, although some significant failings have been detected, resulting in at least one significant and high profile enforcement action. The UK has also recognised that it needs to develop a better of understanding of risks of ML in the capital markets.
d) ***Low weight:*** Insurance and casinos sectors appear to have a good understanding of their risks and are applying sufficient mitigation measures. Estate agent businesses do not have a sufficient understanding of their risks or how to effectively mitigate them. High value dealers have an inconsistent understanding of their risks and therefore inconsistent implementation of preventive measures (although HMRC reflects an improvement in the sector as a whole). Virtual currency exchange providers are not yet covered by AML/CFT requirements. This is an emerging risk and there is not yet evidence to suggest that broad scale ML/TF is occurring in the UK through this relatively small sector.

289. Assessors' findings on Immediate Outcome 4 are based on: interviews with a range of private sector representatives, findings from enforcement actions and input from supervisors, including reviews completed by FCA, HMRC, the Gambling

24 In the UK NRA 2017, TCSP activity is assessed as high risk when provided by lawyers and accountants.

Commission, the SRA and accounting bodies; and information from the UK authorities (including the NRA) concerning the relative materiality and risks of each sector. Meetings with the private sector representatives did not reveal any serious concerns about the implementation of preventive measures and many provided examples of good practice which shows that there are some good examples of implementation, particularly in the more important sectors. However, given the large number of supervised entities and the wide diversity of the sectors, these examples were not necessarily representative of implementation across the sectors as a whole. Indeed, information from the authorities covering a much larger range of firms in each sector (including supervisory reviews and the NRA) flagged concerns about inconsistent implementation of preventive measures which, in general, were confirmed during discussions with the private sector representatives about implementation across their sectors more broadly.

Understanding of ML/TF risks and AML/CFT obligations

290. Since the last mutual evaluation, risk understanding across all sectors has improved, although deficiencies continue to exist. Across all sectors, supervisors noted that larger firms have a better understanding of risks and their AML/CFT obligations, and are able to allocate adequate resources to doing so.

291. The 2017 MLRs introduced clearer and more detailed obligations for all FIs and DNFBPs to identify, assess and review ML/TF risks in line with their business, customer base, products and services offered, and geographic footprint. As the requirement to have firm-specific risk assessments was only recently introduced in June 2017, the experience of implementation is short. Currently, it appears that smaller firms are not always tailoring risk assessments to their specific needs, generally have less robust compliance controls than larger firms and have had less supervisory attention.

Financial institutions[25] (excluding MSBs)

292. The level and understanding of ML/TF risks and AML/CFT obligations varies across sectors and depends upon factors such as sector of operation, products and services they provide, the quality of staff and management, the jurisdictions they operate in, and the adequacy and history of regulation and supervision. Overall, the financial services sector is continuously improving its understanding of ML and TF risks and firms demonstrated their use of guidance such as the FCA's "Financial Crime Guidance".

293. The 14 largest retail and investment banks operating in the UK (which account for 78% of UK current account market and 79% of UK wholesale banking market and present the greatest systemic risks to the UK) have been assessed by the FCA as having comprehensive risk assessments. This is an ongoing process. In its feedback letter to all 14 firms, the FCA placed a significant focus on the firms' risk processes and systems to ensure that senior management were aware of areas for improvement. In addition, most of these banks are also involved in the JMLIT which

25 This category includes asset managers, securities and insurance firms.

gives them a more sophisticated understanding of operational ML/TF risks and a facility to update their understanding on an ongoing basis.

294. It is not clear if this same level of understanding applies to smaller banks and other FIs which, considering the size of the UK financial sector, also face significant ML/TF risks. FCA's review of 21 smaller banks between October 2013 and June 2014 revealed serious failings in their understanding of ML/TF risks. Half of the banks visited had not assessed the ML risk inherent in their business models. Those banks that did undertake business-wide risk assessment did so to varying standards and the vast majority did not carry out adequate assessments of customer risks.[26] FCA's introduction of the Proactive AML Programme (PAMLP) and the Risk Assurance Review applies to smaller firms should lead to industry improvement. However, where weak controls are identified within PAMLP firms, risk assessments continue to be an issue. The limited scope of the PAMLP (see Chapter 6 on IO.3) suggests these issues may be more widespread. The MLRs introduced in June 2017 now contain a clear requirement to undertake risk assessments, and firms have until June 2018 to apply these requirements.

295. The insurance and wealth management firms met with by the assessors appeared to have a good understanding of the ML/TF risks associated with their sectors. The firms generally viewed the ML/TF risks associated with these industries as low, with some exceptions (e.g. insurance products with features of cash value or investment or the risks associated with third-party reliance. The issues noted above in relation to differences in understanding among firms, including smaller firms, also apply to these sectors.

Money Service Businesses (MSBs)

296. Understanding of ML/TF risks by MSBs is varied given the large size and diversity of the MSB sector. Overall, risk understanding across the sector is improving. Large, global MSBs have strong understanding of their domestic and international risks, in line with the NRA, as do many well-run smaller to medium-size MSBs. Improved supervision of the sector (including through HMRC's Large Agent Network programme), strengthening of firm compliance culture, remedial actions by HMRC and foreign regulators, and the need for the industry to lift standards to maintain banking relationships is likely contributing to the increase in firms' risk understanding. Increased compliance may also be due to consolidation in the sector – there has been a reduction in the number of principal firms in the market (it has dropped by over 20% since 2013-14), meaning that a number of smaller firms have become agents of larger firms.

Lawyers, accountants and TCSPs

297. The new obligation to have a firm-specific risk assessment has not yet been implemented by all supervised entities. For example, a recent review by the SRA into

26 This included 8 wealth management/private banks, 7 wholesale banks, and 6 retail banks. The Thematic Review is available at: www.fca.org.uk/publications/thematic-reviews/tr14-16-%E2%80%93-how-small-banks-manage-money-laundering-and-sanctions-risk

50 law firms revealed that 11 did not have risk assessments in place.[27] Although firms have long carried out client-specific risk assessments, there continue to be deficiencies in some cases. For example, the same SRA review found that 31 out of 100 client matter files did not include evidence of the assessment of client-risks.

298. The SRA has developed a risk assessment to help guide law firms on sector specific risks.[28] However, inconsistencies in risk understanding by professional body supervisors (see Chapter 6 on IO.3) create inconsistencies in the understanding of ML/TF risks in the legal, accounting and TCSP sectors. The private sector representatives interviewed showed familiarity with the NRA 2017 but did not necessarily agree with all of its findings.

299. On the whole, the compliance picture is generally improving in relation to lawyers', accountants' and TCSPs' understanding of their risks and AML/CFT obligations. However, supervisors have identified the following categories of firms as being relatively less likely to document their risks or understand their obligations: relatively new or rapidly growing firms; firms with a small number of long-term local clients; and firms which have not allocated adequate resources to AML compliance. The lack of supervision of smaller firms is contributing to the lack of understanding of AML/CFT obligations.

Other DNFBPs (casinos, HVDs, EABs)

300. ***Casinos:*** Casinos met during the onsite were aware of the NRA and the Gambling Commission's ML/TF risk assessment. The Gambling Commission has recently undertaken a review of remote gambling operators (for example, online services) which identified weakness in development of risk assessments by the sector.[29] The Gambling Commission has taken steps to mitigate these weaknesses through enforcement action against the operators, visits to Malta and Gibraltar to inspect some of the operators, changes to their compliance approach and the publication of a letter to the online operators setting out the risks and weaknesses (with recommendations for action to mitigate the identified weaknesses).

301. ***High value dealers (HVDs):*** While categorised as low risk for ML/TF, there is an inconsistent understanding of risks facing the sector. HMRC has noted a rise in the number of firms demonstrating an understanding of their risks and obligations, including a number which have stopped accepting high-value payments in order to keep themselves out of the scope of supervision while contributing to managing the risks associated with cash in the UK. Although this mitigates some exploitation of the sector, the persisting gaps in understanding across the industry are an ongoing vulnerability, with the truncated time period available to conduct CDD exacerbating the vulnerability.

302. ***Estate agent businesses (EABs):*** Increased face-to-face compliance visits by HMRC (since it took over from the Office of Fair Trading in 2014) and other

27 www.sra.org.uk/sra/how-we-work/reports/preventing-money-laundering-financing-terrorism.page

28 www.sra.org.uk/sra/how-we-work/reports/aml-risk-assessment.page#

29. www.gamblingcommission.gov.uk/PDF/Letter-to-remote-casino-operators-January-2018.pdf

interaction with the sector is increasing the EAB's understanding of risk and AML/CFT obligations. HMRC has publicly highlighted the need for estate agents to be alive to risks in relation to PEPs, high-value transactions (super-prime property in London for example) and non-face-to-face clients.

303. EABs noted that, within the system for the sale of property in the UK, they are not always in the best position to detect ML or conduct CDD (as opposed to conveyancers and banks who are more likely to be able to collect this information). EABs stated their belief that the real ML/TF risks relate to letting property which is when they deal with client money. This is despite letting property being an activity neither covered under the FATF Recommendations or the UK's AML/CFT requirements, nor identified as a ML/TF risk by UK authorities.[30]

Application of risk mitigating measures

304. Regulated entities across a broad range of sectors have AML programs designed to mitigate ML/TF risks. Interviews with the private sector reflected a strong knowledge of the AML/CFT requirements as they apply to their context and a strong commitment to apply these measures to ensure that their businesses are clean of criminal proceeds. Thematic reviews by a number of supervisors, however, suggest that while there is upward trend in compliance, some pertinent issues continue to exist, including that smaller firms have less resources committed to combatting ML/TF risk.

Financial institutions (excluding MSBs)

305. There is an upward trend in compliance by banks, both large and small. Larger banks met with during the onsite demonstrated that they have integrated risk mitigation measures into their day-to-day operations, and have taken a leadership role in proactively co-operating with LEAs to develop more sophisticated means to prevent criminal funds from entering UK banks. However, given their global business presence, the size and complexity of their business models, legacy systems, and the need for continued remediation in a number of cases, it is likely that some large banks will face continued challenges in effectively mitigating their risks.

306. The FCA has noticed that many firms engaging in extensive remedial programmes are supported by a much clearer tone from the top on the importance of managing financial crime risk. This was echoed by the banks met during the onsite which noted that the requirement for firms to nominate a senior management figure with responsibility for financial crime has led to a better understanding by senior management of what is needed to achieve effective outcomes.

Money Service Businesses (MSBs)

307. MSBs have been subject to supervision by HMRC since 2002, although there has been increased focus on sub-sectors of MSBs that are the highest risk for ML/TF in recent years due to their vulnerabilities and banking access challenges. While the

30 HMG has noted that the EU's recently agreed 5th Money Laundering Directive will require Member States, including the UK, to place AML/CTF regulation on estate agents letting properties for a monthly rent of EUR 10 000 or more. This goes beyond the scope of the FATF Standards.

private sector firms met with exhibited strong risk mitigating measures, supervisors identified some issues related to insufficient risk management procedures between 2007 and 2017 with a number of MSBs. These had deficiencies related to CDD, ongoing monitoring, enhanced due diligence, recordkeeping, policies and procedures, and training. While increased supervision by HMRC is going some way to address these issues, poor risk management has contributed to these failings.

308. Some firms with agent networks have exhibited bad practice in managing agent risks. In particular, as a result of a review of MSBs in 2014/2015, HMRC identified weaknesses in on-boarding processes (how agents were recruited, including the nature and quality of the checks carried out by principals), monitoring by principals, and training of agents.[31] In response to this, the 2017 MLRs have extended the fit and proper test to MSB agents, but the results of this extension are yet to be seen. However, in the past three years, HMRC's Large Agent Network programme, has led to a greater degree of consistency and an improvement across the sector in terms of levels of regulatory compliance, although further work is required in this area.

Lawyers, accountants and TCSPs

309. Law enforcement has continued concerns about risk mitigation applied by lawyers, accountants and TCSP services where they are provided by lawyers and accountants. There is a diverse population of accountants, lawyers and TCSPs applying a variety of business models. Risk mitigation measures vary, although the firms met with during the onsite all displayed strong risk mitigation measures. The uneven understanding of risks and supervision in these sectors contributes to uneven application of risk mitigation measures, particularly in relation to smaller firms and sole practitioners. For example, data provided by HMRC, in relation to businesses that have been subject to more than one visit as a result of being high-risk or having poor compliance, showed that over 60% of first-time examinations of TCSPs between 2007 and 2017 revealed deficient CDD, ongoing monitoring, and policies and procedures in place, and over 45% had inadequate training. While many of these deficiencies are being addressed (with lawyers, accountants and TCSPs showing the greatest rate of improvements when deficiencies are found), this suggests that risk mitigation is not applied evenly across these sectors.

Other DNFBPs (casinos, HVDs, EABs)

310. ***Casinos:*** Interviewed onshore and remote casinos appeared to have comprehensive risk mitigation controls in place designed to mitigate their risks. Large firms in particular are likely to have a stronger understanding and controls in place, in part due to robust supervision by their foreign regulators. There are issues in relation to controls by some remote casino operators that the Gambling Commission is actively targeting. The Gambling Commission's findings in seven of nine firm onsite examinations revealed that the firms had non-compliant AML/CFT programs. This also evidences the need for improvement in understanding of risk and

31 HMRC, AML/CTF Thematic Review Anti-money laundering Compliance in the Money Service Business Sector, 22 February 2018.

risk management controls in casinos.[32] In 16 out of 27 cases, these weaknesses were resolved following Gambling Commission interventions, and, as mentioned above, the Commission is considering taking regulatory action against the remaining 11 firms

311. ***High Value Dealers:*** The firm interviewed by the assessment team appeared to have a strong understanding of risk and controls in place. Supervisory actions show that application of AML/CFT and sanctions controls to manage risks in the sector, however, is mixed. HMRC has found that the compliance picture is improving due, in part, to the reduced numbers of businesses operating as HVDs. HMRC's focus on pre-registration checks in this sector is making it more difficult for businesses that are not being set up for genuine commercial reasons to register, thereby reducing the number of non-compliant businesses that are registered.

312. ***Estate Agency Businesses:*** HMRC has supervised EABs since 2014-15 and has seen a reduction in the levels of breaches identified over that time. HMRC's engagement with the sector, combined with its programme of interventions targeted at high-risk areas is helping to drive up compliance standards.

Application of CDD and record-keeping requirements

313. Interviews with private sector representatives suggested that FIs and DNFBPs understand their CDD requirements. Smaller firms, including MSBs, noted that customers in the UK context are generally accustomed to providing CDD documentation and do so readily. This suggests that CDD requirements are being applied across a range of sectors. Nevertheless, a review of breaches of the MLRs in 2015-2017, revealed that 23% related to CDD, which was one of the most common failings.[33]

Financial institutions (excluding MSBs)

314. FCA finds that in the majority of standard-risk cases, AML controls work well and a sound record of CDD has been found helpful in investigations. Banks met with during the on-site demonstrated that they are effectively refusing business on ML/TF grounds or when CDD is incomplete in addition to their own business or reputation considerations. Banks also regularly update CDD information. For example, one bank reported that it regularly screens its full customer database to determine any potential change in the customer's risk profile (e.g. negative news or potential reputational impact) and may exit the customer based on the new information.

Money Service Businesses (MSBs)

315. Sampling of customer records at face-to-face compliance visits suggests that MSBs' implementation of record-keeping and CDD requirements is mixed. However, the situation has improved and is now generally better in larger MSBs. Overall, there is a general upwards trend in the understanding and delivery of CDD standards in those MSBs supervised by HMRC—particularly in large principal/agent networks.

32 HMT, AML and CTF Financing; Supervision Report, March 2018.

33 HMT, Anti-Money Laundering and Counter-Terrorist Financing: Supervision Report 2015-17, March 2018.

MSBs met with during the onsite demonstrated a good understanding of CDD rules and demonstrated that they are effectively refusing business on ML/TF grounds or when CDD is incomplete.

Lawyers, accountants and TCSPs

316. Large entities met with during the onsite visit demonstrated good understanding of AML/CFT obligations. Supervisors generally report sound compliance in relation to CDD and record keeping (94% of accountancy firms are compliant or generally compliant). Firms met with during the on-site also demonstrated that they are effectively refusing business on ML/TF grounds or when CDD is incomplete in addition to their own business or generally reputation considerations. Where issues arise, they tend to be in relation to conducting ongoing CDD and applying CDD on existing customers.

Other DNFBPs (casinos, HVDs, EABs)

317. Casinos met during the on-site visit had a good understanding of their CDD and record keeping obligations.

318. A HVD noted challenges inherent in their environment (e.g. tensions between the fast moving nature of cash transactions and possibility of losing a sale because of delays caused by CDD). The firms with advanced systems are better able to deal with these issues.

319. HMRC noted that larger EABs are developing centralised CDD teams which need to sign off before properties are marketed. However, the implementation of CDD measures, especially in relation to the identification of beneficial owners, varies in small firms.

Application of EDD measures

Politically Exposed Persons (PEPs)

320. The UK faces a significant risk of ML in relation to foreign corruption proceeds. Private sector firms displayed a strong understanding of these risks and how they manifested in their businesses. Generally all private sector firms displayed a strong understanding of EDD requirements, particularly in relation to domestic and international PEPs, which they all categorised as high-risk to different degrees (high/high, high/standard, and high/low). Firms use databases, open source information and also rely on third party suppliers to assist with the identification of PEPs.

321. Private sector firms, both large and small highlighted difficulties in establishing the source of wealth. FCA supervisory work has flagged that this is an issue for financial institutions. The large banks met with by the assessors also highlighted this as an issue.

322. All of the 11 largest MSB networks (covering 83% of UK agents) have PEP screening software and standard procedures for dealing with PEPs. The larger accountancy, legal and TCSP firms are more at risk to deal with PEPs considering their geographical reach. Smaller firms tend to be risk averse. However, the CDD issues highlighted in the section above, likely impact on the application of EDD.

323. HMRC has identified that there is an increase in EABs setting up as online businesses with vendor clients. This can make customer verification more difficult. However, the use of sophisticated technology (including innovative software to record CDD, which facilitates photo verification and can even identify the geographical location the photo was taken) is effective in mitigating CDD and EDD risks.

324. HVDs do not tend to operate in situations that require enhanced or specific measures to the same extent as some other sectors and HMRC has seen very limited instances of PEPs in the HVD sector.

325. Casinos have a good understanding of AML/CFT obligations on PEP and, for example, seek prior approval of overseas gamblers' visits to UK casinos.

Correspondent banking

326. Large, multinational financial institutions have made significant improvements in their risk management of correspondent banking relationships following a decade of high profile enforcement actions by foreign regulators and remedial efforts required by the FCA in conjunction with foreign regulators. This remains a work in progress at some large institutions, but the FCA demonstrated a strong commitment to working with UK-based institutions to ensure that effective controls are in place.

327. Large firms with substantial correspondent banking books also have group-wide policies and procedures related to AML/CFT and targeted financial sanctions compliance, and have substantially expanded their compliance staff over the last decade. While significant progress has been made, some gaps in compliance related to correspondent banking persist, particularly at smaller banks. This was demonstrated in a 2014 survey by the FCA which found that while some retail, wholesale, and private banks had implemented effective AML/CFT and sanctions controls, significant and widespread weaknesses persisted at some firms (including in relation to correspondent banking, EDD and the ongoing monitoring of high risk clients). Particularly serious issues were found at six banks, four of which voluntarily limited their business activities until weaknesses are corrected, three were required to appoint a skilled person to conduct a more detailed review and make recommendations for improvements, and three conducted remedial work under the guidance of external consultants. The FCA took enforcement action against two of these banks, as well as updating regulatory guidance with further examples of good practice. The FCA has seen significant improvements as a result.

328. Remedial efforts by the FCA, reputational concerns, enforcement efforts by the UK, high-profile actions taken by foreign regulators, and the establishment Senior Managers and Certification Regime (SMCR) and its attendant liabilities on senior management have led to continued progress in addressing these issues. The gap between examinations of SAMLP and PAMLP banks and limited number of smaller bank examinations, however, leads to an uneven playing field in terms of correspondent banking policies and procedures.

New technologies

329. Banks and MSBs interviewed by the assessment team all stated that they analyse new products and services for ML/TF risks prior to their introduction to the market. The assessment team was satisfied with the examples of policies and procedures provided by these firms. However, discussions with the private sector raised concerns that some of the EABs firms providing online services, with no face-to-face contact with their clients, may not adequately fulfil their AML/CFT obligations.

Wire transfer rules

330. In the UK context, banking institutions and MSBs conduct wire transfers. In June 2017, the UK adopted new EU requirements on cross-border wire transfer reporting which contain new obligations for the FIs that are subject to them. The FCA monitors banks' compliance with new legislative requirements as part of its ongoing supervisory engagement. It has not identified any significant issues with firms' implementation of the new wire transfer regulations. The FSA (predecessor to the FCA) conducted a review of firms' compliance with previous wire transfer legislation in 2011 and found no major weaknesses.

331. HMRC noted that MSBs, in most cases, apply the appropriate identity checks and record-keeping where the requirements to establish the identity of the payer (originator) are triggered. HMRC also noted that compliance is also reinforced because the MLRs overlap with the EU's fund transfer regulations requiring payment institutions to collect and retain information on payers and payees when transferring funds (in addition to the CDD requirements in the MLRs).

Targeted financial sanctions

332. All interviewed firms stated that they ran names through sanctions checks prior to customer on-boarding. Large financial institutions and professional gatekeepers demonstrated more sophisticated understanding of sanctions risks related to Iran and DPRK and have more complex risk management and policies and procedures in place to manage these risks. Some small and medium-sized FIs and financial gatekeepers have a less than uniform understanding of sanctions-related risks and have less sophisticated sanctions compliance programs, as demonstrated by the FCA's 2014 survey. Firms have, however, improved their sanctions compliance programs over the last decade in response to FCA activity and the activities and awareness raising from OFSI.[34]

333. Industry representatives and authorities focused on sanctions agree that due to the vast breadth of the legal, accounting, TCSPs, HVDs, and EABs, these industries have inconsistent levels of understanding of their sanctions obligations. The Gambling Commission provides guidance in relation to these obligations and the National Casino Forum provides guidelines on how casinos can meet their sanctions obligations, including making use of database suppliers for sanctioned persons checks.

34 FCA, How small banks manage money laundering and sanctions risk – Update, November 2014.

334. FCA, HMRC and OSFI all expressed a strong commitment to continuing to improve industry compliance. Extensive outreach efforts by OSFI in particular have helped to improve industry understanding and compliance. OFSI has also dealt with instances of non-compliance through warning letters and direct engagement with firms. However, supervisory limitations to date (which have consisted of non-public action), the limited sanctions that FCA has imposed for sanctions violations, and the lack of any fines by OSFI continue to exacerbate the risks of sanctions evasion by unwitting financial institutions or DNFBPs.

5

Higher-risk countries

335. Financial institutions and DNFBPs met with by the assessment team regularly referred to FATF and EU lists of higher risk jurisdictions. They stated that as a matter of practice they did not risk rate all EEA jurisdictions the same in terms of risk, treating some higher risk than others. They further stated that they did not rely upon foreign affiliates to conduct CDD.

Reporting obligations and tipping off

336. Overall, firms met with during the evaluation understand and implement their reporting obligations adequately, however, it is not clear this applies equally across all sectors as SAR filing is low in some sectors. SAR filings across some of the biggest sectors in the UK show a healthy trend, and it appears that the amount of defensive filing has declined. The UK receives more than 450 000 SARs a year which provides a rich source of financial intelligence for LEAs. While concerns remain about the quality of reports filed, work is ongoing between relevant authorities and firms to improve quality and remind firms of their obligations.

337. SARs filing is highly concentrated on a few institutions. Banks contribute almost 85% of the total SAR fillings, with four banks contributing 80% of the reporting. Although this is consistent with the consolidated nature of the UK's banking sector (five banks account for over 85% of the total market share and banks are constantly involved in the movement of money and therefore most likely to spot a suspicious transactions), it does not explain the low level of reporting across other sectors.

338. While large banks met with at the onsite have a window of 30/60 days to undertake their own investigation prior to filing SARs, there is a requirement to report matters requiring immediate attention to the UKFIU and all confirmed that they report SARs as soon as they reach the threshold of suspicion. The UKFIU accepts bulk reporting by the main reporters to facilitate the filing of SARs. Earlier thematic work by the FCA identified instances where a lack of resources in smaller firms had led to backlogs in alerts generated and potential exposure to undisclosed suspicious activity or sanctions breaches. Remedial action, including interventions, was taken.

339. The level of SAR filings by lawyers, accountants and relevant TCSPs could be improved given the high-risk activity they are exposed to, including high-end money laundering. In addition, SARs filled by accountancy sector, legal sector and MSBs are decreasing. Large accountancy firms met with at the onsite explained this decrease as a sign of increased and better understanding of what is and what is not reportable. The UK authorities, including the supervisors, Home Office and UKFIU have undertaken outreach to raise the quality of reporting and remind businesses of their

SARs obligations. This includes sectoral specific reports, advertising campaigns and industry events focusing on SARs. The Home Office's 'Flag It Up' campaign, which targets the legal and accountancy sectors, has led to a demonstrable increase in visits to the UKFIU's guidance on submitting SARs. Reporting from the gambling sector has increased in the last three years, due to the Gambling Commission's new enforcement strategy which included a focus on suspicious activity reporting and the UKFIU's increase engagement on the issue.

340. Reflecting the high volume of reporting and the wide variety of sectors and businesses incorporated into the UK's AML/CTF regime, there are concerns about the quality of reporting by all reporting entities, including banks. During the on-site visit, some firms indicated that they were sometimes filing SARs in response to unexplained/unusual transactions without additional analysis or investigation. LEAs reported concerns about the quality of the SARs, including that they lacked information on a genuine suspicion of ML/TF.

341. Feedback or additional requests for information are often provided for DAML or DATF requests. However, in general, the reporting entities met with during the on-site noted that they require further feedback from the UKFIU. Nearly all DNFBPs met with at the on-site highlighted the need for information and more timely feedback to refine their systems and produce better SARs. They specifically noted challenges in detecting ML in the absence of feedback on whether SAR submitted is useful or not. The value of SARs has increased as a result of public/private engagement through JMLIT, the UKFIU's engagement groups and supervisory outreach. However, FIs noted the desire for more input from the authorities on the vast majority of SARs which are not submitted as a result of a JMLIT operation. The outreach activities undertaken by the FIU seem to have had a limited effect in this regard and the lack of feedback seems to be having a severe adverse impact on the relevance or value of the SARs.

342. Nearly all DNFBPs highlighted the difficulty of filing SARs online. Reforms to this system are long overdue. Non-banks highlighted that the form is not adapted to the context of different reporting entities and is not fit for the purpose. They also consistently raised concerns about other practical limitations including the 80 000 character limit (and how this impeded their ability to provide detailed analysis they had undertaken) and the inability to save or amend historical filings (information is sometimes lost which means that the process of repopulating the form needs to be started again).[35] The UKFIU's view, is that the character limit is ample to detail the suspicion that triggered the report. Nonetheless, the authorities noted plans to reform the SARs regime, including replacing the current IT system, to improve its operation and address some of these issues.

343. Firms also raised concerns about tipping off as a result of DAML requests which can require that funds be frozen for an extended period of time. Although the extended freezing period has benefits for law enforcement, reporting entities noted that it could put them in a difficult position with their customer. Although reporting

35 The UK indicated that it is currently reforming its SARs regime, including replacing the UKFIU's current IT system, to improve its operation and address these issues. However these improvements were not in place at the time of the on-site visit.

entities make every effort to prevent "tipping off", if the freeze extends too long, it may be inevitable.

Table 28. **SARs reporting by sector**

	From Oct 2011 to Sept 2012	From Oct 2012 to Sept 2013	From Oct 2013 to Sept 2014	From Oct 2014 to Sept 2015	From Oct 2015 to Sept 2016	From Oct 2016 to Sept 2017
Financial Institutions						
Asset Management	367	385	456	421	479	531
Banks	218,021	251,336	291,055	318,445	348,688	360,393
Building societies	9,361	10,844	12,834	15,806	15,078	15,778
Other credit institutions	4819	5150	6058	7249	8133	7305
Capital markets	85	63	40	85	77	93
E-money	2,966	5,495	5,585	6,827	14,866	18,411
MSBs	23,419	21,343	14,990	11,120	10,091	16,597
Insurance	1,657	2,254	1,713	1,170	1,058	1,202
Other financial institutions	2566	2844	3457	3391	3739	5571
DNFBPs						
Accountant / tax advisor	5,893	5,428	4,930	4,618	4,254	4,826
Legal practitioners	4367	3935	3617	3832	3452	2712
TCSPs	70	219	177	101	74	63
EABs	145	215	179	355	514	557
Gaming	761	789	1109	1572	2307	2366
HVDs	280	367	331	135	152	214
OTHER						
Not under MLRs	3888	5860	7655	6755	6489	5334
Total	**278,665**	**316,527**	**354,186**	**381,882**	**419,451**	**441,953**

Internal controls and legal/regulatory requirements impending implementation

344. Many of the firms met with had strong internal control and group-wide policies in place and applied the higher UK standard to other firms in the group. Although there have been issues, including with larger financial institutions (for example, Deutsche Bank was fined over GBP 163 million including for failures in internal controls and UK banks have been subject to very large fines by international regulators), there seems to be a positive trend towards stronger internal controls in large banks.

345. Firms engaging in cross-border banking activities continue to face bank secrecy, data privacy or data protection barriers in other jurisdictions that can impede information-sharing related to suspicious transaction or accounts across the enterprise. However, they have generally developed ways to manage group-wide risk. No UK laws appear to impede outbound information related to suspicious transactional or account information, with firms using consent, the public interest derogation, or the exception for managing risks in current data privacy laws to share information outbound from the UK.

Overall conclusions on IO.4

346. **The UK 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 supervised for AML/CFT compliance under the UK regime. The quality of supervision varies among the 25 AML/CFT supervisors which range from large public organisations to small professional bodies.
b) The statutory supervisors (FCA, HMRC and the Gambling Commission) and the largest legal sector supervisor (which supervises around 90% of solicitors in the UK) have a stronger understanding of the ML/TF risks present in the sectors than the other 22 professional bodies that supervise most accountants and the remainder of the legal sector.
c) Each supervisor takes a slightly different approach to risk-based supervision. While positive steps have been taken, there are significant weaknesses in the risk-based approach to supervision among all supervisors, with the exception of the Gambling Commission.
d) Systemic AML/CFT failings identified at some large multinational UK firms over the last decade raises questions, but the assessors recognises that there is an increasing trend in levying penalties for serious failings.
e) For the accountancy and legal sectors, weaknesses in supervision and sanctions are a significant issue which the UK has put steps in place to address. However, these failings have an impact on the preventative measures applied (Chapter 5 on IO.4) and the quality of financial intelligence (section 3.2 on IO.6).
f) Supervisors' outreach activities, and fitness and propriety controls are generally strong.

Recommended Actions

a) The FCA should consider how to ensure appropriate intensity of supervision for all the different categories of its supervisory population from low risk to high risk.
b) HMRC should consider how to ensure appropriate intensity of supervision for all the different categories of its supervisory population from low risk to high risk. HMRC should ensure that it properly takes into account ML/TF when risk rating firms subject to their supervision. The UK should continue its efforts to address the significant deficiencies in supervision by the 22 legal and accountancy sector supervisors through: ensuring consistency in ML/TF risk understanding; taking a risk-based approach to supervision; and ensuring that effective and dissuasive sanctions apply. The UK should

closely monitor the impact of the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) in undertaking this work.

c) All supervisors should continue to ensure, in accordance with the increased trend for levying penalties, that proportionate, dissuasive and effective sanctions are applied for violations of AML/CFT and sanctions obligations.

d) Supervisors should routinely collect statistics and feedback on the impact of supervisory actions. They should introduce systems for maintaining statistics on the numbers and trends of findings to enable them to better target their supervisory activities and outreach, and demonstrate the impact of their supervision on AML/CFT compliance.

e) The FCA should consider the wider use of criminal background checks as part of its processes to ensure that criminals and their associates are prevented from owning or controlling FIs. This would bring them into line with the approach taken by other statutory AML/CFT supervisors (HMRC, Gambling Commission) where such checks are performed routinely in respect of all relevant persons.

f) Supervisors should ensure that their guidance is timely and fit-for-purpose. For example, legal and accountancy supervisors should continue to provide guidance and outreach to their members and seek to ensure the updates to guidance are provided in a timely manner. The FCA should ensure that the guidance it provides meets the needs of the range of firms within the sectors it supervises.

g) Progress plans to extend AML/CFT requirements and related supervision to virtual currency exchange providers.

347. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, R. 26-28, R.34, and R.35.

Immediate Outcome 3 (Supervision)

348. The Financial Conduct Authority (FCA) supervises the majority of financial institutions. Her Majesty's Revenue and Customs (HMRC) supervises some financial institutions (MSBs which are not supervised by FCA) and a number of DNFBPs (HVDs; estate agents; and accountants and TCSPs not supervised by Professional body supervisors or the FCA). The Gambling Commission supervises casinos. There are 22 legal and accounting sector SRB supervisors. For practical reasons, the assessors were not able to interview representatives of all the legal and accounting sector supervisors but have relied on interviews with the largest supervisors as well as a smaller supervisor from Scotland and Northern Ireland, in addition to reviewing other published materials and evidence submitted, to develop a comprehensive overview of the work of the other supervisors.

349. Positive and negative aspects of supervision were weighted most heavily for the banking sector, heavily for important sectors (MSBs, lawyers, accountants,

including when lawyers and accountants are undertaking TCSP activity[36]), moderately heavy for the securities sector, and less heavily for less important sectors (insurance, casinos, EABs, HVDs). This is because of the relative materiality and risk in the UK context of these supervised populations, as explained above in Chapter 1. Also, see Chapter 1 for a description of each supervisor and which entities they are responsible for supervising.

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

350. Licensing, registration and fitness and propriety checks to prevent criminals from entering the market are generally strong and effective in preventing criminals and their associates from entering the market. HMRC, the Gambling Commission and large Professional body supervisors routinely conduct criminal background checks. The FCA, HMRC and the Gambling Commission have dedicated resources to ensuring that unlicensed or unregistered activity is detected in various 'policing the perimeter' activities.

FCA - Financial Institutions

351. Financial institutions are required to be authorised by the FCA or the Prudential Regulation Authority (PRA) in order to perform their services in the UK. The Prudential Regulatory Authority (PRA) is responsible for the prudential supervision of banks, credit unions and insurers, with the FCA being the conduct and AML/CFT supervisor for these sectors. These sectors are described as dual supervised and while applications for authorisation are made to the PRA, there is a process in place whereby all such applications are considered by both the PRA and FCA against their conditions. While the decision to grant or refuse an application is made by the PRA, it can only authorise a firm with the FCA's consent. The FCA's AML/CFT supervisory population also includes "Annex 1" firms which do not undertake activities requiring an authorisation (e.g. advice on capital structures, financial leasing, commercial lending and safe custody). These firms are nevertheless required to register with the FCA.

352. As part of its authorisation process, the FCA applies a number of controls to prevent criminals and their associates from owning or controlling financial institutions. The controls applied include a fitness and propriety (F&P) test which involves consideration of applicants' criminal convictions status. The FCA's pre-approval is also required for senior management functions and beneficial owners at both market entry and on an ongoing basis post authorisation. Where a firm is dual supervised by the PRA and FCA, the same process is applied by the FCA.

353. The FCA screens applicants against internal and external databases (e.g. its Shared Intelligence Service (SIS) which is a mechanism for UK regulatory bodies, designated professional bodies and recognised investment exchanges to collect and share material on individuals and firms). The FCA takes a risk-based approach to carrying out criminal background checks. It does so only in cases where a concern

36 The 2017 NRA highlights that TCSP activity is high-risk when provided by lawyers and accountants. The use of TCSPs outside these sectors continues to be assessed as medium risk for money laundering.

arises around an individual's fitness and propriety. The number of instances where such checks are performed arising in only a small proportion of applications received. This approach differs from other public AML/CFT supervisors, HMRC and the Gambling Commission which routinely perform such checks in respect of all relevant persons.

354. The table below details the number of applications that have been processed by the FCA. While the number of refused applications is low, the number withdrawn represents a more relevant figure as it is the FCA's experience that it is common for applications to be withdrawn where F&P concerns are raised.

Table 29. **FCA authorisation applications**

Result of authorisation request	2012/13	2013/14	2014/15	2015/16	2016/17
Received	1128	1157	1255	1162	1205
Approved	953	996	1159	1364	1047
Withdrawn	159	113	100	124	120
Refused	2	1	2	2	1

Note: Applications received are not necessarily approved, withdrawn or refused in the same financial year. The data in this table is in relation to all FCA regulated firms and thus includes data on firms who are not subject to the MLRs.

355. In tandem with this regime, the FCA also operates a Certifications regime whereby individuals who do not carry out 'Senior Manager Functions', but whose roles have been deemed "capable of causing significant harm to the firm or its customers", are subject to certification. Although pre-approval by the FCA (and PRA where appropriate) is not required, firms are required to certify at least annually that all staff falling within the scope of the Certification Regime are fit and proper.

356. The FCA also has a dedicated team that investigates cases where persons may be providing financial services without the requisite authorisation. Almost all cases identified are fraud related, such as boiler room fraud or unauthorised deposit taking and collective investment schemes. The FCA collaborates with other agencies, such as the City of London Police and the Serious Fraud Office (SFO) to share intelligence on specific cases or typologies involving this type of activity. The FCA's actions range from publishing warning notices and taking down fraudulent websites, to taking criminal or civil action against companies and individuals.

HMRC - MSBs, and DNFPBs (ASPs, EABs, HVDs and TCSPs)

357. As part of its registration process, HMRC applies a number of controls to prevent criminals and their associates from owning or controlling MSBs, ASPs, TCSPs which are not otherwise supervised by the professional body supervisors or the FCA, EABs and HVDs. HMRC's controls include a F&P test which checks whether an applicant has a criminal record. Information is verified against a number of sources including the Police National Computer which contains information on individuals convicted, cautioned or recently arrested.

358. MSB agents are also subject to F&P testing, and there is a legal requirement on MSB principals to check their agents would pass an F&P test. HMRC checks the principal's compliance with their obligations to F&P test MSB agents as part of its supervision of MSBs. HMRC has also started to undertake background checks on MSB

agents to monitor principals' compliance with their F&P obligations and will use this information to inform its risk-based approach to supervision of MSB principals. HMRC and FCA also co-operate to ensure that there is no duplication or gaps in supervision of the MSB sector, different parts of which fall under HMRC and FCA authority respectively.

359. HMRC's F&P regime applies not only at the point of registration but on an ongoing basis post-registration. This is done through retesting which is intelligence and event driven. Where retested persons are found to no longer be F&P, they are deregistered. HMRC monitors the integrity of its registers by actively identifying firms that should be registered but are not, and checking that firms removed from the register are not continuing to trade unsupervised (also see analysis under core issue 3.4 for statistics on registration penalties).

Professional body supervisors - Legal and accountancy sectors

360. The approved professional body accountancy and legal sector supervisors apply a number of controls to prevent criminals and their associates from owning or controlling accountancy and legal practices, including F&P checks and criminal records checks. In addition to the checks performed at market entry, ongoing compliance with these requirements is monitored by the professional body supervisors. Where an applicant is from another jurisdiction, the relevant professional body supervisor seeks a certificate of good standing from the other jurisdiction's supervisor.

361. A positive feature that helps to prevent criminals from owning or controlling legal and accountancy practices is that some supervisors require a firm's ownership to rest entirely with a practicing member. Other supervisors require that at least one of the principals be a practicing member who is thus subject to F&P checks.

362. Some legal sector supervisors routinely conduct criminal background checks of their members through the Disclosure and Barring Service.[37] However, some accountancy sector supervisors do not carry out criminal background checks and rely on their individual members to declare convictions as part of application process to become a member and report any subsequent convictions to the professional body.

Gambling Commission – Casinos

363. The Gambling Commission applies controls at market entry to prevent criminals from owning or controlling gambling operators. It issues operating licences under which its F&P test is applied (including consideration of previous criminal convictions) to owners and senior managers, and to personal licences for employees involved in gaming and handling cash. The Gambling Commission performs such checks using the Disclosure and Barring Service to establish if an individual has a criminal record. Where an applicant is from another jurisdiction, the Gambling Commission requires that an overseas police report is provided by the applicant.

37 The Disclosure and Barring Service is a non-departmental public body of the Home Office of the United Kingdom. It helps employers make safer recruitment decisions by processing requests for criminal records checks and conducting police records checks.

Table 30. **Gambling Commission – License refusals and withdrawals**

	2013	2014	2015	2016
Operator License Applications:				
Received	5	128**	18	23
Approved	2	128**	17	19
Refused	0	0	2	0
Withdrawn *	3	5	13	4
Operator and Personal Licences refused/rejected for AML/CFT reasons***				
Refused	2	4	2	0
Withdrawn	4	11	15	2

Note: *The number of licence refusals is low because the Gambling Commission always issues 'minded to refuse' letters to applicants which often results in their withdrawal from the process before the licence is refused. **The increase in operator license application in 2014 is due to the introduction of the Gambling, License and Advertising Act 2014 which requires all remote gambling operators to hold a licence from the Commission if their gambling facilities are used in Britain.*** These figures include individuals holding management functions. Reasons for refusal include: failing the Disclosure and Barring check; lack of competence in industry; not fit and proper; not satisfied with source of funds; and not satisfied with ownership of company.

364. The Gambling Commission monitors ongoing compliance with its F&P test through a number of triggers such as changes in ownership, variation to a licence and its supervision work. Personal licences are reviewed every 5 years. The Gambling Commission takes action where it identifies persons operating who do not hold a licence. In 2016, it investigated 24 unlicensed remote casinos which were identified by a combination of ongoing compliance activity and intelligence reports from the public and law enforcement. This resulted in action being taken including issuing cease and desist letters to these operators and notifying other regulators to frustrate the unlicensed activity.

Supervisors' understanding and identification of ML/TF risks

365. Supervisors have a good understanding of the inherent risks facing the sectors that they supervise which is consistent with the NRA findings. All supervisors contributed to the 2015 and 2017 NRAs and (as required through the MLRs) take these into account when formulating their own risk assessments. While FCA and HMRC have taken some positive actions, there are weaknesses in their understanding of firm-specific risks across their large supervisory populations. There are also inconsistencies in risk understanding among the professional body supervisors.

FCA - Financial Institutions

366. The FCA has a good understanding of the inherent ML/TF risks faced by its supervisory population. The FCA builds its understanding of ML/TF through a number of sources such as its supervisory activities, the collection of a data return, and engagement with policy and law enforcement officials regarding emerging risks. The FCA contributed to the UK's 2015 and 2017 NRAs with respect to the financial sector risk assessment and uses the NRA to inform its understanding of wider risks. While the FCA shares the NCA view of ML/TF for the wholesale markets sector, there would be appear to be gaps in its risk understanding for the sector with respect to TF and bribery and corruption risks, which it is working to fill.

367. The FCA's risk model is driven by the inherent risk of ML/TF. The FCA views retail banking, wealth management, private banking, wholesale banking and capital markets as the sectors representing the highest ML/TF risk, retail lending and E-money as medium ML/TF risk, and pension & retirement income, life insurance and retail investments as lower ML/TF risk. This understanding is consistent with the NRA.

368. The FCA continues to develop its risk understanding. In 2016, it issued an annual data return to be completed by approximately 2 000 firms. At the time of the onsite, the majority of these firms had submitted a completed data return. The data collected through this exercise includes information and statistics on firms' customer and geographic exposure, data on SARs and information on firms' AML/CFT control frameworks. The integration of this data will provide a greater sophistication and a more quantitative approach to the FCA's assessment of risk across relevant risk factors at the individual level. While this is a positive initiative that will assist the FCA in its identification and understanding of risk, the FCA could consider extending the application of the data return to a broader range of firms to complete the data return to its entire AML/CFT supervisory population, but vary the regularity of returns depending on the risks identified.

HMRC - MSBs and DNFPBs (ASPs, EABs, HVDs and TCSPs)

369. HMRC has a good understanding of inherent ML/TF risks in relation to the sectors that it supervises, and contributed to both the 2015 and 2017 NRAs. It uses a number of sources to build its understanding of risk, including the NRA, information from other supervisors, external LEAs and information from its own tax business stream. HMRC's risk rating on a sectoral basis is aligned to the risk rating of the sectors in the NRA, with MSBs, TCSPs and ASPs being seen as higher risk, and the EAB and HVD sectors being seen as lower risk. HMRC looks at the nature and activities of the individual businesses it supervises in the context of these overall risks to identify its highest risk businesses. HMRC has also developed 97 risk rules under which individual firms are assigned an individual risk score, which is used as part of its wider risk assessment process. The 97 risk rules are a relatively new initiative. HMRC advised that it intended to cover its total supervisory population of over 27 000 firms by June 2018.

370. The introduction of the risk matrix to assign individual firms a risk score has the potential to improve HMRC's understanding and identification of risk across the firms and sectors it supervises. However, the majority of the rules within this risk matrix are not aligned to inherent ML/TF risk factors or variables and are more aligned to compliance risk and tax compliance risk in particular. Although using information more aligned to assessing risk from a tax perspective can be helpful to feed into the overall risk profile of an individual firm, it appeared that these factors carried too much weight compared to other ML/TF risk factors. .

Professional body supervisors - Legal and accountancy sectors

371. The level of understanding of ML/TF risk varies across the legal and accountancy professional body supervisors. Some supervisors had a strong understanding of ML/TF risk and have risk models in place under which relevant inherent ML/TF risk factors are considered (e.g. the supervisor of all solicitors in

England and Wales). Other legal sector supervisors viewed smaller practices as representing the highest risk as they tend to have fewer resources available to implement strong AML/CFT control frameworks. Some accountancy supervisors had a more limited understanding of ML/TF risk, focusing less on ML/TF-relevant risk factors and more on either the size of the practice or types of services offered or whether client money was being handled.

372. The 2015 NRA highlighted the issue of inconsistent supervision of the legal and accountancy sector. The UK response was to establish an oversight body for these sectors—the Office of Professional Body AML Supervision (OPBAS) as well as to encourage the supervisors to address the findings by developing consistent risk methodology in their affinity groups, to deepen links with law enforcement (especially the NCA), and to reinvigorate the relationship between supervisors, law enforcement and policy makers through the Money Laundering Advisory Committee and the AML Supervisors Forum. One area of inconsistency which led to the UK government establishing OPBAS was concern about the application of a risk-based approach to supervision in the legal and accountancy sectors. OPBAS has highlighted that improving consistency in risk understanding is one of its key areas of focus.

Gambling Commission – Casinos

373. The Gambling Commission has a good understanding of ML/TF risks in the gambling sector and contributed to the 2015 and 2017 NRAs. It assesses risk in a number of ways and looks at risk in terms of the likelihood or probability and impact of gambling services being used for ML/TF. The Gambling Commission considers relevant risk factors such as customer risk, jurisdiction or geographic risk, product risk and means of payment risk. It assesses risk at a sectoral level and then at the individual operator level and also considers the quality or effectiveness of the controls that operators have in place to mitigate risk.

374. The 2015 and 2017 NRAs concluded that gambling as a whole posed a low ML/TF risk. The Gambling Commission has identified that, relatively speaking, the land based casino sector has a higher risk relative to other gambling sectors due to the volumes of cash, the higher inherent risk in the products and services being offered, the money services provided to customers and, in some instances, poor quality of controls. It also views certain products as being higher risk than others (e.g. peer-to-peer gaming such as on-line poker) and considers the remote sector as a whole as having a higher risk in light of the products provided and the fact that customers are not physically present for identification.

Risk-based supervision of compliance with AML/CFT requirements

375. There is an uneven level of sophistication in the development of risk-based models for supervision among the public sector and professional body supervisors. While the FCA and HMRC follow a RBA, their models require substantial improvements based on the breadth of firms in their supervisory population. There is concern that professional body supervisors base their supervisory attention on firm size, rather than a more nuanced understanding of the sectoral risks in line with the NRA or other risk assessments.

FCA - Financial Institutions

376. The FCA has a risk based approach to supervision of FIs. The FCA has approximately 700 sector supervisors who are responsible for assessing firms' overall AML/CFT compliance as part of their broader supervisory functions and undertake less complex AML/CFT work. The sector supervisors are supported by a specialist Financial Crime department of approximately 50 staff who lead on more complex ML/TF issues. The FCA's supervision is divided into three tiers (see the diagram below)

Table 31. **FCA's 3 tiered supervisory model**

	Relevant supervisory population	Inspection cycle	Staff involved in inspection	Length of inspection
Systematic Anti Money Laundering Programme (SAMLP)	14 largest retail and investment banks operating in the UK	Every 4 years	4-5 people.	4-6 months
Proactive Anti Money Laundering Programme (PAMLP)	156 firms from high risk sectors which are smaller than those under the SAMLP	Every 4 years	2-3 people	2-4 days
Risk Assurance Review	19,500 in the FCA's AML/CFT supervisory population	The FCA undertakes a review of a sample of 100 firms each year with 60 reviews by way of onsite inspection and 40 desk based reviews (20 of which include a teleconference). The selection process is 80% random sample and 20% intelligence-led.		

377. The FCA also has the option to place firms under "Enhanced Supervision" where serious failing in a firm's AML/CFT programme have been identified. This measure has been applied to two major banks that have continuous, intensive contact with a dedicated specialist AML team. This is most likely to occur in relation to SAMLP firms and involves a more robust and intensive supervisory approach. The FCA completes 100 onsite AML/CFT inspections each year under the three tiers.

Table 32**. FCA on-site and desk-based inspections**

Number of:	2013/14	2014/15	2015/16	2016/17
Desk based reviews (total)	**96**	**56**	**134**	**154**
Compliant	47	32	77	73
Partially compliant	25	9	45	74
Non-compliant	24	15	6	7
On-site inspections (total)	**33**	**53**	**116**	**100**
Compliant	12	9	10	27
Partially Compliant	17	27	33	27
Non-compliant	4	5	16	4
Awaiting decision*	5	9	57	42
Total number of firms inspected	**129**	**109**	**250**	**254**

Note: The 'awaiting decision' category covers cases where an assessment or determination of the level compliance is not made in the year the inspection occurred (e.g., where a skilled person is appointed).

378. The FCA's AML/CFT supervisory activity is driven by ML/TF risk. However, the FCA should consider the appropriateness of applying a four year cycle to its higher risk firms under the SAMLP and PAMLP, and whether a more frequent cycle is

merited. Only 60 firms are inspected as part of the Risk Assurance Review which covers 99% of the FCA's AML/CFT supervisory population and a wide spectrum of activity and ML/TF risk. There is also concern about the inadequate level of supervisory coverage across firms not subject to engagement cycles. The FCA should consider how to ensure appropriate intensity of supervision for all the different categories of its supervisory population from low risk to high risk.

379. The introduction of the Annual Data Return is a positive feature. Extending the application of the data return to a broader range of firms could assist in the prioritisation and selection of firms for supervisory action.

6

HMRC - MSBs and DNFPBs (ASPs, EABs, HVDs & TCSPs)

380. HMRC takes a risk-based approach to the supervision of the 27 000 firms in its AML/CFT supervisory population using a combination of both on-site inspection and desk-based reviews. HMRC's AML Supervision team (AMLS) comprises 197 full-time equivalent staff. Of these, 130 are involved in compliance work of which around 80 conduct onsite inspections. HMRC develops annual 'Tactical Plans' for each sector it supervises, based on its understanding of risk. HMRC does not apply regular inspection cycles through which it routinely visits firms to carry out inspections.

381. HMRC's supervisory activity covers all of the sectors under its AML/CFT remit. However, there are concerns that some higher risk firms may never be inspected and the appropriate level of resources required for effective supervision may not be obtained over the medium to long-term.

382. In view of the large supervisory population and diverse range of services supervised, HMRC should consider how to ensure appropriate intensity of supervision for all the different categories of its supervisory population from low risk to high risk.

DNFPBs – Legal and accountancy professional body supervisors

383. Deficiencies in the risk understanding among smaller legal and accountancy supervisors have impacted their ability to apply a risk-based approach to supervision. Generally, legal and accountancy supervisors do apply an RBA to their supervision, applying both desk-based and on-site reviews. The scope of the reviews are generally broader than AML/CFT. Some supervisors' approaches do not involve engagement cycles and use thematic reviews for higher risk entities and selection of lower risk entities reviewed as part of a random selection. Other supervisors tend to concentrate mainly on size by dividing their populations by "Gross Fee income" as a metric to allocate firms to each cycle, with firms with lower gross fee income subject to an eight year desk based review cycle and firms with higher income subject to either a four or two year onsite review cycle (see table below). There is a concern regarding this approach as it is focusing on one possible risk factor and is not in accordance with the 2017 NRA which suggests that smaller firms providing a range of services are at high risk.[38] Supervisors should ensure that their approaches to risk based supervision are appropriately aligned to any improvements made to their risk model.

38 NRA 2017, p.44.

Table 33. **Example of an accountancy supervisors' engagement cycle**

Gross fee income:	Percentage of overall supervisory population		
	2014	2015	2016
< GBP 75k (eight-year cycle – desk based)	54	51	54
GBP 75k - 300k (eight-year cycle – desk based)	24	25	24
GBP 300k - 1m (eight-year cycle – onsite)	14	15	14
GBP 1m - 10m (four-year cycle – onsite)	7	8	7
> GBP 10m (two-year cycle – onsite)	1	1	1

DNFPBs – The Gambling Commission

384. The Gambling Commission takes a risk-based approach to supervision of the gambling sector, applying a combination of onsite and desk based reviews. Pursuant to its risk model, the Gambling Commission has rated the 40 largest operators which offer the broadest range of gambling services and have a gross gambling yield of over GBP 25 million as being the highest risk and categorizes these as High Impact Operators. These 40 High Impact Operators represent 80% of the gambling activity in the sector and are subject to a regular inspection cycle (every two to three years although given this is based on risk, higher risk casino operators will have almost continuous engagement). For the smaller operators, the Gambling Commission's approach focuses on reviewing the adequacy of controls at the licencing stage and monitoring such firms post-licencing through desk based reviews. The Gambling Commission also conducts thematic reviews involving on-site visits which also cover the smaller operators. In addition, as part of its risk-based approach, the Gambling Commission monitors adverse media intelligence and law enforcement sources, and customer complaints information, all of which may trigger a supervisory action for any gambling operator.

Remedial actions and effective, proportionate, and dissuasive sanctions

385. Supervisors use a range of remedial actions to encourage compliance. The three statutory supervisors, FCA, HMRC and the Gambling Commission, have demonstrated their ability to sanction individuals in addition to corporations.

FCA - Financial Institutions

386. The FCA has a broad range of remedial actions and sanctions which are applied against both firms and individuals. The types of remedial actions include:

a) the use of action plans
b) attestations by firms that required improvements have been completed, and
c) early interventions using power under s.166 of the FSMA to require a firm to engage the services of Skilled Person to carry out a review and provide a report to the FCA.

387. The types of sanctions include:

a) restricting or suspending a firm's business or licence on either a voluntary basis by the firm or through the use of the FCA's powers to require the business or licence restriction
b) prohibitions, banning individuals from an industry

c) fines and disgorgement, and
d) public censures.

388. The FCA also monitors completion of remedial actions when revisiting a firm as part of its SAMLP and PAMLP inspection cycles. The FCA determines which approach to take based on the circumstances of each case. The FCA can seek to impose sanctions on FIs under its civil administrative sanctions regime or by way of criminal prosecutions.

389. When deciding whether to pursue enforcement action and when determining the appropriate remedy or sanction to impose, the FCA considers a number of factors including the number and duration of breaches, and their impact or harm caused. The FCA also considers any relevant aggravating or mitigating factors. Under the FCA's civil sanctions regime, an early settlement discount of 30% may be applied to the fine where the subject of the case co-operates. The table below provides a summary of the remedial actions and sanctions applied by the FCA since 2012.

Table 34. **FCA AML Enforcement Data**

	12/13*	13/14	14/15	15/16	16/17	Total
Fines	5	4	1	1	3	14
Section 166 FSMA	11	14	6	6	5	42
Attestations	15 between June 2013 and June 2016					15
Business restrictions	12 between 2012-14			2	6	20
Early Interventions	-	4	8	8	7	27

Note: This table includes both formal and informal actions taken. There was limited information from 2012/2013.

390. An important aspect of the enforcement process is the public notice which includes the name of the subject of the action, details from the case and the sanction imposed. This has a deterrent effect on both the individual firm and the wider supervised sector. Providing such information on the breaches is also helpful in signalling to FIs the FCA's expectations in terms of compliance. The following case study provides a good example of the FCA imposing dissuasive sanction on a firm.

Box 27. **Example of FCA intervention – financial penalty – Deutsche Bank**

In January 2017, the FCA fined Deutsche Bank GBP 163 million for serious AML controls failings. During the period January 2012 to December 2015 the firm failed to maintain an adequate AML control framework. This is the largest financial penalty imposed to date by the FCA for AML failings. The bank exposed the UK financial system to the risks of financial crime by failing to properly oversee the formation of new customer relationships and the booking of global business in the UK. As a consequence of its inadequate AML control framework, the bank was used to transfer approximately USD 10 billion of unknown origin from Russia to offshore bank accounts in a manner that is highly suggestive of financial crime (mirror trading). In doing so, the bank breached Principle 3 (taking

reasonable steps to organise its affairs responsibly and effectively with adequate risk management systems) of the FCA's Principles for Businesses and Senior Management Arrangements, Systems and Controls (SYSC) and rules 6.1.1 R and 6.3.1 R.

391. Since 2012, the FCA has concluded 14 AML/CFT enforcement cases relating to 10 firms and four individuals with penalties imposed totalling GBP 343 346 924 and GBP 92 700 respectively. Imposing sanctions on individuals is a positive feature which has acted as a clear deterrent for firms' employees.

392. The FCA should consider increasing its AML/CFT enforcement activity to bolster the deterrent effect of its sanctions. The FCA's enforcement division currently has 75 cases in its pipeline of AML/CFT cases (40 relating to firms and 35 relating to individuals). For those cases ultimately resulting in sanctions, the FCA should also consider the use of other sanctions (e.g. business restrictions).

HMRC - MSBs and DNFPBs (ASPs, EABs, HVDs and TCSPs)

393. HMRC has a range of remedial actions and sanctions available which it can apply to businesses in all the sectors that it supervises. The remedial actions and sanctions used by HMRC include:

a) advice letters and warning letters
b) remedial action plans
c) censuring statements
d) management suspension or prohibition
e) registration suspension or prohibition
f) imposing civil financial penalties, and
g) criminal prosecution for breaches of the MLR.

394. HMRC considers which approach to take based on the facts of each case. Where HMRC determines that a financial penalty is the appropriate sanction, it considers a number of factors to ensure penalties are proportionate and dissuasive with regard to the risk of ML/TF posed. These factors include the size of the business and the nature and severity of the breaches identified. The tables below provide a summary of HMRC sanctions across each of the sectors it supervises. There has been a noticeable increase in compliance penalties in 2016/2017 in relation to MSBs, EABs and HVDs due to an increased focus on supervision and enforcement in relation to these sectors.

Table 35. **HMRC remedial and enforcement actions**

Money Service Businesses (total supervisory population of 1 890)				
	2014/15	**2015/16**	**2016/17**	**2017/18**
Compliance penalties	10	0	12	20
Value of highest penalty	GBP 156 350	0	GBP 18 029	GBP 796 500
Warning letters	69	7	11	Data not yet available
Advice letters	37	14	11	
Remedial action plan issued	38	20	34	

Money Service Businesses (total supervisory population of 1 890)				
Accountants (total supervisory population of 13 627)				
	2014/15	**2015/16**	**2016/17**	**2017/18**
Warnings	28	80	45	46
Action plan	28	171	147	Data not yet available
Compliance penalties	A total of 52 compliance fines of up to GBP 15 000 were applied between 2013/14 and 2015/16.			Data not yet available
Estate Agent Businesses (total supervisory population of 10 236)				
	2014/15	**2015/16**	**2016/17**	**2017/18**
Compliance penalties	3	2	15	9
Value of highest penalty	GBP 15 000	GBP 11 250	GBP 360 000	GBP 99 000
Warning letters	211	43	21	47
Advice letters	41	108	11	28
Remedial action plan issued	138	28	67	Data not yet available
High-Value Goods Dealers (total supervisory population of 679)				
	2014/15	2015/16	2016/17	**2017/18**
Compliance penalties	18	11	16	19
Value of highest penalty	GBP 77 758	GBP 25 000	GBP 15 711	GBP 39 120
Warning letters	206	100	16	62
Advice letters	73	38	0	50
Remedial action plan issued	138	26	67	Data not yet available
Trust and Company Service Providers (total supervisory population of 1 960)				
	2014/15	2015/16	2016/17	2017/18
Warnings	35	35	17	37
Action plan	35	84	34	Data not yet available
Compliance penalties	A total of 12 compliance penalties were imposed over that period of up to GBP 37 500.			

395. HMRC also pursues enforcement action in relation to individuals. A recent case study involving the prosecution of an individual within an MSB highlights HMRC's willingness to apply sanctions and escalate the application of its sanctions in circumstances where repeat non-compliance is identified. Until June 2017, HMRC was unable to publicise the sanctions it has imposed which has impacted on the effectiveness and dissuasiveness of its sanctions. As a result of this, some firms noted that they have little information on HMRC sanctions and would welcome more detail to help inform their understanding of HMRC's expectations. Since June 2017, HMRC has been required to publish details on their penalties.

Box 28. **Example of a HMRC intervention – jailing an MSB owner for repeated AML failures**

An MSB owner was jailed for 12 months for failing to comply with AML regulations. The owner failed to carry out the legal checks required under the MLRs before transferring up to GBP 400 000 of his clients' money to India. Despite being reminded of his obligations during visits from HMRC, he did not verify the identity of all his customers, failed to keep supporting documentation and neglected to train his staff to spot suspicious activity. He was arrested by HMRC officers and pleaded guilty in September 2014 to four charges of failing to comply with the MLRs resulting in a 12 month prison term.

Professional body supervisors - Legal and accountancy sectors

396. Legal and accountancy supervisors have a range of remedial actions and sanctions available to them which are applied in practice including:

a) requiring the firm/practitioner to commit to an agreed action plan
b) expelling firms from membership
c) removing professional accreditation
d) applying fines
e) issuing reprimands, and
f) imposing conditions on members.

397. The table below provides information on the supervisors' application of remedial actions and sanctions since 2013.

Table 36. **Professional body supervisors remedial and enforcement actions for AML-only or AML-related breaches**

Accountancy sector	2013/14	2014/15	2015/6	2017/8	Total
Expulsion/Withdrawal of membership	31	13	19	23	86
Suspension	3	1	2	3	9
Fine	50	33	14	35	97
Reprimand	62	51	41	28	182
Undertaking/condition	46	44	13	70	173
Warning	220	298	238	205	961
Action Plan	272	483	670	582	2007
Legal Sector*	**2013/14**	**2014/15**	**2015/16**	**2016/17**	**Total**
Expulsion/Withdrawal of membership	65	32	7	6	110
Suspension	26	1	8	4	39
Fine	61	12	3	4	80
Reprimand	29	6	0	3	38
Undertaking/condition	8	27	3	3	41

Note: This table brings together the data supplied by accountancy and legal supervisors on similar, but not identical, enforcement actions/programmes. *The data for 2015/16 and 2016/17 only includes AML-only breaches whereas the 2013/14 and 2014/15 data included breaches which included AML but did not relate exclusively to AML.

398. A number of AML/CFT related fines have been applied to members of the legal and accountancy sectors. Those fines have not exceeded GBP 85 000 and GBP 15 000 respectively. One reason for establishing OPBAS was to address the application of proportionate and dissuasive sanctions to these sectors.

399. Since the MLRs 2017 came into force, legal and accountancy supervisors have had the power to refer cases to the FCA or HMRC where unlimited sanctions can be applied under their sanctions regimes. HMRC is currently in discussions with the legal and accountancy supervisors with the aim of putting in place an MOU to provide a mechanism for such referrals. Some supervisors see the MOU as being a key element to have in place before any referrals can be made.

400. The main legal sector supervisor also mentioned the need for greater independence in applying sanctions in lawyer-owned law firms. Currently, unlimited fines can only be imposed on lawyer-owned firms if the case is referred to the Solicitors Disciplinary Tribunal.

Gambling Commission – Casinos

401. The Gambling Commission has a range of remedial actions and sanctions which are applied in practice. These include:

a) issuing a warning to a licence holder
b) attaching an additional condition to a licence
c) removing or amending a condition to a licence
d) suspending or revoking a licence
e) imposing a financial penalty, and
f) publishing the outcome of an enforcement action.

Table 37. **Gambling Commission's use of remedial actions in relation to AML-breaches**

	2013	2014	2015	2016
AML-specific licence conditions attached to a casino operator's licence		0	1	1
AML-specific warnings issued to a casino operator	1	0	1	1
AML-specific compliance failings resulting in voluntary settlements	2	1*	2**	4***

Note: * GBP 24 000 to defray the Commission's costs. ** GBP 845 000 - GBP 950 000. *** GBP 280 000 - GBP 846 000.

402. As well, the Gambling Commission can: issue informal warnings; engage in voluntary settlements with operators; and divest operators of any monies from illicit activity (see case study below).

Box 29. **Example of remedial action taken by the Gambling Commission**[39]

Systemic senior management failure to protect consumers and prevent money laundering resulted in a gambling business being required to pay a penalty of at least GBP 6.2m (GBP 5m for breaching regulations and the divestiture of GBP 1.2m in profit).The Gambling Commission investigation revealed that between November 2014 and August 2016 the business breached anti-money laundering and social responsibility regulations.

Senior management of the business failed to mitigate risks and have sufficient numbers of staff to ensure their anti-money laundering and social responsibility processes were effective. This resulted in ten customers being allowed to deposit large sums of money linked to criminal offences which resulted in gains of around GBP 1.2 million for the business. The business did not adequately seek information about the source of funds.

Impact of supervisory actions on compliance

403. While supervisors have observed that firms' AML/CFT compliance systems are maturing as a result of their supervision, it was difficult to assess this across all sectors without an understanding of supervisory findings over time. The introduction of the Senior Management and Certification regime has had a positive impact on bringing attention to AML/CFT requirements at the highest levels.

FCA - Financial Institutions

404. The FCA notes that its recent supervisory work has shown some encouraging signs. For example, some major banks have put in place significant remediation programmes and other major firms are becoming more innovative in their approach to AML/CFT compliance. However, the FCA does not collect data on numbers of findings from its supervisory activities. Consequently, it was unable to provide any statistics demonstrating that its supervision has had a positive effect on firms' compliance (e.g. through a reduction in the number of inspections findings over time).

405. However, the FCA confirmed that it has seen a change in the nature of findings over time. The FCA reports that inspection findings are now generally more in the space of improvement, refinement or enhancement to controls (rather than significant weaknesses or the absence of key controls, as was being observed by the FCA a number of years previously). Nevertheless, in the absence of statistics on the numbers of findings, or trends in findings, it is difficult to assess the extent of the impact of the FCA's supervision on FIs compliance with AML/CFT requirements.

39. www.gamblingcommission.gov.uk/news-action-and-statistics/news/2018/William-Hill-to-pay-6.2m-penalty-package.aspx

406. The FCA has also observed that firms have conducted gap analyses between their own systems and: (a) the FCA guidance; and (b) issues publicly identified in enforcement actions, to implement improvements to their AML/CFT control frameworks.

407. The FCA has designated the Money Laundering Reporting Officer (MLRO) role as a senior management function under its Senior Management and Certification regime. This recognises the importance of a vetted and competent individual being accountable for firms' AML/CFT compliance. In addition, the FCA has introduced a prescribed responsibility for financial crime to ensure that overall responsibility for the firm's financial crime policies and procedures is discharged by an individual with sufficient seniority to ensure that the firm as a whole is meeting all of its financial crime obligations, including AML/CFT. The FCA believes that these measures should lead to a clearer focus on AML/CFT issues and improved support from firms for their financial crime functions and MLROs. During the onsite visit, FIs said that these measures have had a positive effect in terms of ensuring increased accountability and buy-in at senior management level across firms, and recognising the importance of strong AML/CFT frameworks within their businesses.

HMRC - MSBs and DNFPBs (ASPs, EABs, HVDs and TCSPs)

408. HMRC provided data to demonstrate the effect of its supervision on compliance at the individual firm level. The tables below show that, over time, the number of breaches identified at the first inspection visit decreased by the subsequent visit. This illustrates that the HMRC's remedial actions and sanctions are having a positive impact on the individual firms it has inspected.

Table 38 **Impact of HMRC inspections on firms' compliance (2007 – 2017)**

Average number of breaches at 1st visit	Average number of breaches at subsequent visit	Percentage reduction in breaches
Money Service Businesses		
2.32	0.82	65%
Accountants		
3.41	0.29	91%
Real Estate Agents		
4.50	1.73	62%
High-Value Goods Dealers		
2.82	0.95	66%
Trust and Company Service Providers		
3.64	0.56	85%

409. HMRC believes that its guidance and outreach is also having a positive impact on the wider supervisory population. During inspections, HMRC has observed instances of firms proactively complying with the expectations set out in its published guidance. The assessors also viewed numerous HMRC case studies that demonstrated compliance with the UK's AML/CFT regime, including firms that reference the Joint Money Laundering Steering Group Guidance (JMLSG) and FATF guidance to achieve this.

410. Since introducing the requirement for HVDs to register with HMRC, the number of firms has decreased steadily. Since 2014, the sector has shrunk from over

1 200 firms to under 700. As well, some firms now operate strict no cash policies to ensure they are not required to register and put in place AML/CFT control frameworks. HMRC views this as a positive impact which has reduced the level of risk in the sector.

Professional body supervisors - Legal and accountancy sectors

411. Legal and accountancy sector supervisors see their supervisory actions as having a positive impact on members' compliance with AML/CFT requirements. While supervisors do not have any statistics to demonstrate that the number of findings during onsite reviews is reducing over time, they suggested that incidences of repeat breaches are rare. Supervisors have also observed that, over time, there has been a change in the nature of issues identified. In recent times, onsite reviews have detected more minor issues than before, as members' awareness and understanding of AML/CFT obligations has matured. However, without statistics on the numbers of findings and related trends, it is difficult to assess the impact of supervision on accountants' and lawyers' compliance with AML/CFT requirements, particularly given the inconsistencies which exist in the supervisory regime for these sectors.

Gambling Commission – Casinos

412. The Gambling Commission has observed some improvements across the sector which can be attributed to its supervisory work. Although it does not have any statistical evidence to demonstrate improved compliance in the sector, it has seen instances through its inspection activity of firms being more proactive in implementing improved controls on the back of the publication of enforcement settlements and the sharing of good practices through the workshops held by the Gambling Commission for the sector. The Gambling Commission has also seen some signs that a licence condition imposed on operators in 2016 is having a positive impact. This condition requires operators to have appropriate risk assessments in place that inform their policies, and procedures that are effective, and which must be revised regularly, including to ensure that they remain effective.

Promoting a clear understanding of AML/CFT obligations and ML/TF risks

413. All supervisors undertake a range of outreach activities with the sectors that they supervise. These include issuing guidance which is often authored jointly with the private sector, such as the Joint Money Laundering Steering Group Guidance (JMLSG Guidance), training and other engagement activities.

FCA - Financial Institutions

414. The FCA provides advice to FIs through its published guidance for the sector and other papers such as its thematic reviews. It also undertakes outreach work. The FCA has published guidance on financial crime (Financial Crime: A Guide for Firms, July 2016) which smaller firms in particular find to be a useful source of AML/CFT guidance.

415. The Joint Money Laundering Steering Group also provides comprehensive guidance on AML/CFT for financial institutions, with sector-specific guidance covering 24 different sub-sectors. The FCA contribute to HMT's review and approval of this guidance. However, there are challenges in issuing guidance that is applicable

across a variety of businesses even in the same sector. For example, some firms noted that the FCA guidance concerning the level of senior management sign-off for PEPs is challenging for very large firms with a high volume of PEP customers.

416. As AML/CFT measures become more sophisticated, there appears to be a need for a more tailored or targeted approach to guidance taking into account the significant variation in terms of the scale and complexity of firms within the FCA's AML/CFT supervisory population. Consideration should be given as to whether specific sector guidance should be introduced for lower risk sectors and sectors with smaller firms. Given that the FCA has less interaction with such firms, this would also provide an opportunity to communicate its expectations.

417. The FCA website contains Financial Crime specific pages which are regularly updated and contain more detailed information on ML/TF. The FCA also undertakes other forms of outreach including industry webinars and sector-specific presentations of thematic review findings. It also undertakes large financial crime conferences on a biennial basis which are attended by senior management and practitioners and MLROs from regulated firms. The FCA published speeches from the event on its website and there was wide coverage in the media. The conference attracted 25 587 page views between November 2016 and January 2017. In addition, the FCA regularly attends and presents at external speaking events on AML/CFT.

418. The FCA has convened and run an MLRO risk and policy forum quarterly since 2011. This is attended by MLROs from the largest retail and investment banks (SAMLP firms). The forum covers a number of topics including sharing of best practice on risk management, the findings from FCA thematic reviews and new guidance. The FCA also uses its Regulation Round Up monthly publication, which is emailed to 60 025 firms, to highlight significant AML case outcomes, policy statements and guidance changes.

HMRC - MSBs and DNFPBs (ASPs, EABs, HVDs and TCSPs)

419. HMRC undertakes various forms of outreach aimed at promoting a clear understanding of AML/CFT obligations and ML/TF risks. HMRC has a dedicated team within AMLS responsible for raising awareness and increasing compliance with AML/CFT requirements. HMRC has produced guidance for each sector it supervises. At the time of the onsite, updated guidance had been issued for all sectors to reflect the 2017 MLRs, with the exception of the guidance for EABs which was issued in draft form and awaiting approval.

420. HMRC has rolled out e-learning tools for its supervised sectors. It has also reached out directly to individual firms by issuing emails to its supervisory population and providing information to help businesses comply with their obligations. For example, in July 2017, emails were issued to the MSBs on the introduction of MLR 2017 to advise them of the main changes relevant to MSBs. HMRC has a dedicated email address for businesses to contact with any queries. Each month AMLS generates a 'Voice of the Customer' report to highlight any key issues or recurring themes so that these can be addressed appropriately. Where HMRC's analysis identifies common queries or recurring themes it will respond accordingly (e.g. by improving its guidance). HMRC's other forms of outreach include the publication of a thematic review on the MSB sector in 2018, hosting webinars targeted at individual sectors and presenting at speaking events.

Professional body supervisors - Legal and accountancy sectors

421. Legal and accountancy supervisors undertake a range of outreach activities to promote an understanding of ML/TF risk and AML/CFT obligations. The activities include: publishing HMT-approved guidance and other topic-specific guidance documents; publishing disciplinary actions and best practices cases; AML/CFT seminars and workshops; helplines/hotlines on AML/CFT and wider compliance issues; a compulsory professional development course including an AML/CFT dimension; and dedicated AML web-pages on supervisors' web-sites. Some members of the sector have welcomed the guidance for their sectors, but feel that updated guidance following the introduction of the MLRs in 2017 ((which was published in final form in early March 2018) should have been in place much sooner.

Gambling Commission – Casinos

422. The Gambling Commission undertakes a range of outreach measures to promote an understanding of ML/TF risk and AML/CFT obligations. These measures include: publishing guidance; issuing public statements on the sanctions it applies; publishing and distributing a fortnightly e-bulletin; dedicated AML/CFT pages on its website, hosting a Raising Standards conference in 2016 and 2017 with a focus on AML/CFT; twice yearly AML forum meetings for all nominated officers in the casino sector; and regular meeting with the National Casino Forum (a trade association comprising every land-based casino in the UK), the Remote Gambling Association (remote casinos).

Overall conclusions on IO.3

423. **The UK 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) The UK is a global leader in promoting corporate transparency and goes beyond the FATF Recommendations in this area in some respects. It promotes the use of public registers of beneficial ownership (BO)[40] in a variety of fora and has led by example in establishing a public registry of BO information and a register of trusts with tax consequences in the UK.

b) The UK has a good understanding of the ML/TF risks posed by legal persons and arrangements which is shared by relevant LEAs and policy bodies and was reflected in the 2017 NRA. UK companies, Limited Liability Partnerships and Scottish Limited Partnerships are deemed as high risk. The risks posed by UK legal arrangements are limited.

c) The UK has a comprehensive legal framework requiring all FIs and DNFBPs to conduct CDD and obtain and maintain BO information in a manner that is generally in line with the FATF requirements. Entities appear to comply with these requirements (see Chapter 5 on IO.4). LEAs have access to a range of informal and formal tools, including JMLIT and the NCA s.7 gateway, which typically enable authorities to access basic and BO information from FIs and DNFBPs in a timely manner. Obtaining BO info is more difficult in cases where the legal entity does not have a relationship with a UK FI or DNFBP.

d) Legal persons' basic and BO information is freely and immediately available to the public and all competent authorities through a central register. Unlike in the CDD process, BO information on the People with Significant Control (PSC) register is not verified and there are limited screening checks. Companies House is working to improve the accuracy of the register, including by conducting outreach to encourage end-users (including FIs, DNFBPs and LEAs) to report detected inaccuracies as they are not currently obliged to do so and nor is this generally happening in practice. From January 2020, FIs and DNFBPs will be required to report inaccuracies. Companies House is also working to improve the register's functionality.

40 Where countries choose to establish registries of beneficial ownership information, the FATF Recommendations do not require those registries to be public.

e) The UK has also established a register of the BO of trusts with tax consequences in the UK which is held by HMRC. The information on the trusts register is likely accurate in light of robust screening procedures. BO information on trusts is therefore easily and rapidly accessible to LEAs through this channel.
f) The UK regularly employs sanctions for delays in filing information or accounts. Sanctions for providing incorrect information are applied more rarely as compliance is typically achieved well before prosecution.
g) The UK has taken other steps to mitigate the risks posed by the misuse of UK legal persons and arrangements, and is exploring future projects in this area, in particular steps to mitigate the risks posed by Scottish Limited Partnerships and corporate ownership of UK properties.

Recommended Actions

a) Take steps to mitigate the risks posed by Scottish Limited Partnerships (this could include, for example, requiring the registration of a natural person partner and introducing increased reporting obligations).
b) Improve the quality of information available on the PSC register to ensure that the information is accurate and up-to-date as follows:
   a. pursue planned work with OFSI to screen information against sanctions lists and share this information as appropriate to enhance the effective implementation of targeted financial sanctions
   b. ensure that FIs, DNFBPs and LEAs report identified discrepancies to Companies House
   c. continue to improve the register's functionality (facilitate searching)
   d. where appropriate and well-founded, clearly flag in the register any discrepancies reported by FIs, DNFBPs, or LEAs, and
   e. ensure Companies House continues to report suspicions to relevant authorities, including filing a SAR as appropriate.
   f. Continue to apply the available sanctions to natural and legal persons providing inaccurate basic or BO information.

424. 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.[41]

41 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.

Immediate Outcome 5 (Legal Persons and Arrangements)

Public availability of information on the creation and types of legal persons and arrangements

425. Extensive information on the creation and types of legal persons is publicly available on the UK's central government website (gov.uk) including: guidance on all main types of legal person, including companies and partnerships; guidance on how to set up a legal person; and information on obligations after incorporation.[42] Assistance on creating a charitable organisation is available on the charity regulators' websites while information on community benefit societies and co-operative societies is available from various online sources.[43] The legislation applicable to creating and maintaining companies and partnerships is also publicly available, although information on partnerships is more dispersed across various acts.[44]

426. Information on the creation and types of legal arrangements, including trusts and unincorporated associations, and their purposes, may be obtained from the UK government website[45] and the government-established Money Advice Service.[46] Assistance to create a charitable trust is available from the websites of the three UK charity regulators.[47]

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities created in the country

427. The UK has a good understanding of the ML/TF risks and vulnerabilities of legal persons and arrangements created in its territory. The assessors based this conclusion on: a review of the various risk and threat assessments produced by the UK, including the NRA; discussions with LEAs, regulatory agencies, FIs and TCSPs; and case studies showing the role of legal entities in ML/TF cases in the UK.

428. The UK has undertaken various assessments of the risks posed by key legal persons and arrangements. The 2017 NRA concluded that UK legal persons, particularly limited companies, limited liability partnerships, and Scottish Limited Partnerships (SLPs), pose a high risk for ML, although the proportion of legal persons

42 GOV.UK "Business and self-employed" (accessed 27 March 2018).

43 Co-operatives UK, "Plan your co-op"; Community Shares, "Community benefit societies" (accessed 3 April 2018).

44 Legislation.gov.uk "Companies Act 2006", "Partnership Act 1890", "Limited Liability Partnerships Act 2000", Limited Partnerships Act 1907" (accessed 27 March 2018).

45 GOV.UK "Trusts and taxes", "Unincorporated associations" (accessed 3 April 2018).

46 GOV.UK "Trusts and taxes" (accessed 27 March 2018); the Money Advice Service, "Setting up a trust", "What is a trustee?" (accessed 27 March 2018).

47 GOV.UK "Charity types" and "Setting up a charity: model governing documents"; OSCR "Being a Charity in Scotland www.oscr.org.uk/guidance-and-forms/meeting-the-charity-test-guidance; CCNI "Model governing documents" (accessed 3 April 2018).

abused is very low.[48] The NRA did not identify any specific risks posed by unincorporated associations, community benefit societies or co-operative societies.

429. The ML risk posed by UK legal arrangements was considered low. The NRA acknowledged that the misuse of trusts was a global problem and that trusts remain vulnerable for abuse. Foreign trusts were identified as posing a much higher risk than UK trusts. TF through legal persons or arrangements is rare and deemed a low risk. The 2017 NRA concluded that TCSPs posed a medium risk of ML and a low risk of TF. However, the UK recognised that TCSP risks are heightened when combined with other financial, legal, or accountancy services.

430. Case studies support the conclusions of the 2017 NRA. High-end ML cases consistently show the use of foreign trusts (not UK trusts) and UK legal persons. The UK has supplemented the NRA with additional assessments of the risks posed by legal persons and arrangements (see box 30 below). These assessments are undertaken on a rolling basis to identify emerging trends and ensure a shared, up-to-date understanding of risks.

7

Box 30. **UK risk assessments and reports on the abused of legal entities**

In addition to the 2015 and 2017 NRAs, the UK has conducted various other risk assessments and reports on abuse of legal persons and arrangements for ML including:

- An Intelligence Report on *"The use of corporate entities to enable international money laundering networks"* examined the case of a money launderer based in Dubai to highlight the risks posed by: UK limited companies, limited liability partnerships, and SLPs; the use of nominee partners or directors; and entities banking overseas where regulatory requirements are less stringent.
- A strategic intelligence assessment on *"The use of corporate vehicles to hide beneficial ownership"* highlighted the risks posed by criminals using multiple corporate vehicles and complex structures across different jurisdictions to obfuscate BO.
- An HMRC report on the misuse of trusts for ML/TF purposes concluded that the risks from trusts stemmed predominantly from foreign trusts, often with the involvement of UK-based professional enablers.

431. Relevant competent authorities have a good understanding of the risks posed by legal persons and arrangements, consistent with the assessments undertaken by the UK. LEAs and tax authorities acknowledged the prevalence of foreign trusts and UK companies in high-end ML cases. Agencies also identified changing risks and trends.

48 GOV.UK, "National risk assessment of money laundering and terrorist financing 2017" (accessed 27 March 2018).

432. LEAs noted that as the UK and other jurisdictions improve their regulatory frameworks to prevent misuse of trusts, criminals turn to other jurisdictions to register their trusts. Relevant agencies also recognised that a recent increase in SLPs may be in part due to an increase in criminal misuse of these structures. Since the PSC Register was expanded to require BO reporting from SLPs, new registrations of these entities have dropped by 80%. Other steps are also being taken to respond to these changing risks and trends.

Mitigating measures to prevent the misuse of legal persons and arrangements

433. The UK has longstanding obligations on FIs and DNFBPs which help mitigate the misuse of UK legal persons and arrangements for ML/TF. These requirements mean legal persons and arrangements must undergo CDD and provide BO information at multiple points when dealing with any regulated sectors. The UK's risk assessments have also resulted in proactive steps to reduce the abuse of legal persons and arrangements. These changes enhance transparency, oversight, and regulation. However, vulnerabilities remain through which legal persons and arrangements are open to abuse. These findings are based on a review of the relevant legislative and operational changes and discussions with regulators, LEAs, financial institutions and DNFBPs (particularly TCSPs).

434. The UK is a global leader in advocating for corporate transparency.

Table 39 **UK global leadership in promoting corporate transparency**

Date	Action taken by UK
June 2013	• At the 2013 G8 summit in Lough Erne, the UK pledged to increase the transparency of companies and legal arrangements and ensure BO information was accessible.
April 2016	• The UK introduces a public register of people with significant control (PSC) in companies. • The UK (with Germany, France, Italy, and Spain) announced the pilot Agreement on the Automatic Exchange of Information on BO.
May 2016	• At the UK Anti-Corruption Summit, 32 commitments were made on increasing BO transparency.
April 2017	• The UK opens a call for evidence on a proposal for a public register on the beneficial owners of property controlled by overseas companies. • The International Anti-Corruption Co-ordination Centre opens in London, hosted by the NCA and funded by the UK Department for International Development.
June 2017	• Exchanges of Notes between the UK and all Crown Dependencies and six Overseas Territories come into effect, under which BO information will be shared within 24 hours, and one hour in urgent cases.[49]
January 2018	• The UK announces its intention to legislate for a public register of beneficial owners of non-UK entities that own or buy UK property, or which participate in UK Government procurement.

435. In 2016 the UK added a public register of 'people with significant control' (PSC) to the existing registers operated by Companies House. This register complements existing CDD BO requirements on the regulated sectors which ensure BO information is obtained at various points. For example, BO information will be obtained and verified by FIs when opening a bank account, and by lawyers and accountants when providing relevant services. In the 75% of cases where a TCSP or regulated entity is used to establish a legal person or arrangement, CDD will also be

49 The agreements are available on GOV.UK, "Beneficial ownership: UK Overseas Territories and Crown Dependencies": www.gov.uk/government/collections/beneficial-ownership-uk-overseas-territories-and-crown-dependencies.

conducted at this point. In the remaining 25% of cases in which individuals create companies directly, Companies House does not conduct identification, verification, or other CDD checks. This may create a gap where a company registers directly and is banked offshore, therefore avoiding undergoing CDD. Regulated entities appear to comply with CDD requirements (see Chapter 5 on IO.4). Where a FI or DNFBP cannot apply CDD, including identifying and verifying the BO, they must terminate the relationship and consider submitting a SAR.

436. The PSC register builds upon this framework. The centralised Companies House register contains basic and BO information, including company accounts, directors, and shareholders. Companies, limited liability partnerships, Scottish general partnerships with solely corporate partners, and SLPs are now required to register their PSC (which largely amounts to the beneficial owner of a corporate entity, although in some cases a legal person may be registered on the PSC register where they meet the relevant requirements(see R.24 in the TC Annex)). This creates an additional step for these legal entities which could help deter their misuse. The public nature of the PSC register allows enhanced scrutiny which may also help mitigate the risk of abuse of legal persons. The centralised register (which includes PSC information) was accessed over 2 billion times in 2016/17. Information in the PSC register is also reviewed by Companies House, including a forensic accountant who analyses accounts on the basis of complaints or identified suspicions and provides weekly referrals to LEAs. Improved front-end verification of PSC information could further enhance this progress.

437. Companies House has an ongoing programme to improve the central register. This work includes enhancing the functionality of the PSC register to enable increased searchability. This is an important step because a legal person is permitted to register another legal person (a "relevant legal entity")[50] on the PSC register so increased searchability helps mitigate any opacity in the corporate ownership chain. Where a relevant legal entity is registered on the PSC register, Companies House conducts manual checks to ensure the entity is eligible for registration and to detect any circular ownership structures (e.g. Company A registers Company B as its PSC, while Company B registers Company A). These checks are prioritised by risk, with relevant legal entities registered in financial centres and less transparent jurisdictions receiving a higher priority. The Companies Act 2006 prohibits circular ownership. This issue could be further mitigated by requiring legal persons to also register the ultimate beneficial owner.

438. There has been an 80% decrease in registrations of SLPs since the extension of the PSC register to these entities in 2017. This may be an indication that the register has a deterrent effect on the potential misuse of these legal persons. However, as at March 2018, Companies House estimated that, of 31 000 SLPs, 6 900 had not yet registered their PSC. Companies House was sending letters to these non-compliant entities. There are several particular characteristics that make SLPs appealing for criminal misuse: they have separate legal personality; the partners may be UK or foreign legal persons; and they have less onerous reporting requirements. A 2017

50 A relevant legal entity must keep its own PSC register or be admitted to trading on a specified market which meets adequate transparency requirements, and must be the first in the company's ownership chain.

report by Transparency International UK and Bellingcat found that "71% of all SLPs registered in 2016 are controlled by companies based in secrecy jurisdictions, hiding who is really behind the partnership".[51] In response to these vulnerabilities the UK brought SLPs within the scope of the PSC requirements in 2017. The Department for Business, Energy and Industrial Strategy is also conducting a review of the legal framework around partnerships, including SLPs, to consider ways to mitigate criminal activity by these entities. As at March 2018, the results of the review were with Ministers for their consideration.[52]

439. In July 2017, HMRC launched a BO register for both UK and foreign trusts with tax consequences in the UK. The register covers approximately 100 000 trusts (the number of trusts in the UK is difficult to estimate, but this figure likely accounts for less than half the total number). This number is expected to increase over the coming years as more trusts generate a tax consequence and are therefore required to register. Once registered, the trust remains registered even where it does not generate a tax consequence in subsequent years. The register is not public, but is available to LEAs upon request (without alerting the relevant trustee) which may help detect and interrupt criminal activity by trusts. Unlike the PSC register maintained by Companies House, information on HMRC's trust register is verified through checks against the 22 billion records available in the HMRC database, including tax information. HMRC has also undertaken awareness-raising with LEAs to promote use of the register, ensure LEAs are aware of the register's functionality, and encourage reporting where an LEA detects an inconsistency or issue in the trust register.

440. The UK has made other legislative changes to increase transparency and mitigate the abuse of legal persons in the UK. These include the Small Business, Enterprise and Employment Act 2015 (see Box 31 below).

Box 31. **The Small Business, Enterprise and Employment Act 2015**

The Small Business, Enterprise and Employment Act 2015 made a variety of changes to increase transparency and mitigate the abuse of legal persons in the UK[53].

Abolishing bearer shares entirely: Currently, of the 1 300 companies in the UK which had bearer shares, all but one have dealt with them.

51 Transparency International UK and Bellingcat, "Offshore in the UK: Analysing the use of Scottish Limited Partnerships in corruption and money laundering" (June 2017), pg.1, 9.

52 A consultation document was subsequently published detailing options for reform: GOV.UK "Limited partnerships: reform of limited partnerships law" (April 2018).

53 The Act also introduced a requirement for all company directors to be natural persons which was expected to come into force in 2016. However, the Government announced a delay in implementation date and there remains no set date for implementation. As this measure was not in force at the time of the on-site visit, it cannot be taken into account for the purpose of this evaluation. Currently, under the Companies Act 2006, at least one company director must be a natural person.

> **Applying director duties to "shadow directors" (i.e. a person controlling a company director):** The Act applies director duties to all directors, including those acting as a director or controlling the actions of a company director when not formally appointed by the company. This means that both "nominee" directors (which are not permitted so do not formally exist under UK law) and shadow directors are subject to equivalent obligations and face the same potential sanctions as a director.

441. Recognising that its property market is vulnerable to ML by criminal-controlled legal persons and arrangements, the UK is exploring options to mitigate this through a BO register for overseas entities owning or wishing to buy property in the UK.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons and legal arrangements

442. UK authorities are able to access basic and BO information on legal persons and arrangements[54] via one of three sources: from financial institutions and DNFBPs, from registers, or from the legal entity itself. The variety of sources increases transparency and access to information, and helps mitigate accuracy problems with particular sources. These findings were based on discussions with Companies House, LEAs, FIs, and DNFBPs; and case studies showing the methods typically used to access this information.

Source #1 – Financial institutions and DNFBPs

443. Competent authorities can obtain accurate and up-to-date basic and BO information directly from financial institutions and DNFBPs which demonstrated a solid understanding of their CDD and BO requirements (see Chapter 5 on IO.4). This information can typically be accessed in a timely fashion.

444. There are several channels available for LEAs to obtain information on legal entities from FIs and DNFBPs. At the intelligence-gathering stage, LEAs can request information through JMLIT provided the request is justified, proportionate and necessary. The ability to request information from several entities at once makes this mechanism particularly useful where the requested LEA is not clear whether or which FI or DNFBP has a relationship with the legal entity. Similarly, LEAs may make use of the NCA's s.7 gateway to channel a request through the NCA to ask a FIs or DNFBP to voluntarily provide BO information. Both JMLIT and the s.7 gateway are dependent on the co-operation of the requested institution(s). LEAs report broad success obtaining information through these channels, particularly where they have an existing relationship with the requested institution. This is supported by case studies which demonstrated the close relationship between LEAs and UK financial institutions. LEAs can also compel the provision of BO information through available

54 In the context of trusts, the UK defines the beneficial owner as the settlor, trustee(s), beneficiaries, class of beneficiaries, and any individual who has control over the trust (MLRs, reg.6(1)).

investigative measures such as production or disclosure orders. These orders require judicial authorisation, which can be obtained in a matter of hours for urgent cases. Production orders can be obtained relatively quickly through an electronic filing and granting system. Once issued, the orders typically receive a response within seven days, although immediate disclosure can also be sought. Both production and disclosure orders require suspicion of an indictable offence so are used at the investigative stage once sufficient evidence has been collected to meet this threshold. The SFO has access to additional investigative powers to compel the provision of information believed to be relevant to an investigation or inquiry within a timeframe set by the SFO (typically no longer than 14 days).

445. The availability of BO information via these methods is dependent on the legal entity having a relationship with a UK FI or DNFBP. According to data from Companies House, the vast majority (approx. 97%) of registered companies use a UK bank account to deal with Companies House suggesting they are either banked in the UK or using a UK professional service. As in all jurisdictions, timely access to verified BO information becomes more complicated and less timely where the relevant legal person or arrangement is banked overseas. While this is not the case for the vast majority of UK legal persons, case studies show that this structure is often used in high-end ML cases where a UK legal person avoids the UK CDD requirements by using bank accounts outside the UK (see box 32 below). In such cases, international co-operation may be needed to verify information held in the UK (e.g. on the PSC register). The UK is actively seeking to mitigate issues associated with seeking access to BO information held outside the UK. For example, in 2016, the UK entered into Exchanges of Notes with eight Crown Dependencies and Overseas Territories which have a financial centre under which BO information will be shared within 24 hours and one hour in urgent cases.

Box 32. **The use of corporate entities to enable international ML**

The UK conducted an intelligence report in 2015 into the use of corporate structures to enable ML. The report was based around a case study of a money launderer based in Dubai using UK corporate entities to launder criminal proceeds. The launderer routed the funds to a UAE company from 11 UK entities, including limited companies, limited liability partnerships and SLPs. All corporate entities were banked exclusively in Europe, but outside the UK, so were not subject to AML/CFT checks by UK financial institutions.

Source #2 – Registers of basic and beneficial ownership information

446. The trust and company registers provide fast and easy access to information for LEAs, although there are some limitations in terms of accuracy (for the PSC register of legal persons) and comprehensive coverage of the sector (for the HMRC trusts register).

447. For legal persons, authorities have immediate access to the public Companies House PSC register which holds basic and BO information for companies and partnerships. Competent authorities can also make requests directly to Companies

House for additional information not on the public register. Both domestic and foreign authorities access the public register and request information from Companies House regularly with the number of domestic requests increasing following Companies House outreach to LEAs (see tables 40 and 41 below). Companies House co-operates actively with LEAs through a LEA Data User Group, participation in the Government Agencies Intelligence Network (GAIN), and a Companies House Police Liaison Officer. Companies House makes weekly reports to the National Fraud Intelligence Bureau detailing information on the register which may indicate fraud. These reports are captured on a database that can be accessed by all LEAs. Where the suspicion is such that the threshold for a SAR is met, Companies House will also submit a SAR. A MOU between Companies House and the NCA was signed in early 2017 to facilitate information sharing.

Table 40. **LEA requests for information from Companies House under the Data Protection Act 2016/17***

Agency	Number of requests to Companies House
Police and NCA	44
UKCA	149
HMRC	46
SFO	1

Note: These figures do not include requests received through GAIN which can amount to more than 1 000 annually.

Table 41 **Visits to the Companies House register from foreign IP addresses September 2017**

Country	Number of visits
United States	476 871
India	151 112
Germany	144 821
France	71 648
Italy	59 383

448. Competent authorities and regulated entities do not rely on the PSC register as their sole source of BO information. Companies House estimates that the data is 95% accurate (and notes that this figure is likely to improve in coming years as the requirements bed in). A civil society examination of the data found that the error rate of companies listing ineligible legal persons as their PSC amounted to 0.0034% (with 70% of these companies going on to correct the information) (see box 33 below). Nonetheless, the ease with which a criminal could register inaccurate information means the register is viewed as one source, but not a definitive source for LEAs, FIs or DNFBPs in preventing, detecting, or investigating ML/TF.

449. When details of a PSC are registered, Companies House conducts basic checks on the information submitted (e.g. to ensure a valid address and date of birth has been provided and to check the use of sensitive words in a company name), but does not verify the PSC's identity. The application is then reviewed by one of the 300 examiners at Companies House. Given the wide range of information to which Companies House has access, these checks could usefully be extended to include screening against sanctions lists to ensure effective implementation of targeted financial sanctions obligations and to prevent and detect potential misuses of corporate structures (see Box 33 below). Where an error is detected through

Companies House's initial checks upon receipt of the PSC information, the registration will be rejected.[55] Legal persons are required to submit annual confirmation statements of PSC information which are subject to further checks. If an inaccuracy is detected post-registration, Companies House will typically request correction from the company and, if necessary, can strike the company off the register, or reject a confirmation statement. Inaccurate information can only be removed on application (Companies Act 2006, s.1095). If the inaccuracy raises suspicions, the Companies House LEA Liaison Team will refer the matter to the relevant LEA. Companies House also conducts thematic reviews of information in the register to ensure accuracy.

450. In July 2017, Companies House introduced a reporting feature on the public register to encourage external parties to voluntarily notify it of suspected errors. This feature has been well-used, with Companies House receiving an average of 200 notifications per day through this and other channels. Some frequent users of the register, including certain FIs, DNFBPs and LEAs, stated they would not typically report errors and generally did not appear to appreciate the importance of providing this feedback. An exception to this is the NCA which entered into a MOU with Companies House in early 2017 to allow information-sharing, including where the NCA is not able to verify PSC information obtained from Companies House. NGOs have taken advantage of the register to undertake bulk data analysis and report on potential inaccuracies and issues of concern (see Box.33). Financial institution and DNFBP representatives stated that where the PSC register did not match information provided in the CDD process, they would rely on the customer to alert Companies House and identify the legal person/arrangement through their own CDD. Companies House is engaging with external parties to encourage reporting of inaccuracies and from January 2020, FIs and DNFBPs will be required to report inaccuracies. This will improve the accuracy of the register to the extent the FIs and DNFBPs are successfully identifying the BO. External verification of register information will also be improved by a Companies House programme to reform the register's functionality.

Box 32. **Civil society examination of accuracy of PSC register**

In 2016, a team of data scientists from several civil society organisations analysed the first three months' worth of information available in the PSC register. The team found that of the 1.3 million companies which have registered a PSC:

- 76 persons from the US sanctions list were listed as PSCs
- 267 disqualified directors were listed as PSCs, and
- Approximately 4 500 companies listed other companies on the PSC register in situations where this was not permitted.

In response, Companies House wrote to the 4 500 companies who had registered ineligible corporate PSCs. Most had simply misunderstood the requirements, and approximately 70% corrected the information in response to correspondence from Companies House (resulting in a

55 This occurs in approximately 5% of cases.

compliance rate of 99.99% for this requirement). Further letters were sent to the remaining non-compliant entities. As at March 2018, court action had yet to be taken in respect of these companies, but almost 900 investigations were ongoing.

451. LEAs actively encourage the use of the PSC register as one source of information on BO. For example, in 2017, the NCA had a workshop on using the register to retrieve BO details. However, in light of the lack of verification and to ensure robust evidence is obtained, the register is used in conjunction with other sources. LEAs recognised that information on the PSC register was not always accurate, but noted that such inaccuracies could provide investigative leads (e.g. a discrepancy between the register and other sources of BO information may be a flag for suspicion). FIs and DNFBPs also acknowledged the potential inaccuracies in the register, noting that information was often out-of-date, but considered it could be used as a corroborative source.

452. For trusts, competent authorities are able to access basic and BO information by requesting HMRC to provide information held on its trusts register. Under a Memorandum of Understanding agreed with relevant authorities, HMRC replies to such requests within 15 working days. The trust register contains information exclusively on trusts with tax consequences in the UK. Information on other trusts is not yet available through this mechanism.

Source #3 – Legal entities themselves

453. Competent authorities can also access basic and BO information from the legal entity itself. Companies and partnerships, including Scottish Limited Partnerships, must file basic and BO information with Companies House and maintain a register of their members, shareholders, or partners either at their registered office (which must be within the UK) or at Companies House. The legal person is required to inform Companies House of the location of this information which helps facilitate access to it by competent authorities.

454. Trustees must maintain BO information (including information on the settlor, trustees, beneficiaries, and any other individual with control over the trust). Under the 2017 MLRs, this information must be provided to LEAs upon request and within a reasonable time as set by the requesting authority.

455. LEAs can access information from either trustees or companies via a range of voluntary or compulsory measures (see para.446 above).

Effectiveness, proportionality and dissuasiveness of sanctions

456. UK authorities regularly use effective and proportionate sanctions against legal persons or arrangements which are late to file basic or PSC information. The level of these sanctions is likely dissuasive for natural persons, but less so for the legal entity itself. The assessors' findings were based on: statistics provided on the use of sanctions; discussions with Companies House, HRMC and regulatory authorities; and case studies on the sanctioning of legal entities.

457. Inaccurate filing of basic or PSC information by a legal person is punishable by an unlimited fine and/or up to two years' imprisonment. Late filing of accounts is punishable by a fine of GBP 1 000 and a daily default fine (see TC Annex, R.24 for more information on sanctions). These penalties apply equally to the legal person and company officers and are regularly used (see Table 42 below). They are likely dissuasive for natural persons, including directors and senior management who are most often pursued by the UK, although the level of fine for late filing would be low if imposed on the legal person itself. Failure by trustees to maintain accurate basic and BO information or file information on the BO register is punishable by a set financial penalty imposed by HMRC, and/or a statement of censure.[56]

458. Detecting the provision of inaccurate information requires more investigation than detecting late filings. There is no requirement for the person undertaking the filing to sign the documentation or provide a unique identifier. Instead, a company pin code is used to prove competence. This makes it difficult for Companies House to prove that a specific individual intentionally misfiled accounts on the company's behalf. However, this is mitigated by the imposition of duties on specific persons for relevant information, which ensures a particular individual can be held accountable for the provision of incorrect information. As at March 2018, no sanctions had been issued for failing to register PSC information although Companies House had approx. 50 active investigations, several of which were very close to the prosecution stage.[57]

459. Sanctions for delays in filing are more common. This may be because late filing is relatively easy to detect as Companies House receives an automatic alert where a legal entity is late to file. In 2016/17, Companies House levied GBP 89 million in civil penalties and prosecuted 1 900 directors for delayed filing.

Table 42.**Companies House enforcement actions**

	2014/15	2015/16	2016/17
Failure to deliver accounts			
Charges laid	4 383	4 432	4 046
Convictions	2 122	2 158	1 934
Failure to deliver annual returns			
Charges laid	2 220	2 326	2 406
Convictions	1 231	1 292	1 245
Breach of Director duties			
Charges laid	4 290	4 151	4 005
Convictions	2 003	2 005	1 902

460. The goal of the UK's sanctions regime is to improve compliance. On this basis, the UK will generally only pursue criminal charges where an entity continues to fail to meet their obligation. Where the relevant information is provided or updated, the matter will be laid to rest, although the lack of verification procedures means the information may remain inaccurate. In many cases, a letter may be sufficient to rectify

56 HMRC will bring into force in 2018 a separate penalty regime imposing larger financial penalties against trusts in connection with which ML is proven to have taken place.

57 As at July 2018, 47 931 entities had not registered a PSC. The majority were under active investigation. Companies House had passed 82 cases to prosecutors with seven resulting in conviction and the highest financial penalty.

the deficiencies. Where this is not sufficient, it is important that sanctions are actively used by Companies House to avoid creating a culture of compliance based solely on goodwill (see Box 34 below).

Box 34. **Dealing with legal entities non-compliance**

Case study: Non-compliance with obligation to remove bearer shares

In 2015, the UK outlawed bearer shares. All of the 1 300 companies which originally had bearer shares have dealt with their bearer shares as per legislative requirements. One company was not able to identify the owner of the shares and has taken the appropriate actions. These shares were embargoed from being used.

Overall conclusions on IO.5

461. **The UK has achieved a substantial level of effectiveness for IO.5.**

CHAPTER 8. INTERNATIONAL CO-OPERATION

Key Findings and Recommended Actions

Key Findings

a) In general, the UK provides a broad range of timely and constructive international co-operation. The UK actively seeks and provides MLA and extradition. International co-operation with EU member states is facilitated by a wide range of regional co-operation tools and information-sharing gateways that streamline the process. This is an important positive feature as an overwhelming majority of the UK's international co-operation is with other EU member states.

b) Domestic processes for responding to the high number of MLA and European Investigation Order (EIO)[58] requests received by the UK are generally good. Agencies coordinate informally and have good personal relationships. Where requests are routed through the UKCA, the process could further benefit from more systematic co-ordination between relevant domestic authorities throughout the execution of the request.

c) Formal and informal co-operation is facilitated through an extensive overseas criminal justice network of LEA officers from the NCA, HMRC, CPS, and the Metropolitan Police servicing over 160 jurisdictions. These officials are posted in a targeted fashion in line with the UK's identification of risk and have been vital in improving co-operation. This is a very positive feature of the UK system and many examples were provided demonstrating its effectiveness and ability to streamline co-operation.

d) JMLIT's public/private partnership provides further opportunities for UK's international co-operation system. Results have already been delivered in relation to the few requests received from foreign counterparts. The UK is championing similar partnerships in other countries. This is an innovative approach considered to be an example of best practice.

e) Moderate improvements are required in the UKFIU's ability to provide constructive and timely international co-operation. Improvements are also required to the FCA's international co-operation on MVTS.

f) The public PSC register will facilitate the UK's ability to respond to international requests for beneficial ownership (BO) information on legal persons and, to the extent that this information is accurate, can supplement the UK's ability to share CDD-based BO information under the MLA regime.

58 EIO requests enable competent authorities in the UK to recognise and act on orders made by the relevant prosecutorial or judicial authority in the requesting member state (EU member states excluding Denmark and Ireland).

Recommended Actions

a) To the extent possible, work with international partners to endeavour to ensure that the UK continues to use and access regional co-operation tools and information-sharing gateways comparable to those available under the EU framework.
b) Improve co-ordination on MLA requests routed through UKCA to ensure these requests are tracked and progressed in a timely manner and responses can be provided to foreign counterparts, in particular in large and complex cases, so as to ensure effective co-operation.
c) Implement the recommended actions regarding the UKFIU (see Chapter 3 under IO 6), increase resources available to the FIU international team and ensure the UKFIU provides assistance to a larger extent to international partners.
d) Ensure that where countries are referred to the PSC register in response to a request for BO information on legal persons, they are made aware that verified, CDD-based BO information is available through an international co-operation request to the UK LEAs to obtain this information from FIs or DNFBPs (see Chapter 7 on IO 5).
e) Improve the collection and maintenance of consistent, national statistics on international co-operation.
f) Ensure the FCA effectively responds, in a timely manner, to requests from foreign jurisdictions concerning passported entities or agents of UK payment institutions.

462. 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.

Immediate Outcome 2 (International Co-operation)

463. International co-operation is vital in the UK context, given its position as a global financial centre and the risks it faces as a destination country for foreign proceeds. In general, the UK is active in making and responding to requests for international co-operation, aided by an extensive overseas criminal justice network. The sheer volume of international co-operation makes co-ordination and prioritisation more challenging. Statistics on international co-operation are maintained at an agency level, meaning comprehensive national statistics are not maintained.

Providing constructive and timely MLA and extradition

464. The UK generally provides timely and constructive MLA and extradition and responses are of high-quality. Simplified procedures within the EU enhance the UK's co-operation with EU member states, which account for the vast majority of its MLA and extradition activity. Co-operation on asset recovery is good. Co-ordination and prioritisation of MLA requests can be challenging given the high volume of requests received. Findings in this respect were based on: case studies demonstrating positive co-operation experiences; statistics demonstrating the volume of MLA and

extradition requests received by the UK; feedback from FATF and FSRB delegations; and discussions with the UK's three central authorities (see below) and LEAs responsible for executing requests.

Mutual legal assistance

465. The UK typically provides high-quality, constructive, and timely MLA and a wide range of assistance can be provided. The UK receives an extremely high number of MLA and European Investigation Order (EIO) requests (7 873 in 2017). The number of requests received has been steadily increasing over the past three years (see Table 43 below). The UK has three central authorities: the UK Central Authority (UKCA) in the Home Office for requests relating to England, Northern Ireland, or Wales; the International Mutual Assistance Team in HMRC for requests relating to tax matters; and the International Co-operation Unit of the Scottish Crown Office and Procurator Fiscal Service (COPFS) for requests relating to Scotland. Of the three central authorities, the UKCA handles over 80% of incoming requests. Feedback from delegations confirms that MLA relationships with all central authorities are generally positive, although some countries noted that domestic co-ordination between the UKCA and executing authorities could be improved to prevent delays.

Table 43. **MLA requests received by the UK**

	2015	2016	2017
Requests received by UKCA	**5 783**	**6 510**	**7 132**
Relating to ML	288	248	356
Relating to TF	2	3	4
Requests received by HRMC	**193**	**217**	**212**
Relating to ML	45	64	40
Requests received by COPFS	**441**	**424**	**529**
Relating to ML	0	18	10
Relating to TF	0	0	1
Total number of requests received by UK	**6 372**	**7 151**	**7 873**
Relating to ML	333	330	406
Relating to TF	2	3	5

466. Most of the UK's MLA requests are received from EU Member States. In 2016, the UKCA received 7 132 requests from 108 different countries or territories, 80% of which were EU members. The UK implemented the EIO regime in July 2017 which significantly facilitates evidence-sharing between EU members. In the 8 months between July 2017 and March 2018, the UK executed 879 EIO requests. The UK authorities anticipate that this number will continue to increase as participating EU members transpose the Directive into their domestic law.

467. For non-EU members, the UK can provide MLA pursuant to one of its 39 bilateral arrangements or various multilateral arrangements, or on an ad hoc basis with reciprocity required only for requests relating to tax matters.

468. The UK takes a constructive and proactive approach to providing MLA. The Home Office website provides guidance on requesting MLA which is available in English, Polish and Turkish to reflect some of the UK's most common MLA partners.[59]

59 Gov.uk "MLA guidelines for foreign authorities" (updated 23 March 2015).

The guidance includes specific templates and forms for requesting particular assistance, including requests for evidence, search and seizure, restraint and confiscation, and service of process.

469. The UK has an extensive overseas criminal justice network, including intelligence officials, investigators, and prosecutors. This includes: 168 NCA International Liaison Officers (ILOs) located in 52 countries and servicing 162 jurisdictions; over 40 HMRC Fiscal Crime Liaison Officers (FCLOs) with responsibility for over 100 jurisdictions; 27 CPS International Liaison Magistrates/Criminal Justice Advisors; and the Metropolitan Police SO15 network of counter-terrorism liaison officers. These posted personnel are available to assist their host countries in making MLA and asset recovery requests that are complete and compliant with the UK legal requirements in the first instance. Officials are strategically posted to jurisdictions deemed high priority for the UK based on the quantity of co-operation with the UK and the UK's foreign predicate offence risks. The UK reassesses and reconfigures the postings on a regular basis. In addition, all of the UK central authorities confirmed they would actively assist in providing guidance to requesting countries where possible. Case studies were provided to confirm this (see box 35 below).

Box 35. **UK central authorities' ability to provide collaborative and timely MLA**

Co-operation by the UKCA

In 2016, authorities in the Netherlands arrested an individual in a ML and drug offences investigation. The arrested individual had been using a London property to facilitate meetings of an organised crime group. An NCA ILO based in the Hague assisted the Dutch authorities and liaised with the UKCA to prepare a compliant and complete request for an urgent search of the London property to prevent the destruction of evidence. The morning after receiving the request, the UKCA met with the NCA and Met Police to discuss the request and determined that freezing orders could be a faster route for obtaining the same evidence. The UKCA immediately advised the Dutch authorities who worked with the Met Police to draft the new request, while the UKCA drafted the formal court application and liaised with the court to ensure prioritisation of the request. As soon as the request was finalised, the court order was processed, the freezing order was executed, the property was searched and the obtained evidence was transmitted—all within only two days after the initial request was received.

Co-operation by the COPFS

In 2015, COPFS received a request from Switzerland for bank account information located in Scotland. COPFS liaised with the Swiss authorities and confirmed that the timeframe for executing the request was five days. The COPFS prosecutor drafted the necessary paperwork and obtained leave from the Lord Advocate to seek a court order which was granted on the same day. At the same time, Police Scotland liaised with the relevant bank to confirm

existence of the account and prepare for execution of the incoming order. Upon obtaining the court order, the Police worked with the bank to have it executed by the following morning. Once the evidence was obtained, it was reviewed by the prosecutor and forwarded to Switzerland in electronic and hard copy within 40 hours of receipt of the MLA request.

470. Managing such a large number of MLA requests presents challenges. The UK is nonetheless typically able to provide a timely response to MLA requests. Timeframes largely depend on the complexity of the case and the assistance sought. MLA requests to the UKCA take an average of 144 days for full execution of the request and the case to be closed, those to COPFS take 128 days, and those to HMRC take 178 days (reflecting the increased complexity of tax-related requests). Timeframes are much faster under the EIO regime, with most non-urgent cases executed within 90 days. Urgent requests (either within or outside the EIO system) can be processed within a matter of days (see Box 35 above).

471. A large percentage of MLA and EIO requests are for the execution of production orders on banks—almost 20% of MLA requests and 50% of EIO requests received by the UKCA in 2016 and 2017 respectively. Such requests can be processed quickly under the UK's electronic system which permits the application and granting of such orders electronically, thereby shortening the court process. All central authorities have a system for prioritising requests, based on the urgency of the request, the type of measures, the type of investigation, and the status of the person involved.

472. MLA requests to HMRC are executed by HMRC and requests to COPFS are executed by Police Scotland. Requests received by the UKCA are wider-ranging and are therefore executed by a wide range of relevant LEAs. This, in combination with the extremely large number of requests received, poses challenges for the UKCA in monitoring the execution of requests throughout the entirety of the process, particularly for non-urgent cases. The UKCA has procedures in place for ensuring the request is processed in accordance with its internal timeframes, including internal alerts to follow up on the request with the executing authority. Agencies coordinate informally and have good personal relationships. However, the process could benefit from more systematic, two-way communication and co-ordination between the UKCA and the executing authorities and ongoing feedback on the progress of requests. Feedback from delegations confirmed that this lack of co-ordination sometimes results in communication challenges and delays in rendering assistance.

473. The UK is able to provide a wide range of assistance in asset recovery cases, including in identifying, tracing, restraining and confiscating assets. As in domestic cases, to restrain assets, the UK must prove that there is a real risk of dissipation which can be problematic in cases where restraint is not sought prior to or concurrent with charging (see Chapter 3 under IO.8, para. 187).

474. MLA requests are refused in less than 20% of cases, and often further assistance is provided post-refusal. In 2016, 29% of MLA requests refused by the UKCA were refused because they were sent to the wrong central authority, while 26% were refused because insufficient information was included. In such cases, all central

authorities confirmed that they work with the requesting state to identify the correct authority or the required information.

Extradition

475. The UK operates two extradition regimes: a simplified extradition procedure for EU Member States under the European Arrest Warrant (EAW) framework and a standard procedure for non-EU members with which the UK has an extradition agreement. For all other countries, the UK is able to enter into an ad hoc extradition arrangement where necessary.

476. EAW alerts are received by the NCA (for requests to England, Wales, and Northern Ireland) or COPFS (for requests to Scotland). In 2015/16, the NCA received 14 279 EAW alerts, and the number has been steadily increasing over the past five years as the framework embeds across EU countries (see Table 44 below). The majority of alerts relate to individuals not located in the UK. EAW alerts are dealt with in an expedited fashion. They are assessed within a matter of hours, an initial hearing is held as soon as practicable, and an extradition hearing is held within 21 days of arrest.[60]

477. Standard extradition requests from non-EAW countries are received by the UKCA (for England, Wales, and Northern Ireland) or COPFS (for Scotland). These requests progress at a slower rate, taking an average of nine months from arrest to surrender. Both the UKCA and COPFS make efforts to facilitate the process, including by reviewing draft requests prior to receipt and providing advice to requesting states.

478. The UK does not unduly reject or refuse EAW or standard extradition requests (see Table 44 below). In most cases where refusal to surrender occurs, it happens at the court stage. For EAW requests, there is a large discrepancy between the number of alerts received and the number of persons surrendered which reflects the fact that the UK receives all EAWs regardless of whether the person is located in the UK. Of the standard extradition requests refused in 2017, 17 of 29 (59%) were refused for human rights concerns. Where cases were denied on the basis of insufficient information, disproportionality or lack of dual criminality, the central authorities work with the requesting state to consider whether the request could be reworked.

Table 44. **Extradition requests received by the UK**

	2015	2016	2017
EAW alerts to NCA	**12 134**	**14 279**	**16 598**
Relating to ML*	42	44	97
Persons surrendered	1 093	1 271	1 390
Relating to ML	2	5	2
EAW alerts to COPFS	**176**	**116**	**157**
Relating to ML*	0	0	2
Persons surrendered	78	82	59
Relating to ML	0	0	0
Standard requests to UKCA	**101**	**97**	**95**
Relating to ML	3	3	3
Relating to TF	0	0	0

60 The extradition hearing may be held at a later date on application of one of the parties.

	2015	2016	2017
Persons surrendered	22	24	37
Relating to ML	0	0	2
Relating to TF	0	0	0
Standard requests to COPFS	**2**	**6**	**3**
Relating to ML	0	0	0
Relating to TF	0	0	0
Persons surrendered	0	2	2
Relating to ML	0	0	0
Relating to TF	0	0	0

* TF is not distinguished as a separate category in the EAW system so data on the number of EAW requests related to TF could not be provided. There were no standard requests to either the UKCA or COPFS relating to TF.

479. Throughout the extradition process, the UK maintains regular and direct contact with the requesting state via prosecutors in the CPS and COPFS International Co-operation Unit. The overseas criminal justice network is a useful tool in this respect. This ensures the request is processed in a coordinated manner.

Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

480. As a financial centre with transnational financial flows, many of the UK's ML and predicate offence cases have a transnational element. The UK actively seeks MLA and extradition in such cases, including pursuing requests for restraint, freezing and confiscation. Effectiveness in this regard was demonstrated through case examples and statistics; feedback from FATF and FSRB delegations; and discussions with the UK's three central authorities and LEAs responsible for executing requests.

Mutual legal assistance

481. The decision to seek MLA is typically taken by the prosecutor. Assistance can be sought indirectly through the central authority or directly by the prosecuting agency depending on the type of assistance sought and the relationship with the requested country.

482. All investigating and prosecuting authorities recognised the importance of seeking international assistance in ML, associated predicates, and TF cases with transnational elements and considered this an integral and standard part of the investigative process and a core capability of investigative teams. In 2016, of 208 requests channelled through the UKCA to non-EU countries, 78 related to ML. The importance of international co-operation is recognised in various law enforcement strategy documents, including the NCA Annual Plan 2017-18, the SFO Strategic Plan 2016-19, and the FCA's Business Plan. UK agencies have been particularly active in utilising the EIO system.

Table 45. **Total MLA requests made by the UK (for all offences)**

	2014	2015	2016
CPS	401	272	247
SFO	79	62	66
FCA	1	13	20

	2014	2015	2016
PPS	105	74	86
COPFS	201	163	128

483. In seeking MLA, the UK actively uses its overseas criminal justice network of. This network advises UK agencies on local issues, helps to prepare requests, assists LEAs to follow up on unanswered requests, and helps their host country authorities execute the request. A range of other channels also exist for authorities to follow up on unanswered requests, including direct contact, regional networks, or through diplomatic channels. The UK has established a Video Teleconference project between 13 countries, including several key partners, to share expert knowledge and facilitate assistance, particularly with respect to asset recovery. These mechanisms have been useful in facilitating requests for restraint, freezing and confiscation and have helped the CPS recover GBP 23 million from overseas jurisdictions since 2013.

8

Extradition

484. As with MLA, the decision to request extradition is driven by the prosecutor involved in the case. EAWs are obtained by prosecutors and transmitted by the NCA (for England, Wales, and Northern Ireland) or the COPFS (for Scotland). Extradition requests to non-EU members are made under relevant bilateral, multilateral, or ad hoc arrangements through the UK central authorities (the UKCA and COPFS). The UK actively utilises both processes, making approximately 300 requests per year via the EAW system and approximately 25 per year to non-EU jurisdictions (see Table 46 below). Where requests are unanswered, it is up to the relevant prosecutor to follow up on the request.

Table 46. **Extradition requests made by the UK**

	2015	2016	2017
EAW alerts transmitted by the NCA	**223**	**241**	**345**
Relating to ML*	3	9	8
Persons surrendered	142	112	178
Relating to ML*	0	1	0
EAW alerts issued by COPFS	**15**	**22**	**24**
Relating to ML*	**1**	**2**	**1**
Persons surrendered	9	7	15
Relating to ML*	1	2	0
Extradition requests made through UKCA	**48**	**48**	**19**
Relating to ML	0	1	2
Relating to TF	0	0	0
Persons surrendered	26	22	13
Relating to ML	0	1	2
Relating to TF	0	0	0
Extradition requests made through COPFS	**5**	**1**	**1**
Relating to ML	0	0	0
Relating to TF	0	0	0
Persons surrendered	1	2	1
Relating to ML	0	0	0
Relating to TF	0	0	0

* TF is not distinguished as a separate category in the EAW system so data on the number of EAW requests related to TF could not be provided. There were no extradition requests through either the UKCA or COPFS relating to TF.

Seeking and providing other forms of international co-operation for AML/CFT purposes

485. The UK proactively uses agency-to-agency international co-operation for AML/CFT purposes. LEAs are particularly active in utilising informal co-operation and JMLIT provides a new avenue for enhancing international information-sharing. Co-operation with the UKFIU can be more challenging. The FCA, HMRC, and the Gambling Commission work closely with foreign counterparts, although co-operation by other AML/CFT supervisors is limited. The assessment team's findings were based on: statistics on the volume of co-operation; case studies demonstrating co-operation; feedback received from FATF and FSRB delegations; and discussions with law enforcement authorities, supervisors and the UKFIU.

486. UK LEAs, including police forces, have strong and often long-standing relationships with foreign counterparts resulting in positive, informal co-operation. Co-operation with foreign states is further facilitated by the UK's overseas criminal justice network. This network is available to aid all UK agencies, to assist in developing a shared understanding of key risks, and to facilitate operational co-operation across a range of host country LEAs. Of the 168 NCA ILOs, 15 are accredited financial investigators or have received financial intelligence training. These 15 officers are placed in the jurisdictions most relevant to fighting ML and financial crime, such as major financial centres or strategic partners. In 2015-16, the UK estimated that 10% of the total ILO activity related to high-end ML, with an additional 15% relating to bribery, corruption, sanctions-evasion, and other high-priority economic crimes. The UK's extensive overseas criminal justice network has proved very successful. NCA ILOs gathered 11 000 intelligence reports on serious organised crime in 2016. In 2015/16, as a direct result of intelligence obtained through HMRC's FCLO network, the UK disrupted 70 organised criminal groups and seized GBP 747 000. The network is also active in providing assistance to host countries (see box 36 below). The NCA uses its ILO network to help international partners achieve asset denial in their own jurisdictions, recording nearly GBP 860 million in recorded asset denials between 2013 and 2017.

Box 36. **Use of the overseas criminal justice network to seek and provide international co-operation**

Seeking co-operation: Johnson case

Johnson was prosecuted in the UK for his role in a multi-million GBP tax fraud. He fled the UK in July 2014, was convicted in absentia and a confiscation order of GBP 109 million was issued. In July 2017, he was detained attempting to enter the UAE on a false passport. The UAE made contact with the FCLO based in the UAE. The FCLO worked with UAE law enforcement, immigration and judicial authorities to facilitate Johnson's deportation to the UK within a week of his attempt to access the UAE. This case also resulted in broader co-operation on identifying shared risks, the establishment

of a virtual project to share intelligence and develop operational interventions on ML, and meetings on improving extradition between the UK and UAE.

Providing co-operation: Grand corruption case

In 2016, the NCA ILO at Europol responded to an international enquiry into two individuals suspected of grand corruption. After meetings between the NCA ILO and relevant law enforcement counterparts, a special task force was formed to investigate the activity. Both suspects were subsequently arrested and extradited from their countries of residence to the lead investigating country. A freezing order from that investigating country for a substantial sum was also registered in the UK.

8

487. The UK participates in various multilateral fora to seek and provide co-operation. The UK International Crime Bureau (UKICB) is the National Central Bureau for INTERPOL and handled over 264 000 INTERPOL messages in 2016. The Europol Headquarters hosts 185 officers from across UK law enforcement, including regional police officers. Information is regularly exchanged through the Europol Secure Information Exchange Network Application (SIENA) (in 2016, the UK sent 1 836 disseminations relating to ML and received 2 668). The UK is a member of the Five Eyes ML Working Group, which recently established a project to facilitate member countries' direct sharing of financial information. The UK also hosts the International Anti-Corruption Coordination Centre (IACCC) which combines resource from the UK, Interpol, the United States, Canada, Australia, New Zealand and Singapore to improve intelligence-sharing on grand corruption and ML. Joint investigation teams (JITs) are also actively used. The UK has nine active JITs relating specifically to ML and has completed 11.

488. JMLIT (see Box 2 in Chapter 3) provides unique opportunities for international co-operation on cases and enhancing international public/private information-sharing. LEAs in other countries may submit cases to JMLIT through the NCA. This is a new feature and has not yet been widely used, but, if used regularly, it provides scope to enhance international co-operation. The UKFIU has initiated a pilot to push appropriate inbound Egmont requests through JMLIT. The UK is also championing public/private partnerships in other countries with the goal of establishing a worldwide network of public/private partnerships which could share information between themselves. For example, two NCA officers were deployed to Australia to work with the Australian FIU (AUSTRAC) on the development of the FINTEL Alliance—an Australian public/private partnership launched in 2015. JMLIT also supported the establishment of Hong Kong's Fraud and ML Intelligence Taskforce (launched in May 2017).

489. In most cases, the UKFIU is the UK point of contact for exchanging information with foreign FIUs. The UKFIU participates in the Egmont Group of FIUs and utilises the European FIU information-sharing system, FIU.NET. The UKFIU reported that the average time for responding to Egmont requests was 75 days, although some countries reported that this may extend to 4 months. The UKFIU houses the European Asset Recovery Office (ARO) network and the Camden Asset Recovery Inter-Agency

Network (CARIN) in asset recovery cases. It is also able to access the overseas criminal justice network to make enquiries abroad. The UKFIU has a specific team of 17 officers to deal with international co-operation. This is a low level of resources given the number of disseminations made and received by the UKFIU (see Table 47 below). The resourcing may be a contributing factor in the delays and difficulties reported by some FATF and FSRB delegations in obtaining information from the UKFIU.

Table 47. **Disseminations made and received by the UKFIU**

	2013	2014	2015	2016
Disseminations made by the UKFIU				
ARO intelligence packages	101	136	171	114
FIU-FIU intelligence packages	1 136	1 391	1 264	1 255
CARIN intelligence packages	5	19	38	12
Spontaneous disseminations	983	1 491	1 543	1 304
Total	2 225	3 037	3 016	2 658
Disseminations received by the UKFIU				
ARO intelligence packages	338	297	327	314
FIU-FIU intelligence packages	1 045	1 137	1 412	1 223
Spontaneous disseminations	261	582	640	475
Total	1 644	2 016	2 379	2 012

490. Where the UKFIU receives a terrorism-related request, they are identified and screened by the UKFIU, and then promptly forwarded to the relevant CT unit for direct response. This is facilitated by the NTFIU officer embedded directly in the UKFIU and the strong relationship between the two agencies. One foreign FIU noted the quality of the UKFIU's outreach on TF. Another noted that the UKFIU refers most TF-related SARs to the UK Metropolitan Police for review and analysis without also carrying out its own analysis.

491. Multiple delegations, including several key partners, considered that co-operation with the UKFIU was effective and resulted in quality assistance in a timely manner. Several jurisdictions pointed to regular and ongoing information-sharing resulting in the timely identification of ML, joint investigations, and eventual convictions. Many delegations noted that they had received spontaneous disclosures from the UKFIU and that the requests from the UKFIU were of good quality. For the most part, urgent requests reportedly receive a prompt response. However, several delegations noted an overall lack of proactive co-operation by the UKFIU. One country stated that these issues led it to rely on the NCA ILO network where it would otherwise have co-operated with the UKFIU. The UKFIU often acts as channel through which requests from foreign FIUs are passed to UK LEAs for response. This diagonal co-operation, and the UKFIU's ability to utilise the NCA ILO network, is positive, but there is also a concern that requests passed on to other agencies domestically are not followed up by the UKFIU which can result in uncertainty for the requesting country as to the status of the request and which agency the requesting country should be

dealing with. The UKFIU similarly acts as a channel for outgoing requests from UK LEAs to foreign FIUs and could play a more proactive role in making requests for information.

492. A number of delegations referred to an information sheet which the UKFIU provided in response to requests which listed the information that could be obtained by the UKFIU and shared with requesting states. This feedback raised concerns about the limited nature of the list, for example, the information sheet stated that the UKFIU could only confirm bank details from a sort code and account number and that other bank account information or transaction data must be obtained through formal MLA. The UKFIU recognised that the information sheet provided an overly restricted view on the assistance it could provide to partners and as at March 2018, the information sheet was under review.[61] The limited role and resourcing issues of the UKFIU may also limit the amount of information, analysis and qualified intelligence that the UKFIU can provide to foreign counterparts (see Chapter 3 under IO 6). The strength of the UK's other informal co-operation mechanisms, particularly the overseas criminal justice network, somewhat mitigates this weakness.

493. Co-operation between UK supervisors is consistent with its risks. The FCA co-operates closely and proactively with foreign counterparts (see Box 37 below), including by encouraging information-sharing through an extensive secondment program. The FCA participates in a range of regional networks and groups including the EU Shared Intelligence System and Financial Information Network (FIN-NET), the Basel Committee's AML Expert Group, and the AML Committee of the Joint European Supervisory Authorities. The FCA also has over 40 memoranda of understanding with 130 overseas authorities and international bodies (including the IOSCO Multilateral Memorandum of Understanding). Overall, the FCA provided assistance to approximately 60 jurisdictions in 2016/17. However, the FCA should ensure timely responds to requests from foreign jurisdictions concerning passported entities and agents of UK payment institutions. HMRC co-operates well with foreign counterparts, largely on a bilateral basis or through attendance and participation at colleges of supervisors. The Gambling Commission co-operates with counterparts through forums and bilateral relationships, routinely sharing information on specific cases and best-practices. The Commission made 137 overseas inquiries in 2017. International co-operation by other supervisors is limited.

Box 37. **Co-operation between the FCA and overseas authorities**

A large UK firm is under close AML/CFT supervision by the FCA due to identified failings. The firm has global operations which require FCA supervisors to regularly engage with overseas authorities to enable supervisory co-operation and ensure consistent international supervision. This has included:

61 The UKFIU has since confirmed that the information sheet has been amended to better reflect the range of assistance the UKFIU is able to provide.

- regular engagement with a particular overseas authority to assess the firm's progress implementing an effective and sustainable global financial crime programme
- liaising with overseas authorities to facilitate onsite visits in their jurisdictions and share the resulting findings
- working with a specific overseas authority to assess and share findings on the firm's AML/CFT controls in one of its higher risk business lines, and
- sharing with overseas authorities the findings from in-depth reviews of AML/CFT controls in their respective jurisdictions.

In addition, senior management of relevant authorities and the FCA have met with the firm to ensure consistency in messaging and their regulatory approach.

International exchange of basic and beneficial ownership information of legal persons and arrangements

494. The UK generally has good access to basic and BO information (see Chapter 7 on IO.5) and can provide this information to foreign jurisdictions in a timely manner upon request. However, foreign LEAs may be directed to the public PSC register for BO information, whereas UK LEAs would typically corroborate this information with BO information from financial institutions and DNFBPs where available (see Chapter 7 on IO.5). Where the information is not available from the PSC register, the UK can provide assistance using other sources. The assessment team's findings were based on: discussions with the central authorities, LEAs and the private sector; feedback from FATF and FSRB delegations; and case studies.

495. The UK authorities advised that foreign requests for basic and BO information on legal persons/arrangements are common. Where relevant, the UKFIU and certain LEAs will direct requests for information on legal persons to the public PSC register. In doing so, the requesting agency is not advised that to obtain *verified* BO information it is necessary to seek such information from the relevant FI or DNFBP via a request for formal or informal co-operation. This may result in authorities relying on unverified information (see Chapter 7 on IO.5).

496. Where the requested information is not publicly available on the PSC register, it can be obtained through a request to Companies House (for information on legal persons), to HMRC (for information on trusts), or to the relevant LEA (for information held by FIs or DNFBPs where available). These requests can generally be answered in a timely fashion, with non-urgent requests to Companies House and financial institutions typically receiving a response within two weeks.

497. Overseas legal persons and arrangements feature prominently in UK law enforcement activity. All UK LEAs noted the importance of obtaining basic and BO information to support investigations of ML and serious predicate offences in the UK. The UK recently entered into an agreement with eight Crown Dependencies and Overseas Territories with financial centres to provide LEAs, including tax authorities, with BO information of companies registered in their jurisdiction within 24 hours

(one hour in urgent cases). These agreements remain new, but LEAs including the NCA and SFO are already noting improved co-operation and timely exchange of information, as well as a decrease in cases featuring these jurisdictions. The UK is also advocating the construction of public central registers to collect BO information.

Overall conclusions on IO.2

498. **The UK has achieved a substantial level of effectiveness for IO.2.**

TECHNICAL COMPLIANCE ANNEX

1. This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerological 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.

2. 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 2007. 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 3rd MER.

Criterion 1.1 – The UK identifies and assesses its ML//TF risks through its National Risk Assessment (NRA) process. This includes an overview of the most prevalent proceeds-generating predicate offences in the UK (with indications of how the proceeds of different offences are laundered), the UK's exposure to cross-border ML/TF risks, as well as the risks of different relevant sectors of the UK economy being used to launder these proceeds. The NRA is an overarching assessment of other relevant risk assessments including, but not limited to, the NCA's Annual Strategic Assessment of Serious and Organised Crime, the NCA's annual Economic Crime Strategic Assessment, the Joint Terrorism Analysis Centre's (JTAC) TF Threat Assessment and the EU's supranational ML/TF risk assessment.

Criterion 1.2 – HMT and the Home Office are required to identify and assess the ML/TF risks for the UK via its NRA process (MLRs, reg.16). A wide range of internal and external stakeholders provide input to the assessment of risks by participating in the Anti-Money Laundering Working Group and the Money Laundering Advisory Committee, in particular the NCA (including the FIU), other law enforcement agencies, HMRC, supervisors and private sector representatives. The NRA also includes input from all of England, Wales, Scotland and Northern Ireland. The NCA has responsibility for developing a consolidated picture of all threats related to serious and organised crime and also works with the private sector through the JMLIT to identify and share information on ML/TF risk.

Criterion 1.3 – The first NRA was published in October 2015 and a second NRA was published in October 2017. HMT and the Home Office are required to take appropriate steps to ensure that the risk assessment is kept up to date (MLRs, reg.16). Other government agencies (including the NCA) produce multiple assessments each year on areas of high risk.

Criterion 1.4 – The UK's NRA is a public document and the results are available to all relevant competent authorities and SRBs, FIs and DNFBPs. HMT and the Home Office are also required to provide the NRA to the UK parliament, relevant supervisory authorities, the European Commission and the European Supervisory Authorities (MLRs, reg.16).

Criterion 1.5 – The UK Government must ensure that the NRA is used to consider the appropriate allocation and prioritisation of resources being used to counter ML/TF. This includes ensuring that the NRA identifies areas of low risk, areas of high risk (where enhanced customer due diligence apply), and reviewing the appropriateness of rules made by supervisory authorities in light of the ML/TF risks identified (MLRs, reg.16(2)-(3)). In 2016, the UK also developed an AML/CFT Action Plan which addresses some of the key ML threats and vulnerabilities identified in the NRA. Prioritisation of resources at an operational level occurs through the National Strategic Tasking and Coordination Group which has a Money Laundering Strategic Action Plan. Allocation of resources in relation to national security (including terrorism and terrorist financing) occurs under the Strategic Defence and Security Review, the last of which occurred in 2015.The UK has also demonstrated that it monitors emerging ML/TF risks and considers appropriate mitigation measures, for example, in relation to virtual currency exchange providers (see R.15).

Criterion 1.6 – In relation to exemptions from the FATF Standards:

(a) In most cases, where there is proven low risk, the UK applies limited and justified exemptions for a number of categories of entities when they are carrying out activities that may fall under the MLRs. This includes, for example, registered societies (when issuing withdrawable share capital or accepting deposits) and local authorities providing limited financial services (MLRs, reg.15).

The UK has an exemption on undertaking CDD for electronic money (e-money) in specific circumstances which are assessed (including in both NRAs) to present lower risks of ML/TF (i.e. limited re-loadability and lack of anonymity) (MLRs, reg.38). The 2017 MLRs have reduced the thresholds above which CDD must be applied (from EUR 2 500 to EUR 250, or EUR 500 if the funds must be used in the UK) given the elevation of TF risk from low to medium between the 2015 NRA and the 2017 NRA.

(b) The UK has one exemption in place for high-value goods dealers engaging in financial activity on an occasional or very limited basis such that there is a low risk of ML/TF (for example, annual turnover of less than GBP 100 000 and customers are limited to transactions of less than EUR 1 000 be that individual or linked payments) (MLRs, reg.15(1f–3)). This exemption is in line with the Recommendations which require dealers in precious metals and stones to be covered only when engaging in a cash transaction with a customer equal to or above EUR 15 000.

Criterion 1.7 – (a) The UK requires FIs and DNFBPs to take enhanced measures to manage and mitigate higher risks (including in relation to correspondent banking and PEPs) (MLRs, regs.33-35). (b) The UK also requires that FIs and DNFBPs document their risks and incorporate information on higher risks into their risk assessments (MLRs, reg.18).

Criterion 1.8 – The UK allows FIs and DNFBPs to apply simplified due diligence measures when they have identified a low-risk relationship or transaction. The FI or DNFBP's assessment of low-risk must take into account its supervisors' risk

assessment which in turn must take into account the country's assessment of risks (MLRs, regs.37, 17 and 18). The MLRs also provide guidance on what may be considered as a low risk factor and, in some cases, these factors are not based on an assessment of risks (see c.10.18).

Criterion 1.9 – Supervisors and SRBs are required to ensure that FIs and DNFBPs are implementing their obligations under R.1 (MLRs, reg.46(4a)). See analysis of R. 26 and R. 28 for more information.

Criterion 1.10 – FIs and DNFBPs are required to take appropriate steps to identify, assess and understand their ML/TF risks (for their customers, the countries or geographic areas in which they operate, their products and services, their transactions and their delivery channels). This includes being required to:

a) document their risk assessment (MLRs, regs.18(4) & 18(6));

b) consider all relevant risk factors in determining the level of overall risk and the relevant mitigation measures (MLRs, regs.18(2) & 19);

c) keep their assessments up to date (MLRs, reg.18(4)); and

d) have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs (MLRs, reg.18(6)).

Criterion 1.11 – FIs and DNFBPs are required to:

a) have risk mitigation polices, controls and procedures in place which are approved by senior management and are monitored and enhanced as necessary (MLRs, reg.19)

b) see 1.11(a) above, and

c) take enhanced measures to manage and mitigate higher risks that are identified (see analysis of c.1.7).

Criterion 1.12 – The UK allows simplified due diligence measures where low-risk has been identified (see analysis of c. 1.9) and criteria 1.9 to 1.11 are met. Simplified due diligence is not permitted when the FI or DNFBP suspects ML or TF (MLRs, s.37(8c)).

Weighting and Conclusion

There is a minor deficiency in relation to guidance provided in the MLRs about potential lower risk situations (e.g. clients or businesses based in the EU) which are not based on risk. This is considered a minor deficiency as FIs must nevertheless weigh a number of factors before applying simplified CDD. **Recommendation 1 is rated largely compliant.**

Recommendation 2 - National Cooperation and Coordination

In its 3rd MER, the UK was rated compliant with these requirements. While the main ministerial-level bodies have continued to operate, some of the mechanisms for national cooperation and coordination have changed since 2007.

Criterion 2.1 – The UK's Strategic Defence and Security Review (2015), Counter-Terrorist Finance Strategy and the Action Plan for AML/CFT (April 2016) are the main

national AML/CFT policies and are informed by identified risks. ML and TF policies are regularly reviewed and kept up to date through regular meetings of the Money Laundering Advisory Committee, the Money Laundering Working Group and through Ministerial oversight committees. The Strategic Defence and Security Review, and the resulting CONTEST strategy, are reviewed regularly and guide the allocation of resources for counter-terrorism (CT) initiatives, including CFT, and the CFT Strategy is reviewed annually by the Home Office. Policy in relation to domestic terrorism threats in Northern Ireland is the responsibility of the Secretary of State of Northern Ireland with Northern Ireland's input being provided through Ministerial oversight bodies.

Criterion 2.2 – HMT and the Home Office share responsibility for AML/CFT policy. HMT leads the regulation of businesses and working with domestic supervisors. The Home Office leads the law enforcement response.

Criterion 2.3 – For the AML strategy, the ministerial-level Criminal Finances Board (CFB) provides leadership and direction on AML policy and is supported by the official-level Money Laundering Working Group. At an operational level, the National Strategic Tasking and Coordination Group (which includes the NCA, police forces across the UK, HMRC, the Security Services and the Border Force) has a ML Strategic Action Plan (SAP) and a Criminal Finance Threat Group which is responsible for coordinating tactical activity against the ML risks identified in the SAP.

The Home Office leads on the UK's CFT strategy and CFT policy is part of the UK's broader CT strategy (CONTEST). Similar to the CFG, for TF issues, there is a ministerial-level Terror Finance Board chaired by the Minister for Security, and attended by senior representatives of relevant policy ministries, law enforcement, intelligence agencies and charities regulators, which sets the policy direction and the Terrorist Finance Board (officials) that provides support. The Terror Finance Board reviews and approves the TF strategy and oversees its implementation.

Domestic terrorism in Northern Ireland falls under the responsibility of the Secretary of State of Northern Ireland and there are a range of mechanisms (the Strategic Oversight Group, Operational Coordination Group, Tackling Paramilitaries Taskforce) which aid policy and operational co-ordination on domestic terrorism and organised crime issues.

Criterion 2.4 – The UK's counter proliferation financing policies are coordinated under the UK's National Counter Proliferation Strategy is the responsibility of the Foreign Secretary and is supported by the interagency Cross-Whitehall Sanctions Group. At a working level, the Restricted Enforcement Unit, the Cross-White Hall Sanctions Group (Working Level) and the Economic Sanctions Enforcement Group coordinate on a range of operational counter-proliferation issues. Where specific enforcement issues arise, these are pursued by the relevant national agencies (e.g. OFSI or the NCA), in conjunction with local police forces.

Weighting and Conclusion

All criteria are met. **Recommendation 2 is rated compliant.**

Recommendation 3 - Money laundering offence

In its 3rd MER, the UK was rated compliant with these requirements.

Criterion 3.1 – The UK has three offences in the Proceeds of Crime Act 2002 (POCA) which criminalise ML in line with the Vienna and Palermo Conventions and apply to all jurisdictions of the UK:

a) Concealing etc.: This offence applies to any person who conceals, disguises, converts, transfers or removes from the UK any criminal property (s.327)
b) Arrangements: This offence applies where a person enters into or becomes concerned in an arrangement which he knows or suspects will facilitate another person to acquire, retain, use or control criminal property (s.328)
c) Acquisition, use and possession: This offence applies where a person acquires, uses or possesses criminal property (s.329)

Criterion 3.2 – The ML offences cover all offences under UK law or conduct which would constitute an offence in the UK if it had occurred there (POCA, s.340(2)).

Criterion 3.3. – The UK does not apply a threshold approach.

Criterion 3.4 – The ML offences extend to any property "wherever situated and includes money; all forms of property, real or personal, heritable or moveable; things in action and other intangible or incorporeal property", which constitutes or represents the benefit of crime "in whole or part and whether directly or indirectly" (POCA, s.340(3)).

Criterion 3.5 – When proving that property is the proceeds of crime, there is no requirement that a person be convicted of a predicate offence (POCA, ss.327-329, 340).

Criterion 3.6 – The ML offences apply to all conduct which occurred in another country and which would have constituted an offence in the UK if it had occurred there (POCA, s.340(2)). It is a defence if the person knew, or reasonably believed, that the conduct was lawful under local law *and* the conduct would have constituted an offence punishable by less than 12 months' imprisonment (POCA, ss.327(2A), 328(3), 329(2A); POCA (Money Laundering Exceptions to Overseas Conduct Defence) Order 2006).

Criterion 3.7 – The ML offences apply to any person, including those who commit the predicate offence. It is "immaterial who carried out the [predicate offence]" (POCA, ss.327-329; 340(4)).

Criterion 3.8 – For all three POCA ML offences, proof of knowledge and intent can be inferred from objective factual circumstances (*R v Anwoir and others* (2008)).

Criterion 3.9 – Proportionate and dissuasive criminal sanctions apply to natural persons convicted of ML. The ML offences are punishable by up to 14 years' imprisonment, an unlimited fine, or both (POCA, s.334).

Criterion 3.10 – Criminal liability and proportionate, dissuasive sanctions apply to legal persons convicted of ML, without prejudice to the criminal liability of natural persons. Legal persons are punishable by an unlimited criminal fine (POCA, ss.327-329, 334; Interpretation Act 1978, sch.1).

Criterion 3.11 – A specific ML offence applies to those who enter into or become concerned in an arrangement that facilitates ML (POCA, s.328). Specific legislation and common law cover conspiracy, attempts, aiding and abetting, and incitement

(Criminal Attempts Act 1981, s.1; Northern Ireland Criminal Attempts and Conspiracy Order 1983; Criminal Law Act 1967, s.1; Accessories and Abettors Act 1861, s.8; Serious Crime Act 2015, Part.2; Criminal Procedure (Scotland) Act 1995, ss.293, 294).

Weighting and Conclusion

All criteria are met. **Recommendation 3 is rated compliant.**

Recommendation 4 - Confiscation and provisional measures

In its 3rd MER, the UK was rated compliant with these requirements.

Criterion 4.1 – The UK has measures enabling it to confiscate property whether held by criminal defendants or by third parties:

(a) Laundered property can be confiscated upon conviction (criminal confiscation) or without conviction (civil forfeiture). Civil forfeiture permits the recovery of property valued over GBP 10 000 (POCA, ss.6, 92, 156, 243, 244, 266, 287).

(b) Property directly or indirectly obtained through ML or predicate offences can be confiscated under either the criminal or civil regime (POCA, ss.6, 92, 156, 266). The confiscation of instrumentalities used or intended for use in ML and relevant predicates is broadly permitted by a range of miscellaneous provisions (e.g. Misuse of Drugs Act 1971, s.27; Serious Crime Act 2015, ss.26, 61; Forgery and Counterfeiting Act 1981, s.7; Modern Slavery Act, s.11).

(c) Property used or intended for use in terrorism offences or that was received as payment or reward for terrorism offences can be confiscated under the normal criminal or civil regimes, or under an alternative regime which permits confiscation of such property from individuals convicted of a relevant terrorism-related offence (Terrorism Act 2000 (TACT), ss.23-23B). Cash may also be confiscated if it was intended for TF, represents the assets of a terrorist organisation, or is or represents property obtained through terrorism (Anti-terrorism, Crime and Security Act 2001 (ATCSA), s.1).

(d) Both the criminal and civil confiscation regimes permit the UK to confiscate property of corresponding value to laundered property or criminal proceeds. Under the criminal confiscation regime, if the prosecution can prove that the defendant had a "criminal lifestyle", there is a presumption that any property transferred to the defendant in the six years prior to criminal proceedings or held by the defendant at any time after conviction is subject to confiscation (POCA, s.10, 142, 223).

Criterion 4.2 – The UK has measures that enable its competent authorities to:

- **a)** Identify, trace and evaluate property that is subject to confiscation through disclosure, production, customer information, account monitoring, and unexplained wealth orders; as well as powers of entry, search and seizure (POCA, ss.345, 352, 357, 362A, 363, 370, 380, 387, 391, 396A, 397, 404; Criminal Finances Act 2017, ss.1, 4; Serious Organised Crime and Police Act 2005 (SOCPA), ss.62, 66; TACT, sch.5, 5A, 6, and 6A).
- **b)** Restrain or freeze property that is subject to confiscation to preserve the property and prevent its transfer or disposal prior to a decision on confiscation or forfeiture (restraint: POCA, ss.41, 120, 190, 362J; Criminal

Finances Act 2017, ss.2, 5; Police and Criminal Evidence Act 1984 (PACE), ss.8, 19, 22; seizure: POCA, ss.47C, 127C, 195C; civil orders: 245A, 255A).

c) Take steps to prevent or void actions (whether contractual or otherwise) taken to prejudice the ability to freeze or recover property that is subject to confiscation. The courts have the legal authority to take such decisions. Confiscation and related proceedings are governed by due judicial process.

d) Take other appropriate investigative measures through the powers described in R.31.

Criterion 4.3 – UK laws protect the rights of bona fide third parties (POCA, ss.9, 95, 159, 266, 281, 308; TACT, s.23B).

Criterion 4.4 – The UK has mechanisms in place to manage and, where necessary, dispose of frozen, seized and confiscated property. This includes the ability to appoint a management receiver to take possession, manage, and deal with the property or an insolvency practitioner to protect creditors (POCA, ss. 48, 49, 125, 196, 197; TACT, sch.4).

Weighting and Conclusion

All criteria are met. **Recommendation 4 is rated compliant.**

Recommendation 5 - Terrorist financing offence

In its 3rd MER, the UK was rated compliant with these requirements.

Criterion 5.1 – The UK's TF offences cover the conduct criminalised in art.2 of the UN Convention for the Suppression of TF (TF Convention). The UK criminalises the provision, receipt, and invitation to provide money or other property with the intent or reasonable suspicion that it may be used for the purposes of terrorism (TACT, s.15). It is also an offence to enter into or become concerned in an arrangement which results in money or property being made available to another, where the person knows or suspects that it may be used for the purposes of terrorism (TACT, s.17). An activity is "for the purposes of terrorism" where (a) there is an act or threat of serious violence, property damage, life endangerment, health or safety risks, or serious electronic interference; (b) the act or threat is designed to intimidate, or influence a government or international body (unless firearms or explosives are used); and (c) the act or threat is committed with the purpose of advancing a political, religious, racial or ideological cause (TACT, s.1). All activities covered by the Conventions and Protocols in the Annex to the TF Convention have been criminalised. The funding of these activities can be pursued as a TF offence where the activity was committed "for the purposes of terrorism" and the necessary elements are met. Where this is not the case, the funding of these activities would be criminalised as aiding and abetting of the criminal act.

Criterion 5.2 – The UK's TF offences extend to any person who provides or collects money or other property, or becomes involved in an arrangement that makes money or property available, with the intent or reasonable suspicion that that it may be used, for the purposes of terrorism (TACT, ss.1, 15, 17). This includes fundraising for the benefit of a proscribed terrorist group (TACT, s.1, 15). The low level of intent required ("reasonable cause to suspect") means the offences cover the provision or collection

of money or property, directly or indirectly, for use, in full or in part, by an individual terrorist or terrorist group, whether or not it is linked to a specific terrorist act (*R v Majdi Shajira* (2015); *R v Hana Khan* (2015); *R v Golamaully and Golamaully* (2016)).

Criterion 5.2*bis* – The UK criminalises the preparation of terrorist acts, terrorist training, and terrorist financing (TACT, ss.5, 6-8, 15-18). The wording of these offences and the courts' application of them in practice suggests they are sufficiently broad to cover financing the travel of individuals who travel to another jurisdiction for the purpose of perpetrating, planning, preparing, or participating in terrorist acts or terrorist training (*R v Mohammed Kahar* (2015)).

Criterion 5.3 – TF offences apply to money or "other property", which is given a broad definition, covering any property "wherever situated and whether real or personal, heritable or moveable, and things in action and other intangible or incorporeal property" (TACT, s.121). This definition would appear to cover any funds or other assets whether from a legitimate or illegitimate source.

Criterion 5.4 – The UK's TF offences do not require that the funds or other assets were actually used to carry out or attempt a terrorist act or were linked to a specific terrorist act; it is sufficient that it is intended or reasonably suspected that the funds could be used for this purpose (TACT, s.1, 15, 17).

Criterion 5.5 – The prosecution can prove intent or reasonable suspicion as required for TF offences by relying on inferences from objective factual circumstances (*R v Hana Khan* (2015); *R v Mohammed Kahar* (2015)).

Criterion 5.6 – Natural persons convicted of a TF offence are punishable by proportionate and dissuasive criminal sanctions of up to 14 years' imprisonment, an unlimited fine, or both (TACT, s.22).

Criterion 5.7 – Criminal liability and proportionate, dissuasive sanctions apply to legal persons convicted of a TF offence, without prejudice to the criminal liability of natural persons. Legal persons are punishable by an unlimited criminal fine (TACT, s.22; Interpretation Act 1978, sch. 1).

Criterion 5.8 – The broad nature of the UK's TF offences would largely cover attempts. Specific legislation and common law cover conspiracy, attempts, aiding and abetting, and incitement (Criminal Attempts Act 1981, s.1; Northern Ireland Criminal Attempts and Conspiracy Order 1983; Criminal Law Act 1967, s.1; Accessories and Abettors Act 1861, s.8; Serious Crime Act 2015, Part.2; Criminal Procedure (Scotland) Act 1995, ss.293, 294).

Criterion 5.9 – TF offences are ML predicate offences (POCA, s.340(2)). There is also a specific ML offence in TACT which creates an offence for a person to enter into or become concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property by concealment, removal from the jurisdiction, transfer to nominees, or in any other way (TACT, s.18).

Criterion 5.10 – The UK's TF offences apply regardless of whether the defendant was in the same country or a different country from the one in which the terrorist or terrorist organisation is located, or where the terrorist act occurred or will occur (TACT, s.1(4)).

Weighting and Conclusion

All criteria are met. **Recommendation 5 is rated compliant.**

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

In its 3rd MER, the UK was rated compliant with these requirements. New legislative provisions were introduced under the Terrorist Asset-Freezing Act 2010 in relation to 1373 listings which replaced the Terrorism (United Nations Measures) Order 2006 previously assessed under the 3rd MER.

Criterion 6.1 – For designations under UNSCRs 1267/1989 and 1988 ("UN sanctions regimes"):

a) The Foreign and Commonwealth Office (FCO) is the competent authority responsible for proposing designations to the UN via the UK Mission to the UN.

b) There is an MOU that serves as a mechanism for identifying targets for designation. The MOU allows operational agencies to propose targets which are reviewed against the UNSCR criteria by HMT, FCO and operational partners.

c) The evidentiary standard of proof applied to a designation proposal is a 'reasonable suspicion' of association with the relevant terrorist organisation. The decision is not conditional on the existence of a criminal proceeding.

d) Submissions are made using the UN standard forms and procedures for listing.

e) In its submissions, the FCO, in liaison with operational partners, provides unclassified information supporting the basis for the designation and usually allows its status as a designating state to be made known.

Criterion 6.2 – The UK implements designations pursuant to UNSCR 1373 through both national and European mechanisms. The national mechanism is found in the Terrorist Asset-Freezing etc. Act ("TAFA") and the EU mechanism via CP 2001/931/CFSP and Council Regulation 2580/2001:

a) For the national system, HMT, through its Office of Financial Sanctions Implementation (OFSI), is the competent authority for making designations under section 2 of the TAFA. This provision has also been used to make designations at the request of other countries, if the relevant statutory test in the TAFA is met.

For the EU mechanism, the FCO, in consultation with NTFIU, HMT, Home Office and the intelligence agencies, is responsible for proposing designations to the EU Council. The EU Council is responsible for deciding on the designation of persons or entities (Regulation 2580/2001 and Common Position 2001/931/CFSP) and relies on a prior decision of a competent authority (for example, for the UK a prior decision could be a decision made under TAFA or a proscription made under TACT).

b) A similar process to the one described under c.6.1(b) sets out the process for identifying targets for designation based on the UNSCR 1373 criteria.

c) Concerning requests received from operational partners in the UK, HMT convenes a meeting with key partners to discuss the merits of the proposed designation, including if they 'reasonably believe' that the criteria in the TAFA are met and a designation can be made promptly. Concerning requests received under the EU listing regime, the CP 931 Working Party62 at the EU Council verify that there is a reasonable basis for the designation against the criteria in UNSCR 1373.[63]

d) As set out above in c.6.3(c), the evidentiary threshold for the national mechanism ('reasonable belief') and the EU mechanism ('reasonable grounds') are in line with the Standard.

e) When requesting another country to give effect to freezing mechanisms, the UK supplies as much identifying and supporting information as possible. The UK has made a number of freezing proposals to the EU under the CP931. At the European level, there is an alignment procedure that allows for requesting non-EU member countries to give effect to the EU list.

Criterion 6.3 –

a) HMT has an MOU in place to solicit relevant information from operational partners on potential designations. Operational partners can use the powers outlined under R.31 to collect or solicit information to identify persons and entities that may meet the criteria for designation.

b) Authorities are implicitly permitted to operate ex parte against a person or entity who has been identified and whose designation is being considered as the TAFA does not require that the person in question be present or consulted during the designation process. EU designations must take place 'without prior notice' (*ex parte*) being given to the person or entity identified.[64] The UN Sanctions Committees also operate on an ex parte basis when making designations.

Criterion 6.4 – Designations pursuant to the UN sanctions regimes are implemented in the UK without delay. While the UK implements the sanctions through EC regulations (which do give rise to delay in implementation), the UK has supplemented this system by allowing all UN sanctions to be immediately effective in the UK for a period of up to 30 days or until the EU adds the new listings to an existing sanctions regulation (Policing and Crime Act 2017, ss.154-155).

The national designation mechanism under the TAFA implements TFS without delay by taking immediate legal effect as criminal penalties apply immediately for breaches of these financial restrictions (s.32). The EU-only mechanism is implemented by

62 'Common Position 2001/931/CFSP on the application of specific measures to combat terrorism Group. All Council CP working parties are comprised of representatives of the EU Member States' governments.

63 The criteria in Common Position 2001/931/CFSP comply with those in UNSCR 1373.

64 EC Reg.1286/2009 para. 5 of the Preamble and art.7a(1).

Council regulations (taken in application of Regulation 2580/2001) that are implemented immediately and directly into UK law. As a result, these sanctions are implemented 'without delay'.

Criterion 6.5 – The following standards and procedures apply for implementing and enforcing TFS:

a) All natural and legal persons in the UK,[65] and UK nationals or bodies constituted under UK Law wherever they are located, are required to freeze the funds or economic resources of a designated person, without delay and without prior notice (TAFA, ss.10-15, 18 & 32-34; EC Regulations 881/2002 art.2(1), 1286/2009 art.1(2), 753/2011 art.3, 754/2011 art.1 and 2580/2001 art.2(1a)). See also analysis of c.6.3-6.4.

b) Freezing actions pursuant to the TAFA, and at the EU level (under the 1267/1989 and 1988 regime), apply to funds or economic resources owned, held or controlled, directly or indirectly, by a designated person/entity (TAFA, s.11; EC regulation 881/2002, art.2; EC regulation 753/2011, art.3). This extends to interest, dividends and other income on or value accruing from or generated by assets (TAFA, s.39; see definition of funds in the EC regulations, art.1). There is no express application to funds or assets belonging to people who are acting on behalf of, or at the direction of, designated persons/entities. To some extent, this is met by the requirement to freeze funds or assets "controlled by" a designated entity (EC regulation 881/2002, art.2; TAFA, s.11).

For UNSCR 1373, the freezing obligation in EU regulation 2580/2001 (art.1(a) and art.2(1)(a)) applies to assets belonging to, owned or held by the designated individual or entity, and does not expressly apply to funds or assets controlled by, or indirectly owned by, or 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 addressed as the European Council is empowered to designate any legal person or entity controlled by, or acting on behalf of, a designated individual or entity (EU regulation 2580/2001, art.2(3) (iii) and (iv)).

Neither the TAFA nor the EU regulations expressly require the freezing of jointly owned assets. In line with EU guidance, OFSI defines ownership as 50% or more of the proprietary rights of another entity or a majority interest in the entity. OFSI's non-binding guidance clarifies that in practice, jointly-held assets may be frozen particularly if there is a risk that funds or assets will become available to a designed person or entity (FAQs - 1.1.7 and 3.1.14).

c) All natural and legal persons in the UK, and UK nationals or bodies constituted under UK Law wherever they are located, are prohibited from making funds or economic resources available (directly or indirectly) to or for the benefit of, a designated person, except under license or where a statutory exemption

65 A 'person' in UK Law applies equally to natural and legal persons with regard to criminal liability.

is in place (TAFA, ss.12-15; EC Regulations 881/2002 art.2(2), 753/2011 art.3(2)). In the case of TAFA, the prohibition also includes financial services.

d) OFSI has mechanisms in place to communicate designations (and any changes to the lists) to FIs and DNFBPs including publication in its consolidated list of financial sanctions targets on the gov.uk website. The communication does not always occur immediately but usually happens within one business day (which can take up to three to four calendar days). When OFSI is aware that UK FIs or DNFBPs have dealings with a person due to be designated, OFSI communicates with these businesses immediately (before the consolidated list is updated) to ensure they are aware of the asset freeze. OFSI provides an email notification service for this website which updates its 21 000 subscribers. OFSI provides clear guidance to FIs and DNFBPs on their obligations by answering frequently asked questions on the gov.uk webpage.

e) FIs and DNFBPs are required to report any assets frozen or actions taken in related to designed persons or entities (Council Regulation (EU) 2016/1686, art.10; Council Regulation (EC) No 881/2002, art.5). In addition, if FIs or DNFBPs have reasonable cause to suspect that a person is a designated person and that person is a customer of their institution, they must also state the nature and amount or quantity of any funds or economic resources held by them for that customer (Schedule 1 ISIL (Da'esh) and Al-Qaida (Asset-Freezing) Regulations 2011, schedule 1; European Union Financial Sanctions (Amendment of Information Provisions) Regulations 2017; TAFA, s.19).

f) The rights of bona fide third parties are protected under the EU sanctions regime (Regulations 881/2002 art.6; 753/2011 art.7). Under TAFA, there are no specific provisions to protect the rights of bona fide third parties. They may have protection under common law against any external challenges provided they had implemented the asset freeze as per their legal requirements.

Criterion 6.6 – The following de-listing, unfreezing and access procedures apply:

a) The UK, in the OFSI Financial Sanctions Guidance, has highlighted the procedure for submitting de-listing requests to the UNSC, either directly to the UN Office of the Ombudsperson or via the UK (section 8.1). The FCO has a mechanism in place to submit de-listing requests to the UN Sanctions Committees after coordinating with law enforcement and security and intelligence agencies and seeking a ministerial decision.

b) TAFA designations expire after 12 months unless renewed (TAFA, s.4). If a designation no longer meets the statutory test, it is revoked and a formal notice issued on the gov.uk website. For 1373 designations, the EU has de-listing procedures under its 'working method'.[66] De-listing is immediately effective and may occur ad hoc or after mandatory 6-monthly reviews.

c) There are procedures to allow, upon request, review of the TAFA designation and related decisions before the High Court (TAFA, s.26 & 27). Designations under the EU's 1373 regime may be challenged through the Court of Justice of the EU. A listed individual or entity can write to the Council to have the designation reviewed or can challenge the relevant Council Regulation, a

66 http://data.consilium.europa.eu/doc/document/ST-10826-2007-REV-1/en/pdf

Commission Implementing Regulation, or a Council Implementing Regulation in Court, per the Treaty on the Functioning of the European Union (TFEU), article 263 (4)). Article 275 also allows legal challenges of a relevant CFSP Decision.

d) For 1267/1989 and 1988, designated persons/entities are informed of the listing, its reasons and legal consequences, their rights of due process and the availability of de-listing procedures including the UN Office of the Ombudsperson (UNSCR 1267/1989 designations) or the UN Focal Point mechanism (UNSCR 1988 designations). At the EU level, there are procedures that provide for de-listing names, unfreezing funds and reviews of designation decisions by the Council of the EU (EC Regulation 753/2011, art.11; EC Regulation 881/2002, art.7a). These procedures are set out in the OFSI guide to financial sanctions.

e) See (d) above.

f) There are publicly known procedures (available on the OFSI website) for obtaining assistance in verifying whether persons or entities having the same or similar name as designated persons or entities (i.e. a false positive) are inadvertently affected by a freezing mechanism.[67] Where the guidance does not clarify the issue, OFSI can provide assistance.

g) HMT communicates EU/UN de-listings or HMT revocations of designations under TAFA, by reflecting this change in its consolidated list of financial sanctions targets within one business day. The notification does not occur immediately and can take up to three to four calendar days. Subscribers to this site receive notification of this change.

Criterion 6.7 – HMT operates a licencing system to allow designated persons or entities access to funds (TAFA, s.17). In practice, HMT grants licences on the basis of the criteria set out in UNSCR 1452. The UK has requested, and received, blanket approval from the UN 1267 Committee for basic needs licences. At the EU level, there are procedures in place to authorise access to frozen funds or other assets which have been determined, amongst others, to be necessary for basic expenses, for the payment of certain types of expenses, or for extraordinary expenses pursuant to UNSCR 1452 (EC Regulations 753/2011, art.5; 881/2002, art.2a).

Weighting and Conclusion

The fundamental technical aspects of the regime are in place which, most importantly, enables freezing without delay. However, there are minor deficiencies in relation to a number of criteria. The requirement to freeze assets that are jointly owned is not expressly stated in the regulations or legislation although guidance assists to provide some clarity on the issue. The communication of designations by OFSI is not immediate (although the legal requirement to freeze occurs immediately). Under the domestic listing mechanism, there are no specific provisions in law to protect the rights of bona fide third parties. **Recommendation 6 is rated largely compliant.**

67 EU Best Practices for the effective implementation of restrictive measures and OFSI Financial Sanctions Guidance (August 2017), section 8.4 on mistaken identity.

Recommendation 7 – Targeted financial sanctions related to proliferation

This is a new Recommendation which was not assessed in the 3rd MER report.

Criterion 7.1 – UN financial sanctions are implemented by way of EU Regulations which take direct effect in the UK. UNSCR 1718 on DPRK is transposed into the EU legal framework through EC Regulation 2017/1509 and Council Decision 2016/849/CFSP. UNSCR 2231 on Iran is transposed into the EU Legal framework through EC Regulation 267/2012 as amended by EC Regulations 2015/1861 and 1862. The UK has enacted additional legislation to ensure that financial sanctions occur 'without delay' by making sure that new UN sanctions listings can have immediate effect in the UK for 30 days, or until the EU adds the new listings to an existing sanctions regulation, whichever is sooner (Policing and Crime Act 2017, ss.154-155).

Criterion 7.2 – The OFSI in HMT is the competent authority responsible for implementing TFS in the UK.

a) EU Regulations require all natural and legal persons within the EU to freeze the funds or other assets of persons or entities designated under the EU's anti-proliferation regimes. These regulations are supplemented by domestic instruments which make it an offence for all natural and legal persons within the country not to freeze assets pursuant to the EU's anti-proliferation measures (the *Iran SI* and the *DPRK SI*).

b) The EU regulations prohibit dealing with funds or economic resources owned, held or controlled by a designated person, and prohibit making funds, financial services and economic resources available to a designated person or for their benefit. The same prohibitions, with the exception of the explicit prohibition on the provision of financial services, are given effect by regulations in the UK (*Iran SI* & *DPRK SI*, regs.3-7). The freezing obligation under the EU framework extends to all types of funds (EC Regulation 329/2007, art.1(4) & 6; EC Regulation 267/2012, art.1(l) & 23(1-2)). This requirement extends to funds or assets that are owned, held or controlled by a designated person/entity (see for example, EC Regulation 329/2007, art.6(1). Further non-binding OFSI Guidance notes that where there is an evidenced causal link, the requirement to freeze the funds or assets 'controlled' by a designated person also extends to and the funds or assets belonging to people who are acting on behalf of or at the direction of designated persons/entities [OFSI FAQs 1.1.7 and 3.1.14]. Neither the UK nor the EU regulations expressly require the freezing of jointly owned assets. However, OFSI provides guidance on the freezing of jointly-owned assets (see analysis of c.6.5(b)).

c) Under the relevant EU and UK regulations, the prohibition to prevent funds, financial services and economic resources being made available applies to UK nationals and any other legal person, or entity, incorporated or constituted under UK law. This applies to anyone residing or located in the UK and UK nationals living overseas (The Iran (European Union Financial Sanctions) Regulations 2016, reg.1; The Democratic People's Republic of Korea (European Union Financial Sanctions) Regulations 2017; reg.1).

d) OFSI uses the same mechanisms described in criterion 6.5(d) to communicate designations and any changes to the lists and the same deficiencies apply in relation to communication of PF designations.

e) FIs and DNFBPs must immediately provide to the competent authorities all information to facilitate compliance with the EU regulations, including information about the frozen accounts and amounts (Council Regulation (EU) 2017/1509, art.50; Council Regulation (EU) 267/2012, art.40). In addition, FIs and DNFBPs are required to report to the HMT if they know or suspect that a person is a designated person or has done something in contravention of the TFS regime (*Iran SI*, schedule pursuant to reg.16; DPRK SI, schedule pursuant to reg.29). These provisions are sufficiently broad to cover reporting on attempted transactions.

f) The rights of bona fide third parties are protected by the relevant EU regulations which are directly applicable in the UK (Council Regulation (EU) 2017/1509, art.50; Council Regulation (EU) No 267/2012, art.42).

Criterion 7.3 – Financial institutions and DNFBPs are required to report to OFSI if they know or have reasonable cause to suspect that their customer is a designated person or that a breach has occurred, or if they have frozen funds under the relevant regulations. OFSI also has powers to request information from relevant institutions or designated persons in relation to sanctions evasion. It is a criminal offence to breach the freezing and prohibition of the provision of funds and the information gathering and information disclosure provisions in the statutory instruments which carry criminal penalties of between 3 months and 2 years in prison (Iran SI, regs.11(4), 13(3), 19 and the schedule; DPRK SI, regs.24, 26, 29 and the schedule).

Supervisors do not have an express obligation to monitor and ensure compliance by FIs and DNFBPs with proliferation financing sanctions. Supervisors consider this to be part of the broader supervisory system in terms of requirements on higher risk countries and can apply sanctions if the relevant MLR regulations are not adhered to (see analysis of R.26-28). For example, under the Financial Services and Markets Act 2000 (FSMA), the FCA is required to give regard to the importance of minimising the extent to which regulated firms and individuals could be used for the purpose of carrying out financial crime – this includes violations of financial sanctions obligations. Other supervisors currently rely on very general supervisory functions to check sanctions compliance but this would benefit from further clarification and consistency.

Criterion 7.4 – The UK has developed and implemented publicly known procedures to submit delisting requests to the Security Council where the relevant person no longer meets the criteria for designation.

a) The UK, in the OFSI Financial Sanctions Guidance, has highlighted the procedure for submitting de-listing requests to the UNSC, either directly to the focal point or via the UK (section 8.1). The EU Council communicates its designation decisions and grounds for a listing to designated persons, who have the right to request a review of the EU decision independently of whether a request is made at UN level (Treaty on the Functioning of the European Union (TFEU), in the fourth paragraph of art. 263 & 275).

b) There are publicly known procedures (available on the OFSI website) for obtaining assistance in verifying whether persons or entities having the same or similar name as designated persons or entities (i.e. a false positive) are inadvertently affected by a freezing mechanism.[68] Where the guidance does not clarify the issue, OFSI can provide assistance.

c) HMT operates a licencing system to allow designated persons or entities access to funds as required by EU Regulations 267/2012 and 2017/1509 which are enforced in UK law through UK Statutory Instrument (SI) 2016 No.36 and UK SI 2017 No.218 (most recently amended by SI 2017 No.999).

d) HMT communicates EU/UN de-listings by reflecting this change in its consolidated list of financial sanctions targets within one business day. The notification does not occur immediately and can take up to three to four calendar days. Subscribers to this site receive notification of this change.

Criterion 7.5 – With regard to contracts, agreements or obligations that arose prior to the date on which accounts became subject to targeted financial sanctions:

a) The European regulations permit the payment to the frozen accounts of interests or other sums due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that these amounts are also subject to freezing measures (Art.34 Regulation 2017/1509 and Art.29 Regulation 267/2012).

b) Provisions authorise the payment of sums due under a contract entered into prior to the designation of such person or entity, provided that this payment does not contribute to an activity prohibited by the regulation, and after prior notice is given to the UN Sanctions Committee (Art. 25 Regulation 267/2012).

Weighting and Conclusion

The fundamental technical aspects of the regime are in place which, most importantly, enables freezing of proliferation-related assets without delay. However, there are minor deficiencies in relation to a number of criteria. The requirement to freeze assets that are jointly owned or indirectly controlled by designated persons is not is not expressly stated in the regulations or legislation although guidance assists to provide some clarity on the issue. The communication of designations by OFSI is not immediate (although the legal requirement to freeze occurs immediately) and most supervisors, other than the FCA, rely on very general provisions to undertake checks on sanctions compliance, which would benefit from further clarification and consistency.

Recommendation 7 is rated largely compliant.

68 EU Best Practices for the effective implementation of restrictive measures and OFSI Financial Sanctions Guidance (August 2017), section 8.4 on mistaken identity.

Recommendation 8 – Non-profit organisations

In its 3rd MER, the UK was rated largely compliant with the requirements relating to NPOs. As the requirements in Recommendation 8 have changed considerably since then, the 3rd round analysis is no longer relevant.

Criterion 8.1 –

(a) The UK has identified its charity sector, comprising 380 000 entities, as falling within the FATF definition of NPO. Of these, 80% are based in England. The charity sector broadly aligns with the FATF definition of NPOs, encompassing institutions which raise or disburse funding for a broad range of charitable purposes, including religious, cultural, educational, or communal, which serve the public interest.

The UK's 2017 NRA includes a chapter on NPOs which identifies NPOs as generally being low risk for both ML and TF (a decrease from the 2015 NRA, which identified the sector as medium-high risk for TF). A Domestic Sector Review of the charity sector was completed in 2017 to identify the features and types of charities most at risk of TF abuse. These assessments drew on information from NPO regulators and relevant government departments, as well as published information and analysis. The Charity Commission for England and Wales (CCEW) has also analysed its casework to provide further information on risk. Together, these efforts have enabled the UK to conclude that a small number of recently-established charities remain at higher risk—specifically, those that are based in three specific regional areas of England, operating internationally in certain high-risk countries, and using operating methods common amongst small or medium-sized charities, such as delivery agents, cash couriers, and aid convoys.

(b) The UK has taken steps to identify the nature of TF threats to NPOs and how terrorist actors abuse those NPOs, including through ongoing assessments and case analysis. These efforts show that typical threats include: fundraising on behalf of a purported charity; generating and moving of terrorist funds by charity aid convoys; diversion of terrorist funds from charity aid convoys to terrorist activity; and theft from charities operating in high-risk areas.

(c) The UK has taken steps to review the adequacy of laws and regulations governing at-risk NPOs. The CCEW reviewed the Charities Act (England and Wales) 2006 in 2015. One goal of this review was strengthening the CCEW's powers to disqualify charity trustees to better counter the abuse of charities for terrorist purposes (Explanatory Note to the Charities Act 2016; Hansard HL vol.762, col.801, 803). No relevant reviews have been undertaken in Scotland or Northern Ireland.

(d) The UK periodically reassesses information on the NPO sector to ensure effective implementation of measures. Assessments of NPO-related TF risks have been undertaken in 2017 (the Domestic Sector Review), 2015 (as part of the NRA), and 2013 (to contribute to relevant FATF work).

Criterion 8.2 –

(a) The UK has policies to promote accountability, integrity, and public confidence in the administration and management of NPOs. The three charity regulators (the CCEW, the Charity Commission for Northern Ireland (CCNI), and the Office of the Scottish

Charity Regulator (OSCR)) have issued statements of their goals and policies to promote accountability, integrity and public confidence in the charities they regulate. To further enhance accountability and public confidence, CCEW, CCNI, and OSCR have each published a document explaining their respective approaches to regulating their sectors.

(b) All UK charity regulators have outreach and educational programmes to raise awareness of TF risks for NPOs and measures to prevent abuse. The CCEW is most active in this area, in line with the UK's identified risks, but the CCNI and the OSCR have also taken steps.

(c) The UK has consultation processes in place to work with NPOs to develop best practices and policies to address TF risks. For example, the Cabinet Office consulted charities during the 2014 review of the Charities Act; encouraged charities to participate in the FATF review of Recommendation 8; consulted charities on changes to the annual return process to combat abuse of the sector, including TF; and developed a Compliance Toolkit in collaboration with the charity sector.

(d) The charity regulators' outreach efforts have encouraged NPOs to conduct transactions via regulated financial channels. One chapter of the CCEW's Compliance Toolkit covers international and domestic fund transfers and encourages the use of regulated banking services where possible. Specific social media and website alerts from the CCEW also emphasise this message. The OSCR's Guidance and Good Practice for Charity Trustees includes a section on charity finances and encourages the use of regulated financial channels. The OSCR and the CCNI have also provided links to the CCEW guidance encouraging the use of regulated financial channels, and specific guidance (e.g. for charities operating in Syria) also highlights the importance of using regulated financial channels. In early 2018, the charity regulators issued a joint regulatory alert on the importance of using regulated financial channels. This was published on their respective websites and promoted on social media.

Criterion 8.3 – The CCEW, the CCNI, and the OSCR are responsible for monitoring and supervising charities. All charities are required to register with the relevant supervisor except lower risk charities in England and Wales. Registers are public and include information on the trustees. Certain individuals are disqualified from acting as trustees; in England and Wales this includes those convicted of terrorism or ML. Charities must file an annual return and financial statement unless they operate in England and Wales and earn less than GBP 10 000. Charity trustees must keep accounting records of all income and expenditure (Charities Act 2011, ss.29, 30, 130-134, 145, 163, 170, 178; Charities Act (Northern Ireland) 2008, ss.16, 65, 68, 86; Charities and Trustee Investment (Scotland) Act 2005, s. 44). All fundraising activities must comply with strict requirements (Code of Fundraising Practice)).

Criterion 8.4 –

(a) The charity regulators are responsible for monitoring charities' compliance with registration and accounting requirements. The CCEW conducts proactive monitoring of higher-risk charities including on-site compliance checks. The CCNI and the OSCR tend to monitor in response to allegations of non-compliance, although both agencies also identify certain high-risk charities or classes of charity. Monitoring may include on-site compliance checks at charity offices, meeting trustees and/or staff, obtaining and reviewing financial information or internal control procedures; reviewing online

activity etc. The UK Fundraising Regulator monitors fundraising practices in response to complaints. In Scotland, the Scottish Fundraising Standards Panel is responsible for considering fundraising complaints that are unresolved following consideration by the relevant charity.

(b) Charities in the UK are liable to effective, proportionate, and dissuasive sanctions for violations of their obligations. Depending on the violation, sanctions can include freezing accounts, deregistration, and unlimited criminal fines (Charities Act 2011, ss.34, 41, 60, 75A, 76, 79, 80, 84B, 173, 181A, 183; Charities Act (Northern Ireland) 2008; ss.16, 19, 25, 33, 71, 134, 150-158; Charities and Trustee Investment (Scotland) Act 2005, ss.6, 30, 31, 34, 45, 70, 83).

Criterion 8.5 –

(a) The UK has policies in place to ensure effective co-operation, co-ordination and information-sharing amongst appropriate authorities holding relevant information on NPOs. Charity regulators are able to share information with each other and law enforcement and have established contact points (Charities Act 2011, ss.54-59; Charities Act (Northern Ireland) 2008, ss.24; Charities and Trustee Investment (Scotland) 2005, s.24). Any suspicions of TF must be reported to law enforcement (Terrorism Act 2000, s.19). The charities regulators meet twice annually at the UK Charity Regulators Forum and the CCEW also participates in inter-agency TF working groups.

(b) The charity regulators have the expertise and capability to perform initial examinations of NPOs suspected of TF before the matter is passed to law enforcement, which has the necessary expertise to conduct a full examination. The CCEW has specialist officers to deal with suspected TF and works closely with TF investigative units in relevant law enforcement agencies.

(c) All charity regulators are able to obtain full access to information on the administration and management of particular NPOs. This includes powers to: obtain information and evidence; order production; freeze property; and restrict transactions. The CCEW is also able to undertake searches (Charities Act 2011, ss.47, 48, 52, 76; Charities Act (Northern Ireland) 2008, ss.22, 23, 33; Charities and Trustee Investment (Scotland) 2005, s.29, 31, 34).

(d) Any individual who through the course of their work (paid or voluntary) develops a suspicion or belief that a terrorism offence has been committed must report this to law enforcement (Terrorism Act 2000, s.19). The CCEW, the CCNI, and the OSCR have all put in place Serious Incident Reporting regimes which require charity trustees to report any allegations of abuse, including TF abuse. These reports are promptly shared with law enforcement where relevant.

Criterion 8.6 – The charity regulators are identified as the appropriate points of contact for information on NPOs. Each regulator is able to respond to domestic and international information requests from public authorities, provided that the sharing is not restricted on data protection or human rights grounds (Charities Act 2011, ss.54-59; Charities Act (Northern Ireland), s.24; Charities and Trustee Investment (Scotland) 2005, s.24; Data Protection Act 1998; Human Rights Act 1998). The CCNI has a MOU with its counterpart in the Republic of Ireland to facilitate information-sharing between the two agencies. This information-sharing also exists in addition to

the UK's MLA processes (see R.37). It is also possible for international agencies to directly access the public charity registers.

Weighting and Conclusion

All criteria are met. **Recommendation 8 is rated compliant.**

Recommendation 9 – Financial institution secrecy laws

In its 3rd MER, the UK was rated compliant with these requirements. The detailed analysis set out at paragraphs 617 – 625 of the 3rd MER continues to apply.

Criterion 9.1 – There are no financial institution secrecy laws that inhibit the implementation of AML/CFT measures in the UK.

(a) *Access to information by competent authorities*: English common law sets out a bank's duty of confidentiality and states that there are four exemptions to an FI's duty to not disclose client information, including where disclosure is under exemption by law (i.e. under a court order or a statutory requirement to provide information) (Decision of the Court of Appeal in *Tournier v National Provincial and Union Bank of England* [1924] 1KB 461). Analysis under R.27, 29 and 31 sets out the statutory powers available to competent authorities to request information from FIs, which were strengthened in 2017.

(b) *Sharing of information between competent authorities:* A range of mechanisms exist to exchange information between agencies at an operational level (see analysis of R.2) and there are no financial institution secrecy laws that inhibit this sharing. Information sharing between competent authorities also occurs at an international level (see analysis of R.40).

(c) *Sharing of information between FIs*: There are no financial institution secrecy laws that restrict the sharing of information between financial institutions where this is required by R.13, 16 or 17. Since June 2017, all wire transfers must contain information on a customer's name, address and account number (EC Regulation No. 847/2015). Financial institutions are also able to share information between themselves and law enforcement via the NCA, as long as the disclosure is relevant to the functions of the NCA which include combatting serious or organised crime (Crime and Courts Act, s.7(1)). Information shared by institutions and individuals under this framework does not breach any obligation of confidence owed by the person making the disclosure (Crime and Courts Act, s.7(8)). A voluntary disclosure regime is also available under the Criminal Finances Act 2017 which allows the sharing of information between regulated entities under certain conditions where that information will or may assist in detecting money laundering (s.11 which inserts s.3339ZB into the Proceeds of Crime Act 2002).

Weighting and Conclusion

The criterion is met. **Recommendation 9 is rated compliant**.

Recommendation 10 – Customer due diligence

In its 3rd MER, the UK was rated partially compliant with these requirements. The deficiencies related to a lack of clear obligations or actions required in terms of: doubts about previously obtained customer ID data; identification and verification of the beneficial owner; authorisation of persons acting on behalf of the customer; identifying the purpose and nature of the business relationship; undertaking ongoing monitoring and keeping CDD data up-to-date; dealing with CDD in relation to existing customers; and terminating a business relationship if proper CDD cannot be conducted.

Under R.10, the principle that FIs should conduct CDD should be set out in law. In the case of the UK, the Money Laundering Regulations are secondary legislation made under the powers conferred through the European Communities Act 1972. The regulations are secondary legislation that has been approved by parliament, is legally binding and impose mandatory requirements with civil and criminal sanctions. The MLRs therefore have the same legal force as primary legislation.[69]

Criterion 10.1 – FIs are prohibited from keeping anonymous accounts or passbooks (MLRs, reg.29(6)&(7)).

Criterion 10.2 – FIs are required to undertake CDD measures when:

- **a)** Establishing business relations;
- **b)** Carrying out an occasional transactions above the threshold of EUR 1 000 (which is stricter than the applicable threshold in the FATF Recommendations of EUR 15 000 but does not include situations where transactions are carried out in several, linked transactions which is appropriate given the stricter threshold);
- **c)** Carrying out occasional transactions that are wire transfers covered under R.16;
- **d)** There is a suspicion of ML/TF; or
- **e)** There is a doubt about the veracity or adequacy of previously obtained customer ID data (MLRs, reg.27(1) & EU Regulation 2015/847).

Criterion 10.3 – FIs are required to identify the customer (whether permanent or occasional, a natural or a legal person) and verify its identity using reliable, independent source documents, data or information (MLRs, regs.28(2)&(18) and 27(1)).

Criterion 10.4 – FIs are required to verify that any person purporting to act on behalf of the customer is so authorised and are also required to verify the identity of that person (MLRs, reg.28(10)).

Criterion 10.5 – FIs are required to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information

69 The Sanctions and Anti-Money Laundering Act 2018, which passed through parliament in 2018, will provide the legislative basis for the UK's AML/CFT regime after the UK leaves the EU.

or data obtained from a reliable source, such that the financial institution is satisfied that it knows who the beneficial owner is (MLRs, reg.28(4)&(18)).

Criterion 10.6 – FIs are required to understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship (MLRs, reg.28(2c)).

Criterion 10.7 – FIs are required to conduct ongoing due diligence on the business relationship, including:

- **a)** scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the FI's knowledge of the customer, their business and risk profile, including where necessary, the source of funds (MLRs, reg.28(11a)); and
- **b)** ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant (MLRs, reg.28(11b). There is a more general requirement to apply enhanced ongoing monitoring in higher risk ML/TF cases (reg.33(1g)).

Criterion 10.8 – There is no explicit requirement to understand the ownership and control structure of customers that are legal persons. However, FIs are likely to collect some of this information as a step in identifying the customer's beneficial owners (see c.10.10) and non-binding JMLSG Guidance suggests that it is good practice to take reasonable measures to do so.

Legal arrangements cannot be customers in the UK as they do not have legal personality in their own right. In the example of a trust, the trustee would be the customer and the beneficial owner is the trust (or similar legal arrangement) and in this situation, there is a requirement to take reasonable measures to understand the ownership and control structure of the legal arrangement (MLRs, regs.28(2c) & (4b-4c)).

There is no explicit requirement for FI's to understand the nature of the customer's business. However, in certain circumstances this requirement may be implied within other obligations to assess whether a situation is high risk for ML or TF in order to know whether EDD must be applied (reg.33(6a)).

Criterion 10.9 – For customers that are legal persons, FIs are required to identify the customer and verify its identity through the following information (MLRs, reg.28(3)):

- **a)** name, legal form and proof of existence;
- **b)** the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons holding a senior management position in the legal person; and
- **c)** the address of the registered office and, if different, a principal place of business.

However, the requirement to identify and verify the names of senior managers is not absolute – FI's need only to take reasonable measures to determine and verify these details.

For legal arrangements, the MLRs do not explicitly cover the specific information required under points a) to c). However, as outlined in c.10.8, legal arrangements

cannot be customers in the UK; the trustee is the customer. If the trustee is a legal person, they will undergo the CDD process outlined above (MLR, reg.28(3)). If the customer is a natural person, no specific obligations apply in identifying the legal arrangement (MLRs, reg.28(2)). While there is a general requirement to understand the ownership and control structure of a trust, foundation or similar legal arrangement (reg.28(4c)), the specific information required under points a) to c) are not explicitly covered.

Criterion 10.10 – For customers that are legal persons, FIs are required to identify and take reasonable measures to verify the identity of beneficial owners by collecting the following information (reg.28(3-7)):

- **a)** the identity of the natural persons who ultimately has a controlling ownership interest in a legal person (defined as 25% of the shares of voting rights in the body corporate) (MLRs, reg.5); and
- **b)** the identity of the natural person(s) (if any) exercising control of the legal person through other means (the definition of beneficial ownership under reg.5 includes the concept of control); and
- **c)** where no natural person is identified under (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official (MLRs, regs.28(6) & (7)).

These requirements do not apply when the customer is listed on the regulated market (reg.28(5) which is consistent with footnote 33 of the Methodology).

Criterion 10.11 – For customers that are legal arrangements, FIs are required to identify and take reasonable measure to verify the identity of beneficial owners through (MLRs, reg.28(4)):

- **a)** for trusts, the identity of the settlor, trustees, beneficiaries or class of beneficiaries and any individual who has control over the trust (reg.6(1))
- **b)** for other types of legal arrangements, the identity of persons in equivalent or similar positions (reg.6(3)).

Criterion 10.12 – In the insurance context, in addition to the CDD measures required for the customer and the beneficial owner, FIs are required to conduct the following CDD measures on the beneficiary of life insurance and other investment related insurance policies, as soon as the beneficiary is identified or designated (MLRs, reg.29):

(a) for a beneficiary that is identified as specifically named natural or legal persons or legal arrangements – the name of the person (reg.29(3a));

(b) for a beneficiary that is designated by characteristics or by class or by other means – obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the pay-out (reg.29(3a));

(c) for both the above cases – the verification of the identity of the beneficiary should occur at the time of the pay-out (reg.29(4)).

Criterion 10.13 – While there is a general requirement for FI's to take into account customer risk factors in deciding whether to apply enhanced CDD (reg.33(6)), there is no specific requirement in the MLRs or in the industry guidance (non-binding JMLSG Guidance) for FIs to include the beneficiary of a life insurance policy as a relevant risk factor. Further, there is no specific requirement to take enhanced measures which include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of pay-out.

Criterion 10.14 – In general, FIs are required to verify the identity of the customer and the beneficial owner before establishing a business relationship or conducting transactions for occasional customers over EUR 1000 or over EUR 15 000 for HVDs and casinos (MLRs, reg.30(2) and reg.27). There are two exceptions to this general rule. First, FIs may complete verification during the establishment of the business relationship, provided that: **(a)** this occurs as soon as practicable after the contact is established; **(b)** this is necessary not to interrupt the normal conduct of business; and **(c)** there is little risk of ML/TF (reg.30(3)). Second, FIs may complete verification after an account has been opened provided that there are adequate safeguards in place to ensure that no transactions are carried out by or on behalf of the customer before verification has been completed (reg.30(4)).

Criterion 10.15 – There is no direct requirement that FIs should adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification. However, there is a general requirement that FI's develop risk management practices (MLRs, reg.19(3a)) and FIs are required to ensure that there are adequate safeguards in place to ensure that no transactions are carried out before the verification has been completed (reg.30(4)).

Criterion 10.16 – FIs are required to apply CDD requirements to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained (MLRs, regs.27(8) & 27(1d)).

Criterion 10.17 – FIs are required to perform enhanced due diligence where the ML/TF risks are higher (MLRs, reg.33(1)). A non-exhaustive range of risk factors are included in the regulations (reg.33(6)).

Criterion 10.18 – FIs are only permitted to apply simplified CDD measures where lower risks have been identified, through an adequate analysis of risks by the country or the financial institution (MLRs, reg.37(1)). However, the regulations also outline several factors that indicate lower risks that must be taken into account by FIs which include factors that are not based on an assessment of risk – for example, residence in the EEA is considered a low risk factor (see reg.37(3(a)(ii-iii) & 37(c)(i)). Nonetheless, the regulations put the onus on the FIs to make a determination on low risk and note that the presence of one or more risk factors may not always indicate that there is low risk of ML/TF in a particular situation. In addition, the simplified measures are required to be commensurate with the lower risk factors, and are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply (reg.37(2) & (8)).

Criterion 10.19 – Where an FI is unable to comply with relevant CDD measures, it is required to (MLRs, reg.31):

a) not open the account or perform the transaction and terminate the business relationship; and

b) consider making a SAR in relation to the customer.

Criterion 10.20 – In cases where FIs form a suspicion of ML/TF, and they reasonably believe that performing the CDD process will tip-off the customer, they are permitted not to pursue the CDD process if they file a SAR (MLRs, reg.28(15) & (15)).

Weighting and Conclusion

While most of the CDD measures put in place by the UK meet the FATF Standards, minor deficiencies exist: the requirement to understand a customer's ownership and control structure and business activity is not clear; the requirement to identify and verify the names of senior managers is not absolute (FIs are only required to take reasonable measures); the beneficiary of a life insurance policy is not specified as a potential risk factor and there is no specific requirement to take enhanced measures at the time of pay-out; and guidance on lower risks in relation to EEA members are not based on an assessment of risk. **Recommendation 10 is rated largely compliant**.

Recommendation 11 – Record-keeping

In its 3rd MER, the UK was rated compliant with these requirements.

Criterion 11.1 – FIs are required to maintain all necessary records on transactions, for at least five years following completion of the transaction (MLRs, reg.40). 'Carrying on a business in the UK' is defined broadly under the MLRs and includes both domestic and international transactions (reg.9).

Criterion 11.2 – FIs are required to keep all records obtained through CDD measures and supporting documents for at least five years following the termination of the business relationship or after the date of the occasional transaction (MLRs, reg.40). In addition, the FCA Handbook imposes a requirement on FIs to maintain 'adequate records' which includes information obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken (FCA Handbook, SYSC 3.2.20).

Criterion 11.3 – FIs must keep transaction records sufficient to enable the transaction to be reconstructed (MLRs, reg.40(2b)).

Criterion 11.4 – While there is no broad requirement requiring FIs to ensure that all CDD and transaction records are made available to authorities swiftly, these requirements are addressed under separate legal provisions which allow authorities to request information from FIs (see R.27, 29 & 31). For example, FIs must provide requested information to their supervisors, including CDD information and transaction records, within a 'reasonable period' of time which is specified by the supervisor on each request (MLRs, reg.66). Authorities can also seek a production order to obtain customer and transaction data from FIs. Once issued, FIs usually have seven days to serve the documents requested (POCA, s.345(5)).

Weighting and Conclusion

All criteria are fully met. **Recommendation 11 is rated compliant.**

Recommendation 12 – Politically exposed persons

In its 3rd MER, the UK was rated not compliant with these requirements as it did not have in place any enforceable obligations in relation to PEPs.

Criterion 12.1 – The UK does not distinguish between domestic and foreign PEPs. In relation to both foreign and domestic PEPs, their family members and close associates, in addition to performing the CDD measures under R.10, FIs are required to (MLRs, reg.35):

- **a)** put in place risk management systems to determine whether a customer or the beneficial owner is a PEP (reg.35(1)).
- **b)** obtain senior management approval before establishing (or continuing, for existing customers) such business relationships (reg.35(5a)).
- **c)** take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs (reg.35(5b)).
- **d)** conduct enhanced ongoing monitoring on that relationship (reg.35(5c) & 33(1d)).

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 (reg.35(12a) & (14h)).

Criterion 12.3 – The measures set out in c.12.1 apply to the family members and close associates of all types of PEPs (reg.35(1)).

Criterion 12.4 – In relation to life insurance policies, FIs must take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are PEPs or family members or close associates of PEPs (reg.35(6)). This must occur before any payment is made under the insurance policy and before benefit of the insurance policy is assigned, in whole or part, to another person (reg.35(7)). FIs are also required to inform senior management before the pay-out of the policy proceeds and to conduct enhanced scrutiny on the whole business relationship with the policyholder is scrutinised on an ongoing basis (reg.35(8)). There is no specific requirement in the MLRs to consider making a SAR when higher risks are identified but the general requirement to report suspicious activity (set out in R.20) applies. The non-binding JMLSG guidance informs insurance firms that the general requirement to report suspicious activity applies in circumstances where higher risks are identified (section 7.11 of Part 2).

Weighting and Conclusion

All criteria are met. **Recommendation 12 is rated compliant**.

Recommendation 13 – Correspondent banking

In its 3rd MER, the UK was rated not compliant with these requirements as there were no enforceable obligations pertaining to correspondent banking.

Criterion 13.1 – With regard to cross-border correspondent banking relationships and other similar relationships with a third country (i.e. non-EEA), financial institutions are required to (MLRs, reg.34(1a-1e)):

- **a)** gather sufficient information about a respondent institution to understand fully the nature of its business and use publicly available information the reputation of the institution and the quality of supervision to which it is subject (these provisions are sufficiently broad to identify whether it has been subject to ML/TF investigations or regulatory actions)
- **b)** assess the respondent institution's AML/CFT controls
- **c)** obtain approval from senior management before establishing new correspondent banking relationships, and
- **d)** document the respective responsibilities of each institution.

However, these measures apply only to respondent institutions outside the EEA. For correspondent banking relationships within the EEA, a risk-based approach is taken (MLRs, reg.33(2)). However, this is not in line with R.13 which requires that the above measures be applied to all cross-border correspondent banking relationships.

Criterion 13.2 – With respect to "payable-through accounts" held by customers of non-EEA respondent banks, FIs are required to satisfy themselves that the respondent bank has: **(a)** performed CDD obligations those customers; and **(b)** is able to provide relevant CDD information upon request of the correspondent bank (MLRs, reg.34(f)). This requirement does not apply to correspondent banking relationships within the EEA unless the correspondent deems the correspondent banking relationship is deemed to be high-risk (MLRs, reg.33(2)).

Criterion 13.3 – FIs are prohibited from entering into, or continuing, correspondent banking relationships with shell banks (MLRs, reg.34(2)). FI's must undertake EDD to satisfy themselves that respondent FIs do not permit their accounts to be used by shell banks (MLRs, reg.34(3)).

Weighting and Conclusion

Mandatory EDD measures regarding correspondent banking relationships apply only to respondent institutions outside the EEA. **Recommendation 13 is rated partially compliant**.

Recommendation 14 – Money or value transfer services

In its 3rd MER, the UK was rated largely compliant with these requirements. The deficiencies focused on effectiveness issues in relation to the adequacy of the supervisory regime and sanctions imposed, and concern about the lack of applicable requirements in relation to beneficial ownership, PEPs and transaction monitoring.

Criterion 14.1 – Natural or legal persons that provide MVTS are required to be registered by either the FCA or HMRC (whichever they are supervised by) and are subject to a fit and proper test (MLR, regs.54, 56 & 58).

Criterion 14.2 – HMRC, which undertakes the bulk of supervision of MVTS providers, undertakes analysis of providers that have not (but are required to be) registered and proactively contacts them to ensure that they either become registered or cease trading. Both HMRC and FCA have a range of enforcement powers when assessing non-compliance, including non-compliance with the requirement for an MVTS provider to be registered in order to operate. This includes the civil power to fine or publicly censure, impose temporary or permanent prohibitions on management and issue injunctions (MLRs, regs.76, 78 and 80). Criminal sanctions (imprisonment for up to two years and/or a fine) are also available for contravening requirements in the MLRs (reg.86).

Criterion 14.3 – MVTS providers are regulated as 'MSBs' under the MLRs and are subject to monitoring for AML/CFT compliance by both HMRC and FCA. All relevant AML/CFT regulations apply to MVTS providers (MLRs, reg.8 & 10, which apply parts 1-6 and 8-11 to MSBs). HMRC supervises the majority of MVTS providers. The FCA supervises financial institutions who also undertake MVTS activities.

Criterion 14.4 – MVTS providers are required to provide a list of their agents' full names and addresses to the FCA or HMRC with their registration application. There is no express requirement for MVTS providers to maintain a current list of agents which is accessible to competent authorities in in the UK and countries outside of the UK where the MVTS's agents operate. However, once the MVTS provider is registered, it is required to inform the registering authority of any 'material change' affecting any matter contained in their application for registration within 30 days of the change and this includes any changes in agents (MLRs, regs.57(2i) & 57(4)). The FCA also requires MSB agents to be registered. MVTS providers are also required to have systems which enable them to respond fully and rapidly to enquiries from any law enforcement authority so agent details are available to law enforcement on request (MLRs, reg.21(8)). Agents of authorised payment institutions and small payment institutions cannot provide services through an agent unless the agent is included on the register (Payment Services Regulations 2017, reg.34(1)).

Criterion 14.5 – MVTS providers are required to establish and maintain AML/CFT programmes and ensure that they are being complied with through the organisation, including subsidiaries and branches (MLRs, regs.19-20). HMRC guidance for MSBs also includes agents in this requirement. Penalties for regulatory breaches can apply to agents as well as to principals.

Weighting and Conclusion

All criteria are met. **Recommendation 14 is rated compliant**.

Recommendation 15 – New technologies

In its 3rd MER, the UK was rated compliant with these requirements.

Criterion 15.1 – In relation to new technologies, the UK has identified and assessed the risks associated with new payment methods (electronic money, virtual currencies

and crowdfunding) in its 2015 and 2017 NRAs and in separate assessments by the FCA, NCA and HMRC and through fora such as the Criminal Finances Board and the Terrorist Finance Board. The UK acknowledges the inherent vulnerabilities associated with the anonymity of VCs, and while the risk of ML/TF in this area is assessed as low, the UK acknowledges that there are intelligence gaps and VCs are being used in illicit activity (particularly in online marketplaces for the sale and purchase of illicit goods and services). As a result, the UK intends to regulate virtual currency exchange providers under its implementation of the EU's fifth Anti-Money Laundering Directive.

FI's are required to have polices, controls and procedures to assess ML/TF risks for new technologies that are being adopted (MLRs, reg.19(4c)). Non-binding JMLSG Guidance advises firms to apply this to new products and business products and delivery mechanisms and the use of new or developing technologies for both new and pre-existing products (JMLSG Guidance, para 4.23).

Criterion 15.2 –

(a) and **(b)** FIs are required to assess relevant ML/TF risks, in preparation for and during the adoption of new technology and to take measures to mitigate any ML/TF risks (MLRs, reg.19(4c)). The non-binding JMLSG Guidance clarifies that this must occur prior to the launch of new products, business practices or the use of new or developing technologies. There is also a requirement that FIs, in considering whether to apply EDD, consider if new products, business practices or delivery mechanism are used (MLR, reg.33(6)).

Weighting and Conclusion

The UK has assessed the risks associated with new technologies and there is a requirement for FIs to have polices, controls and procedures to assess ML/TF risks for new technologies, however there is no requirement on FIs to assess the risks of new products and business products and delivery mechanisms, although this is covered in non-binding guidance.

Recommendation 15 is rated largely compliant.

Recommendation 16 – Wire transfers

In its 3rd MER, the UK was rated partially compliant with these requirements. The key technical compliance deficiencies included the failure to apply the requirements within the EU and an ineffective sanctions regime. The UK has implemented new requirements under EU Regulation 2015/847 which came into force in the UK on 26 June 2017.

Criterion 16.1 – FIs are required to ensure that all cross-border wire transfers[70] of EUR 1 000 or more are accompanied by **(a)** the required and accurate originator information (name, account number, address, official personal document number, customer ID number or date and place of birth), and **(b)** beneficiary information

70 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.

(name and account number) (EU Regulation 2015/847, art.4). If the transaction is not made from/to a payment account, a unique transaction identifier is required rather than the account number (art.4(3)).

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).

Criterion 16.3 – All transfers of below EUR 1 000 are required to be accompanied by the required originator and beneficiary information (EU Regulation 2015/847, art.6(2)).

Criterion 16.4 – Originator information provided for transactions of less than EUR 1 000 need not be verified, unless 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)).

Criterion 16.5 and 16.6 – For domestic wire transfers (which in this case also includes intra-EU wire transfers), ordering FIs need to provide only the payment account numbers (or unique transaction identifiers) with the transfer. The ordering FI must be able to provide complete information on the originator and the beneficiary, if requested by the beneficiary FI, within three working days which is consistent with the second part of criterion 16.5 and criterion 16.6. There is also a general obligation for FIs to respond to requests from authorities on originator and beneficiary information (EU Regulation 2015/847, arts.5 & 14).

Criterion 16.7 – The ordering and beneficiary FIs are required to retain information on the originator and the beneficiary for five years (EU Regulation 2015/847, art.16).

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 originator and beneficiary information that accompanies it (EU Regulation 2015/847, art.10).

Criterion 16.10 – (*Not applicable*) 'Technical limitations' cannot be used to justify an exception to the requirement in Article 10 of the EU Regulation 2015/847 to send the beneficiary all the information about the originator and the beneficiary received with the transfer of funds. Accordingly, this criterion is not applicable to the UK.

Criterion 16.11 – Intermediary FIs are required to take reasonable measures, that are consistent with straight-through processing, to identify cross-border wire transfers that lack originator or beneficiary information (EU Regulation 2015/847, art.11).

Criterion 16.12 – Intermediary FIs are required to have risk-based procedures for determining (a) when to execute, reject, or suspend a wire transfers that lack the required originator and beneficiary information and for taking the appropriate follow up action (EU Regulation 2015/847, art.12).

Criterion 16.13 – The beneficiary FI is required to detect whether the required information on the originator or beneficiary is missing (EU Regulation 2015/847, art.7).

Criterion 16.14 – The beneficiary FI is required to verify the identity of the beneficiary of cross-border wire transfers of over EUR 1 000 and maintain this information for 5 years (EU Regulation 2015/847, art.7 & 16).

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 originator or required beneficiary information; and (b) the appropriate follow up action (which could include reporting to authorities in cases of routine failure to provide information) (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, art.2(1)).

Criterion 16.17 –

- **a)** EU Regulation 2015/847 requires all payee and intermediary institutions to take into account information from both sides as a factor when assessing whether an STR has to be filed.
- **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 EU permissions for intra-group sharing of STR data (see 18.2(b)), MVTS providers are obliged to report in the countries of the ordering and beneficiary sides of the transaction. In addition, relevant to EU passporting, EU Directive 2015/849 requires compliance officers 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 (Art. 33).

Criterion 16.18 – All natural and legal persons in the UK, including FIs, are required to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities when conducting wire transfers (see analysis of R.6).

Weighting and Conclusion

All criteria are met. **Recommendation 16 is rated compliant.**

Recommendation 17 – Reliance on third parties

In its 3rd MER, the UK was rated partially compliant with these requirements. Deficiencies related to the lack of a requirement to obtain relevant ID data from introducers and the lack of a requirement to assess another countries' compliance with AML/CFT standards before allowing introductions from those countries.

Criterion 17.1 – FIs are permitted to rely on third-parties to apply CDD measures of their behalf, but the FIs remain ultimately liable for any failure to apply such measures (MLRs, reg.39). Under the MLRs, FIs are required to:

- **a)** obtain immediately the necessary CDD information (reg.39(2a)).
- **b)** enter into an agreement with the third party to immediately obtain, on request, any identification data and any other relevant CDD documentation (reg.39(2bi)).

c) rely on the third-parties only if they are subject to the UK's MLRs or subject to the EU's 4AMLD and its compliance requirements (or equivalent requirements in another country) (reg.39(3)). Third parties are also required to retain copies of CDD data for 5 years in accordance with R.11 (reg.39(2bii)).

Criterion 17.2 – FIs are prohibited from engaging third-parties that are established in a country deemed high-risk by the EC. No other information of the level of country risk is required to be taken into account by FIs (MLRs, reg.39(4)). Further, reliance on members of the EU is not based on an assessment of the level of country risk.

Criterion 17.3 – A FI can rely on a third-party introducer which is part of the same financial group, if the following conditions exist (MLRs, reg.39(6)):

a) the group must apply CDD and rules on record-keeping and programmes against money laundering in accordance with the MLRs, the 4AMLD or rules of a similar effect which are largely in line with R.10-12 and 18.

b) the group must be supervised by an authority of an EEA state with responsibility for the implementation of the 4AMLD or another equivalent authority of a third country.

c) the group must mitigate any higher country risk through its AML/CFT policies (reg.20(4)).

While the key criteria of this section appear to be met, 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

The MLRs do not require FIs to have regard to all available information on country risk before engaging a third-party introducer, in particular, the permitted reliance on intermediaries within the EU is based on the presumption that all EU members have equivalent AML/CFT standards for R.10 and R.11, rather than on individual country risk assessments undertaken by the authorities. **Recommendation 17 is rated largely compliant.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In its 3rd MER, the UK was rated largely compliant with the internal control requirements and not compliant with the foreign branches and subsidiaries requirements. There were no measures in place covering foreign branches and subsidiaries and in relation to internal controls, no direct requirement for firms to maintain an independent audit function and no screening procedures for employees.

Criterion 18.1 – FIs are required to implement programs against ML/TF, which have regard to the ML/TF risks and the size of the business, and which include the following internal policies, procedures and controls (MLRs, part 9):

a) Nominate an officer responsible for the FI's compliance with the MLRs at the management level, where appropriate with regard to the size and nature of its business. This should be a member of the board of directors (or if there is no board, its equivalent management body) or one of its senior management (reg.21(1a)). The FCA Handbook, which all firms are required to take into

account (reg.21(10b)), requires firms (other than sole traders) to appoint a nominated officer.

b) Carry out screening procedures to ensure high standards when hiring employees (reg.21(1b)). The high standards relate to the integrity of the person and their skills, knowledge and experience. In addition, the FCA applies a 'fit and proper' test in its authorisation process for persons in 'controlled functions' in firms, which includes being an ML reporting officer.

c) Ongoing employee training programmes (regs.24(1)(a)(ii) & 24(2-3)).

d) Establish an independent audit function to test the system (reg.21(1c)).

Criterion 18.2 – FIs are required to implement group-wide AML/CFT programmes which are applicable to all branches and majority-owned subsidiaries of the financial group (MLRs, reg.20(1a)). These include the measures in c18.1 (reg.20 &19(3b)) and:

a) Policies and procedures for sharing information required for preventing ML/TF (reg.20(b)). This broad provision is interpreted to include sharing of information for the purposes of CDD and ML/TF risk management but this is not explicit in the regulations nor in the guidance.

b) Authorities interpret the broad provision under reg.20(b) to mean that branches and subsidiaries must provide customer, account and transaction information to the parent undertaking for AML/CFT purposes. The 4AMLD states that information on suspicions that funds are the proceeds of criminal activity or are related to terrorist financing reported to the FIU shall be shared within the group, unless otherwise instructed by the FIU (EU Directive 2015/849, art.45(8)). In addition to the provision in the 4AMLD mentioned above in 18.2(a), institutions within the same group are exempted from SAR tipping off provisions if the institution to which a disclosure is being made is situated in the EEA or to a country imposing equivalent AML requirements (POCA, s.333B; TACT, s.21E). However, outside of sharing data in relation to suspicious transactions, in the absence of other details, it is not established that all the information required by criterion 18.2 (b) is covered

c) Adequate safeguards on the confidentiality and use of the information exchanged (art.20 (5)). The information must be shared as appropriate between the members of the group, subject to any restrictions on information sharing imposed by or under any enactment or otherwise.

Criterion 18.3 – FIs are required to ensure that their branches and subsidiaries outside of the EEA have in place AML/CFT measures that are comparable to those required in the UK to the extent permitted by the other state (MLRs, reg.20(3)). If the legislation of the other state does not permit the application of equivalent AML/CFT measures, the parent undertaking must notify its supervisor and take additional measures to handle the additional ML/TF risk (reg.20(4)). There are no similar provisions for branches and subsidiaries within the EEA. Instead, the parent undertaking must ensure that the subsidiary or branches follow the law of the other EEA state (reg.20 (2)).

Weighting and Conclusion

The UK meets most elements of R.18; however, the full scope of information to be exchanged under group-wide AML/CFT programmes is not clearly articulated in regulation or guidance and FI's are not required to ensure that their branches and subsidiaries in the EEA have in place similar AML/CFT measures to the UK based on the assumption that all EEA members have implement the 4AMLD adequately. These are minor deficiencies FIs met during the onsite appear to interpret information sharing requirements broadly and FIs appear to be applying UK AML/CFT standards when operating in other jurisdictions. **Recommendation 18 is rated largely compliant**.

Recommendation 19 – Higher-risk countries

In its 3rd MER, the UK was rated partially compliant with these requirements as FIs were not required to give special attention to risks emanting from countries which do not sufficiently apply the FATF Recommendations and there was no requirement for them to examine the background and purpose of such transactions and make the written findings available to authorities. The 2017 MLRs have introduced new requirements in relation to higher-risk countries.

Criterion 19.1 – FIs must apply EDD to business relationships and transactions with natural and legal persons (including FIs) from a 'high-risk third country' (MLRs, reg.33 (1b)). A 'high-risk third country' is defined as a country identified by the European Commission (4AMLD, art.9 (2)). 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 individual third countries, and this has included adopting the FATF public statement (4AMLD, art.9(4)); Commission Delegated Regulation 2016/4180). In addition, HMT issues an *Advisory Notice on Money Laundering and Terrorist Financing controls in Overseas Jurisdictions* to update FIs on the latest FATF lists when they are amended. The requirements in the MLRs do not extend to other EU countries (should they be identified by the FATF).

Criterion 19.2 – HMT has the power to direct FIs to apply counter-measures if called to do so by: (a) FATF; and (b) independently of any call by the FATF (Counter Terrorism Act 2008, s.62 and Schedule 7, Part 1, para.1(2)&1(3)). The types of requirements that can be imposed by the HMT directive and are consistent with INR19, include undertaking enhanced customer due diligence, ongoing monitoring, systematic reporting and limiting or ceasing business (Schedule 7, Part 3). However, the UK is not able to apply countermeasures within the EU (Schedule 7, para.1 (5)).

Criterion 19.3 – HMT publishes an advisory notice on *Money laundering and Terrorist Financing controls in higher risk jurisdictions* based on the EC and FATF's list of high-risk jurisdictions. This notice is updated immediately after the EC and FATF lists are published and HMT sends an email alert to subscribers of the HMT notices. The list reflects the latest advice by the FATF.

Weighting and Conclusion

The UK has mechanisms in place to apply counter-measures for higher-risk countries however these do not apply to EU countries. **Recommendation 19 is rated largely compliant.**

Recommendation 20 – Reporting of suspicious transaction

In its 3rd MER, the UK was rated compliant with these requirements.

Criterion 20.1 – If an FI suspects or has reasonable grounds to suspect that a person is engaged in ML or TF, it is an offence to fail to make a report to a nominated officer of the NCA or a constable (i.e. the FIU) (POCA 2002, ss.330(4), 331(4), 332(4), 339ZG(3); TACT 2000, ss.19(2)&(7B), 21A(4)). This obligation applies to all FIs and DNFBPs (POCA, Schedule 9; TACT, Schedule 3A). It is implied that the requirement to report suspicions in relation to ML also extends to suspicions of predicate offending.

The report must be made as soon as practicable, or reasonably practicable, after acquiring that knowledge or forming that suspicion, or acquiring those reasonable grounds to suspect, that the other person has been or is engaged in ML/TF. Assessors were satisfied that the 'as soon as reasonably practicable' threshold meets the requirement for SARs to be reported promptly once a suspicion is formed. While large banks met with at the onsite have a window of 30/60 days to undertake their own investigation prior to filing SARs, there is a requirement to report matters requiring immediate attention to the UKFIU and all banks confirmed that they report SARs as soon as they reach the threshold of suspicion.

Criterion 20.2 – FIs are required to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction. There are no minimum thresholds for reporting under the POCA or TACT and the relevant offences are broad enough to cover attempted transactions.

Weighting and Conclusion

All criteria are met. **Recommendation 20 is rated compliant.**

Recommendation 21 – Tipping-off and confidentiality

In its 3rd MER, the UK was rated compliant with these requirements.

Criterion 21.1 – FIs and their directors, officers and employees are protected by law from both criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU (POCA, ss.337-338; TACT, ss.20 & 21B). This protection is available for any authorised disclosure made in good faith, even if the person making the disclosure did not know what the underlying criminality was, and regardless of whether illegal activity actually occurred.

Criterion 21.2 – Financial institutions and their directors, officers and employees should be prohibited by law from disclosing the fact that an SAR or related information is being filed with the FIU (POCA, s.333A; POCA, s.21D). There are reasonable exceptions for sharing information within a financial group or between institutions within the EEA or with countries with equivalent AML/CFT requirements to facilitate intra-group information sharing, or concerning shared clients, or shared transactions or services, for the purposes of preventing ML or TF (POCA, ss.333B-D; TACT s.21E-G).

Weighting and Conclusion

All criteria are met. **Recommendation 21 is rated compliant**.

Recommendation 22 – DNFBPs: Customer due diligence

In its 3rd MER, the UK was rated partially compliant with these requirements for similar deficiencies set out under R.10.

Criterion 22.1 – DNFBPs are required to comply with the CDD requirements set out in Recommendation 10 in the following situations:

a) Casinos – which are holders of a casino operating licence under the Gambling Act 2005 and when its customers engage in financial transactions equal to or above EUR 2 000 (which is more stringent than the EUR 3 000 threshold in the Standards) (MLRs, reg.8(2h) & 27(5)). In order to track a customer's spend, casinos are required to link CDD information for a particular customer to the transactions that the customer makes (Gambling Commission guidance, part 6.3).

b) Real estate agents – when they are involved in transactions for a client concerning the buying and selling of real estate. The real estate agent is considered to enter a relationship with the purchaser (in addition to the seller) at the point when the seller accepts the purchaser's offer (MLRs, regs.8(2f) & 4(3)).

c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above EUR 10 000 (MLRs, reg.8(2g) & 14(1a)).

d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for, or carry out, transactions for their client concerning the buying and selling of real estate and business entities; managing of client money, securities or other assets; opening and management of bank, savings or securities accounts; organisation of contributions for the creation, operation or management of companies; creating, operating or management of trusts, companies, foundations or similar structures (MLRs, 8(1c-d) &12(1)).

e) Trust and company service providers when they perform such services as: forming companies or other legal persons; acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; or acting as (or arranging for another person to act as) a nominee shareholder for another person (MLRs, reg.8(1e) & 12(2)).

The deficiencies identified under R.10 also apply to DNFBPs.

Criterion 22.2 – DNFBPs are required to comply with the same record-keeping requirements as FIs under the MLRs – see analysis of R.11.

Criterion 22.3 – DNFBPs are required to comply with the same PEPs requirements as FIs under the MLRs – see analysis of R.12.

Criterion 22.4 – DNFBPs are required to comply with the same new technologies requirements as FIs under the MLRs – see analysis of R.15.

Criterion 22.5 – DNFBPs are required to comply with the same third-party reliance requirements as FIs under the MLRs – see analysis of R.17.

Weighting and Conclusion

Based on minor deficiencies identified in R.10, 15 and 17 which are equally relevant to DNFBPs, **Recommendation 22 is rated largely compliant**.

Recommendation 23 – DNFBPs: Other measures

In its 3rd MER, the UK was rated largely compliant with these requirements. For DNFBPs, there was no requirement to nominate a compliance officer, to undertake screening procedures, apply special attention to customers from countries that did not comply with the FATF Standards, examine the background and purpose of transactions and for authorities to make written findings.

Criterion 23.1 – DNFBPs are subject to the same SAR reporting requirements as FIs (see analysis of R.20). All DNFBPs are required to comply with the SAR requirements set out in Recommendation 20, subject to the following qualifications:

- **a)** Lawyers, notaries, other independent legal professionals and accountants – when, on behalf of, or for, a client, they engage in a financial transaction in relation to the activities described in criterion 22.1(d). There are exemptions for legal professional privilege which comply with footnote 48 (for example, POCA, s.330(6b); TACT, s.19(5-6)).
- **b)** Dealers in precious metals or stones – when they engage in a cash transaction with a customer equal to or above EUR 10 000.
- **c)** Trust and company service providers – when, on behalf or for a client, they engage in a transaction in relation to the activities described in criterion 22.1(e) (POCA, Schedule 9; TACT, Schedule 3A).

Criterion 23.2 – DNFBPs are required to comply with the same internal control requirements as FIs under the MLRs– see analysis of R.18.

Criterion 23.3 – DNFBPs are required to comply with the same higher-risk countries requirements as FIs under the MLRs – 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. The activities set out in c22.1 are covered under the POCA and TACT (POCA, schedule 9; TACT refers to the entities covered under the MLRs).

Weighting and Conclusion

Minor deficiencies in relation to R.18 and R.19 are equally relevant to DNFBPs. **Recommendation 23 is rated largely compliant.**

Recommendation 24 – Transparency and beneficial ownership of legal persons

In its 3rd MER, the UK was rated partially compliant with these requirements. The technical deficiencies were: adequate, accurate beneficial ownership information was not promptly available to competent authorities; legal ownership/control information on the company's registrar was not verified or reliable; and no measures to prevent misuse of share warrants for ML. The FATF standards in this area have been significantly strengthened since the 3rd MER.

Criterion 24.1 – The UK has mechanisms that identify and describe the different types, forms and basic features of legal persons. In addition to the types of legal persons registered with Companies House (reflected in Table 1 in Chapter 1), the UK also recognises other legal persons such as community benefit societies and co-operative societies as legal persons.

Information on the basic features of common legal persons (namely limited companies and partnerships), the process for their creation, and obligations for company records is also publicly available on gov.uk. Information on the features and obligations for societies is publicly available in the Co-operative and Community Benefit Societies Act 2014 and on the FCA website. The government also provides information online on obligations for companies and partnerships to obtain and record beneficial ownership information.

Criterion 24.2 – The UK's NRA assesses the ML/TF risks associated with all types of legal person operating in the UK. The National Crime Agency (NCA), the Joint Financial Analysis Centre (JFAC), and HMRC have also undertaken assessments of the ML/TF risks of legal persons in the UK based on their case experience. These reports conclude that where ML occurs, it will likely be conducted through UK legal persons, most commonly private limited companies and limited liability partnerships (although the numbers involved are only a tiny minority of the overall population).

Criterion 24.3 – Most legal persons (private companies limited by shares, private companies limited by guarantee, private unlimited companies, public limited companies, limited liability partnerships, and limited partnerships (including Scottish Limited Partnerships)) must be registered with Companies House (Companies Act 2006, s.7; Limited Liability Partnerships Act 2000, s.3; Limited Partnerships Act 1907, s.5). The Companies House registry is public and records: the name of the legal person; information on the form and status of the legal person; the address of the registered office; constitutional and governing documents; and director and member or partner details (Companies Act 2006, ss.9-13; Limited Liability Partnerships Act 2000, s.2; Limited Partnerships Act 1907, s.8).

Scottish General Partnerships are required to register with HMRC for tax purposes, but are otherwise not required to register.[71] These entities have not been identified as high risk nor featured in investigations. Nonetheless, they may be vulnerable to abuse due to their separate legal personality and the ability to have solely corporate partners.

71 This also applies to other UK General Partnerships, although these do not have legal personality.

Societies must register with the FCA and provide the society's: name, registered office, type and function, membership and voting rules, and name and address of members and secretary (Co-operative Societies and Community Benefit Societies Act 2014, ss.2, 14). Most of this information is publicly available on the FCA Mutuals Public Register, with the exception of members' addresses and the society's membership and voting rules.

Other types of company in the UK comprise at most 0.4% of companies in the UK and have not been identified as being high risk. These companies are not required to register, but are nonetheless subject to certain oversight requirements where they are undertaking economic activity; e.g. unregistered companies, companies incorporated by Royal Charter, non-Companies Act companies, and overseas companies with a presence in the UK are required to submit to Companies House various documents including company name, form, address, officers, and other basic information (Companies Act 2006, ss.1040, 1043).

Criterion 24.4 – Relevant legal persons must maintain the information set out in criterion 24.3 (Companies Act, ss.9-13; Limited Liability Partnerships Act 2000, s.2; Limited Partnerships Act 1907, s.8; Co-operative and Community Benefit Societies Act 2014, s.14). Private companies limited by shares, private companies limited by guarantee, private unlimited companies, and public limited companies must keep an up-to-date register of members or shareholders, including the number of shares held by each shareholder, categories of shares, and associated voting rights. This information must be kept at the company's registered office (which must be within the UK) or at Companies House. Companies House must be kept informed of the location of the information (Companies Act 2006, ss.9, 113-115). Most partnerships with legal personality must maintain information on the members or partners and notify Companies House of any changes (Limited Liability Partnerships Act 2000, ss.2, 3; Limited Partnerships Act 1907, ss.8, 9). This requirement does not apply to general partnerships registered in Scotland, except those whose members are exclusively limited companies. Societies must maintain a register of members and officers at their registered office in Great Britain of the Channel Islands (Co-operative and Community Benefit Societies Act 2014, s.30).

Criterion 24.5 – The UK requires legal persons to ensure that the information referred to in criteria 24.3 and 24.4 is accurate. For legal persons registered with Companies House, the information must be confirmed annually and Companies House must be informed of any changes within 14 or 15 days, depending on the information concerned. As the companies register is public, there is some public scrutiny of the information (Companies Act 2006, ss.26, 30, 87, 167, 276; Limited Liability Partnerships Act 2000, s.9; Limited Partnership Act 1907, s.9). Societies must inform the FCA of any changes in order for them to be affected and confirm this information during their annual returns (Co-operative and Community Benefit Societies Act 2014, ss.10-16, 77-78).

Criterion 24.6 – The UK utilises various mechanisms to ensure access to information on the beneficial ownership of a legal person:

Companies and partnerships are required to obtain and hold up-to-date information on "people with significant control" (PSCs) (Companies Act 2006, ss.790M; Limited Liability Partnerships (Register of People with Significant Control) Regulations 2016,

sch.1; Scottish Partnerships (Register of People with Significant Control) Regulations 2017, reg.17). This is largely consistent with the FATF definition of beneficial owner and captures: individuals who hold, directly or indirectly, 25% of the shares or voting rights in a company; individuals who hold, directly or indirectly, the right to appoint or remove a majority of the board of directors of the company; and individuals with a right to exercise, or who actually exercise, significant influence or control over the company (Small Business, Enterprise and Employment Act 2015, sch.3; Companies Act 2006, sch.1A).

Information on PSCs must be held by the legal person and registered with Companies House which maintains a public register of PSCs. PSCs have a corresponding obligation to inform the legal person of their status. Companies and partnerships with legal personality must obtain and register information on: the PSC's name, date of birth, and nationality; the place where the PSC usually lives; their service and usual residential address; the date they became a PSC in relation to the legal person; an indication of the nature of control over the legal person; and any restrictions on disclosing the PSC's information (Small Business, Enterprise and Employment Act 2015, s.81, sch.3; Companies Act 2006, sch.1A; Register of PSC Regulations 2016; Information about PSC (Amendment) Regulations 2017; Scottish Partnerships (Register of PSC) Regulations 2017). The UK has issued guidance for the different types of legal persons on the steps that should be taken to identify their PSCs. Legal persons have legal powers to request information on beneficial ownership (Companies Act 2006, ss.790D-J; Scottish Partnership (Register of People with Significant Control) Regulations 2017, regs.10, 11).

Companies with securities admitted to trading on a regulated market in the UK, EEA, or specified markets in Switzerland, the US, Japan and Israel are exempt from the requirement to register PSC information. These entities are subject to disclosure requirements under the EU Transparency Directive and equivalent regimes (EU Transparency Directive 2004/109/EC, arts.9-16; Register of PSC Regulations 2016, sch.1).

Societies are required to maintain a complete and up-to-date list of members and the FCA requires societies to submit the details of the members of their governing Committee or Board to the FCA as part of their annual return (Co-operative and Community Benefit Societies Act 2014, ss.89, 143). If a member of the society is a company or partnership, they hold and provide PSC information as outlined above. There is no requirement that a Committee member disclose if they are acting under another's control.

Financial institutions and DNFBPs are also required to identify and take reasonable measures to verify beneficial owners as part of their customer due diligence requirements (MLRs, regs.8(2), 12(2), 28(4)).

Criterion 24.7 – The UK requires legal persons to keep PSC information accurate and up-to-date. PSC information must be confirmed annually. If there are any changes, companies registered with Companies House and Scottish partnerships must inform Companies House within 14 days. For other legal persons, their own records must be updated within 14 days, and Companies House must be informed within an additional 14 days (Companies Act 2006, ss.790D, 790E, 790M). As the PSC register is public, it is subject to public scrutiny. Companies House is currently implementing reforms to facilitate reporting of any concerns with the register. Where an irregularity is

detected, Companies House follows up and can refer the issue to for investigation. Societies must maintain an up-to-date list of Committee and society members and advise the FCA of any changes to the Committee as part of the annual return (Co-operative and Community Benefit Societies Act 2014, s.30).

Criterion 24.8 – The UK has measures in place to ensure companies co-operate with competent authorities to the fullest extent possible in determining the beneficial owner. All company officers or partners are responsible for the company's obligations and are therefore responsible for compliance with the company's obligation to determine and register any PSC (Companies Act 2006, s.790F; Scottish Partnerships (Register of People with Significant Control) Regulations 2017, reg.12). Companies have powers to obtain information from believed PSCs and are entitled to share this information with authorities (Companies Act 2006, s.960D). All companies must have at least one natural person director. Limited liability partnerships must have at least one natural person partner. However, this requirement does not apply to Scottish Limited Partnerships or Scottish General Partnerships which may have solely corporate partners, including offshore corporates. There are no residency requirements for natural person directors or partners, although residency information must be provided to Companies House. The UK's public PSC register further facilitates the ability of competent authorities to determine the beneficial ownership of a legal person. Societies must have a registered office in Great Britain or the Channel Islands (Co-operative and Community Benefit Societies Act 2014, s.2D). A society is required to provide a copy of its annual return, including Committee membership information, to any person upon request and free of charge (Co-operative and Community Benefit Societies Act 2014, s.90).

Criterion 24.9 – Companies House has a duty to retain registration and PSC information on the public register for two years after a legal person is dissolved or struck off, with a discretionary power to transfer records to the National Archives at any time after two years (Companies Act 2006, s.1084; Public Records Act 1958). Pursuant to an agreed policy, Companies House will transfer this information to National Archives for permanent preservation 20 years after the legal person is dissolved or struck off. There are no requirements on societies or the FCA to maintain society information. Authorised insolvency practitioners who manage a company or society's liquidation must retain records on the liquidated company, including the company name, details of distributions of assets and statutory returns, and tax information, for six years after the liquidation (Insolvency Practitioners Regulations 2005, reg.13). Company directors are required to maintain business documents (bank statements, invoices, and receipts) for seven years after the date on which a company is struck off (VAT Act 1994, sch.11; Finance Act 1998, sch.18). This does not apply to a society's Committee members. Neither insolvency practitioners nor company directors are required to keep information on directors, members or shareholders; constitutional and governing documents; or beneficial ownership information.

Criterion 24.10 – Competent authorities, including law enforcement, have powers to obtain timely access to basic ownership and PSC information of companies and partnerships. Any authority can access Companies House registers to obtain basic ownership and PSC information. Certain personal information is withheld from the public register (e.g. residential addresses and dates of birth), but is available to competent authorities and law enforcement on request (Companies Act 2006, ss.240-

244, 790ZF, 709ZG, 1087B). The FIU also has instant access to its own version of the Companies House database. Companies House has a dedicated team which liaises with relevant authorities and law enforcement and monitors their information needs. Where information is not available on a public register, LEAs and supervisory authorities are also able to require a financial institution or third party to provide specific information, including on Scottish General Partnerships and societies. These entities must also make customer and transaction records available to competent authorities where appropriate (see Recommendation 11).

Criterion 24.11 – Bearer shares were prohibited in May 2015. Holders were given until February 2016 to surrender the warrant and register their interest in the company (Small Business, Enterprise and Employment Act 2015, ss.84-86, sch. 4).

Criterion 24.12 – The UK allows companies to have nominee shareholders. These are used most commonly by licenced or supervised sectors, such as stockbrokers or TCSPs, though there is no restriction on the use of nominee shareholders in other sectors. The use of nominees in other sectors is mitigated to some extent through the PSC register which requires that for the purpose of the register, shares and voting rights are held by the nominator and not the nominee (Companies Act 2006, Sch.1A, para.19). The UK does not recognise the concept of nominee directors, but does recognise shadow directors. A de facto or shadow director is subject to the same obligations as a regular company director and may be held liable for failure to meet these obligations. These obligations include acting in the best interest of the company and exercising independent judgment (Companies Act 2006, ss.170, 173, 1079B, sch.1A; Small Business, Enterprise and Employment Act 2015, s.105). For societies, depending on the specific rules of the society, a Committee member may be able to act on another's behalf.

Criterion 24.13 – The UK operates a range of sanctions to enforce compliance with legal person transparency obligations. Failure to provide basic and PSC registration information will result in the legal person remaining unregistered. The late provision of this information is punishable by fine of GBP 1 000 in addition to a daily default fine for the company and its officers (Companies Act 2006, s.853L). The provision of inaccurate information can be punishable by up to two years' imprisonment, an unlimited fine or both (Companies Act 2006, s.1112). Failure to maintain a register of shareholders is punishable by a fine of up to GBP 1 000, in addition to a daily fine for continued contravention, for the company and its officers (Companies Act 2006, s.113). If a society fails to comply with its information and record-keeping obligations, its officers or Committee members are subject to a fine of GBP 1 000. Failure by a legal person to provide a copy of PSC information to competent authorities or allowing authorities to inspect this information can result in a fine of up to GBP 1 000. A breach of directors' duties would typically result in disqualification and a ban from acting as a director for 2-15 years depending on the breach.

Criterion 24.14 – The UK can rapidly provide international cooperation in relation to basic ownership and PSC information:

(a) UK authorities can facilitate access to basic information held by company or society registries. Foreign authorities can freely access basic information via the online Companies House registry.

(b) Authorities can exchange information on shareholders through a variety of channels, including MLA and police-to-police assistance (see R.37 and R.40). Companies House typically respond to law enforcement requests for information within 24 hours.

(c) The PSC information provided by the legal person can be obtained via the online register, without need for engagement with UK authorities or resort to investigative powers.

Criterion 24.15 – The UK monitors the quality of assistance they receive from other countries in response to requests for basic or beneficial ownerships information or requests for assistance in locating beneficial owners residing abroad. While there are no formal structures in place, relevant officers will assess the information received against the information requested. Additional advice or guidance is provided to the requested agency if further information is required, and feedback is regularly provided.

Weighting and Conclusion

The UK meets or mostly meets all criteria in this Recommendation. Some minor deficiencies remain. Not all Scottish General Partnerships are required to register in the UK or maintain relevant information. These entities have not been identified as high-risk, but are entitled to legal personality, can carry out activities throughout the UK and internationally, and can have solely corporate partners. Some other types of low-risk legal person are also not subject to registration requirements. The ability of Scottish General and Limited Partnerships to have corporate partners may also create difficulties in ensuring these entities co-operate with competent authorities in determining the beneficial owner. The requirement on many of these corporate partners to register a PSC somewhat mitigates these difficulties. For registered legal persons, information and records are maintained by Companies House for 20 years in practice; however, the legal obligation only requires that they are kept for two years. Minor gaps also exist in the requirements on insolvency practitioners, company directors, and societies to maintain a legal person's basic and beneficial ownership information post-dissolution. The risks posed by nominee shareholders are largely mitigated, but these individuals need only register where they meet the threshold of beneficial ownership. Overall, these deficiencies are not considered significant. **Recommendation 24 is rated largely compliant.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

In its 3rd MER, the UK was rated partially compliant with these requirements. The technical deficiencies were: adequate, accurate and timely beneficial ownership information was not available to the competent authorities in a timely fashion; nature of beneficial ownership information held varied; and information maintained by trust service providers (other than lawyers and accountants) was not necessarily reliable as they were not monitored for compliance with their AML/CFT obligations. These standards were significantly strengthened since the 3rd MER.

Criterion 25.1 –

(a) Trustees of all UK express trusts and foreign express trusts which receive income from UK sources or have taxable assets in the UK ("specified trustees") are required to maintain information on all PSCs and potential beneficiaries of the trust. This includes the settlor, the trustee(s), the beneficiaries, class of beneficiaries, and any person exercising ultimate control over the trust. The protector of a trust is not explicitly defined in UK law, but would be captured where they exercise control over the trust. For natural persons, the information held must include their: name; date of birth; role in relation to the trust; and national insurance number or unique taxpayer reference or if the person has no such number, their residential address, or if the person is outside the UK, their passport details or equivalent information. For legal entities, the information held must include its: name; unique taxpayer reference; location of registered office; legal form and governing law; name of the relevant register and registration name; and role in relation to the trust. Where beneficiaries include a class of beneficiaries, the trustee must also maintain a description of the class. The trustees must also provide this information to HMRC which maintains a register (MLRs, regs.6(1), 42(2), 44(1) & 45; *Re Evans* (1999); *Pitt v. Holt* (2013)).

(b) Specified trustees are required to hold the full name of legal, financial, or tax advisers to the trust. This includes investment advisers or managers, accountants, and tax advisers, and other regulated agents (MLRs, regs.44(1) & 45(5)).

(c) Professional trustees who are obliged entities (i.e. subject to money laundering regulations) are required to maintain this information for five years after their involvement with the trust ceases (MLRs, reg.44(9)). Professional trustees who are not obliged entities (which are limited in number), are subject to general common law obligations which require the maintenance of records on the trust, although it is not clear that this would require the maintenance of specific records for five years after their involvement with the trust ceases (*Jones v. Firkin-Flood* (2008); *R.N.L.I v. Headley* (2016)).

Criterion 25.2 – The UK requires that specified trustees keep the above information accurate and as up-to-date (MLRs, regs.44 & 45).

Criterion 25.3 – Specified trustees are required to disclose their status to financial institutions and DNFBPs when entering a business relationship or conducting a transaction in their capacity as a trustee. Trustees must also report any changes to PSCs within 14 days (MLRs, reg.44(2)(a)).

Criterion 25.4 – Trustees are not prevented from providing domestic law enforcement authorities with any information relating to the trust, whether in relation to a domestic matter or as part of a MLA request. Specified trustees are required to provide PSC or beneficiary information to law enforcement upon request and within a reasonable period as specified by the requesting authority (MLRs, reg.44(5)).

Trustees must provide financial institutions and DNFBPs with the identities of the trust's PSC where there is a business relationship or relevant transaction (MLRs, reg.44(2)). Financial institutions are also able to request information from trustees on the assets of the trust to be held or managed under the terms of the business relationship and no legal barriers exist to prevent trustees providing this information (MLRs, reg.28(2)(c)).

Criterion 25.5 – UK law enforcement authorities (including NCA, the Police, HMRC, the FCA, and the SFO) have powers to obtain timely access to information held by trustees, FIs, and DNFBPs, on the PSC of a trust. Specified trustees are required to comply with a request from law enforcement for information on the PSC, a contact address for the trustee, or a statement of accounts for the trust (detailing the assets held by the trust and their location). This information must be provided within a reasonable period as specified by law enforcement (MLRs, reg.44(5)). Authorities also have access to HMRC's register of taxable trusts which includes beneficial ownership information, the trustee's contact address, and a statement of accounts (MLRs, reg.45).

Law enforcement authorities have information and inspection powers which provide for timely access information held by FIs and DNFBPs on the beneficial ownership of a trust, its assets, and the residence of its trustees where this is of relevance to a criminal or civil investigation (Finance Act 2008, sch.36; POCA, s.345; Serious Organised Crime and Police Act 2005, s.62).

Criterion 25.6 – The UK is able to provide rapid international co-operation relating to information on trusts and other legal arrangements:

(a) HMRC can share information on trusts, including beneficial ownership, with other competent authorities and law enforcement. This includes information held on the HRC trusts register. This information can be obtained through MLA or direct agency-to-agency assistance (see R.37 and 40). HMRC is also required to ensure that the NCA can share data from the trusts register with competent authorities in the EEA (MLRs, reg.45(13)).

(b) Law enforcement authorities can share domestically-available information on trusts and legal arrangements with foreign authorities through MLA or direct agency-to-agency assistance. The FIU is also able to share information on trusts obtained via a SAR with EU FIUs via FIU.net.

(c) Law enforcement authorities are able to exercise domestically-available investigative powers to obtain information from trusts, including beneficial ownership information, on behalf of non-UK authorities through MLA or direct agency-to-agency assistance.

Criterion 25.7 – Specified trustees are legally liable if they breach certain obligations, including the obligation to maintain accurate and up-to-date information on the trust. Such a breach is subject to an administrative fine of an unlimited amount determined by the supervising authority, or a statement of censure (MLRs, reg.76). Trustees may also be subject to a common law civil suit and required to pay compensation for a breach of their trustee duties.

Criterion 25.8 – Specified trustees are liable to an unlimited administrative fine, determined by the supervising authority, or a statement of censure if they breach their obligation to provide to requesting law enforcement authorities information about the PSC (MLRs, reg.76). Failure to comply with law enforcement information and inspection powers is a criminal offence.

Weighting and Conclusion

All criteria are met. **Recommendation 25 is rated compliant.**

Recommendation 26 – Regulation and supervision of financial institutions

In its 3rd MER, the UK was rated largely compliant with these requirements. Deficiencies related to effectiveness issues which, in the 4th round, are assessed separately from technical compliance under IO.3.

Criterion 26.1 – The FCA regulates and supervises almost all persons and entities falling under the FATF-definition of financial institutions. The only financial institutions not supervised by the FCA are 'excluded money service businesses' which are supervised by HMRC (see analysis of R.14). (MLRs, regs.7(1a) and (1c)).

Criterion 26.2 – All individuals and firms carrying out a regulated activity in the UK are required to be authorised or registered by the FCA (Financial Services and Markets Act 2000, s.19). Financial institutions (including Core Principles financial institutions and MVTS or money or currency changing services) must also be registered by their supervisor (MLRs, regs.54-56). The FCA's authorisation process provides a process to ensure that shell banks are not established in the UK. UK-authorised firms are required to locate their head offices in the UK, increasing their proximity to supervision by UK authorities (MLRs, reg.34(2) & (3)).

Criterion 26.3 – The FCA and HMRC take regulatory measures to prevent criminals and their associates from holding a significant or controlling interest, or a management function, in a financial institution. The FCA's authorisation process assesses whether certain individuals within a firm are fit and proper persons (FSMA, s.61). The FCA also assesses whether individuals who seek to acquire or increase control over a firm are suitable to do so (FMSA, s.186). This includes consideration of issues such as the integrity, financial soundness and whether the change would increase the risk of ML/TF. The HMRC registration process also requires that directors, beneficial owners, agents and nominated officers of MVTS providers are fit and proper persons (MLRs, reg.58 and Schedule 3). Both HMRC and FCA consider previous criminal convictions as part of their assessment (MLRs, reg.58(3) as well as searching the FCA's intelligence database where relevant. This occurs on an ongoing basis as the ownership of the FI changes.

Criterion 26.4 –

- **a)** The FCA's regulation and supervision of core principles institutions are in line with the core principles, including the application of consolidated group supervision for AML/CFT purposes. The FCA supervises FIs' obligation to establish and maintain policies, controls and procedures to mitigate and manage ML/TF risks and ensure that they also apply to all their subsidiaries and branches in other jurisdictions, including outside the EEA (MLR, regs.19-20 & 46). The FCA is required to adopt a risk-based approach to its supervisory functions and to base the frequency and intensity of its on-site and off-site supervision on risk profiles it develops (MLRs, reg.46 & 17(4)).
- **b)** The information set out at (a) above, also applies to the FCA and HMRC's supervision of MVTS.

Criterion 26.5 – The frequency and intensity of on-site and off-site AML/CFT supervision of FIs is determined on the basis of:

a) the supervisors' assessment of an FI's risk profile (reg.46(1c))

b) the ML/TF risks present in the country, in so far as these risks must be reflected in risk assessments undertaken by the supervisory authority (MLRs, reg.17(c-d)), and

c) the characteristics of the FI, including the degree of discretion allowed to the FI under the RBA (reg.46(3b)) and the diversity and number of FIs in the sector

Criterion 26.6 – Supervisors must review the risk profiles at regular intervals and also when there are major events or developments that may alter the ML/TF risk relevant to the FIs (MLRs, reg.17(8)).

Weighting and Conclusion

All criteria are met. **Recommendation 26 is rated compliant.**

Recommendation 27 – Powers of supervisors

In its 3rd MER, the UK was rated largely compliant with these requirements. The deficiencies identified were the lack of powers in relation to entities not subject to the supervisory regime (for example, financial leasing and consumer credit sectors) and the inability to apply sanctions to the directors and senior managers of MVTS providers.

Criterion 27.1 – The FCA and the HMRC are required to supervise, monitor and ensure compliance by FIs with AML/CFT requirements (MLRs, reg.46). The FCA is the supervisory authority for credit and FIs which are authorised persons but not excluded money services businesses. HMRC is the supervisory authority for money services businesses which are not supervised by the FCA (MLRs, reg.7).

Criterion 27.2 – Supervisors have the authority to conduct inspections, both with and without a warrant (MLRs, regs.69-70).

Criterion 27.3 – Supervisors are authorised to compel production of any information that is reasonably required in the exercise of the supervisor's functions from any person without the need for a court order (MLRs, reg.66).

Criterion 27.4 – A range of disciplinary and financial sanctions are available to the HMRC and the FCA under the MLRs. They have the authority to withdraw, restrict or suspend a FI's licence (HMRC – reg.60 and FCA – reg.77) and have powers to impose civil penalties of such amounts as they consider appropriate, make public statements censuring the persons concerned (reg.76) and prohibit individuals from managing a relevant FI or MVTS (regs.80-83).

Weighting and Conclusion

All criteria are met. **Recommendation 27 is rated compliant**.

Recommendation 28 – Regulation and supervision of DNFBPs

In its 3rd MER, the UK was rated partly compliant with these requirements. Deficiencies related to the lack of AML/CFT supervision of real estate agents, some TCSPs and accountants and notaries in England and Wales; and inadequate powers of sanction for the Gambling Commission.

Criterion 28.1 – Casinos are subject to AML/CFT regulation and supervision in the UK.

a) Casinos are required to be licensed under UK law. It is an offence to carry out gambling services without a license or outside of the conditions of that license (MLRs, reg.14(1b) and Gambling Act 2005, ss.33, 65 & 69). Casinos are legally prohibited in Northern Ireland (Betting, Gambling, Lotteries and Amusements (Northern Ireland) Order 1985).

b) Applicants for a casino license are required to provide full information on the identity and ownership of the applicant/firm/persons associated with the firm so as to prevent criminals and their associates from holding a significant or controlling interest, or holding a management function, or being an operator of a casino. Persons who will be responsible for a key function are also expected to hold a personal license and all those persons with 10% or more equity in a company providing gambling services will also need to be approved (Gambling Commission, Licence conditions and codes of practice, January 2017 prepared under the authority of the Gambling Act 2005, s. 23). The Gambling Commission has the power to refuse an application if the applicant, or a person relevant to the application, has a conviction for a relevant offence or if the Commission has concerns about the suitability or integrity of the applicant (Gambling Act 2005, ss.69-71). Once, licensed, a license holder's ongoing suitability will be assessed through compliance activity.

c) The Gambling Commission is the supervisory authority for casinos and is required to monitor and supervise casinos for compliance with the MLRs (MLRs, regs.7(d), 8(2h) and 46). The Gambling Commission's *Licencing Conditions and Codes of Practice* require licence holders to assess and mitigate ML/TF risks.

Criterion 28.2 & 28.3 – Accountants, lawyers, notaries, HVDs, TCSPs and real estate agenda are subject to the MLRs and are monitored for compliance with these requirements (see table below). Supervisory authorities are required to monitor the entities they are responsible for, including carrying out on-site and off-site supervision based on a risk-based approach (MLRs, reg.46).

Table 48. Supervision of DNFBPs (other than casinos)

Sector	Relevant provision in the MLRs	Designated competent authority or self-regulating body
Accountants	7(b) – professional bodies set out in Schedule 1 7(c)(iv) – HMRC for auditors, external accountants and tax advisers who are not supervised by a professional body	HMRC Institute of Chartered Accountants England and Wales Association of Chartered Certified Accountants Institute of Chartered Accountants in Scotland Association of Accounting Technicians Association of International Accountants Association of Taxation Technicians Chartered Institute of Management Accountants Chartered Institute of Taxation Institute of Certified Bookkeepers Institute of Financial Accountants International Association of Bookkeepers Institute of Chartered Accountants in Ireland Insolvency Practitioners Association
Lawyers & notaries	7(b) – professional bodies set out in Schedule 1	Council of Licensed Conveyancers Faculty of Advocates (Scottish Bar Association) Faculty Office of the Archbishop of Canterbury General Council of the Bar (England and Wales) General Council of the Bar of Northern Ireland Law Society of Scotland Law Society of Northern Ireland Law Society England and Wales Chartered Institute of Legal Executives
High Value Goods Dealers	7(c)(i)	HMRC
Estate Agent Businesses	7(c)(vii) – HMRC for those not supervised by the professional bodies	HMRC
Trust and Company Service Providers	7(b) – professional bodies set out in Schedule 1 7(c)(iii) – HMRC for any TCSPs not supervised by the FCA or professional bodies	FCA HMRC All the above legal and accountancy professional body supervisors.
Other	7(c)(v-vi) – in relation to bill payment service providers, telecommunications, digital and IT payment service providers not supervised by the FCA	HMRC

Criterion 28.4 – (*Met*)

a) The FCA, HMRC, Gambling Commission and the self-regulated bodies have adequate powers to perform their supervisory functions, including powers to monitor compliance (MLRs, regs.46 & 49).

b) Lawyers, accountants, real estate agents and HVDs, must apply to the relevant supervisory authority to have their beneficial owners, officers and managers approved. This approval cannot be granted if the applicant has been convicted of a relevant offence (MLRs, reg.26). For TCSPs, HMRC applies the same process as it does for FIs – see c.26.3.

c) Supervisors of DNFBPs have sanctions available to them in line with R.35 to deal with the failure to comply with AML/CFT requirements (for the FCA & HMRC: MLRs, regs.76, 80 & 86; for all SRBs: MLRs, regs.49(1d) & 76).

Criterion 28.5 – The supervision of DNFBPs is required to be undertaken on a risk-sensitive basis.

a) Supervisors are required to adopt a risk-based approach to the frequency and intensity of their AML/CFT supervisory functions. Supervisors are required to develop sectoral risk assessments and risk profiles for each entity or group in their sector and, in doing so, they consider the characteristics of the DNFBPs, including their diversity and number (MLRs, regs.17 & 46(2c)).

b) In assessing the adequacy of AML/CFT internal controls, policies and procedures of DNFBPs, supervisors are required to develop an record risk profiles for each entity or group in their sector (MLRs, reg.17(4)), including take account the degree of discretion available to them (reg.46(3)).

Weighting and Conclusion

All criteria are met. **Recommendation 28 is rated compliant**.

Recommendation 29 - Financial intelligence units

In its 3rd MER, the UK was rated largely compliant with these requirements. Effectiveness issues were considered as part of the previous assessment but under the 4th round are no longer included in this technical compliance assessment, but are assessed separately under IO.6. Since the last evaluation, the FATF standards in this area were strengthened. Also, the UKFIU is now housed by the NCA (instead of the Serious Organised Crime Agency which it replaces).

Criterion 29.1 – The UKFIU is a law enforcement-style FIU which sits within the Prosperity Command in the NCA. The Director General of the NCA has the power to designate persons or officers to perform the functions of an FIU, specifically to receive STRs (see c.29.2(a)). The Director General has issued a general authorisation for all officers working within the UKFIU. An NCA policy document (EC05) establishes the UKFIU within NCA and sets out its role in terms of the receipt, analysis and dissemination of SARs. This document can be amended by the UKFIU and the NCA Prosperity Director.

Criterion 29.2 – The UKFIU serves as the central agency for the receipt of disclosures filed by reporting entities, including:

a) ML SARs filed by reporting entities (POCA 2002, ss.330(4), 331(4), 332(4), 339ZG(3)). TF SARs, can be reported to the UKFIU or to a 'constable' which includes, but is not exclusively, a member of the UKFIU (TACT 2000, ss.19(2)&(7B), 21A(4)). However, where a disclosure is made to a constable, he/she is required to disclose it in full to the FIU as soon as practicable after the disclosure has been made (TACT, s. 21C(1)).

The UK also operates a 'consent regime' which forms part of the SAR reporting regime. Under this regime, reporting entities must temporarily freeze transactions which potentially constitute ML/TF in order to seek a defence against money laundering or defence against terrorist financing (DAML or DATF) from the NCA prior to completing the transaction. The UKFIU, in consultation with law enforcement, has seven working days to provide a notice of refusal to the reporting entity (with additional extensions of time available). If such a notice is not provided, the entity is deemed to have a defence against ML or TF. A DAML or DATF request is a type of SAR, as it is

made by reporting entities to the UKFIU, and the UKFIU keeps a record of these transactions and the outcome of the DAML and DATF requests on its database (POCA, ss.335-338; TACT, s.21B).

b) The UK does not require the reporting of cash transactions, wire transfer and or any additional types of threshold-based activity apart from the cross-border cash declarations (nor is this required by the FATF Standards).

Criterion 29.3 – In relation to obtaining and accessing information:

a) The UKFIU is able to obtain and use additional information from reporting entities as needed to perform its analysis of STRs on a voluntary basis (Crimes and Courts Act, s.7). The UKFIU can also undertake follow-up queries on DAML and DATF requests. It can also seek a Further Information Order issued by a magistrate's court or a sheriff in Scotland (POCA, s. 339ZH introduced by s.12 of the Criminal Finances Act 2017) where there is a suspicion of ML. However, if it is not clear if these orders can be obtained in a fashion that allows the UKFIU to perform it analysis functions as these new powers have not been tested by the UKFIU.

b) The UKFIU has direct and indirect access to a wide range of financial, administrative and law enforcement information to help it undertake its functions. The UKFIU has direct access to databases that contain the following information: NCA and national police intelligence, asset recovery database, national flagged entities and persons, registry of companies, land registry information, sanctions lists, credit rating databases and information aggregated by World Check. It has indirect access to information from Europol Focal Points, HMRC (including tax and customs information – see also c.32.6) and other government departments, including the Joint Financial Analysis Centre and the FCA.

Criterion 29.4 – In relation to analysis undertaken by the UKFIU:

a) Due to the large amount of SARs it receives and its limited human and IT resources, the UKFIU focuses its resources on identifying priority STRs and matching financial information against operational targets in order to disseminate that information to LEAs in a timely manner. In most cases, the UKFIU disseminates the SARs to LEAs for further analysis. In limited situations, such as responding to terrorist attacks, the UKFIU undertakes operational analysis to support broader law enforcement efforts.

b) The UKFIU provides strategic analysis in the form of period reports including SAR statistics, typologies and trends. It has also produced specific review of the legal charity sector, accountancy, banking, non-regulated gambling, corruption, real estate agents, the UK property sector, MSBs, TCSPs and professional enablers. However it has limited IT capability to undertake complex strategic analysis.

Criterion 29.5 – The UKFIU is able to disseminate information to law enforcement authorities conducting ML, TF and predicate offence investigations through an information gateway using secure online portals or secure government emails (Crime

and Courts Act 2013, s.7). For an analysis of the UKFIU's ability to disseminate information to international counterparts, see c.40-9-40.11.

Criterion 29.6 – The UKFIU protects information in the following ways:

a) There are multiple rules, guidelines, principles in place governing the information security, confidentiality, handling, storage, dissemination and access, along with training and monitoring of access to and use of the database by end-users. All SAR information is handled at the 'official' or 'secret' level within Government.

b) UKFIU staff are security cleared and vetted and undertake training to understand their responsibilities in handling and disseminating confidential information.

c) Access to the NCA's facilities is secured, protected and restricted. The UKFIU's database is limited to those with a 'secret' security clearance who have been accredited as Financial Investigators, Intelligence Officers or Administrators (End-User Agreements on Access to SARs).

Criterion 29.7 – In relation to operational independence and autonomy:

a) The NCA is a non-ministerial government department and is operationally independent. The designation by the NCA Director General provides the authority for the UKFIU to carry out its functions. The Head of the UKFIU is appointed by the NCA Director Prosperity. The Head of the UKFIU is a senior manager within the NCA and makes decisions to analyse, request and/or disseminate information. When dealing with cases that involve political sensitivities, high values, impact on the NCA's reputation or carry a risk of legal challenge, the Head of the UKFIU can, but is not obliged to, refer the case NCA senior management. The UKFIU is not sufficiently independent from the NCA in defining its role or its priorities.

b) The Head of the UKFIU can sign, on his/her own authority, non-binding MOUs with domestic competent authorities and foreign UKFIU counterparts.

c) Although the UKFIU is a part of the NCA, it has distinct and separate core functions as set out in EC04 (DAML/DATF regime) and EC05 (SAR regime).

d) To some extent, the UKFIU is able to obtain and deploy the resources needed to carry out its functions. The Head of the UKFIU has control over the UKFIU's budget; however, this budget is determined on a yearly basis by NCA Finance and allocated to the Director of the Prosperity Directorate where the UKFIU is housed. The Director of the Prosperity Directorate also has the ability to surge resources, both from, and to, the UKFIU.

Criterion 29.8 – The UKFIU was a founding member of the Egmont Group and granted full membership in June 1995.

Weighting and Conclusion

There are some concerns about the operational independence of the UKFIU and in relation to its ability to perform its key functions due to the lack of resources. The UKFIU has a limited ability to conduct operational and strategic analysis and it is not

clear if it can seek all the additional information it requires from reporting entities to perform its analysis. R.29 is rated **partially compliant**.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

In its 3rd MER, the UK was rated compliant with these requirements.

Criterion 30.1 – In the UK, the Police and the National Crime Agency (NCA) have overarching responsibility for investigating ML and most associated predicates. Specialised investigative units provide investigative assistance and expertise. These include nine Regional Organised Crime Units (ROCUs) within the Police, the Scottish Crime Campus which brings together relevant law enforcement agencies, the Economic Crime Unit of the Police Service of Northern Ireland, and the Joint Agency Task Force of the Police Service of Northern Ireland. If the predicate offence is tax-related, it, and any associated ML, will be investigated by HMRC while complex fraud and corruption, and any associated ML, is investigated by the Serious Fraud Office (SFO).

TF is investigated by the National Terrorist Financial Investigation Unit (NTFIU), within the Police. In England, Wales, and Scotland, the NTFIU is supported in this role by financial investigators within the Counter-Terrorism Units of the regional Police forces. In Northern Ireland, TF investigations are pursued by the Crime Operations Department of the Police.

Criterion 30.2 – All law enforcement agencies responsible for investigating predicate offences in the UK are able to pursue parallel financial investigations of related ML/TF regardless of where the offence occurred. Agencies are also permitted to transfer cases where desirable.

Criterion 30.3 – The Police, NCA, HMRC, the SFO, and accredited financial investigators are designated to exercise powers to identify, trace, and freeze and seize suspected proceeds of crime or property subject to confiscation (see R.4). Specific Asset Confiscation Enforcement teams exist within the Police, the NCA and the HMRC to help these agencies enforce confiscation orders.

Criterion 30.4 – Recommendation 30 applies to all relevant authorities responsible for investigating predicate offences. In addition, the UK Secretary of State may issue orders empowering certain groups or persons to exercise financial investigation powers.

Criterion 30.5 – The UK has no specific anti-corruption enforcement authority. Corruption is investigated by the SFO (significant or complex cases) or the Police (all other cases of corruption). Both agencies can investigate associated ML/TF offences and exercise relevant powers to identify, trace, freeze and confiscate assets.

Weighting and Conclusion

All criteria are met. **Recommendation 30 is rated compliant.**

Recommendation 31 - Powers of law enforcement and investigative authorities

In its 3rd MER, the UK was rated compliant with these requirements.

Criterion 31.1 – Competent law enforcement authorities in the UK are able to access necessary document and information for use in investigations, prosecutions, and related actions:

(a) Production or disclosure orders can be used to obtain records and information held by FIs, DNFBPs, and other natural and legal persons in the context of ML, TF and predicate offence investigations (POCA, ss.345, 347, 357, 363, 370, 380, 382, 391, 397, 404; POCA 2002 (References to Financial Investigators) (England and Wales) Order 2015; POCA 2002 (References to Financial Investigators) (Amendment) Order 2009; Terrorism Act, sch.5A, 6, 6A; PACE, sch.1).

(b) Persons and premises can be searched (POCA, ss.352, 387; POCA 2002 (References to Financial Investigators) (England and Wales) Order 2015; POCA 2002 (References to Financial Investigators) (Amendment) Order 2009; PACE, s.1, 8; Police and Criminal Evidence (Northern Ireland) Order 1989 (PACE NI), s.3, 10).

(c) Witness statements can be taken voluntarily by a constable or can be compelled by a court (Criminal Procedure (Attendance of Witnesses) Act 1965, s.2; Judicature (Northern Ireland) Act 1978, s.51; Criminal Justice Act 1987, s.2).

(d) Evidence can be obtained and seized (PACE, s.19; PACE NI, s.21; Criminal Justice Act 1987, s.2).

Criterion 31.2 – Competent law enforcement authorities conducting ML, TF or predicate offence investigations can conduct undercover operations, intercept communications, and access computer systems (Regulation of Investigatory Powers Act 2000, s.29; Investigatory Powers Act 2016, ss.19, 102, 103; Police Act 1997, s.93). Controlled delivery can be performed on the basis of a range of powers and guidance (Regulation of Investigatory Powers Act 2000; Police Act 1997; HRMC Criminal Justice Procedure).

Criterion 31.3 – UK law enforcement authorities conducting a ML, TF, or predicate offence investigation can apply to a judge for a customer information order which allows them to identify, in a timely manner, whether natural or legal persons hold or control accounts (POCA, ss.363, 397; Terrorism Act, sch.6). Law enforcement is able to obtain and execute these orders without prior notification of the owner (POCA, s.369(1)).

Criterion 31.4 – Financial investigators, intelligence officers, and administrators from competent authorities conducting ML, TF and predicate investigations are able to access FIU information directly via secure systems and gateways. If necessary, they may obtain additional information on request (Crime and Courts Act 2013, s.7).

Weighting and Conclusion

All criteria are met. **Recommendation 31 is rated compliant.**

Recommendation 32 – Cash Couriers

In its 3rd MER, the UK was rated largely compliant with these requirements. The technical deficiencies were that: authorities could not detain cash purely for a false disclosure; no requirement to retain identification and amount data upon false disclosure or a suspicion of ML/TF; and no comprehensive system to share cross-border disclosure data with the FIU.

Criterion 32.1 – For travellers entering or leaving the EU via the UK, the UK applies a declaration system under EU Directive 1889/2005; however, this does not apply to those travelling to or from an EU member state.[72] A declaration disclosure system also exists for mail and cargo transportation of cash outside of the EU (Customs and Excise Management Act 1979, s.77; postal Packets (Revenue and Customs) Regulations 2011; Customs Notices 143, 275).

Criterion 32.2 – Natural persons entering or leaving the EU must declare in writing cash or BNIs over EUR 10 000 (EU Directive 1889/2005; Control of Cash (Penalties) Regulations 2007).

Criterion 32.3 – Any person entering or leaving the UK must truthfully answer questions or produce items if requested by HMRC officers (Customs and Excise Management Act 1979, s.78).

Criterion 32.4 – Upon discovery of a false declaration, HMRC can compel a person to provide further information on the cash or NBIs (Customs and Excise Management Act 1979, ss.77, 78). It is standard practice for HMRC to require further information on the origin and purpose of currency or BNIs.

Criterion 32.5 – A false declaration is subject to an administrative fine of GBP 5 000 from HMRC (Control of Cash (Penalties) Regulations, reg.3). These penalties are not proportionate or dissuasive.

Criterion 32.6 – Cross-border cash declarations which are reported to HMRC are provided to the NCA on a monthly basis under an MOU between the agencies which has been in place since 22 January 2018, with the first exchange of information under the MOU in February 2018 (see c.32.6). This information can then be provided to the UKFIU, but there are limitations as to what data can be stored in line with the Operating Procedure for dealing with Bulk Personal Data. This data can also be accessed by HMRC secondees to the UKFIU.

Criterion 32.7 – HMRC, the UK Border Force, the NCA, and the Police co-operate through joint investigations and Joint Border Intelligence Units. These agencies regularly discuss cash at the border in the inter-agency Criminal Finances Threat Group and Cash at the Border Governance Group.

Criterion 32.8 –

(a) HMRC, the Police, and accredited financial investigators can seize for 48 hours currency or BNIs valued over GBP 1 000 where there is a suspicion that it is the

72 This declaration system replaces the UK's previous disclosure system (assessed in the previous MER) which is now rendered redundant.

proceeds of crime or intended for use in unlawful conduct. If necessary, the initial seizure period can be extended by a magistrate (POCA, ss.289, 294).

(b) HMRC officers are able to impose penalties and detain cash moving into or out of the EU in contravention of EU Regulations, including on the grounds of a false declaration (EU Directive 1889/2005, art,4(2); Control of Cash (Penalties) Regulations 2007, s.3). A false declaration may also provide grounds for suspicion which would justify seizure using the powers outlined above in (a) (POCA, s.294).

Criterion 32.9 – The UK declaration and disclosure systems allow for some international co-operation and assistance. To facilitate such co-operation, HMRC retains:

(a) all declarations, which include the amount of currency or BNIs declared and identification data of the bearer; including

(b) where there is a false declaration; and

(c) there is a suspicion of ML/TF.

Criterion 32.10 – The use of data and information collected through the UK's declaration system is governed by data protection principles which ensure the fair and lawful use of information, safe and secure handling, and penalties for abuse of data (Data Protection Act 1998, ss.4, 40, 55A). The UK declaration system does not unreasonably restrict legitimate travel and trade.

Criterion 32.11 – Persons transporting funds or BNIs in relation to ML or TF may be subject to penalties for these offences, i.e. natural persons are subject to 14 years' imprisonment, or an unlimited fine, or both, while legal persons may receive an unlimited fine (POCA, ss.327, 328, 329, 334; Terrorism Act, s.15) (see R.3 and R.5). This is in addition to the possible penalties for providing a false declaration.

The currency or BNIs would be subject to civil and criminal forfeiture as set out in Recommendation 4. UK authorities may also apply the cash forfeiture regime if the cash or BNIs valued over GBP 1 000 and is determined to be the proceeds of crime or intended for use in unlawful conduct (POCA, s.298).

Weighting and Conclusion

There is no declaration or disclosure system for cross-border transportation of cash or BNIs to or from an EU member state. This deficiency is given less weight as the UK NRA identifies states outside the EU as posing a higher ML/TF threat. The fines available for submitting a false declaration are not sufficiently proportionate or dissuasive. Cross-border cash declarations are shared with the UKFIU, but as the MOU between the NCA and HMRC had only been in place one month before the onsite it was not clear what information could be stored by the UKFIU. **Recommendation 32 is rated largely compliant.**

Recommendation 33 – Statistics

In its 3rd MER, the UK was rated largely compliant with these requirements. Since then, the Methodology for assessing compliance with this Recommendation has changed significantly.

Criterion 33.1 – The UK keeps statistics on:

(a) SARs received and disseminated. The data on SARs received can be broken down by sector and TF SARs can be explicitly identified.

(b) ML and TF prosecutions and convictions. Statistics on ML investigations are not consistently maintained but can be collected when required. Prosecution and conviction statistics are maintained individually by the separate UK jurisdictions.

(c) Property frozen; seized and confiscated.

(d) MLA and extradition requests are maintained independently by the three central authorities, UKCA, HMRC, and COPFS. In addition, the UK maintains data on intelligence-sharing by the FIU.

Weighting and Conclusion

The UK does not maintain national statistics on ML investigations. **Recommendation 33 is rated largely compliant.**

Recommendation 34 – Guidance and feedback

In its 3rd MER, the UK was rated compliant with these requirements.

Criterion 34.1 – Competent authorities and supervisors in the UK have established guidelines and feedback procedures to assist FIs and DNFBPs in applying national AML/CFT measures, and in particular, in detecting and reporting suspicious transactions.

Supervisors

HMT is responsible for approving industry guidance developed by supervisors and industry bodies (except the FCA). Before approval, the guidance is reviewed by the Money Laundering Advisory Committee, comprised of representatives from across the public and private sector. The guidance is updated or supplemented to reflect emerging risks and is currently being updated to reflect the new MLRs. HMT has approved the following guidance:

- The Joint Money Laundering Steering Group (JMLSG), which consists of the main UK trade associations in the UK financial services industry, provides industry guidance to promulgate good practice in countering ML/TF and to give practical assistance in interpreting the MLRs. This has been updated to reflect the new MLRs.
- The Legal Sector Affinity Group (which is comprised of legal sector supervisors) has issued draft updated AML Guidance to reflect the new MLRs. The Law Society also includes AML issues in professional development training, and provides AML/CFT seminars, webinars, workshops, and other outreach, and has issued a Lawyer's Guide to Detecting and Preventing ML.
- The Consultative Committee of Accountancy Bodies has issued a draft updated AML Guidance to reflect the new MLRs.
- HMRC provides general AML guidance on the UK government website as well as providing specific AML guidance for high value dealers, TCSPs, MSBs, and estate

agents. HMRC's Anti-Money Laundering Supervision team also uses targeted emails and webinars to provide further guidance to estate agencies.

- The Gambling Commission provides AML/CFT Guidance for casinos, other operators, and small businesses. This was updated in September 2017 to reflect the MLRs. The Commission also provides updates and relevant information via its website.

In addition, the FCA's Handbook contains AML/CFT guidance for FIs, and its Financial Crime Guide includes thematic reviews of higher-risk areas. This guidance is supplemented by targeted outreach events including webinars and presentations, and a biennial Financial Crime Conference.

FIU/NCA

The NCA (which houses the FIU) has issued a range of guidance, including an Introduction to SARs, Submitting Better Quality SARs, Requesting a Defence from the NCA under POCA and TACT, and SAR Guidance Notes. These are available to reporting entities on the NCA website. The FIU has also produced specific reviews of the accountancy, banking, non-regulated gaming, and TCSP sectors.

The NCA is required to provide annual feedback on the SARs it receives (MLRs, reg.104(1)). It does this through the SAR Annual Report which includes statistics on SARs received and case studies on their use, and two additional yearly SARs Reporters' Booklets which contain case studies and advice on submitting better-quality SARs. The Annual Report and Reporters' Booklets are published on the NCA website. In addition, the FIU sends biannual feedback questionnaires to end users with direct access to the SAR database asking for statistics and feedback on their use of SARs over the previous six months. Provision of feedback in this manner is required to obtain direct access to the SAR database.

Other competent authorities

Law enforcement authorities, banks, and the FCA participate in the Joint Money Laundering Intelligence Taskforce (JMLIT) which shares information and provides direct feedback.

The Office of Financial Sanctions Implementation (OFSI) has issued a Guide to Financial Sanctions to help individuals and businesses comply with financial sanctions. The guide is regularly updated. Additional guidance has also been issued on monetary penalties for financial sanction breaches and to assist charities in complying with financial sanctions.

Weighting and Conclusion

All criteria are met. **Recommendation 34 is rated compliant.**

Recommendation 35 – Sanctions

In its 3rd MER, the UK was rated largely compliant with these requirements. Technical deficiencies related to the inability for HMRC to extend administrative penalties to directors and managers.

Criterion 35.1 – A range of proportionate and dissuasive criminal, civil and administrative sanctions are available, ranging from administrative warning letters to cancellation of licences to fines and imprisonment.

Persons who fail to disclose information, tip off a suspect or prejudice an investigation if found guilty are liable to a maximum of 5 years imprisonment and/or an unlimited fine for a conviction on indictment, or to a maximum 6 months imprisonment and/or an unlimited fine for a summary conviction (POCA, ss.327-333 & 342).

a) ***Targeted financial sanctions*** (R.6): OFSI has a range of enforcement measures available to it, which includes the issuing of administrative warning letters and civil penalties and the ability to publicise breaches to dissuade other breaches (Policing and Crime Act 2017, ss.146-149; max penalty of GBP 1 million or 50% of the total value of the breach, whichever is greater). Where FIs breach a sanction due to a failure in the systems and controls, the FCA may also levy penalties on that FI (see analysis of c.7.3 above). Criminal sanctions are also available for breaches of targeted financial sanctions. LEAs can open a criminal investigation into a suspected sanctions breach by referral from a competent authority (OFSI) or they can start an investigation independently. A person guilty of breaching the UNSCR1267 or UNSCR1373 asset freeze is liable to a maximum of 7 years imprisonment and/or a fine (on indictment), and to a maximum of 6-12 months and/or a fine (TAFA, s.32(1); ISIL (Da'esh) and Al Qaida (Asset Freezing) Regulations 2011, reg.14; Afghanistan (Asset-Freezing) Regulations 2011 reg.14 as amended by PACA 2017, s.144). There are offences related to licences or confidentiality requirements in the TAFA which can lead to imprisonment for up to 2 years, fine, or both, for convictions on indictment or up to 6-12 months for summary convictions and/or a fine (s.32(2)). There are also offences related to breaches of reporting conditions or information requests in TAFA which can lead on summary conviction to imprisonment of up to 6 months-51 weeks and/or a fine (TAFA s32(4)). There are similar offences related to breaches of reporting conditions or information requests in the Al Qaida (Asset Freezing) Regulations 2011, reg.14; Afghanistan (Asset-Freezing) Regulations 2011, reg.14 as amended by s.144 Policing and Crime Act 2017. These can lead on summary conviction to imprisonment of up to 6-12 months and/or a fine. The UK also has the power to impose Deferred Prosecution Agreement and Serious Crime Prevention Orders (Policing and Crime Act 2017, ss.150-151).

b) ***NPOs*** (R.8): All three UK Charity Regulators have access to a range of sanctions for failing to comply with relevant requirements. See analysis of c.8.4(b).

c) ***Preventive Measures and Reporting*** (R.9-23): For *FIs and DNFBPs supervised by FCA or HMRC*, a range of sanctions are available including, applying for an injunction to prevent a likely breach (MLRs, reg.80); imposing fines at any level that is sufficient for them to be effective or publically censuring its supervised population (reg.76); suspending or restricting an authorisation (reg.77); and refusing, suspending or cancelling a registration (regs.59-60).

The MLRs set out the process and factors that should be taken in to account as these sanctions are imposed – this includes ensuring fines take in to

account the gravity and duration of the breach, previous breaches and the potential systemic consequences of the breach, and the necessary content of any public censure.

The FCA also has available to it a range of general powers under the Financial Services and Markets Act 2000 to sanction companies that do not comply with the MLRs. These powers include, but are not limited to, public censure and a fine.

A person or entity found guilty of an offence of breaching a relevant requirement under the MLRs, on indictment, is liable to a maximum of 2 years imprisonment and/or a fine, and to a maximum of 3 months and/or a fine on summary conviction (MLRs, regs.86-88 & 92).

For *DNFBPs supervised by SRBs*, depending on the rulebooks of the 9 legal professional body supervisors and the 13 accountancy professional bodies, the relevant SRB can issue suspensions, fines, public censure and a takeover of the management of a firm. As a requirement of becoming an AML supervisor, HMT verifies that all SRBs have powers to remove or impose restrictions and that its members are liable to effective proportionate and dissuasive sanctions (MLRs, reg.49). SRBs are also able to refer cases to HMRC or FCA, who may then issue a sanction using its powers, including the imposition of unlimited fines. In 2018, the UK set up a new Office for Professional Body AML Supervision to work with SRBs to enhance their supervision and sanctions powers as necessary.

For land-based and online *casinos*, the Gambling Commission has powers to place restrictions or attach conditions on a casino's operating license or remove or amend an existing licence, give a warning, require a remote casino to be physically based in the UK or to suspend or revoke a license (Gambling Act 2005, ss.75, 77-78, 90, 116-121) in response to breaches of its licencing conditions (some of which related to AML/CFT measures for example, Licence Condition 12.1 & 5.1). A person commits an offence if he/she breaches a condition placed on their licence and is liable, on summary conviction, to imprisonment for up to 51 weeks (6 months in Scotland) (Gambling Act 2005, s. 139).

Criterion 35.2 – Sanctions are applicable not only to FIs and DNFBPs but also to their directors and senior management.

a) ***Targeted financial sanctions:*** the OFSI sanctions listed above apply to individuals and persons as well as entities, and therefore cover both directors and senior managers.

b) ***Preventive Measures and Reporting*** (R.9-23):

For *FIs and DNFBPs, supervised by HMRC or FCA:* In addition to other sanctions available in the MLRs, if an officer (which includes a director, chief executive or the management committee) is knowingly concerned in a breach of the MLRs, the FCA or HMRC may prohibit the person from holding office or issue a fine to the officer (MLRs, regs.3, 76 & 78).

If the FCA or HMRC are satisfied that an officer, manager or (in the case of FIs/MSBs/TCSPs) a beneficial owner identified in the application will fail to

comply with their AML obligations, it may refuse, suspend or cancel the registration of that applicant (MLRs, regs.59 and 60).

There are criminal offences available for when a 'connected person' contravenes the MLRs (reg.86) with a maximum imprisonment of 2 years for conviction on indictment. The FCA also has powers to sanction directors and senior management through its Senior Managers Regime including imposing a fine, public censures or statements on the individual, suspend or restrict the senior manager's approval or prohibit an individual from performing certain regulated functions (FSMA, ss.56, 63 & 66). For *DNFBPs supervised by SRBs*, all SRBs have the power to remove or restrict the regulated activities of managers, beneficial owners or others with a controlling interest in the entity; although not set out in legislation or regulation, this is a condition put on SRBs by HMT prior to be being appointed as an AML supervisor. Depending on their rulebooks, SRBs also have access to other sanctions, including suspension, fines and public censure.

For *casinos*, the sanctions available to the Gambling Commission under c35.1 in relation to entities are also available for directors and senior management (Gambling Act 2005, s.80).

Weighting and Conclusion

All criteria are met. **Recommendation 35 is rated compliant.**

Recommendation 36 – International instruments

In its 3rd MER, the UK was rated compliant with these requirements.

Criterion 36.1 – The UK has signed and ratified the Vienna Convention (December 1988 and June 1991 respectively), the Palermo Convention (December 2000 and February 2006), the TF Convention (January 2000 and March 2001), and the Merida Convention (December 2003 and February 2006).

Criterion 36.2 – The UK has implemented the Vienna Convention, the Palermo Convention, and the Merida Convention. One reservation was made to the Vienna Convention stating that in certain circumstances the UK would grant immunity only upon request. This does not impair implementation of the Convention.

Weighting and Conclusion

All criteria are met. **Recommendation 36 is rated compliant.**

Recommendation 37 - Mutual legal assistance

In its 3rd MER, the UK was rated largely compliant with these requirements. The technical deficiencies related to the ability of the UK authorities (excluding Scotland) to handle MLA requests in a timely and effective manner and the inability of the UK to ensure timely and effective turnaround of all requests.

Criterion 37.1 – The UK has a legal basis for the provision of a wide range of MLA, including: service; obtaining statements and evidence; entry, search and seizure;

production, customer information, and account monitoring orders; prisoner transfer; and restraint and confiscation (Crime (International Co-operation) Act 2003 (CICA); POCA (External Investigations) Order 2013 and 2014; POCA (External Requests and Orders) Order 2005). This assistance can be provided in respect of proceedings for ML, TF and predicate offences regardless of the existence of a treaty or assurances of reciprocity, although certain types of assistance are available only to countries with which the UK has a treaty relationship (see c.37.8).

Criterion 37.2 – The UK has three designated central authorities for MLA requests. The Home Office UK Central Authority (UKCA) handles requests to or from England, Wales and Northern Ireland. Revenue and Customs (HMRC) handles requests to or from England, Wales and Northern Ireland which relate to tax and fiscal customs matters. Finally, COPFS handles all MLA requests to and from Scotland. Information and guidance is available online to help requesting countries identify the relevant central authority.

Each central authority has its own IT-based case management system and mechanisms for the prioritisation and execution of requests. The UKCA has an electronic case management tool which allows cases to be monitored from creation to closure, and afterwards. Urgent requests are flagged for closer monitoring. HRMC maintains a spreadsheet of requests and cases are monitored by the International Mutual Assistance Team. Urgent requests are marked as such, and a specific system is in place to monitor urgent requests. COPFS has a computer-based case management system in which all requests are logged and urgent requests are identified. For all central authorities, requests under the European Investigation Order must be recognised within 30 days and executed within a further 90 days (Criminal Justice (European Investigation Order) Regulations 2017, No.730).

Criterion 37.3 – The UK accedes to the vast majority of MLA requests and does not subject requests to unreasonable or unduly restrictive conditions. The grounds for denying a request depend on the assistance sought, and may include: double jeopardy; contravention of human rights; public interest; the lack of a criminal or administrative investigation or proceedings; or the lack of reasonable grounds to suspect that an offence has been committed or that an investigation or proceedings have been commenced abroad (CICA, ss.14, 21; POCA (External Requests and Orders) Order 2005, ss.21, 68, 107; POCA (External Investigations) Order 2013 and 2014). The central authorities also have discretion to deny a request on the basis that it is trivial, politically motivated, made for the purpose of persecution, would result in imposition of the death penalty, or would prejudice the sovereignty, security, essential interests, or public order of the UK (MLA Guidelines for Foreign Authorities, pg.15). Dual criminality is required in certain circumstances (see criterion 37.6).

Criterion 37.4 – The UK does not refuse MLA requests solely on the basis that the offence involves fiscal matters, even where this is a possible ground for refusal in the relevant treaty (CICA, ss.32(7), 35(6), 37(7), 40(6); POCA (External Investigations) Order 2013 and 2014). However, requests relating to fiscal matters may be denied for lack of dual criminality if they are made by a non-treaty country and proceedings have yet to be initiated (CICA, s.14(4)). Secrecy or confidentiality does not constitute a ground for denying a request, with the exception of legal professional privilege (CICA, ss.26; POCA (External Investigations) Order 2013 and 2014).

Criterion 37.5 – The UK maintains the confidentiality of MLA requests received. This is required by most MLA treaties. Central authorities will neither confirm nor deny the existence of a request, nor disclose its content outside the necessary agencies or courts unless required and typically only with consent of the requesting authority.

Criterion 37.6 – England, Wales, and Northern Ireland require dual criminality for MLA requests for non-coercive actions from non-treaty or non-Commonwealth countries where the request relates to fiscal matters and proceedings have yet to be initiated (CICA, s.14(4)). In Scotland, dual criminality is a technical requirement for all MLA requests, both non-coercive and coercive, and the offence must be punishable by imprisonment. This deficiency is considered minor as a lack of dual criminality will not result in automatic refusal and the Scottish authorities will endeavour to execute the request through informal co-operation where possible.

Criterion 37.7 – The UK takes a conduct-based approach to assessing dual criminality. Technical differences between the offence's categorisation do not prevent the provision of assistance provided the underlying conduct is criminalised in both jurisdictions.

Criterion 37.8 – The UK can utilise all powers specified under R.31 in response to a MLA request provided they would also be available to domestic authorities and subject to the same conditions (e.g. judicial approval). This includes production orders, search and seizure, and obtaining witness statements, in addition to other investigative techniques such as undercover operations.

Weighting and Conclusion

Dual criminality is required for: MLA in Scotland, and requests from non-treaty or non-Commonwealth countries relating to fiscal matters and proceedings which have yet to be initiated regardless of whether the action requested is coercive or non-coercive. In practice the number of requests denied on these bases is small, and can be addressed through informal co-operation, so this deficiency is minor. **Recommendation 37 is rated largely compliant.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation

In its 3rd MER, the UK was rated compliant with these requirements.

Criterion 38.1 – The UK has the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize, and confiscate property:

(a) Laundered property can be identified on behalf of a requesting state through search and seizure, production orders, disclosure orders, customer information orders, and account monitoring orders provided there is an investigation in the requesting country into whether the property was illegally obtained, the whereabouts of illegally-obtained property, or ML (CICA, ss.32, 35, 37, 40; POCA (External Investigations) Order 2014, ss.6, 13, 16, 22, 29; POCA, s.447). This property can then be seized or restrained where the is an ongoing investigation or proceedings in the requesting state, or the requesting state has obtained a corresponding foreign order (POCA (External Requests and Orders) Order 2005, ss. 6, 56, 93; POCA, s. 447). A UK court may also freeze potential evidence, including instrumentalities, on the basis of

a foreign freezing order (CICA, s.20). Confiscation orders can be obtained on the basis of an equivalent order from the requesting state (POCA (External Requests and Orders) Order 2005, ss.22, 69, 108; Criminal Justice (International Co-operation) Act 1990 (Enforcement of Overseas Forfeiture Orders) Order 2005, s.19). The UK has also implemented the EU framework on mutual recognition of freezing and confiscation orders. Such orders from EU countries can be executed directly without being referred to a court or central authority.

(b) Proceeds can be identified, seized, and restrained on behalf of a requesting state using the mechanisms described in criterion 38.1(a).

(c) and **(d)** Instrumentalities used or intended for use in ML, TF or predicates can be identified, seized, and restrained on behalf of a requesting state using the mechanisms described in criterion 38.1(a).

(e) Property of corresponding value can be identified, seized, and restrained on behalf of a requesting state using the mechanisms described in criterion 38.1(a).

Criterion 38.2 – The UK is capable of providing assistance in the context of non-conviction based confiscation and related proceedings, including in circumstances where a perpetrator is unavailable by reason of death, flight, absence, or where the perpetrator is unknown. Instrumentalities, proceeds and laundered property can be identified through a range of available investigative measures which can be exercised on behalf of another state (POCA (External Investigations) Order 2013, ss. 6, 13, 16, 22, 29, 40, 47, 50, 56, 63). A UK court can also issue an order to freeze or confiscate this property, or property of a corresponding value, where there is an ongoing investigation or proceeding in the requesting state, or where a corresponding foreign order has been issued, provided there is dual criminality (POCA (External Requests and Orders) Order 2005, ss. 143, 144, 147, 161).

Criterion 38.3 – UK police forces can coordinate on seizure and confiscation with requesting states through police-to-police arrangements, multilateral organisations, or Joint Investigation Teams (JITs). The UK has mechanisms to manage and dispose of property frozen, seized or confiscated on behalf of a foreign state, including the appointment of management receivers or administrators or enforcement receivers (Criminal Justice (International Co-operation) Act 1990 (Enforcement of Overseas Forfeiture Orders) Order 2005, ss. 12, 22).

Criterion 38.4 – The UK is able to share confiscated property with other countries and endeavours to enter into 50:50 sharing arrangements the country to which it has provided assistance. Stolen state assets (e.g. the proceeds of corruption) are returned to the requesting state in full, less reasonable expenses

Weighting and Conclusion

All criteria are met. **Recommendation 38 is rated compliant.**

Recommendation 39 – Extradition

In its 3rd MER, the UK was rated compliant with these requirements.

Criterion 39.1 – The UK is able to execute extradition requests in relation to ML/TF without delay. There are two categories of incoming extradition request: a Part 1

request from European countries under the European Arrest Warrant system, and a Part 2 request from any other country.

(a) ML and TF are extraditable offences under UK law, provided they carry a sentence of at least 12 months' imprisonment in the requesting country (Extradition Act 2003, ss. 64, 65, 137, 138). There are

(b) Case management systems are in place for all incoming extradition requests. Clear processes exist for the timely consideration and execution of requests (Extradition Act, Parts. 1, 2). Part 1 requests are received by the NCA. For requests directed to England, Wales, or Northern Ireland, the NCA then decides whether the request is sufficient to arrest the individual. For requests directed to Scotland, the NCA forwards the request to the Scottish Ministers and the Cabinet Secretary for Justice makes this decision. In both cases, a court then decides whether to extradite. Part 2 requests to England, Wales, and Northern Ireland are received by the UK Central Authority while requests to Scotland are received by the Scottish Ministers. A court then decides on arrest and eligibility for surrender before the Secretary of State makes the final decision on extradition. Urgent requests are flagged and prioritised and a requesting country may also make a provisional arrest request in advance of submitting a formal request for extradition (Extradition Act, ss. 5, 73). Statutory time limits exist to ensure the extradition process proceeds in a timely fashion (Extradition Act, ss. 35, 117).

(c) The UK does not place unreasonable or unduly restrictive conditions on the execution of requests. The courts may deny extradition on the basis of: double jeopardy; passage of time; the person's physical or mental condition or age; forum; where extradition would be contrary to the Human Rights Act 1998; or where the request was made for the purpose of prosecution or prejudice on account of race, religion, nationality, gender, sexual orientation, or political opinion (Extradition Act, ss. 11, 21, 79, 87).

Criterion 39.2 – The UK extradites its nationals; there is no barrier under UK law preventing the extradition of British nationals on the sole basis of nationality.

Criterion 39.3 – The UK takes a conduct-based approach to assessing dual criminality; technical differences between the offence's categorisation do not prevent extradition provided the underlying conduct is criminalised in both jurisdictions.

Criterion 39.4 – The UK provides a simplified extradition mechanism for EAW requests. This allows for the direct transmission of requests between relevant European authorities without the use of diplomatic channels (Extradition Act, s. 3). The extradition process may also be simplified where the requested person consents (Extradition Act, ss. 46, 128).

Weighting and Conclusion

All criteria are met. **Recommendation 39 is rated compliant.**

Recommendation 40 – Other forms of international co-operation

In its 3rd MER, the UK was rated compliant with these requirements. These requirements were strengthened since the 3rd round MER.

General principles

Criterion 40.1 – The UK ensures that their competent authorities, including the NCA, the Police, the FIU, HMRC, the FCA, and DNFBPs supervisors, are able to provide a wide range of international co-operation in relation to ML, TF and predicate offences. Timeframes vary depending on the assistance and authority involved, but assistance is generally able to be provided rapidly.

Assistance can be provided both spontaneously and on request (Crime and Courts Act 2013, s.7 (NCA, FIU, Police); Criminal Justice Act 1987, s.3 (SF)); Financial Services and Markets Act 2000, s.354 (FCA); Anti-Terrorism, Crime and Security Act 2001, s.19 (HMRC); MLRs, reg.50 (FCA, HMRC, DNFBP supervisors)).

Criterion 40.2 –

(a) Competent authorities have legal bases for providing co-operation, including UK law or multilateral or bilateral agreements (Crime and Courts Act 2013, s.7 (Police, NCA, FIU); Financial Services and Markets Act 2000, s.354 (FCA); Anti-Terrorism, Crime and Security Act 2001, s.19 (HMRC); MLRs, reg.50 (FCA, HMRC, DNFBP supervisors).

(b) Nothing prevents the competent authorities from using the most efficient means to co-operate. Relevant authorities can co-operate directly with their counterparts in accordance with UK law.

(c) Competent authorities have clear and secure gateways, mechanisms or channels to facilitate, transmit and execute requests for assistance. Co-operation largely occurs through mechanisms established by the EU, Egmont, Europol, and Interpol. For example, the NCA uses Interpol and Europol mechanisms, secure electronic communication channels, or international liaison officers; the FIU uses Egmont Secure Web and FIU.net; the FCA uses its own established secure gateways; and HMRC uses secure electronic communication channels.

(d) Competent authorities have processes in place to assess and prioritise requests and ensure timely assistance is provided. For example, the FIU assessing requests upon receipt and uses a triage system to determine the request's priority. Police-to-Police requests are assessed for priority on a case by case basis and timeframes are agreed with the requesting agency. Where requests are made under multilateral or bilateral mechanisms all agencies work within the set timeframes for providing assistance.

(e) Competent authorities have processes for safeguarding any information received. The UK government classification system enables staff to assess the sensitivity of information and restrict it accordingly. The requesting authorities' classification marking will be respected. Where a requests is made pursuant to a multilateral or bilateral arrangement, any relevant confidentiality conditions will apply. Competent authorities are also bound by data protection laws (Data Protection Act 1998; Official Secrets Act, s.3).

Criterion 40.3 – Competent authorities have a range of bilateral and multilateral agreements and MOUs to facilitate co-operation with foreign counterparts. Such agreements are not required for UK authorities to provide assistance, but can be established promptly if required by foreign authorities.

Criterion 40.4 – Most competent authorities are able to provide timely feedback upon request to foreign authorities who have provided assistance, although this is not systematic and inconsistent across agencies. Many authorities endeavour to provide feedback even where this is not requested. The NCA utilises international liaison officers for this purpose.

Criterion 40.5 – The UK does not place unreasonable or unduly restrictive conditions the provision of information or assistance (Crime and Courts Act 2013, s.7; Overseas Security and Justice Assistance Guidance). Where the provision of assistance would jeopardise an ongoing domestic investigation, the FCA may agree with the requesting authority to delay the provision of assistance, but will not refuse the request outright. The UKFIU has provided an overly restrictive view to counterparts on the assistance it could provide, but as at March 2018, the policy was under review (see c.40.11).

Criterion 40.6 – The NCA, the FIU, and the NTFIU have internal guidance which ensures that information exchanged by competent authorities is used only for the purpose for, and by the authorities, for which the information was sought or provided, unless prior authorisation has been given by the requested competent authority (NCA Information Charter; National Intelligence Model and Handling Process). Other competent authorities, including the UKFIU, the Police, HMRC, the SFO, and the FCA, do not have law or guidance, but rely on standards set by relevant international bodies or arrangements (Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198), art.46(7); International Organisation of Securities Commissions Multilateral MOU (IOSCO MMOU), para.10; Europol Codes; relevant MOUs; etc.). These agencies apply equivalent standards outside the context of these particular frameworks and will use exchanged information only for the specified purpose or with the consent of the requested country.

Criterion 40.7 – Competent authorities are required to protect exchanged information in the same manner that they would protect equivalent domestic information. Agencies handling international classified information must be regularly inspected to ensure the information is sufficiently protected and secure. Competent authorities can refuse to provide classified information where the requesting authority cannot protect it effectively (Official Secrets Act, s.3; Data Protection Act 1998).

Criterion 40.8 – Competent authorities are able to conduct inquiries on behalf of foreign counterparts and exchange information which is domestically obtainable (Crime and Courts Act 2013, s.7 (NCA, UKFIU); Financial Services and Markets Act 2000, ss.169, 354A (FCA); MLRs, reg.50 (FCA, HMRC, DNFBP supervisors)).

Exchange of information between FIUs

Criterion 40.9 – The UKFIU has an adequate legal basis for providing co-operation on ML, TF and predicate offences regardless of whether their counterpart FIU is administrative, law enforcement, judicial or other in nature (Crime and Courts Act 2013, s.7; EU Council Decision 2000/642/JHA, art.7; CETS, art.46).

Criterion 40.10 – The FIU generally provides feedback to foreign counterparts on request, as well as endeavouring to provide spontaneous feedback where possible, on the use of information and the outcome of any analysis. The UKFIU will use the NCA's

International Liaison Officers to facilitate the provision of feedback. However, feedback from delegations suggests that in some cases, the sending FIU does not receive feedback, including on TF matters.

Criterion 40.11 – The UKFIU is able to exchange:

(a) information which it can access or obtain directly or indirectly (although the limitations identified in R.29 apply here); and

(b) other information which it can obtain or access, directly or indirectly, at the domestic level (Crime and Courts Act 2013, s.7).

However, the UKFIU has provided counterparts with written guidance on the information it can provide which has provided an overly restrictive view on the assistance available in relation to indirectly obtained information or additional information from reporting entities. The UKFIU has recognised this issue and as at March 2018, the policy was under review.

Exchange of information between financial supervisors

Criterion 40.12 – The FCA and HMRC have a legal basis for providing co-operation to their foreign counterparts, including exchanging supervisory information relevant to AML/CFT purposes. Such co-operation is permitted under UK law, as well as under multilateral or bilateral agreements (Financial Services and Markets Act 2000, ss.169, 354; MLRs, reg.50).

Criterion 40.13 – The FCA and HMRC are able to exchange domestically-available information with foreign counterparts, including information held by financial institutions, provided sharing is proportionate and appropriate (Financial Services and Markets Act 2000 (Disclosure of Confidential Information) Regulations 2001, reg.9, 12; MLRs, reg.50).

Criterion 40.14 – The FCA and HMRC can exchange any information they hold (including regulatory information, prudential information, and AML/CFT information) with relevant authorities provided the disclosure is relevant to the functions of the foreign authority or where relevant to prevent or detect ML and TF (Financial Services and Markets Act 2000, ss.169, 354; MLRs, regs.50, 52).

Criterion 40.15 – The FCA and HMRC are able to exercise domestic powers and conduct inquiries on behalf of overseas regulators, including conducting an investigation and obtaining information or documents (Financial Services and Markets Act 2000, ss.169, 354; MLRs, reg.50). Both the FCA and HMRC can permit representatives of an overseas regulator to assist in an investigation (e.g. by helping prepare an interview, or attending and asking questions).

Criterion 40.16 – The FCA acts in accordance with the IOSCO MMOU, which requires supervisors to use requested information solely for the purposes specified or within the general framework for use, unless prior consent is obtained from the requested authority (IOSCO MMOU, para.10). Where a request is made outside the IOSCO MMOU, the FCA would comply with any restrictions imposed on the use of the material by the foreign authority and would seek permission before using the material for a purpose other than for which it was given. HRMC will use requested information only for the purpose specified in the request. Where either agency had a legal obligation to disclose the information, the overseas authority would be informed and a mutually-agreeable position would be determined.

Exchange of information between law enforcement authorities

Criterion 40.17 – Law enforcement authorities (including the NCA, the NTFIU, the Police, HMRC, and e SFO) 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 (Crime and Court Act, s.7; POCA, part.8; Commissioners for Revenue and Customs Act 2005, s.20; Criminal Justice Act 1987, s.3(5)).

Criterion 40.18 – Law enforcement authorities are able to conduct inquiries and use domestically-available, non-coercive powers and investigative techniques to conduct inquiries and obtain information on behalf of foreign counterparts. Where coercive information is required, UK law enforcement can open an investigation (if there is a UK nexus) or a formal MLA request can be made (see R.37). Co-operation occurs mostly through EU, Egmont, Europol, and Interpol mechanisms and the UK abides by any restrictions on use imposed by these regimes (Crime and Court Act, ss.7, 8).

Criterion 40.19 – Law enforcement authorities in the UK are able to form joint investigative teams (JITs) to conduct co-operative investigations with foreign authorities. A bilateral or multilateral arrangement is not required by the UK to enable joint investigations, but can be entered into if required by other parties. JITs are typically facilitated by the NCA's International Liaison Officers, but can also be brokered directly where agencies have an existing relationship. JITs are formed for a set period and for a specific purpose (Crimes and Courts Act, s.7; Council Framework Decision on JITs (2002/465/JHA); Convention on Mutual Assistance in Criminal Matters between Member States; Second Additional Protocol to the Council of Europe Convention on Mutual Assistance; Convention on Mutual Assistance and Co-operation between Customs Administrations).

Exchange of information between non-counterparts

Criterion 40.20 – Competent authorities can exchange information indirectly with international non-counterpart authorities provided this is necessary and proportionate (Crime and Court Act, s.7; Financial Services and Market Act 2000 (Disclosure of Confidential Information Regulation 2001), reg.4; Anti-Terrorism, Crime and Security Act 2001, s.19). These authorities are bound by the same duties of confidentiality as set out above (see criterion 20.6).

Weighting and Conclusion

All agencies have the powers and abilities to provide a wide range of international assistance. There are some limitations in the UK's provision of assistance relating to the lack of feedback and an overly restrictive policy on the information the UKFIU can provide to counterparts. **Recommendation 40 is rated largely compliant.**

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations		
Recommendations	**Rating**	**Factor(s) underlying the rating**
1. Assessing risks & applying a risk-based approach	LC	• Guidance provided in the MLRs as to lower risk factors (e.g. clients or businesses based in the EU) are not always based on risk
2. National co-operation and co-ordination	C	• The Recommendation is fully met
3. Money laundering offences	C	• The Recommendation is fully met
4. Confiscation and provisional measures	C	• The Recommendation is fully met
5. Terrorist financing offence	C	• The Recommendation is fully met
6. Targeted financial sanctions related to terrorism & TF	LC	• The requirement to freeze assets that are jointly owned is not expressly stated in the regulations or legislation although guidance assists to provide some clarity on the issue • The communication of designations by OFSI is not immediate and can take up to 3-4 days Under the domestic listing mechanism, there are no specific provisions in law to protect the rights of bona fide third parties
7. Targeted financial sanctions related to proliferation	LC	• The requirement to freeze assets that are jointly owned is not expressly stated in the regulations or legislation although guidance assists to provide some clarity on the issue • The communication of designations by OFSI is not immediate and can take up to 3-4 days • Most supervisors, other than the FCA, rely on very general provisions to undertake checks on sanctions compliance, which would benefit from further clarification and consistency
8. Non-profit organisations	C	• The Recommendation is fully met
9. Financial institution secrecy laws	C	• The Recommendation is fully met
10. Customer due diligence	LC	• There is no explicit requirement to understand the ownership and control structure of customers that are legal persons (although FIs are likely to collect some of this information as a step in identifying the customers' beneficial owner) • There is no explicit requirement for FI's to understand the nature of the customer's business • The requirement to identify and verify the names of senior managers is not absolute (FIs are only required to take reasonable measures) and the requirements for legal arrangements are not clearly specified in line with c.10.9 • While broad requirements exist, there is no specific requirement for FIs to include the beneficiary of a life insurance policy as a potential ML/TF risk factor and there is no specific requirement to take enhanced measures at the time of pay-out • The Money Laundering Regulations provide guidance on lower risks in relation to EEA members which is not based on an assessment of risk

Compliance with FATF Recommendations		
Recommendations	**Rating**	**Factor(s) underlying the rating**
11. Record keeping	C	• The Recommendation is fully met
12. Politically exposed persons	C	• The Recommendation is fully met
13. Correspondent banking	PC	• Mandatory EDD measures regarding correspondent banking relationships apply only to respondent institutions outside the EEA
14. Money or value transfer services	C	• The Recommendation is fully met
15. New technologies	LC	• There is no requirement on FIs to assess the risks of new products and business products and delivery mechanisms, although this is covered in non-binding guidance
16. Wire transfers	C	• The Recommendation is fully met
17. Reliance on third parties	LC	• The MLRs do not require FIs to have regard to all available information on country risk before engaging a third-party introducer, in particular, the permitted reliance on intermediaries within the EU is based on the presumption that all EU members have equivalent AML/CFT standards for R.10 and R.11, rather than on individual country risk assessments undertaken by the authorities
18. Internal controls and foreign branches and subsidiaries	LC	• The full scope of information to be exchanged under group-wide AML/CFT programmes is not clearly articulated in regulation or guidance • FI's are not required to ensure that their branches and subsidiaries in the EEA have in place similar AML/CFT measures to the UK based on the assumption that all EEA members have implement the 4AMLD adequately
19. Higher-risk countries	LC	• The UK has mechanisms in place to apply counter-measures for higher-risk countries however these do not apply to EU countries
20. Reporting of suspicious transaction	C	• The Recommendation is fully met
21. Tipping-off and confidentiality	C	• The Recommendation is fully met
22. DNFBPs: Customer due diligence	LC	• Minor deficiencies in relation to R.10, 15 and 17 are equally relevant to DNFBPs
23. DNFBPs: Other measures	LC	• Minor deficiencies in relation to R.18 and R.19 are equally relevant to DNFBPs
24. Transparency and beneficial ownership of legal persons	LC	• Not all Scottish General Partnerships are required to register in the UK or maintain relevant information • Some types of low-risk legal person are not subject to registration requirements • The ability of Scottish General and Limited Partnerships to have corporate partners may create difficulties in ensuring these entities co-operate with competent authorities in determining the beneficial owner • Information and records on companies registered with Companies House are only required to be maintained by Companies House for two years • There are no requirements on societies, their committee members, or their regulator (the FCA) to maintain basic or beneficial ownership information post-dissolution

Compliance with FATF Recommendations		
Recommendations	**Rating**	**Factor(s) underlying the rating**
		• Neither insolvency practitioners nor company directors are required to keep information on directors, members or shareholders; constitutional and governing documents; or beneficial ownership information of companies' post-dissolution • Nominee shareholders need only register where they meet the threshold of beneficial ownership
25. Transparency and beneficial ownership of legal arrangements	C	• The Recommendation is fully met
26. Regulation and supervision of financial institutions	C	• The Recommendation is fully met
27. Powers of supervisors	C	• The Recommendation is fully met
28. Regulation and supervision of DNFBPs	C	• The Recommendation is fully met
29. Financial intelligence units	PC	• It is not clear if the UKFIU can seek all the additional information it requires from reporting entities - it was not clear if Further Information Orders can be obtained in a fashion that allows the UKFIU to perform it analysis functions as these new powers have not been tested • The UKFIU has a limited ability to conduct operational analysis due to the large number of SARs and limited human and IT resources • The UKFIU has limited IT capability to undertake complex strategic analysis • The UKFIU is not sufficiently independent from the NCA in defining its role or its priorities • The UKFIU's budget is determined on a yearly basis by the Director of the Prosperity Directorate in the NCA and the Director has the ability to surge resources, both from, and to, the UKFIU – it is not clear that it is able to obtain and deploy resources free from undue influence or interference
30. Responsibilities of law enforcement and investigative authorities	C	• The Recommendation is fully met
31. Powers of law enforcement and investigative authorities	C	• The Recommendation is fully met
32. Cash couriers	LC	• There is no declaration or disclosure system for cross-border transportation of cash or BNIs to or from an EU member state • The fines available for submitting a false declaration are not sufficiently proportionate or dissuasive • Cross-border cash declarations are shared with the UKFIU, but there is a minor deficiency due to limitations as to what data can be stored
33. Statistics	LC	• The UK does not maintain national statistics on ML investigations
34. Guidance and feedback	C	• The Recommendation is fully met
35. Sanctions	C	• The Recommendation is fully met

Compliance with FATF Recommendations		
Recommendations	**Rating**	**Factor(s) underlying the rating**
36. International instruments	C	• The Recommendation is fully met
37. Mutual legal assistance	LC	• Dual criminality is required for: MLA in Scotland, and requests from non-treaty or non-Commonwealth countries relating to fiscal matters and proceedings which have yet to be initiated regardless of whether the action requested is coercive or non-coercive
38. Mutual legal assistance: freezing and confiscation	C	• The Recommendation is fully met
39. Extradition	C	• The Recommendation is fully met
40. Other forms of international co-operation	LC	• The provision of feedback is not systematic and is inconsistent across agencies, including the UKFIU • The UKFIU has provided an overly restrictive view to counterparts on the assistance it could provide

Glossary of Acronyms[73]

ACB	Asset Confiscation Enforcement
AML	Anti-money laundering
AMLS	AML Supervision
ARO	Asset Recovery Offices
ATCSA	Anti-Terrorism, Crime and Security Act 2001
AUSTRAC	Australian FIU
ASP	Accountancy Service Providers
BEIS	Business, Energy and Industrial Strategy
BNI	Bearer negotiable instruments
BO	Beneficial ownership
CARIN	EU Camden Asset Recovery Inter-Agency Network
CCEW	Charity Commission for England and Wales
CCNI	Charity Commission Northern Ireland
CDD	Customer due diligence
CFA	Criminal Finances Act 2017
CFT	Counter-terrorist financing
CHIEF	Customs Handling of Import & Export Freight
COPFS	Crown Office and Procurator Fiscal Service
CPACC	Counter Proliferation and Arms Control Centre
CPS	Crown Prosecution Service
DAML	Defence Against Money Laundering
DATF	Defence Against Terrorist Financing
DIT	Department for International Trade
DNFBP	Designated non-financial businesses and professions
DPA	Deferred Prosecution Agreement
DPRK	North Korea
EAB	Estate agent businesses
EAW	European Arrest Warrant
EDD	Enhanced due diligence
EEA	European Economic Area
EIO	European Investigation Order
EU	European Union
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FCLO	Fiscal Crime Liaison Officer
FCO	Foreign and Commonwealth Office
FI	Financial institution
FIN-NET	EU Shared Intelligence System and Financial Information Network
FIS	Fraud Investigation Service

73 Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

FIU	Financial Intelligence Unit
FSMA	Financial Services and Markets Act 2000
FSRB	FATF-style regional body
FTF	Foreign terrorist fighter
GAIN	Government Agency Intelligence Network
HMRC	Her Majesty's Revenue and Customs
HMT	Her Majesty's Treasury
HVD	High value dealers
IACCC	International Anti-Corruption Coordination Centre
ICAEW	Institute of Chartered Accountants in England and Wales
ILO	International Liaison Officer
IO	Immediate Outcome
ISIL	Islamic State of Iraq and the Levant
JFAC	Joint Financial Analysis Centre
JMLIT	Joint Money Laundering Intelligence Task Force
JTAC	Joint Terrorism Analysis Centre
JMLSG	Joint Money Laundering Steering Group
ICIJ	International Consortium of Investigative Journalists
ICU	International Corruption Unit
IDR	Intelligence Development Referral
IT	Information technology
LEA	Law enforcement agencies
LSEW	Law Society of England and Wales
MER	Mutual evaluation report
MI5	Security Service
ML	Money laundering
MLA	Mutual legal assistance
MLR	Money Laundering Regulations 2017
MLRO	Money Laundering Reporting Officer
MOD	Ministry of Defence
MOU	Memorandum of understanding
MSB	Money service business
MVTS	Money or value transfer services
NCA	National Crime Agency
NHS	National Health Service
NIH	National Intelligence Hub
NPO	Non-profit organisation
NRA	National Risk Assessment
NSS	National Security Strategy
NTFIU	National Terrorist Financial Investigation Unit
OCTF	Organised Crime Task Force
OECD	Organisation for Economic Co-operation and Development
OFSI	Office of Financial Sanctions Implementation
OMET	Offender Management and Enforcement Team
OPBAS	Office for Professional Body Anti-Money Laundering Supervision
OSCR	Office of the Scottish Charity Regulatory
PACE	Police and Criminal Evidence Act 1984
PACE NI	Police and Criminal Evidence (Northern Ireland) Order 1989
PAMLP	Proactive Anti-Money Laundering Programme
PEP	Politically exposed person
PF	Proliferation financing

PNC	Police National Computer
PND	Police National Database
POCA	Proceeds of Crime Act 2002
PPSNI	Public Prosecution Service of Northern Ireland
PRA	Prudential Regulatory Authority
PSC	People with Significant Control
PSNI	Police Service of Northern Ireland
RART	Regional Asset Recovery Teams
RIS	Risk and Intelligence Service
ROCU	Regional Organised Crime Unit
SAMLP	Systematic Anti-Money Laundering Programme
SAP	Strategic Action Plan
SAR	Suspicious activity report
SFO	Serious Fraud Office
SCPO	Serious Crime Prevention Orders
SDSR	Strategic Defence and Security Review
SIENA	Europol Secure Information Exchange Network Application
SIS	Shared Intelligence Service
SOCPA	Serious Organised Crime and Police Act 2005
SRA	Solicitors Regulation Authority
SRB	Self-regulatory body
SYSC	FCA Senior Management Arrangements, Systems and Controls
TACT	Terrorist Act 2000
TAFA	Terrorist Asset-Freezing Act 2010
TCSPs	Trust and company service providers
TF	Terrorist financing
TFEU	Treaty on the Functioning of the European Union
TFS	Targeted financial sanctions
TPIM	Terrorism Prevention and Investigation Measures
UAE	United Arab Emirates
UK	United Kingdom
UKCA	United Kingdom Central Authority
UKFIU	United Kingdom Financial Intelligence Unit
UKICB	UK International Crime Bureau
UN	United Nations
UNSCR	UN Security Council Resolution
VAT	Value-added tax

www.fatf-gafi.org

December 2018

Anti-money laundering and counter-terrorist financing measures - United Kingdom

Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in the United Kingdom as at the time of the on-site visit on 5-23 March 2018.

The report analyses the level of effectiveness of the United Kingdom'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.