Anti-money laundering and counter-terrorist financing measures

Republic of Korea

Mutual Evaluation Report

April 2020

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 February 2020 Plenary meeting.

Citing reference:

FATF (2020), *Anti-money laundering and counter-terrorist financing measures – Republic of Korea,* Fourth Round Mutual Evaluation Report, FATF, Paris
http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-korea-2020.html

Photo Credit - Cover: ©

Table of Contents

Executive Summary

1. This report summarises the AML/CFT measures in place in the Republic of Korea as at the date of the on-site visit from 30 June to 18 July 2019. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Korea's AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

a) Korea shows a good understanding of its money laundering (ML) and terrorist financing (TF) risks informed by an ongoing risk assessment process. Its identification and cross-government response to the emerging risks posed by virtual assets is particularly positive. A deeper understanding of the risks relating to legal persons and arrangements would be useful. Strong policy and operational structures are in place to co-operate and co-ordinate at the national level on AML/CFT issues with involvement from a broad range of public and private sector agencies and institutions. However, co-ordination on proliferation financing (PF) issues is largely *ad hoc* and would benefit from a more formal system.

b) Financial institutions (FIs) and casinos are subject to a comprehensive AML/CFT framework which is generally well implemented. However, there are technical gaps and shortcomings in implementation relating to TF and PF-related targeted financial sanctions (TFS), and requirements for domestic politically exposed persons (PEPs) and PEPs of international organisations. FIs and casinos and their supervisors generally have a sound understanding of AML/CFT risks. Supervisors largely take a risk-based approach to supervision with the exception of the casino supervisor in Korea's self-governing province, Jeju. These strengths are somewhat undermined by designated non-financial businesses and professions (DNFBPs) other than casinos not being subject to Korea's AML/CFT framework nor monitoring.

c) Law enforcement agencies (LEAs) make good use of financial intelligence. This could be strengthened by increasing the resources of the Korean financial intelligence unit (KoFIU) and enhancing the strategic and operational analysis, in particular related to high-risk areas such as tax crime. LEAs take a "follow the money" approach which has been further strengthened by operational and structural changes since 2017. Korea makes efforts to pursue ML in line with its risks. However, while tax crime is identified as Korea's largest proceeds-generating offence, Korea's predicate offence framework only covers a tiny portion of tax offences preventing the pursuit of ML related to tax crime. Despite steps to prevent and detect the use of borrowed name accounts, (see para.39), this remains a common typology and is inherently difficult to investigate.

d) Asset recovery is actively pursued and has been a formal government priority since 2017 which has allowed for increased resources and specialisation. Between criminal asset recovery, tax levies, and restitution, Korea is able to deprive criminals of a reasonable value of proceeds. Further efforts are needed to increase the recovery of assets subject to confiscation and take advantage of available mechanisms to facilitate and ensure recovery. Authorities confiscate and recover both proceeds and assets of equivalent value in a manner largely in line with Korea's risks.

e) Korea has not had any TF prosecutions or convictions, which is consistent with its risk profile. Inquiries into 86 suspicions of TF show Korea is pursuing TF in line with its risks and vulnerabilities and demonstrate that authorities are well equipped to identify and investigate TF should it arise. Inter-agency co-operation and co-ordination in this area is strong and agencies actively use alternative measures.

Risks and General Situation

2. The main ML risks faced by Korea include seven major proceeds-generating offences: tax crimes; illegal gambling; fraud; corruption; market manipulation; trade-based ML related to property flight; and embezzlement/breach of trust. Korea identifies high ML risks from its vulnerability to the abuse of cash transactions (the main ML/TF instrument in Korea) and virtual assets (which have recently emerged). In response, Korea has issued regulations requiring the application of enhanced customer due diligence (CDD) when obliged entities are dealing with virtual assets. Virtual asset services providers (VASPs) are, however, not yet obliged entities.

3. The TF risk is currently low. Korea does not have any home grown terrorist groups, has not suffered any terrorist attacks in recent times[1] and there is no evidence of Korean non-profit organisations (NPOs) being used for TF. To date, there has been only one confirmed case involving terrorist-related activity (incitement by one individual). Nonetheless, Korea is aware that it remains at risk of being an intermediary for TF activities and its TF risks are increasing.

4. Korea is exposed to cross-border ML/TF risks from its large international trade flows and open, export-driven economy which could create an environment

1. No terrorist attacks have occurred since the bombing of Korean Air Flight 858 on 29 November 1987.

vulnerable to ML/TF activities, particularly via international transactions. On the other hand, Korea's exposure to cross-border remittance risks is much more limited as it has a relatively small foreign-born population and relatively small migrant remittance flows. Korea's foreign currency controls also help to mitigate the risks of cross-border transactions. "Borrowed name" accounts (where an individual allows a third party to use their account) are a common typology for both ML and tax crime (see para.39).

5. Korea has a well-developed financial sector, but is not a regional or international financial centre. Many of the DNFBP sectors (particularly lawyers, accountants, and dealers in precious metals and stones) are materially small.

6. A series of high-level and widely publicised corruption scandals involving two former Korean Presidents with strong ties to Korean conglomerates has greatly impacted public attitude and led to the strengthening of Korea's transparency, corporate governance and anti-corruption measures. Overall, FIs appear to be particularly sensitive to reputational risk. Financial inclusion is relatively high, and the estimated size of the shadow economy is below the global average.

Overall Level of Compliance and Effectiveness

7. Korea has implemented an AML/CFT system that is effective in some respects. Good results were achieved in Korea's use and development of financial intelligence, its understanding of its ML/TF risks, its efforts to recover criminal proceeds, its formal and informal co-operation with other jurisdictions, and its ability to pursue TF investigations and prosecutions, given its risks and context. Major improvements are needed to strengthen supervision and implement preventive measures, prevent misuse of legal persons and arrangements, investigate and prosecute ML, and implement TFS.

8. In terms of technical compliance, Korea's legal and institutional framework is largely strong and generally complies with the FATF Standards. However, improvements are required in relation to: applying a risk-based approach; TFS; NPOs; PEPs; requirements for and monitoring of DNFBPs; and the transparency of legal persons.

9. Since its last evaluation, Korea has improved its legal framework, including its ML and TF offences and confiscation regime. Confiscation has been formally designated as a high-government priority. CDD and enhanced measures have been strengthened, as have controls across financial groups and supervision. Suspicious transaction reporting (STR) requirements have been enhanced, and Korea has significantly enhanced inter-agency co-operation and information sharing. However, as at the time of its last MER, further work is required to prioritise ML investigations and ensure that all DNFBPs are brought within the scope of Korea's AML/CFT regime.

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

10. Korean authorities largely show a good and consistent understanding of Korea's ML/TF risks. Their risk understanding is informed by an ongoing risk assessment process that has generated three national risk assessments (NRAs) that demonstrate ongoing improvements to the risk assessment process and risk understanding. Additional input from NPOs and DNFBPs could further enhance Korea's

understanding of risk. National policies and activities are generally in line with the NRA, and could be further strengthened by a cohesive government-wide plan. Korea's response to virtual assets is a good example of the authorities' ability to co-ordinate and move quickly to address emerging risks.

11. National co-ordination and co-operation on AML/CFT issues is well developed at the policy and operational level. Policy co-ordination is enriched by dedicated sub-committees enabling representatives from a wide range of government agencies, private sector institutions and NPOs to provide input. Clearer co-operation mechanisms on PF would further strengthen the system.

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

Use of financial intelligence (Immediate Outcome 6)

12. Korea's LEAs regularly use financial intelligence to support investigations and prosecutions, trace criminal proceeds and identify risks. LEAs have access to a wide range of financial intelligence and make good use of KoFIU products, although there is scope for additional strategic analysis in high-risk areas. Additional permanent staff and continuing improvements to KoFIU's IT resources would further improve the quality of analysis and intelligence.

13. KoFIU has taken steps in recent years to improve the quality of suspicious transaction reports (STRs) which has improved the overall quality of reports. The utility of reports is limited by gaps in the reporting framework, as DNFBPs other than casinos are not subject to STR reporting requirements.

ML offence (Immediate Outcome 7)

14. Korean authorities take a "follow-the-money" approach in their law enforcement activities which leaves them well placed to identify and investigate ML. Policy and operational changes since 2017 have had a positive impact on the number of prosecutions and operational co-ordination among the relevant agencies works well. Korea's efforts to pursue ML in line with its identified risks are seriously undermined by the fact that tax crime, the most frequent and prevalent proceeds-generating offence, is not a predicate offence for ML. LEAs are successful in investigating, prosecuting and obtaining convictions for self-laundering, but it is not clear that standalone ML, third party ML or ML based on a foreign predicate are actively pursued. It does not appear that a ML conviction has a notable impact on sentencing. Alternative measures are pursued in tax crime cases, but are otherwise rare.

Confiscation (Immediate Outcome 8)

15. Korean authorities robustly pursue asset recovery and take steps to deprive criminals of a range of assets, including tangible and intangible assets and property of equivalent value. The confiscation process is streamlined and efficient with several strong features that should be actively used by authorities. Confiscation outcomes and target areas are broadly in line with Korea's risks and between criminal asset recovery, tax levies, and restitution, Korea is able to deprive criminals of a reasonable value of proceeds. Korea has had notable recent successes confiscating virtual assets. Korea could strengthen the system further by continuing to pursue efforts to recover a higher

percentage of confiscated assets and expanding its ability to confiscate the proceeds of fraud.

16. Relevant authorities are aware of the risks of cross-border movements of currency and bearer negotiable instruments (BNI) and measures are in place to detect this activity. Seizure and confiscation powers are used relatively infrequently. The sanctions imposed tend to be low compared to the amounts moved, but nonetheless have proved somewhat dissuasive based on recidivism rates.

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

TF offence (Immediate Outcome 9)

17. Korea has assessed its terrorism and TF risks as low, which is reasonable. It has had only one terrorism-related prosecution and one TF investigation with no TF prosecutions or convictions, which is consistent with its risk profile. There have been 86 instances where suspicions of TF have arisen but have not been substantiated following an LEA enquiry. These instances indicate that Korea is pursuing TF in line with its specific TF risks and vulnerabilities. Because of the lack of cases, LEAs lack TF experience, but have nonetheless demonstrated that they are well equipped to identify and investigate TF using a wide range of intelligence sources. There is strong inter-agency co-operation and TF investigations are integrated with national strategies. The penalties available for TF would allow effective, proportionate and dissuasive sanctions, but have not yet been tested in practice. Alternative measures are actively used, particularly deportation.

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

18. TFS are implemented in Korea without delay, however, there are some technical gaps and a scope issue as DNFBPs (other than casinos) are not covered. FIs and casinos are prohibited from dealing with designated entities and subject to a freezing obligation, although there are concerns that due to the lack of TFS-specific guidance funds may be rejected (rather than frozen) in some circumstances. Due to the limited scope of Korea's AML/CFT regime, DNFBPs (other than casinos) are not subject to or supervised for compliance with TFS. Korea has co-sponsored designations at the United Nations (UN), made a domestic designation, given effect to foreign designation requests, and frozen 272 million South Korean won (KRW) (206 666 euros (EUR)) of TF-related assets.

19. Korea has assessed NPOs as low risk for TF abuse. Korea has identified certain groups of at-risk NPOs based on their overseas operations or a particular shared characteristic. Involvement of NPOs themselves and a deeper understanding of the NPO sector as a whole would help strengthen and nuance this assessment. At-risk NPOs operating abroad are subject to strong reporting and supervision requirements and have access to ongoing outreach and support. Other at-risk NPOs would benefit from active engagement.

20. Korea has robust mechanisms for tracing and confiscating assets that could be used in the TF context, although there are no such cases to date. Overall, Korea's TF measures are consistent with its TF risk profile which is low.

Proliferation financing (Immediate Outcome 11)

21. Awareness of PF issues related to the Democratic People's Republic of Korea (DPRK) is very high in Korea. A ministry (the Ministry of Unification) is solely dedicated to matters related to DPRK. Both DPRK and Iran-related sanctions are actively implemented. Korea has designated 108 natural persons and 90 legal persons/entities domestically pursuant to the PF-related UN Security Council Resolutions (UNSCRs) and has co-sponsored 11 designations, but has not yet frozen any assets under these resolutions. There is good co-operation between authorities on designations, but there is no formal co-ordination on PF-related matters which is done on an *ad hoc* basis when needed.

22. The same framework described above in IO.10 is used to implement PF-related TFS and raises the same serious concerns (including the absence of guidance on TFS). FIs and casinos showed a good understanding of TFS obligations, particularly in the banking sector where proliferation-related assets are most likely to be found. FIs and casinos are supervised for compliance with these requirements and supervisors provide regular outreach, including on TFS. The limited scope of Korea's AML/CFT framework means that DNFBPs (except casinos) are not subject to or supervised for compliance with PF-related TFS.

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

23. The banking, securities and insurance sectors undertake the majority of financial activity in Korea with other types of FIs having a much smaller financial sector penetration. FIs and casinos are subject to comprehensive AML/CFT measures covering most aspects of the FATF Recommendations. However, the regulatory framework does suffer from some gaps. Domestic PEPs are not covered which is a serious issue, given Korea's identification of corruption as a major predicate offence. Casinos are subject to comprehensive AML/CFT obligations which is positive, as illegal gambling is another major predicate offence in Korea. However, other DNFBPs are not covered, even though the NRA identifies existing or emerging ML/TF risks in some of these sectors.

24. Larger individual FIs and casinos have a good understanding of their ML/TF risks and obligations due in part to vigorous outreach, training, and other efforts by Korean authorities. Smaller FIs and some casinos have a reasonable risk understanding, but need further improvements. In general, FIs and casinos understand and implement their obligations relating to CDD, beneficial ownership (BO), TFS, new technologies and PEPs (including domestic PEPs, although this is not a legal requirement). However, the use of borrowed name accounts (see para.39) creates some challenges. Most FIs and casinos are reporting suspicious transactions and the quality of STRs is improving. However, concerns about defensive reporting remains, particularly in the banking sector.

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

25. Licensing and registration measures for FIs and casinos are largely robust. While Korea's institutional and supervisory framework is complex, entrusted agencies (see para.84) have excellent co-operation and co-ordination. Except for casinos, DNFBPs are not subject to the AML/CFT framework or supervised.

26. Most supervisors have a good understanding of the ML/TF risks in their sectors and have a strong risk-based system for supervision. The exception is the supervisor of casinos in Korea's self-governing province (Jeju) which takes a rules-based approach to supervision. Supervision by KoFIU and the Financial Supervisory Service (FSS) would benefit from increased resources. Supervisors take remedial actions through administrative or monetary sanctions which are effective and dissuasive, but not fully proportionate. KoFIU has been active in providing guidance and outreach to supervised sectors, but need to issue targeted TFS guidance.

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

27. Korea has a growing understanding of the ML/TF risks associated with legal persons. It has identified the types of legal persons at risk of ML/TF, but authorities do not yet have a clear understanding of why these entities are particularly vulnerable and it is not clear that the risks are being effectively mitigated. This is important as LEAs reported seeing an increased use of complex typologies involving corporate structures in both ML and predicate offence cases. Steps have been taken to prevent misuse of legal persons, including prohibiting bearer shares, and nominee shares and directors. Basic and legal ownership information on legal persons is publicly available through a comprehensive network of registries. Competent authorities can trace BO information relatively easily through these registries, unless foreign ownership or a particularly complex corporate structure is involved. However, information on the registers may not always be accurate and up-to-date. Competent authorities may also seek BO information collected through the CDD process directly from FIs or casinos, although this channel will require a warrant in many cases so cannot be used at the intelligence-gathering stage. Sanctions for legal persons that fail to comply with their reporting obligations are limited.

28. Two types of trusts may be created under Korean law—commercial trusts and civil trusts (which are very rare). The risks of commercial trusts are significantly mitigated as these trusts are administered by licensed and regulated FIs. Limited information is available on the existence and characteristics of civil trusts and foreign trusts operating in Korea.

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

29. Korea has an effective framework for seeking and providing mutual legal assistance (MLA) and extradition. Co-operation under bilateral treaties is particularly effective and arrangements are in place to streamline co-operation with major partners. Korea should explore similar arrangements with other jurisdictions, particularly those featuring most often in Korea's ML and tax crime cases.

30. Competent authorities, including LEAs and supervisors, have channels in place to co-operate with counterparts, including posting attachés and liaison points in strategically important countries. The number of requests to and from KoFIU is increasing and current staffing levels may need to be reviewed if this trend continues. Overall, Korea's level of co-operation with foreign jurisdictions is generally in line with its risks, although the assessment team expected to see a higher level of co-operation related to BO information given the risks posed by asset flight and tax crime.

Priority Actions

Korea should:

a) Extend the AML/CFT framework to apply to all DNFBPs, and designate a supervisor for these sectors.
b) Expand the scope of AML/CFT obligations to include domestic PEPs and PEPs of international organisations.
c) Amend the law to expand the range of tax crimes that are ML predicate offences (for example, to align this range of crimes with those that require STR reporting) to ensure Korea is able to prosecute ML based on tax crime.
d) Continue exploring measures to promote the actual recovery of assets ordered for confiscation and systematically take advantage of available mechanisms and measures to facilitate confiscation and recovery.
e) Continue the positive efforts to pursue policy measures to prevent the use of accounts in borrowed names and explore tools to facilitate and enhance LEAs' ability to investigate and trace the movement of funds using such accounts.
f) Extend the freezing obligation to DNFBPs and all natural and legal persons, and address the identified technical deficiencies.
g) Issue targeted guidance on implementing TFS, including the freezing obligation, and ensure there is a forum for co-ordination on PF.
h) Continue to upgrade KoFIU's IT resources and increase the number of permanent staff to ensure institutional knowledge is maintained within KoFIU.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings[2]

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
Substantial	**Substantial**	**Moderate**	**Moderate**	**Moderate**	**Substantial**
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**	
Moderate	**Substantial**	**Substantial**	**Moderate**	**Moderate**	

Technical Compliance Ratings[3]

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	**LC**	**LC**	**C**	**LC**	**PC**
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
PC	**PC**	**LC**	**LC**	**C**	**PC**
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
C	**C**	**C**	**LC**	**C**	**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**	**PC**	**PC**	**PC**
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
LC	**LC**	**C**	**PC**	**C**	**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
LC	**LC**	**C**	**LC**	**LC**	**LC**
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**	**LC**	**LC**		

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

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

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 30 June to 18 July 2019.

The evaluation was conducted by an assessment team consisting of:

- Mr. Ayesh Ariyasinghe, Financial Intelligence Unit, Sri Lanka (legal & law enforcement expert)
- Ms. Daria Kudryashova, Rosfinmonitoring, Russian Federation (financial expert)
- Ms. Jennifer Sha Sha Fok, Department of Justice, Hong Kong, China (legal & law enforcement expert)
- Ms. Melanie Knight, Financial Conduct Authority, United Kingdom (risk, BO & targeted financial sanctions expert) and
- Mr. Qipeng Xu, People's Bank of China (financial expert)

with the support from the FATF Secretariat (Ms. Valerie Schilling, Ms. Liz Owen and Ms. Marlene Christiansen) and the APG Secretariat (Mr. Mohammad Al-Rashdan). The report was reviewed by: Mr. Ian Wong, Singapore Police Force; Mr. Markus Forsman, Ministry of Finance, Sweden; Mr. Michael Hertzberg, United States Treasury; and Mr. Filipe Manuel Peixoto Pereira, Directorate for Justice Affairs, Macao, China.

The Republic of Korea (Korea) previously underwent a FATF Mutual Evaluation in 2009, conducted according to the 2004 FATF Methodology. The 2009 evaluation and 2014 follow-up report have been published and are available at the following link.

The 2009 Mutual Evaluation concluded that Korea was compliant with 5 Recommendations; largely compliant with 14; partially compliant with 11; and non-compliant with 11. Korea was not rated compliant or largely compliant with any of the 16 Core and Key Recommendations.

Korea was placed on the regular follow-up process immediately after the adoption of its 3rd round mutual evaluation report. In June 2014, Korea 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

31. The Korea consists of the southern portion of the Korean Peninsula and its adjacent islands, located between China and Japan. The northern portion of the Korean Peninsula is the separate country of DPRK. After the outbreak of the Korean War in 1950, Korea and DPRK entered into an armistice agreement in 1953. Since then, there have been continuous efforts to transform the armistice regime into a peace regime.[4] Korea has nine provinces of which one—the Jeju Special Self-Governing Province (the SGP)—is self-governing.

32. Korea's population of 51.8 million, includes 2.2 million foreign nationals residing in Korea (4.2% of the total population) of which 1 million are from China, 680 000 are from Southeast Asia, and an estimated 305 000 are illegal aliens, including 219 000 short-term residents and 86 000 long-term residents.

33. Korea has a presidential system combined with elements of a parliamentary cabinet system and a Constitution. The Korean government comprises the executive, legislature and judiciary with separation of powers among these three branches. The President serves a single five-year presidential term and appoints the Prime Minister (who leads the executive) with the consent of the National Assembly. The Prime Minister recommends ministers and members of the State Council to the President for appointment and leads the Cabinet. The ministers, members of the State Council and heads of some authorities are appointed after passing parliamentary hearings. The Korean National Assembly is a 300-member unicameral legislature tasked with passing bills, supervising government agencies, examining the suitability of the appointment of the heads of government institutions stipulated in the Constitution of Korea through hearings and ratifying a variety of international treaties. Korean lawmakers serve four-year terms and enjoy the privilege of legislative immunity and the privilege of freedom from arrest during a legislative session.

34. The Korean legal system is a combination of continental civil law (historically modelled on that of Japan which was based on German law) and Anglo-American law. It includes the principle of due process, the Miranda rule, the prior warrant requirement, the right to remain silent, the presumption of innocence, freedom of the press, freedom of assembly and association, the right to be free from torture and the right to a fair trial.

35. The Korean judiciary is composed of three tiers of courts. At the top is the Supreme Court, below it are 6 High Courts, and as first instance courts are 27 District Courts and 57 Branch Courts. There are also three specialised courts: the Administrative Court, Family Court and Patent Court. The Constitutional Court reviews the constitutionality of laws and regulations and adjudicates on the impeachment of

4. Korean Ministry of Foreign Affairs (2013), "A Peace Regime on the Korean Peninsula", www.mofa.go.kr/eng/wpge/m_5477/contents.do.

the President and public officials, the dissolution of parties, and jurisdictional disputes between government entities and constitutional complaints.

ML/TF Risks and Scoping of Higher Risk Issues

Overview of ML/TF Risks

36. Korea is a comparatively low-crime country by international standards. It has experienced recent high-profile cases of economic crime, such as tax evasion, embezzlement and corruption.[5] According to the Korean police and prosecution service, Korea has no mafia- or yakuza-like organised crime syndicates and instead has loosely connected networks of "brotherhoods" involved in crimes such as online gambling,[6] loan-sharking, extortion and prostitution. Drug-related crimes are not at serious levels and the aforementioned brotherhoods are not generally involved in drug trafficking. However, Korea has the potential to be used as a transit point for drug trafficking, as it is known that its drug-related problems are not serious (which may lead to complacency) and the country has one of Asia's largest ports. There are no official estimates of the underlying levels of proceeds generating crime in the country.

37. Korea is exposed to cross-border risks from its immense international trade flows and open, export-driven economy that could create an environment vulnerable to ML/TF activities, particularly via international transactions. Inbound and outbound cross-border transactions are strictly controlled and monitored through foreign currency controls which helps mitigate Korea's cross-border ML/TF risks. Moreover, Korea has a relatively small foreign-born population and relatively small migrant remittance flows which further limits its exposure to cross-border remittance risks.[7]

38. Cash is widely used and vulnerable to ML/TF risks, but the proportion of cash transactions is declining with the rising use of credit, debit and pre-paid cards, and the development of financial technology. Korea does not issue very high denomination bank notes (which pose inherent high ML/TF risks because they make it easier to transport large sums) with the highest denomination being only KRW 50 000 (EUR 38). Korea has also implemented measures to prevent cash being used for tax crime which is a major proceeds-generating crime. The cash receipt system obliges businesses to issue cash receipts upon customer request; and the income deduction system grants income tax exemptions on expenditures paid by credit, debit or pre-paid cards or issued by cash receipt.[8]

39. Another common typology of both ML and tax crime is the use of "borrowed name" accounts. Under this typology, an individual opens an account in his/her own name and subsequently allow a third party to use the account. Sometimes, the third party is a related person (e.g. family member or close associate). Other times, the third

5. BBC News (2018), "South Korea's presidential scandal", www.bbc.com/news/world-asia-37971085; Reuters (2018), "Korean Air chief indicted on embezzlement, other charges: prosecutors", www.reuters.com/article/us-korean-air-probe/korean-air-chief-indicted-on-embezzlement-other-charges-prosecutors-idUSKCN1MP0GS; Reuters (2019), XinHuaNet (2019), "S.Korea's tax agency to intensify probe into companies' tax evasion", www.xinhuanet.com/english/2019-01/28/c_137781406.htm.
6. Gambling is only allowed in licensed casinos in Korea, whereas online gambling in Korea is considered a crime.
7. IMF World Economic Outlook (April 2018). World Bank Remittance data as of April 2019 cite Korea's migrant remittance inflows and outflows at 0.4% and 0.8% of GDP respectively. United Nations Department of Economic and Social Affairs report on Trends in International Migrant Stock: The 2015 Revision (link) which provides data for 232 jurisdictions.
8 Korea's National ML/TF Risk Assessment (2018), pg.108-111.

party purchases the use of the account from an account-holder who is otherwise unrelated/unconnected to them. Sometimes unemployed or low-income individuals sell the use of their accounts to make money. Although this is not a very sophisticated typology, it occurs quite frequently in Korea and makes it challenging to determine who actually controls an account.

40. For ML, Korea's 2018 NRA identifies seven major proceeds-generating offences: tax crimes; illegal gambling; fraud; corruption; market manipulation; ML related to property flight; and embezzlement/breach of trust. Korea identifies high ML risks from its vulnerability to the abuse of cash transactions (the main ML/TF instrument in Korea) and virtual assets.[9]

41. The NRA notes that banks have the strongest AML/CFT controls, but face medium-high ML/TF risks because of their high transaction volumes, broad customer base, and varied products and services. Securities companies also pose medium-high ML/TF risks despite the relatively small assets held by the sector, as they make frequent large deposits and withdrawals. Korea identifies medium ML/TF risks for insurance companies, non-banking depository institutions, specialised credit finance businesses, casinos, cross-border small-value remitters, lawyers, and dealers in precious metals and stones (DPMS). The NRA identifies low ML/TF risks for accountants, notaries, currency exchangers and credit businesses given the nature of the services they provide in the Korean context.

42. For TF, the NRA identifies the risk as being low. Korea does not have any home grown terrorist groups and has not suffered any terrorist attacks in recent times.[10] Its immigrant population is relatively small, although some foreigners from high-risk countries do reside in Korea, concentrated mainly in industrial areas around Busan and Jeju Island. Over the past ten years, Korea has investigated 86 individuals suspected of having links to international terrorist groups and raising funds to support terrorist activities overseas. However, investigations by the Korean authorities did not confirm any of these suspicions and the individuals were ultimately deported. There is also no evidence of Korean NPOs being used for TF. To date, there has been only one confirmed case involving terrorist-related activity (incitement by one individual).

43. Nevertheless, Korea acknowledges that it is at risk of being an intermediary for TF activities, partly due to its reputation as a terrorism and TF-free jurisdiction. The authorities consider Korea's TF risk to be increasing for the following reasons. First, Korea has a long-standing ally relationship with the United States (U.S.) (a target of terrorism). Second, Korea has a history of dispatching its army forces to the Middle East. Third, a large number of Korean companies are operating abroad (1 929 companies in 23 countries). Fourth, the number of foreign residents is growing. Fifth, ISIL declared in November 2015 that Korea was one of the 60 countries it would threaten with terrorism.

Country's Risk Assessment & Scoping of Higher Risk Issues

9 The FATF revised R.15 in October 2018 and its interpretive note in June 2019 to require countries to apply preventive and other measures to virtual asset service providers and virtual asset activity. This evaluation does not assess Korea's compliance with revised R.15 because, at the time of the on-site visit, FATF had not yet revised its assessment Methodology accordingly. Korea will be assessed for technical compliance with revised R.15 in due course, in the context of its mutual evaluation follow-up process.

10 No terrorist attacks have occurred since the bombing of Korean Air Flight 858 on 29 November 1987.

1

44. In November 2018, Korea published its third National Money Laundering and Terrorist Financing Risk Assessment (the 2018 NRA) which builds on Korea's first and second NRAs conducted in 2013-2014 and 2015-2016 respectively.

45. Korea's AML/CFT Policy Co-Ordination Committee prepared the 2018 NRA. The KoFIU Commissioner leads the Committee comprising 12 relevant competent authorities including LEAs, prosecutors, supervisors, customs authorities, intelligence and tax services. Using terminology and concepts based on the 2013 FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment, the 2018 NRA identifies Korea's major sources of illegal funds, ML/TF threats and vulnerabilities, and analyses its ML/TF risks. Following the "CELF" approach, (see para.93), the NRA analyses Korea's major predicate crime, its economic and geographical environments, legal framework to deter ML/TF, and financial system, including implementation of measures to deter ML/TF (see Chapter 2, Figure 2.1.).

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

a) **AML/CFT obligations and supervision of higher risk DNFBPs:** The NRA recognises casinos, dealers in precious metals and stones (which are often the subject of STRs), and lawyers as medium risk, notably for tax offending (a high-risk predicate). However, with the exception of casinos, DNFBPs are not subject to AML/CFT requirements or supervision. The assessors focused on how well casinos are implementing their AML/CFT obligations, and the impact of uncovered DNFBPs on the effectiveness of Korea's AML/CFT regime.
b) **Pursuit of ML related to major predicate offences:** The assessors focused on the extent to which LEAs successfully investigate and prosecute ML related to tax crimes, fraud and illegal gambling, and confiscate the proceeds. They also focused on Korea's understanding and mitigation of its cross-border ML risks, its international co-operation efforts, and whether its LEAs focus on the predicate offence at the expense of pursuing an accompanying ML investigation or charge.
c) **Virtual assets:**[11] Korea identifies virtual assets as high-risk for ML. The assessors focused on the extent to which obliged entities are aware of their ML/TF risk and the measures, if any, they are taking to mitigate this risk.
d) **Access to BO information:** Large enterprise structures with interlocking shareholdings dominate Korea's corporate landscape. This creates challenges for identifying the BO of legal persons. The assessors focused on the Korean authorities' understanding of BO, the risks it poses, and the measures in place to ensure competent authorities can access and share BO information. The assessors also considered the extent to which FIs are implementing preventive measures to prevent individuals from laundering money through accounts in borrowed names and the ability of LEAs to trace criminal proceeds in such accounts.

11. The FATF revised R.15 in October 2018 and its interpretive note in June 2019 to require countries to apply preventive and other measures to VASPs and virtual asset activity. This evaluation does not assess Korea's compliance with revised R.15 because, at the time of the on-site visit, FATF had not yet revised its assessment Methodology accordingly. Korea will be assessed for technical compliance with revised R.15 in due course, in the context of its mutual evaluation follow-up process.

e) **PF and TFS:** Korea has inherent vulnerabilities to PF from certain contextual factors (its geographic location and resulting familial ties, historic trade and business relationships with bordering countries, and three recent investigations into unsanctioned trade with DPRK). The assessors focused on the extent to which Korea identifies designated persons and entities and subjects them to freezing measures and prohibitions related to PF and TF, and the co-operation and co-ordination that exists between agencies on PF.

47. Through the scoping note exercise, the assessors identified one area for lesser focus. Notaries have a limited role in Korea and are responsible for preparing deeds and documents for signing. The Minister of Justice appoints notaries for five years with the possibility of a three-year extension. They do not perform financial business or activities listed in Recommendations 22 and 23. Given their limited functions, the assessors restricted their focus on notaries to the instances where they are combining their notarial role with another relevant function, such as that of a lawyer.

Materiality

48. Korea has the world's 11th largest economy with a gross domestic product (GDP) of EUR 1.4 billion. However, Korea is not an international finance hub or a centre for company formation and registration. The contribution of the financial sector to its GDP is around 4.9%, lagging behind those in other advanced countries.[12] Korea's shadow economy (estimated to be between 8% and 25% of GDP) is smaller than the average size of 31.9%.[13] Financial inclusion is high in Korea with more than 94% of the population over 15 years of age holding an account with a FI.[14]

49. Korea is an export-driven economy that imports raw materials from other countries to make finished products for export. Its major trading partners include China, Japan, the U.S., Saudi Arabia, Germany, the United Arab Emirates, Singapore, and Australia. Since trade is significant for its economy, Korea has actively implemented open-door economic policies including 15 free trade agreements with 53 countries.

50. Since the 1980s, Korea's fast pace of economic growth has been led by family-owned and managed Korean conglomerates called chaebol which are characteristic of Korea and rapidly grew on the strength of special government protection and support.

Structural Elements

51. Korea has all of the main structural elements required for an effective AML/CFT system including: political stability; a high-level commitment to address AML/CFT issues; stable institutions with accountability, integrity and transparency; the rule of law; and a capable, independent and efficient judicial system.

Background and Other Contextual Factors

52. Since the 1997 Asian crisis, led by overinvestment and a lack of financial supervision, Korea has implemented measures to enhance transparency in corporate

12. The contribution of the financial sector to the GDP in 2013 was 11.9 percent in Singapore, 6.6 percent in the United Kingdom, 6.5 percent in the United States, and 6.1 percent in Japan.
13. IMF Working Paper on Shadow Economies Around the World (2017) (link) estimated the average size of the shadow economy (both illegal and legal hidden activities) to be 31.9%, based on a study of 158 jurisdictions.
14. See World Bank data on account ownership, 2011 and 2014 (% age 15+) at the following link.

management, accounting and governance. In particular, Korea revised its accounting standards in line with global standards and significantly improved corporate governance of the *chaebol*. Transparency and corporate governance further improved as a large number of *chaebol* ended or considerably curtailed their family-based ownership structures and business management.

53. Korea first established its AML/CFT regime in 2001. Around the same time, it implemented measures to increase transparency and reduce corruption in the public and public sectors. Since its last MER, Korea has implemented the following measures:

a) In 2014, Korea amended the *Political Funds Act* to improve transparency in the flow of political funds and establish a culture of "clean" elections.
b) In 2016, Korea's anti-corruption law—the *Improper Solicitation and Graft Act*—came into force.
c) In 2017, the new government administration established anti-corruption policy as a national task and formed the Anti-Corruption Policy Council which is operated with the President as the chairperson.
d) In April 2018, the Anti-Corruption Policy Council formulated and began to implement a five-year national anti-corruption plan in conjunction with the relevant authorities.

54. Despite these measures, recent high-level and widely publicised corruption scandals involving two former Korean Presidents with strong ties to Korean conglomerates occurred, greatly affecting public attitude. Awareness of corruption and the potential risks of domestic PEPs is very high, particularly in the financial sector, which appears to be relatively risk averse and highly sensitive to reputational risks.

55. For PF, an important contextual factor is Korea's geographical proximity to neighbouring DPRK. At the time of this evaluation, Korea imposes sanctions on DPRK beyond those required by R.7 and IO.11 and the UN sanctions regime. Korean FIs have no relationship with FIs in DPRK, no wires transfers or other financial transactions are being undertaken between the two countries (other than humanitarian aid), and South Koreans could not travel to DPRK without government approval. Moreover, the population generally has a very high level of awareness of proliferation and related issues involving DPRK, given the long-standing political situation between Korea and DPRK, including a ministry dedicated to matters related to DPRK; the Ministry of Unification.

AML/CFT strategy

56. Korea's national AML/CFT strategy to build "AML/CFT systems that lead to building transparent and credible society" was formulated through discussions at the AML/CFT Policy Co-ordination Committee that were reported to cabinet meetings and finally adopted as official government policy. The strategy has three objectives:

a) **Build an advanced AML/CFT framework:** To this end, Korea is improving its AML/CFT system by submitting a wide variety of revised bills to the National Assembly and making efforts to upgrade systems in inadequate areas, including imposing AML/CFT obligations on the DNFBP sectors.
b) **Effectively use financial intelligence:** Each year, KoFIU collects, compiles and analyses more than 500 000 STRs, about 9 million cash transaction reports (CTRs), over 4 million reports on foreign exchange transactions and more than 60 000 reports on import and export means of payment.

Furthermore, KoFIU actively co-operates to provide information requested by LEAs, as needed, to facilitate investigations, prosecutions and confiscations.

c) **Build private sector capacity to implement AML/CFT requirements and firmly establish risk-based AML/CFT supervision and inspection**: KoFIU and the FSS have closely co-operated each year to assess AML/CFT performance at FIs that are subject to their supervision and developed a RBA system under which all FIs are electronically connected.

Legal & institutional framework

57. Three laws and subsequent amendments comprise the foundation of Korea's AML/CFT system:

a) the 2001 *Proceeds of Crime Act* (*POCA*) criminalises ML and covers the confiscation of criminal proceeds (including terrorist funds) and related MLA;
b) the 2001 *Financial Transaction Reports Act* (*FTRA*) sets out AML/CFT preventive measures; and
c) the 2007 *Act on Prohibition Against the Financing of Terrorism and Proliferation of Weapons of Mass Destruction* (*PFOPIA*) criminalises TF, implements TFS and covers MLA related to TF and PF.

58. Additionally, implementation of AML/CFT measures in Korea is based on:

a) the 1995 *Act of Special Cases Concerning the Prevention of Illegal Trafficking in Narcotics* (*ASPIT*) which regulates punishments against illegal transactions involving narcotics, related ML, and confiscation of proceeds;
b) the 1993 *Real Name Financial Transactions Act* which prohibits financial transactions under false names and numbered accounts, mandates every financial transaction to be implemented in real names and guarantees the confidentiality of financial transactions;
c) the *Act on International Judicial Mutual Assistance in Criminal Matters*; and
d) the *Act on Special Cases Concerning the Confiscation and Return of Property Acquired Through Corrupt Practices.*

Ministries and Co-ordinating bodies – Central organisations

59. **Financial** Services **Commission (FSC)** is responsible for licensing FIs, and for laws and regulations on various AML/CFT issues:

a) **Korea Financial Intelligence Unit (KoFIU)** (a subsidiary of the FSC and Korea's FIU) performs the policy function of overall management of Korea's AML/CFT policies, and submits legal amendments to the National Assembly under the direction of the FSC Chairman.
b) **Financial Industry Bureau** (under the FSC) is responsible for policies to prevent shell banks being established.
c) **Capital Markets Bureau** (under the FSC) is responsible for policies to identify the beneficial owners of companies.

60. **Ministry of Justice (MOJ) (International Criminal Affairs Division)** is responsible for: criminalising ML; seizing, freezing and collecting criminal proceeds; MLA regarding implementation of related UN resolutions; concluding extradition agreements; and providing policy support by amending relevant laws.

61. **Ministry of Economy and Finance (Foreign Exchange Policy Division)** is responsible for regulations on cross-border financial transactions and wire transfers,

payment and receipt guidelines for foreign transactions by persons subject to restrictions on foreign transactions, etc.

62. **Office for Government Policy Co-ordination (National Counter-Terrorism Commission)** co-operates with the National Intelligence Service (NIS) on overall management of national counter-terrorism policies in accordance with the *Act on Counter-Terrorism for the Protection of Citizens and Public Security*. It maintains a close partnership with the FSC to operate the Terrorism Information Integration Centre, which promotes the policy of intercepting in advance the formation of the sources of TF.

63. Ministry **of Foreign Affairs (MFA)** is responsible for international co-operation on TF:

a) **International Security Division** (under the MFA) relays designation requests from foreign countries to the FSC which reviews and discusses such matters with the relevant ministries (Ministry of Economy and Finance, MOJ, and MFA) to determine whether or not to designate the requested persons.
b) **Office of the Director for Disarmament and Non-proliferation** (under the MFA) in charge of co-ordinating an ad hoc intergovernmental panel of relevant ministries on the proliferation of weapons of mass destruction (WMDs) and is responsible for international co-operation in cases involving designation requests to or from foreign countries.

Criminal Justice and Operational Agencies

64. **Korea Financial Intelligence Unit (KoFIU)** is Korea's financial intelligence unit and is in charge of AML/CFT supervision. KoFIU is placed within the FSC.

65. **Korean National Police Agency (NPA)** is a LEA designated to investigate ML/TF and provide related international co-operation. A special team at the NPA Headquarters is dedicated to investigating cases of national importance or ML. The Criminal Investigation Bureau (within the NPA) sends information from KoFIU on suspicious transactions to local police stations.

66. **Supreme Prosecutors' Office (SPO)**, five High Prosecutors' Offices (Seoul, Daejeon, Daegu, Busan and Gwangju), and 58 District Prosecutors' Offices (DPOs) order and supervise ML/TF investigations conducted by LEAs and conduct their own investigations.

a) **Criminal Asset Recovery Division** (established in 2018 under the Anti-Corruption Department at the SPO)[15] focuses on tracing and confiscating criminal proceeds and investigating ML. Similar units exist in each DPO around the country, for example, the **Recovery of Proceeds of Crime Department** (established in 2018 under the Seoul Central DPO) focuses on tracing and confiscation.
b) **Asset Recovery Interagency Network–Asia Pacific (ARIN-AP)** (established in 2013 and led by the SPO) promotes a global communication network focused on quick exchange of information to recover criminal proceeds and facilitate related MLA.

15. This Division was originally established in 2006 under the High-tech and Financial Crime Investigation Division of the SPO.

67. **National Tax Service (NTS)** investigates alleged tax crime. Its International Investigation Division is in charge of analysing information provided by KoFIU. If the head of the division suspects a case of tax crime, the case is transferred to a related department or an office of the NTS in charge of the case.

68. **Korea Customs Service (KCS)** investigates false import and export reports relating to funds diversion, contraband, violation of trademarks or other exclusive rights related to import or export goods, evasion of customs duties or contraband subject to aggravated punishment, concealment of assets offshore, and related ML.

69. Korea Coast Guard (KCG) investigates ML/TF at the border areas including the coasts and ports, and exercises control over illegal entry, ML by illegal cash transfer, etc.

70. Fair Market Division and Capital Market Investigation Unit of the FSC investigate market manipulation and insider trading offences under the Act on Capital Market and Financing Investment Business and related ML.

71. National Election Commission has a Political Funds Investigation Division (established in 2004) to eradicate illegal political funds. KoFIU sends STRs related to illegal political funds to the National Election Commission for appropriate measures.

72. National Intelligence Service (NIS) collects information on and tracks terrorist suspects, including information related to their financial transactions. The NIS provides information to relevant agencies, which then can advance full-fledged investigations.

Financial sector and DNFBPs

73. Korea's financial sector accounts for approximately 5% of the production sector of the national GDP as of 2017. Korea is not an international financial hub. Overall, its FIs and DNFBPs are not as developed and their services not as promoted as much as in other advanced countries.[16] The Korean government strictly controls access to the financial market to avoid "over-burdening" it and has only issued two new banking licences in over 15 years.

74. The following table sets out what types of FIs in Korea conduct the financial activities covered by the FATF Recommendations.

Table 1.1. FIs conducting the financial activities covered by the *FATF Recommendations*

Types of Activities	Financial Institutions Conducting Financial Activities in Korea
A. Acceptance of Deposits and other repayable funds from the public (including private banking)	• Banks under the *Korea Development Bank Act*, the *Industrial Bank of Korea Act*, the *Banking Act*, the *Agricultural Co-operative Act*, and the *Fisheries Co-operatives Act* • Agricultural co-operatives pursuant to the *Agricultural Co-operatives Act* • Fisheries co-operatives pursuant to the *Fisheries Co-operatives Act* • Forestry co-operatives pursuant to the *Forestry Co-operative Act* • Credit unions pursuant to the *Credit Unions Act* • Community credit co-operatives pursuant to the *Community Credit Co-operatives Act*

16. See OECD STAN Databases re-citation of Causes and Solutions of Continued Deficit in Business Service Account Balance 2010 commissioned by the Ministry of Economy and Finance. It compares the added value of business services (including legal, accounting, tax, consulting, technology development, market research and public opinion polling, architectural and engineering, specialised design, photography, etc.) in Korea with that of other major countries such as France, Germany, Japan, the United Kingdom and the United States.

Types of Activities	Financial Institutions Conducting Financial Activities in Korea
	• Mutual savings banks pursuant to the *Mutual Savings Banks Act* • Korea Post pursuant to the *Postal Savings and Insurance Act*
B. Lending (consumer credit, mortgage credit, factoring with or without recourse, and finance of commercial transactions including forfeiting)	• Banks under the *Korea Development Bank Act,* the *Export-Import Bank of Korea Act,* the *Industrial Bank of Korea Act,* the *Banking Act,* the *Agricultural Co-operative Act,* and the *Fisheries Co-operatives Act* • Merchant banks, investment traders or investment brokers pursuant to the *Financial Investment Services and Capital Markets Act* • Insurance companies pursuant to the *Insurance Business Act* • Agricultural co-operatives • Fisheries co-operatives • Forestry co-operatives • Credit unions • Community credit co-operatives • Specialised credit finance businesses pursuant to the *Specialised Credit Financial Business Act* • Mutual savings banks
C. Financial leasing (except for financial leasing arrangements in relation to consumer products)	• Merchant banks • Specialised credit finance businesses
D. Money or value transfer services (except for any natural or legal person that provides institutional or non-institutional financial activities solely with message or other support systems for transmitting funds)	• Banks, including the Korea Development Bank, the Industrial Bank of Korea, the Agricultural Co-operative Bank (NH Bank) and the Fisheries Co-operative Bank (Suhyup Bank) • Merchant banks, investment traders or investment brokers • Agricultural co-operatives • Fisheries co-operatives • Forestry co-operatives • Credit unions • Community credit co-operatives • Credit card companies under the *Specialised Credit Financial Business Act* • Mutual savings banks • Communications Agency • Cross-border small value remitters registered in accordance with article 8(3)2 of the *Foreign Exchange Transaction Act*
E. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)	• Banks, including the Korea Development Bank, the Industrial Bank of Korea, the Agricultural Co-operative Bank (NH Bank) and the Fisheries Co-operative Bank (Suhyup Bank) • Investment traders or investment brokers • Agricultural co-operatives • Fisheries co-operatives • Forestry co-operatives • Credit unions • Community credit co-operatives (limited to debit cards & checks) • Credit card companies • Mutual savings banks
F. Financial guarantees and commitments	• Banks, including the Korea Development Bank, the Industrial Bank of Korea, the Agricultural Co-operative Bank (NH Bank) and the Fisheries Co-operative Bank (Suhyup Bank) • Merchant banks and Investment traders • Credit guarantee funds pursuant to the *Credit Guarantee Fund Act* • Technology credit guarantee funds pursuant to the *Technology Credit Guarantee Fund Act*
G. Trading in: (a) money market instruments (cheques, bills, certificates of deposit, derivatives, etc.) (b) foreign exchange (c) exchange, interest rate and index instruments	• Banks, including the Korea Development Bank, the Industrial Bank of Korea, the Agricultural Co-operative Bank (NH Bank) and the Fisheries Co-operative Bank (Suhyup Bank) • Merchant banks, investment traders or investment brokers • Insurance companies • Agricultural co-operatives

Types of Activities	Financial Institutions Conducting Financial Activities in Korea
(d) transferable securities (e) commodity futures trading	
H. Participation in securities issues and the provision of financial services related to such issues	• Banks, including the Korea Development Bank, the Industrial Bank of Korea, the Agricultural Co-operative Bank (NH Bank) and the Fisheries Co-operative Bank (Suhyup Bank) • Merchant banks, investment traders or investment brokers
I. Individual and collective portfolio management	• Banks, including the Korea Development Bank, the Industrial Bank of Korea, the Agricultural Co-operative Bank (NH Bank) and the Fisheries Co-operative Bank (Suhyup Bank) • Merchant banks, collective investment companies, discretionary investment companies, trust companies under the *Financial Investment Services and Capital Markets Act* • Insurance companies • Investment companies for the establishment of small and medium enterprises pursuant to the *Support for Small and Medium Enterprise Establishment Act*
J. Safekeeping and administration of cash or liquid securities on behalf of other persons	• Banks, including the Korea Development Bank, the Industrial Bank of Korea, the Agricultural Co-operative Bank (NH Bank) and the Fisheries Co-operative Bank (Suhyup Bank) • Merchant banks, collective investment companies, discretionary investment companies, trust companies • Insurance companies • Agricultural co-operatives
K. Otherwise investing, administering or managing funds or money on behalf of other persons	• Banks, including the Korea Development Bank, the Industrial Bank of Korea, the Agricultural Co-operative Bank (NH Bank) and the Fisheries Co-operative Bank (Suhyup Bank) • Merchant banks, collective investment companies, discretionary investment companies, trust companies • Insurance companies • Agricultural co-operatives • Fisheries co-operatives • Investment companies for the establishment of small and medium enterprises pursuant to the *Support for Small and Medium Enterprise Establishment Act* • New technology venture capital businesses under the *Specialised Credit Finance Business Act*
L. Underwriting and placement of life insurance and other investment related insurance (including insurance undertakings and to insurance intermediaries [agents and brokers])	• Banks, including the Korea Development Bank, the Industrial Bank of Korea and the Agricultural Co-operative Bank (NH Bank) • Insurance companies • Agricultural co-operatives • Credit unions • Credit card companies
M. Money and currency changing	• Banks, including the Korea Development Bank, the Industrial Bank of Korea, the Agricultural Co-operative Bank (NH Bank) and the Fisheries Co-operative Bank (Suhyup Bank) • Merchant banks, investment traders, investment brokers, collective investment companies, discretionary investment companies, trust companies • Insurance companies • Agricultural co-operatives • Fisheries co-operatives • Currency exchangers registered in accordance with article 8(3)1 of the *Foreign Exchange Transactions Act*

75. Korea has various financial markets. The Korean authorities consider three of them to be at risk of ML/TF: the deposit loan market, the securities market and the foreign exchange market. Korea's AML/CFT system therefore focuses on managing the ML/TF risks in these markets. Measured by total assets in the financial industry, banks including overseas branches account for the largest share (55%) followed by life insurance companies (15%), financial companies (which have increased to 7.3%,

reflecting the greater share of financial investment companies in relation to the capital market), and local agriculture, fishery and forestry unions (7.3%).

Table 1.2. Scale of assets & transactions by FIs (as of late 2017)

Types		General State (Unit: Numbers, Agents)					Soundness Indicators (Unit: KRW trillion)[17]		
		Companies[1]	Employees	Agents	Branches (agencies)	Foreign company Branches	Total assets	Net worth	Capital
Banks	Domestic	19	128 496		6 971	-	2 737.6	188.2	61.5
	Overseas branches	31	2 412		36	-	185.7	13.0	4.3
Financial Investment Companies	Investment Trading & Brokerage I (Securities Companies)	55	35 835		1 182	11	390.0	52.2	16.9
	Collective Investment Companies (Asset Management Companies)	215	7 328		-	-	7.1	5.7	2.1
	Investment Trading & Brokerage II (Futures Companies)	5	382		1	-	3.3	0.4	0.1
	Non-Bank FIs	1	81		5	-	1.9	0.3	0.3
Insurance Companies	Life Insurance	25	25 391	106 989	3 488 (6 450)	9	832.8	71.4	10.3
	Indemnity Insurance	32	32 446	81 968	2 993 (29 277)	14	277.1	35.2	3.0
Mutual savings	Mutual Savings Banks	77	9 004		318	-	59.7	6.8	4.3
Mutual Financial Companies	Credit Co-operatives	898[2]	17 336		1 649	-	82.1	6.9	4.8
	Agriculture, Fishery & Forestry Unions	1 358[3]	106 176		5 308	-	390.4	27.9	12.0
	Community Credit Co-operatives	1 315	29 142		3 168	-	150.5	12.4	6.3
Credit-Specialised Companies	Credit cards	8	10 978		351	-	113.9	26.5	5.2
	Hire-Purchase Companies	21	21		276	-	67.1	9.7	2.5
	Leasing Companies	26	26		177	-	54.2	7.6	2.3
	New Technology Venture Capital Companies	42	42		53	-	9.8	2.8	1.3
	TOTAL	4 128	4 128	188 957	25 976 (35 727)	34	5 363.2	467	137.2

Notes:
1 This table excludes some of the financial company groups including financial holding companies, credit rating companies and investment advisory companies.
2 Including domestic branches of foreign financial companies.
3 Local unions.
Source: *Monthly Financial Statistics* (FSS), *Major Financial Statistics* (FSC).

76. Other institutions conducting financial affairs include post offices, currency exchangers, small value remitters, electronic financial service providers and credit businesses:

a) **Post offices** use branches across the country to sell small insurance products and treat small household savings in the farming and fishing villages as tasks

17. KRW 1 trillion is the equivalent to approx. EUR 768 million.

secondary to postal service. The total amount of the savings accounts in the post offices is KRW 124.4 trillion (EUR 94.7 billion) as of late 2017.

b) **Currency exchangers:** There are around 1 610 registered currency exchangers as of February 2018 of which 593 are individual money exchangers and the remaining 1 017 are mainly run by hotels, local agricultural or fishery co-operatives, etc. Currency exchangers may only buy (not sell) foreign currencies from Koreans and foreigners (they do not undertake wire transfers). For foreigners, currency exchangers may also provide the service of exchanging Korean currency to foreign currency within the amount of money exchanged when the foreigner entered the country. One currency exchanger provides exchange services through ATM-style kiosk machines using automated passport ID checks and verification.

c) **Small value remitters:** 12 small value remitters are licensed, these do small value domestic and cross-border wire transfers strictly limited to 3 000 U.S. dollars (USD) per transaction (most are around USD 1 000) and USD 20 000 of business per customer per year.

d) **Electronic financial service providers:** 146 electronic financial service providers are licensed and have been subject to AML/CFT requirements since 1 July 2019. Although electronic financial service providers can apply for authorisation to provide cross-border wire transfers up to KRW 2 million (EUR 1 515), none have yet done so. Instead, electronic financial service providers currently focus on simple domestic money transfers and simple payment. They do not offer accounts.

e) **Credit businesses** raise funds by external borrowings, and manage the funds at higher interest rates (24% per annum) and conduct small lending to self-employed or workers who find it hard to get loans from financial companies. As of late 2017, the number of registered credit businesses is 8 084, of which 218 are large (mainly foreign) credit businesses subject to external audit and account for about 86% of the Korean credit business industry.

DNFBP sectors – Size, makeup and key features

77. The following table sets out the DNFBPs operating in Korea, what activities they conduct and the size of each sector.

Table 1.3.DNFBP sectors in Korea

Type	Description of the sector & activities conducted	Size of the sector
Casinos	• Provide casino gaming to foreign tourists (16 casinos of which 8 are on Jeju Island and 8 in mainland Korea, in hotels serving foreign tourists which prohibit Koreans from entering). In 2017, these casinos were visited by 2 216 foreigners. • Providing casino gaming to Koreans (1 casino located four hours from Seoul in a former mining town – Kangwon Land Casino). In 2017, this casino was visited by 5 331 Koreans. • Only land-based casinos exist in Korea, there are no licensed ship-based casinos. The law bans on-line casinos or casinos without a place of business.	17 casinos* with an average spending per visitor of: • KRW 523 000 (EUR 398) for foreigners • KRW 286 000 (EUR 218) for Koreans *as of late 2017
Accountants (certified public accountants)	• Certified public accountants conduct accounting and auditing, tax advisory services for corporations, management advisory services for managers, etc. and advisory services relating to establishing companies.	18 473 certified public accountants of which: • 9 840 (53%) belong to accounting firms

Type	Description of the sector & activities conducted	Size of the sector
	• Accountants registered as "audit force" are a team of three or more accountants with their own offices to provide external audit services. • Certified public accountants do not provide business services, financial transaction services, bank account opening or cash depository services for customers.	• 1 362 (7%) are registered as "audit force" • 687 (4%) operate as individuals • 6 584 (26%) engage in other businesses after suspending the certified public accounting business
Accountants (tax accountants)	• Tax accountants conduct registering tasks including preparation of tax report registers, reconciliation of differences between corporate financial accounting and the *Customs Act,* settlement of accounts including preparation of financial statements, filings of tax appeals, etc. • Their major tasks are writing tax report registers, with their services including settlement such as preparing financial statements of small companies.	11 725 tax accountants of which: • 3 521 belong to law firms • 7 716 operate individual offices • 488 suspended the business
DPMS	• Most of the supplies of precious metals and stones in Korea depend on import • Dealers engage in manufacturing, workmanship, processing, transactions, brokerage or mediation of precious metals and stones, sales of watches, etc. • Business is concentrated in large cities such as Seoul (75% of wholesalers), Busan or Gyeonggido Province	• 11 151 dealers in charge of processing and sales with 19 962 engaging in industry* • Average annual sales per business is KRW 0.143 billion with most of the businesses being small *as of late 2014
Lawyers	• Lawyers handle legal issues as well as wider areas including accounting, management, technology development, investment strategies, conducting representation of corporations and individuals, consultation and advisory, preparation and review of contracts, dispute settlement, etc.	17 759 lawyers with 949 law firms of which: • 9 044 (51%) belong to law firms • 73% are concentrated in Seoul* *as of March 2016
Notaries public	• Notaries public prepare notarial deeds or certify documents written and signed by private persons. • They are not allowed to operate a financial business.	• 217 operating notary offices
Real estate agents	• Transactions of real estate, sales of new houses, brokerages for real estate leasing, etc. • Brokerage fees are 0.2 to 0.9% of the transaction value in sales or exchanges, and 0.2 to 0.8% in leasing • 59% of all real estate agents are located in Seoul and Gyeonggido Province	102 100 real estate agents* of which: • 100 997 (99%) are individuals conducting brokerage business • 1 103 (1%) are companies *as of late 2017
Trust and company service providers (TCSPs)	• Services regarding the establishment of companies and trusts are generally provided by lawyers. • Although a small number of companies are advertising such services on-line, the Korean authorities indicate that these business provide simple advisory services, rather than the broader range of more complex TCSP services	TCSPs are not recognised in Korea as a separate profession

Relative weighting of the different types of FIs and DNFBPs

78. This section explains how the assessors weighted the relative importance of the different types of FIs and DNFBPs in Korea, taking into account the country's unique risks, materiality and context:

- **Most important is the banking sector** because it has by far the largest share of the financial sector's total assets, undertakes the vast majority of cross-border transactions, and also faces risks from high transaction volumes, a

broad customer base, varied products and services offered, and exposure to emerging risks from virtual assets. The NRA identifies banks as having medium-high risks.

- **Highly important sectors are:**
  - **Securities firms and brokers:** Although this sector is relatively small in terms of assets held, it is exposed to risks from the nature of the business (frequent large deposits and withdrawals), cross-border risks (foreign investment) and emerging risks from virtual assets. Moreover, the NRA identifies them as having medium-high risks, and market manipulation and other unfair trade practices are major predicate offences.
  - **Casinos:** Although there is a relatively small number of casinos (17), they are very exposed to cross-border risks as their business exclusively targets foreigners (with the exception of one casino that serves Korean nationals). Moreover, illegal gambling and other illegal speculative acts are major predicate offences in Korea. The NRA identifies them as having medium risks.
  - **Insurance companies:** Korea has a relatively large insurance sector accounting for 15% of the financial industry's total assets. Although insurance products and services generally carry lower ML/TF risks, the sector is vulnerable to voice phishing and other types of financial fraud (major predicate offences in Korea). The NRA notes that insurance proceeds are used for illegal purposes and identifies them as having medium risks.
- **Moderately important are DPMS**: Although not materially significant, the NRA identifies DPMS as having medium risks as they are often used for tax evasion (customs duties) and flight of assets overseas via cash transactions and frequently the subject of STRs filed by reporting entities. No cases have been identified of DPMS being used to evade sanctions.
- **Less important sectors are**:
  - **Currency exchangers:** This sector is materially small and offers limited services (buying, but not selling foreign currency, and not doing wire transfers) which greatly limits its ML/TF risks. The NRA identifies their risks as low.
  - **Electronic financial service providers:** Materially, this sector is also very small. The ML/TF risks are limited as electronic financial service providers offer very basic services (simple domestic money transfers and simple payment) with no cross-border activity undertaken to date. The NRA identifies their risks as low.
  - **Small value remitters:** This is a materially small sector. The NRA identifies the risks of cross-border small value remitters as medium, but restrictions on transaction size (USD 3 000) and the annual volume of business per customer (USD 20 000) limit small value remitters' usefulness as a way to effectively launder large amounts of proceeds. While TF may involve very small amounts, Korea's TF risk is low which also impacts the weighting of this sector.

- **Accountants:** In Korea's context, accountants traditionally provided a limited range of services mainly focused on auditing. The NRA identifies the risks of accountants as low, but notes that potential risks are emerging as more accountants are starting to provide capital flow and management services that may be used for ML/TF purposes. Over 40% of Korea's 30 198 accountants do not fall within the FATF definition of a DNFBP as they either work in-house or for external audit teams or do business focused on filing tax returns on behalf of clients once the books are closed.
- **Lawyers:** Korea has a relatively small legal sector that traditionally focused on litigation-related affairs. Of Korea's 17 759 lawyers, almost 50% do not fall within the FATF definition of a DNFBP as they work in-house. The most frequent ML typology involving lawyers is high-level CEOs/managers of large corporations using the corporation's own in-house legal professionals to set up complex corporate structures to facilitate embezzlement or tax crime and related ML. The NRA identifies lawyers' risks as medium with emerging risks as the sector expands and lawyers start to offer more client asset management and consulting services.
- **Real estate agents:** The NRA identifies the risks of real estate transactions and loan-back schemes using mortgages; however, ML through the real estate sector does not appear to be a widespread typology. Korea has implemented measures banning ownership of real estate in another person's name.

79. Notaries in Korea do not provide the types of services classified as financial activities under the FATF Standards. TCSPs are not a separate sector in Korea, with lawyers generally providing these activities.

Preventive measures

80. The 2001 FTRA sets out AML/CFT preventive measures. All financial institutions and casinos are subject to comprehensive AML/CFT requirements, but other types of DNFBPs are not. These exemptions have not been justified based on low risk.

Legal persons and arrangements

81. As of the end of 2017, there were 769 684 legal persons in Korea categorised as indicated in the table below.

Table 1.4. Types of legal persons operating in Korea (as of the end of 2017)

Domestic	For-profit	Partnership company	939
		Limited partnership company	3 731
		Stock company	690 241
		Limited Company / Limited Liability Company (LLC)	33 645
	Non-profit (Incorporated Association / Incorporated Foundation		39 226
Foreign			1 902
TOTAL			769 684

82. The categories of for-profit legal persons are set out in the Commercial Act (art.169):

a) **Partnership Companies:** All partners have direct, joint and unlimited liability for company debts.
b) **Limited Partnership Companies:** A partnership company combined with elements of limited partners in that the general partners participate in the material business operation, while the limited partners provide capital and participate in the distribution of profits from the business.
c) **Stock Companies:** Subscribers hold indirect and limited liability to the extent of the amount of the subscription price. The shares are freely transferable, in principle. Korean law does not allow companies to issue bearer shares.
d) **Limited Companies:** Like subscribers of a stock company, partners hold indirect and limited liability for company debts, only with the company assets as collateral. However, there are differences from a stock company in that, under certain circumstances, partners may be liable for compensation for losses in capital and limited companies have a simpler organizational structure.
e) **Limited Liability Companies:** Korea newly introduced this structure under the *Commercial Act* in April 2011. Limited liability companies have some material characteristics of a partnership (similar to a partnership company or a limited partnership company) and its partners hold indirect and limited liability (similar to stock companies and limited companies).

Supervisory arrangements

83. KoFIU is responsible for general supervision over AML/CFT tasks for the financial sector. It is also the competent authority overseeing nine casinos in mainland Korea for their implementation of AML/CFT requirements.

84. For financial institutions, the Commissioner of KoFIU assigns AML/CFT inspection responsibilities to various agencies ("entrusted agencies") and conducts joint inspections with them when necessary. The entrusted agencies report their inspection results to the Commissioner of KoFIU and have the authority to execute reprimand or correction orders when necessary. KoFIU directly levies and collects administrative fines for violations detected through inspections. The Board of Audit and Inspection of the Republic of Korea and other higher agencies conduct audits of inspection programs at the assigned agencies with the aim of helping ensure their effectiveness.

85. For casinos located in the SGP, the Commissioner of KoFIU assigns AML/CFT inspection responsibilities to the provincial government. The Korea Casino Association is a business group representing the industry, but is not a self-regulatory body (SRB) and does not conduct any supervisory or regulatory tasks.

86. Other DNFBPs are not subject to AML/CFT requirements. However, they do have their own regulatory authorities and SRBs that can impose sanctions for violations of their rules. Examples include the Korea Association of Realtors, the Korean Bar Association, the Korean Institute of Certified Public Accountants and the Korean Association of Certified Public Tax Accountants.

1

Table 1.5. Agencies assigned AML/CFT inspection responsibilities by KoFIU

Agency assigned inspection responsibilities by KoFIU	Type of financial institutions being inspected
Financial Supervisory Service (FSS) (within the FSC)	• Banks, merchant banks, mutual savings banks • Investment traders, investment brokers, collective investment companies, discretionary investment businesses, specialised credit finance institutions • Trust companies • Securities companies • Transfer agents • Insurance companies • New technology venture investment associations • Financial holding companies • Agricultural Co-operative Bank, Agricultural Co-operative Life Insurance, Agricultural Co-operative Property & Casualty Insurance • National Federation of Fisheries Co-operatives • National Forestry Co-operatives Federation • Cross-border small value remitters
FSS & the National Agricultural Co-operative Federation	• Agricultural co-operatives
FSS & the National Federation of Fisheries Co-operatives	• Fisheries co-operatives
FSS & the National Forestry Co-operatives Federation	• Forestry co-operatives
FSS & the National Credit Union Federation of Korea	• Credit unions
FSS & the Korea Federation of Community Credit Co-operatives	• Community credit co-operatives
Ministry of Science & ICT	• Post office (Korea Post)[18]
Ministry of SMEs and Start-ups	• Investment companies for the establishment of SMEs • SME establishment investment associations
Korea Customs Service (KCS)	• Currency exchange businesses
Jeju Special Self-Governing Province (SGP)	• Casinos in operation within the province

International co-operation

87. Due to its globalised and open economy, with free flows of trade and other global activities, Korea faces international ML/TF risks including those from unfair trade, tax crime and market manipulation using overseas shell companies. International trade in Korea is often a vehicle for ML/TF.

88. Korea has special arrangements with three of its largest trading partners (the U.S., Japan and China) which greatly speeds and facilitates international co-operation with these countries. At the FIU level, KoFIU's five major partner countries are: the U.S.; Hong Kong, China; China; the United Kingdom (U.K.); and Singapore. Korea has concluded multiple bilateral MLA and extradition treaties. The number of countries bound by such treaties is 74 for MLA and 77 for extradition treaties. The central authority for MLA is the MOJ.

18. Korea post is a government agency and the only post office allowed in Korea. In the legislation it is covered under "communication agency".

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

Key Findings and Recommended Actions

Key Findings

a) Korea shows a good understanding of its ML and TF risks. Korea's risk understanding is informed by an ongoing risk assessment process that has resulted in three NRAs (2014, 2016 and 2018) supplemented by additional assessments in specific areas. Each NRA reflects lessons from the previous NRA, resulting in ongoing improvements to the risk assessment process and an improved assessment and understanding of Korea's risks. Korea's identification and cross-government response to the emerging risks posed by virtual assets is particularly positive. National policies and the activities of competent authorities reflect Korea's risk understanding to a large extent, although no measures are in place for DNFBPs (except for casinos) and national action plans do not comprehensively reflect all relevant activities and cross-government work.

b) The 2018 NRA process received input from a wide range of relevant government agencies and private sector institutions, resulting in a broad and consistent risk understanding in line with the NRA. Most LEAs and supervisors have a strong risk understanding, with the exception of the recently designated supervisor, the SGP, responsible for supervising casinos in Jeju.[19] Additional input from NPOs and DNFBPs could further enhance Korea's risk understanding.

c) FIs and casinos are required to apply enhanced measures when they identify high-risk customers, and may apply simplified measures when they identify low-risk customers. The legal framework provides an exemption from verifying the identity of ultimate owners and controllers of specific companies and government bodies. Korea demonstrated that these exemptions were based on proven lower risk for these types of entities.

d) Korea has strong policy and operational structures in place to co-operate and co-ordinate at the national level on AML/CFT issues. A broad range of agencies is involved in these structures including LEAs, supervisors and the private sector. Korea manages TF co-ordination at two separate levels (the AML/CFT level and the counter-terrorism level). Co-ordination on PF issues is largely *ad hoc* and would benefit from a more formal system.

19. The supervisory responsibility of casinos in Jeju was transferred from KoFIU to the SGP in March 2019, four months before the on-site.

2

Recommended Actions

Korea should:

a) Continue to expand its risk understanding and improve future NRAs by seeking additional information, data and opinions from the DNFBP and NPO sectors, and NPO-related organisations including Korea's Council for Overseas Development Co-operation (KCOC) and Korea International Co-operation Agency (KOICA).
b) Enhance the domestic co-operation and co-ordination system by:
    i. leveraging the LEAs Committee or using other appropriate channels to regularly and frequently share general information on ML/TF investigative techniques or offending trends and to exchange information and manage ML/TF cases to the extent possible while maintaining confidentiality; and
    ii. ensuring there is a regular forum in which relevant agencies can exchange information on PF, undertake horizon scanning and monitor PF trends.

89. 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 Coordination)

Country's understanding of its ML/TF risks

90. Korea shows a good understanding of its risks, as demonstrated by its activities and priorities. Korea informs its risk understanding through an ongoing risk assessment process. Korea's risks are well assessed and captured in its 2018 NRA. The NRAs have improved and evolved, contributing to an increasingly robust risk understanding.

91. These conclusions are based on: a review of Korea's NRAs, other relevant risk assessments, and related government policy statements and documents; discussions with individuals who participated in the NRAs; and discussions with KoFIU, the FSS, the FSC, entrusted agencies (see para.84), the SPO, the NPA, the KCG, the NTS, the KCS, and the private sector (including FIs, DNFBPs and NPOs).

92. Korea has undertaken three NRAs in 2014, 2016 and 2018. Discussions with the authorities emphasised Korea's strong focus on understanding its emerging and evolving risks. Each NRA took a slightly different approach with Korea applying the lessons learned in the previous NRA to improve and enhance the methodology for the next one. The 2014 NRA was undertaken by the Institute of Finance (a financial research centre) and took a more academic than practical approach. While major government agencies participated, there was a lack of participation from some relevant agencies which led Korea to question the outcomes. The 2016 NRA was by Dongguk University and took a more statistical approach. The risks identified were broadly consistent with those identified in the 2014 NRA, which gave Korea some confidence in the findings. Nonetheless, they considered there were flaws in the methodology, including a lack of analysis of cross-border transactions.

93. The 2018 NRA aimed to address earlier deficiencies. A joint committee of 12 government agencies developed the NRA, which ensured cross-government input and buy-in. The NRA identified risks based on qualitative and quantitative data provided by agencies and the private sector. Preliminary findings were then tested and further refined through discussions among the agencies to identify any gaps. The methodology for the 2018 NRA was broad, employing a "CELF" approach (see Figure 2.1 that considered a wide range of relevant factors to come to an overall risk assessment. The outcomes of the 2018 NRA are consistent with the 2014 and 2016 NRAs in most areas (e.g. the identification of tax crime and fraud as prominent risks) despite the shortcomings in the previous NRAs' processes. Nonetheless, the NRAs also show an evolution in Korea's risk understanding, which reflects its efforts to refine and improve the methodology across each NRA. For example, the 2018 NRA newly identifies the emerging threat of virtual assets.

Figure 2.1. CELF methodology for the 2018 NRA

Source: 2018 NRA, pg.8.

94. The 2018 NRA identified nine major risk areas. Seven of these risks relate to major proceeds-generating offences: tax crime, illegal gambling, financial fraud, corruption, unfair trading, asset flight and embezzlement. These were identified based on a range of offending data and discussions with investigative and inquiry authorities. The other two risks relate to high-risk vulnerabilities: the abuse of cash transactions

and virtual assets. These vulnerabilities were identified based on Korea's context and case studies. While the rate of cash transactions in Korea is comparable to other countries, such transactions are considered vulnerable due to their anonymity. Korea has also traced the use and return of high-value bills and has noted a lower return rate, which may indicate the misuse of such instruments. A review of ML case studies by Korea also confirmed that cash is its most common ML/TF instrument. Korea considers that the anonymity of virtual assets also creates risks, although case studies suggest that criminal activity in this area more often stems from fraudulent or misused VASPs (e.g. illicit fund-raising disguised as initial coin offerings) rather than virtual asset transactions themselves. VASPs are also vulnerable as they are not yet subject to AML/CFT regulations.

95. The 2018 NRA includes a section specifically dedicated to analysing TF risk. Korea has not prosecuted TF and has only had one terrorism prosecution (a case of incitement). Consequently, the NRA's findings rely on a small number of examples and potential areas of threat and vulnerability based on Korea's environment and context. The vulnerabilities considered in the 2018 NRA are wide-ranging from NPO activity to remittance and immigration trends. The threats are similarly broad, including legitimate economic activities, kidnapping and ransom, and disguised religious activities. Korea could have benefited from seeking additional views from the NPO sector and NPO-related organisations, including KCOC and KOICA (see Chapter 4).

96. Korea supplements the NRA process with additional assessments in specific areas. These include a ML/TF risk assessment of legal persons and legal arrangements (see Chapter 7) and an assessment of the risk of TF abuse of NPOs (see Chapter 4). The 2018 NRA also drew on agency-specific risk assessments, including on tax crime (by the NTS), asset flight (by the KCS), and financial fraud (by the NPA), as well as on a sector-specific risk assessments of the financial sector (by the FSS). These assessments support and are consistent with the findings of the 2018 NRA, further demonstrating Korea's risk understanding.

97. Korean government authorities, including LEAs, most supervisors and entrusted agencies, showed a strong and consistent understanding of Korea's ML/TF risk areas in line with Korea's 2018 NRA. The case studies and examples provided by various government agencies throughout the assessment largely supported the NRA's findings and were consistent with the identified risk areas. Notably, even supervisors of smaller sectors demonstrated a sound knowledge of the NRA and a good understanding of the risks within their supervised sectors. Risk understanding by the SGP supervisor was less robust and showed a limited understanding of ML/TF risks. The 2018 NRA has clearly been widely circulated and agencies met at the on-site were consistently aware and supportive of the NRA's findings.

98. Private sector actors have fed into each NRA to varying extents. The 2014 NRA obtained private sector views through a symposium on the underground economy and black market during which private sector attendees provided views on Korea's key risk areas. The 2016 NRA obtained views of the private sector via the FSS. Following the 2016 NRA, the FSS held a forum with the private sector to publicise the findings and seek their views. Korea took these opinions on board in the 2018 NRA. The private sector also had direct input through questionnaires via FSS and indirect input via relevant supervisors.

99. It is positive that Korea attempted to understand the risks of DNFBPs not yet covered by the AML/CFT regulatory framework and sought their input in the NRA process. For the 2016 NRA, the government commissioned a report on DNFBP risks

from the Institute of Finance, which met with industry associations to discuss their perceived risk and sought data, including through a questionnaire distributed to DNFBPs. However, DNFBPs had limited buy-in to the process and provided only a 20% response rate. For the 2018 NRA, the authorities collected information on DNFBPs' activities and business profiles through trade or industry associations or from the NTS, but Korea acknowledges that information on the DNFBP sector was limited. In practice, this may have resulted in blind spots in Korea's risk understanding, for example in relation to Korea's underground DPMS sector or the risks posed by professional enablers. Discussions with LEAs showed that ML and predicate offence cases are becoming more complex, with increased use of corporate structures. If this trend continues, professional enablers may become an emerging risk in the future. Subsequent NRAs would benefit from increased input and data from the DNFBP sectors to ensure that Korea thoroughly assesses and understands this risk.

National policies and activities to address identified ML/TF risks

100. Korea's national AML/CFT policies aim to address the identified ML/TF risks. Korea has updated these policies, as it has revised its risk assessments. Although its policies and plans can be general and dispersed across various documents, Korea demonstrated that its activities target identified risks. Nonetheless, there are areas where ongoing and prolonged vulnerabilities have yet to be addressed (e.g. the lack of coverage of most DNFBPs).

101. These conclusions are based on: national AML/CFT strategies; Korea's three NRAs and other risk assessment documents; and discussions with KoFIU, the FSS, the FSC, entrusted agencies, the SPO, the NPA, the KCG, the NTS and the KCS.

102. Korea has revisited its AML/CFT policies and plans in response to each NRA. After its first 2014 NRA, Korea developed an AML/CFT System Development Strategy to respond to the identified risks. The Strategy established a work programme with specific measures linked to the identified risks. Korea updated the Strategy with each subsequent NRA (see R.1). The update following the 2016 NRA saw the Strategy arranged around 25 tasks, although these focused more on improving general compliance with the FATF Standards than specifically responding to the risks of the 2016 NRA. After the 2018 NRA, the Strategy was reorganised again around three broad goals: building an advanced AML/CFT framework, using financial information efficiently, and building capacity in the private sector. While these goals are general, Korea has taken specific measures to respond to identified risks (see Box 2.1).

103. The 2018 NRA itself also sets out proposed counter-measures for each risk identified. For example, on virtual assets, the NRA noted that the government would issue guidelines regulating transactions between financial institutions and VASPs. This was done in January 2018. Importantly, the NRA also identifies measures to combat Korea's TF risk, such as monitoring the use of illegal wire transfers and raising TF awareness among reporting entities. This is positive as the AML/CFT System Development Strategy largely focuses on ML risk. The NRA and AML/CFT System Development Strategy reflect some planned measures to address identified risks, while other activities are independently undertaken by individual agencies (see paras.113-114 below). In the future, it may prove useful for Korea to draw together various work streams into one comprehensive plan for action that reflects all relevant activities before moving forward with planned actions.

104. Korea's legislative programme shows activity relating to risks identified in the NRAs. For example, Korea made legislative changes: following the 2014 NRA to ensure

enhanced customer due diligence (EDD); following the 2016 NRA to extend AML/CFT obligations to credit and electronic transaction businesses; and following the 2018 NRA to improve CTRs and bring VASPs within the scope of the AML/CFT framework. However, significant legislative changes remain pending. Since the 2014 NRA, Korea has identified that extending the AML/CFT framework to all DNFBPs is necessary to respond to the identified risks in this sector. However, Korea has not yet enacted the necessary legislation.

Box 2.1. Measures to respond to risks identified in 2018 NRA

- Korea has amended legislation to respond to particular risk areas, including lowering the threshold for CTRs and imposing enhanced consumer protections and limitations on the use of virtual assets.
- Korea has increased resources to certain agencies in line with identified risk areas, e.g. by increasing LEAs' financial and human resources to combat tax crime and increasing supervisory inspection staff.
- Korea made operational and institutional changes to respond better to its identified risks, particularly the high-risk proceeds-generating offences. It created dedicated units to investigate financial fraud (within the NPA) and unfair trading (within the FSS). Agencies have also launched a joint investigation unit for asset flight (see Box 3.13 in Chapter 3).

105. Korea has also demonstrated its ability to respond to emerging and ongoing risk areas. The response to the emerging risk posed by virtual assets has been positive (see Box 2.2). Steps have also been taken to respond to the ongoing threats posed by accounts in borrowed names (see para.39), including various legislative changes between 1993 and 2018 to require real names to be used in financial and virtual asset transactions, and to encourage legal persons to register shares in real names. Nonetheless, these accounts remain a major risk and common methodology for ML in Korea and further mitigation measures could be considered (see Chapter Chapter 3. on IO.7).

Exemptions, enhanced and simplified measures

106. Korea based its legal framework for applying simplified and enhanced measures on the findings of the NRAs and other risk assessments. However, exemptions for uncovered DNFBPs and domestic PEPs are not based on proven low risks nor in line with the FATF Standards.

107. These conclusions are based on reviews of the NRA and other relevant risk assessments, and discussions with the authorities and private sector.

108. In general, FIs and casinos are required to impose enhanced measures for higher risk situations and only allowed to apply simplified measures for lower risks situations. The AML/CFT Regulation sets out high-risk customer types, products and services with increased ML/TF risks for which enhanced CDD is mandatory. It also sets out the types of lower risk customers, products and services for which simplified CDD is allowed.

109. FIs and casinos are exempt from verifying the identity of the ultimate owner or controller of specific companies and government bodies.[20] Korea demonstrated that allowing simplified customer due diligence (SDD) to be applied for these specific entities/bodies was based on a proven low risk.

110. Lack of coverage for domestic PEPs is inconsistent with the NRA, which recognises domestic corruption as a major predicate offence, and the FATF Standards. Additionally, the AML/CFT framework does not cover DNFBPs (other than casinos) which is not based on a proven low risk either. Given the relative weighting of the DNFBP sectors (see para.78), the lack of coverage has been considered a moderate shortcoming for the assessment under IO.1.

Objectives and activities of competent authorities

111. The objectives and activities of Korea's competent authorities are, for the most part, in line with the risks identified in its NRAs. Korea has had notable success responding to the identified emerging risks posed by virtual assets.

112. These conclusions are based on: various agencies' policy and strategy documents; and discussions with KoFIU, the FSS, the FSC, entrusted agencies, the SPO, the NPA, the KCG, the NTS, the KCS and the private sector.

113. Supervisors' objectives and activities are largely consistent with national AML/CFT policies and the ML/TF risks identified by Korea. As the lead AML/CFT policy-maker and one of the key agencies involved in developing the 2018 NRA, KoFIU's supervision activities are guided and informed by the NRA's findings. Entrusted agencies take a risk-based approach to supervision and apply more focus and resources to areas of higher risk. The exception is the SGP supervisor who does not apply a risk-based approach and instead approaches supervision in a rules-based manner.

114. LEAs' objectives and activities are in line with Korea's risks as identified in the 2018 NRA. Authorities pursue targeted 'crackdowns' in identified high-risk areas, for example on illegal gambling and fraud. A major exception is tax offending which is generally pursued and sanctioned directly by the NTS, rather than pursued through to criminal prosecution and conviction despite its identification as the highest risk proceeds-generating offence (this issue is discussed in more detail and given more weight in IO.7, see Chapter Chapter 3.). Agencies were well able to describe common methodologies and schemes associated with the most prevalent predicate offences. LEAs have also created new teams, both within and across agencies, to respond to areas of higher risk. For example, specialised teams were set up within the NPA to respond to financial fraud in light of the higher risks identified in this area and an inter-agency task force was established on asset flight.

115. A particularly positive finding is the authorities' understanding of and response to virtual assets (which were identified as high risk in the 2018 NRA) (see Box 2.2).

20. See c.1.8.

Box 2.2. Korea's response to identified risks posed by virtual assets

The Kimchi Premium: Identifying a risk

In the second half of 2017, the use of virtual assets in Korea started to increase. Speculation and interest in the market led to significant price increases in Korea, referred to as the 'Kimchi premium'. Authorities noticed this increase and analysed available information to determine the risks posed by virtual assets, including for committing predicate offences, ML and TF. Korea identified financial fraud (the use of virtual assets in pyramid schemes and voice phishing) and ML through virtual assets as major risk areas.

The Cross-Government Response: Measures to address the risk

Relevant agencies (including KoFIU, the NPA, the NTS, and the SPO) formed a cross-government group to respond to the risks posed by virtual assets. The group targeted the risks from various angles, including LEA crackdowns, enhanced consumer protections and limitations on the use of virtual assets (e.g. a ban on initial coin offerings).

In 2018, as part of these measures, the FSC released *Guidelines on Virtual Assets* to raise awareness of the risks of virtual assets and add obligations for FIs. Korea has already amended the Guidelines twice to respond to new knowledge and understanding of the risks of virtual assets.

Korea does not permit FIs to deal with virtual assets. Consequently, VASPs manage all virtual assets in Korea. Although Korea does not yet licence or supervise VASPs, a team at the FSC monitors their activities. Korea plans to bring VASPs under its AML/CFT regime soon. VASPs themselves acknowledge the need for licensing and regulation and some are already voluntarily complying with certain obligations (e.g. limiting trading by individuals from FATF-identified high-risk countries).

In July 2018, KoFIU also made on-site visits to six FIs, staying with each for one week, to review transaction data related to virtual assets. In doing so, KoFIU detected two cases involving misuse of virtual assets, resulting in the prosecution and conviction of two defendants. Both defendants were sentenced to imprisonment for three years and confiscation orders were imposed. KoFIU in partnership with FSS undertook another round of inspections in April 2019.

LEAs also actively pursue cases involving virtual assets. In 2017, the Korean courts heard their first case involving virtual asset confiscation and ruled that virtual assets could be frozen and confiscated. Since then, authorities have had success tracing and recovering proceeds held or moved through virtual assets.

These measures resulted in a notable reduction in the Kimchi premium.

National co-ordination and co-operation

116. Korea has strong structures in place to facilitate and encourage co-ordination and co-operation at a national level on AML/CFT issues. These structures benefit from covering a wide range of agencies and institutions at the policy and operational level, including LEAs, supervisors and the private sector. Korea would benefit from a clearer co-operation mechanism for PF issues.

117. These conclusions are based on a review of existing bodies and committees and discussions with KoFIU, the FSS, the FSC, the SPO, the NPA, the KCG, the NTS and KCS.

118. Korea achieves co-ordination and co-operation on AML/CFT issues through a structure of committees. The AML/CFT Policy Co-ordination Committee (established in 2002) is at the top of this structure with oversight of Korea's AML/CFT policy and implementation. This Committee comprises 12 Director General-level representatives from relevant agencies, including KoFIU, LEAs and supervisors.[21] The Committee's regular meetings are relatively infrequent (occurring twice per year), but it also has the ability to meet more often on an ad hoc basis if necessary. Five working-level committees covering different policy and operational areas are below the AML/CFT Policy Co-ordination Committee (see Table 2.1). In some cases, Korea could make better use of these committees to exchange a wider range of information related to AML/CFT issues.

Table 2.1. Korea's working level AML/CFT committees

	Meeting frequency	Membership	Focus
AML/CFT Policy Implementation Committee	Every six months	12 agencies: the FSC; the Ministry of Economy and Finance; the MOJ; the MFA; the Ministry of Trade, Industry and Energy; the NIS; the National Election Commission; the NTS; the KCS; the SPO; the NPA; and the FSS.	This Committee shares information related to AML/CFT issues, ensures an ongoing and up-to-date understanding of risk, and monitors the implementation of decisions from the Policy Co-ordination Committee.
LEAs Committee	Every six months	8 LEAs: KoFIU; the SPO; the NPA; the KCG; the NTS; the KCS; the NIS; and the National Election Commission.	The mandate of the LEAs Committee is limited to reviewing the use of financial intelligence information from KoFIU. Agencies would benefit from meeting more frequently and using the committee to also share more general information on ML/TF investigative techniques or offending trends and exchange information and manage ML/TF cases to the extent possible while respecting case confidentiality.

21. The 12 participating agencies are: the FSC; the Ministry of Economy and Finance; the MOJ; the MFA; the Ministry of Trade, Industry and Energy; the NIS; the National Election Commission; the NTS; the KCS; the SPO; the NPA; and the FSS.

	Meeting frequency	Membership	Focus
Inspection Agencies Committee	Every six months	KoFIU and 11 entrusted agencies: the FSS; the Ministry of SMEs and Startups; the Ministry of Science and ICT; the Ministry of the Interior and Safety; the KCS; National Agricultural Co-operatives Federation; National Federation of Fisheries Co-operatives; National Forestry Co-operation Federation; Credit Co-operatives Association; Credit Community Co-operative Federation; and the SGP supervisor.	This Council shares information on AML/CFT supervisory issues and discusses inspection methods and management.
Private Sector Consultation Committee	Every six months	The Korea Casino Association plus 11 financial associations: Korea Federation of Banks; Korea Financial Investment Association; Korea Life Insurance Association; General Insurance Association of Korea; Credit Finance Association; Korea Federation of Savings Banks; National Agriculture Co-operative Federation; National Federation of Fisheries Co-operatives; National Credit Union Federation of Korea; National Forestry Co-operatives Federation; and community credit co-operatives.	The Committee's purpose is to provide input on FIs' and casinos' implementation measures and provide feedback on difficulties encountered by reporting entities.
NPOs CFT Agencies Committee	On an *ad hoc* basis (e.g. three times between July 2018 and July 2019)	8 agencies: Office for Government Policy Co-ordination; the National Intelligence Service; Ministry of the Interior and Safety; the FSC; the MFA; the NTS; the FSS, and KOICA.	This Committee provides a forum to discuss measures to prevent the misuse of NPOs for TF. Membership could usefully be extended to all NPO registrars, including those that register certain high-risk NPOs, and other agencies involved in NPO monitoring and supervision, such as KOICA (see Chapter Chapter 3.).

119. This committee structure handles both AML and CFT. A high-level committee, the National Counter-Terrorism Commission, governs and oversees all counter-terrorism issues, which includes TF matters. The Commission is led by the Prime Minister with participation from 21 ministers of relevant agencies, including the NIS, KoFIU, the NPA and several other bodies also represented in the AML/CFT Policy Co-ordination Committee.[22] A working-level counter-terrorism committee below the Commission meets every 1-2 months to discuss counter-terrorism policy and ongoing investigations, including TF investigations. There is considerable overlap in the membership of the counter-terrorism groups and the AML/CFT Policy Co-ordination Committee, meaning the decisions and activities of these committees feed into each other and are shared. The National Counter-Terrorism Commission has overall responsibility and oversight and is briefed on activities and decisions from the working-level committees.

120. In practice, agencies demonstrated a good level of co-operation and collaboration. Joint operations are not uncommon, especially to respond to risk areas that touch upon the work of several agencies. For example, Korea has taken cross-

22. Other representatives: the Minister of Strategy and Finance; Minister of Foreign Affairs; Minister of Unification; Minister of Justice; Minister of National Defence; Minister of the Interior and Safety; Minister of Trade, Industry and Energy; Minister of Health and Welfare; Minister of Environment; Minister of Land, Infrastructure, and Transport; Minister of Oceans and Fisheries; Minister of the Office for Government Policy Coordination; Chairman of the Nuclear Safety and Security Commission; Chief of the Presidential Security Service; Commissioner of the Korea Customs Service; Administrator of the National Fire Agency; and Commissioner of the Korea Coast Guard.

agency responses to virtual assets (see Box 2.2) and asset flight (see Box 3.13). Agencies also establish mechanisms to facilitate information-sharing and ongoing communication where necessary. For example, a messenger service exists between relevant agencies to communicate regularly on MLA cases (see para.470) and a secure intelligence channel is in place to share counter-terrorism intelligence between intelligence agencies and LEAs. KoFIU is staffed largely by secondments from other agencies, which allows those agencies to easily share information, build relationships and ease communications through their seconded staff (although there are drawbacks to this staffing structure; see para.134). This arrangement also helps staff develop networks and contact points that are used post-secondment. Korea aims to ensure that data protection and privacy rules always govern information sharing. This is achieved through legislative requirements, as well as practical measure such as confidentiality agreements and restricting access to documents. Regular training sessions would ensure key users remain sensitive to and aware of relevant requirements.

121. Korea also has structures in place to co-operate and share information between the public and private sectors. In addition to seeking input from FI and casino associations via the Private Sector Consultation Committee, (see Table 2.1 above), Korea has established an AML/CFT Policy Advisory Council made up of appointed legal experts and advisors from academia and research institutes. This Council meets twice a year to discuss and deliberate on AML/CFT policies and acts as a sounding board for the government.

122. Korea could improve its PF co-operation mechanisms. In theory, the various AML/CFT committees can discuss PF issues, but it is not clear that this occurs in practice. The MFA holds ad hoc meetings on TF and PF designations, which cover identification of potential targets for designation and decisions from the relevant UNSC (see Chapter Chapter 4. on IO.10 and IO.11). However, these do not provide a forum for regular discussion of PF issues. Korea also has a National Security Council which meets on a regular basis to discuss security issues, but does not focus specifically on PF. Korea hosts an annual conference with the UN on disarmament and non-proliferation issues, but this is an international conference not a forum for domestic co-operation. Ad hoc co-operation occurs in response to relevant issues. This is positive, but Korea would benefit from an established forum to allow relevant agencies to exchange information, monitor trends and risks, and ensure consistent implementation of PF measures.

Private sector's awareness of risks

123. Korea has taken steps to ensure that FIs and DNFBPs are aware of the results of the NRA, and these efforts appear to have been successful for the covered sectors.

124. These conclusions are based on a review of the NRA, and discussions with KoFIU, the supervisory authorities (the FSS, the FSC and entrusted agencies) and the private sector.

125. As part of developing the NRAs, authorities consulted FIs and most DNFBP sectors, including those that are not covered. The authorities sought their input through sector associations, consultations and questionnaires. Since publishing the 2018 NRA, the authorities have taken steps to share and communicate its results and raise awareness of the NRA to obliged entities.

126. All private sector entities met during the on-site had a good understanding of the main risks and vulnerabilities identified in the NRA. They had a generally good level

of awareness of the NRA's results and reported finding it to be useful. Larger FIs and casinos have a good understanding of the sectoral risks and undertake risk assessments at an institutional level considering their customer base, products, services, etc. Larger FIs equally showed a good understanding of the potential risks posed by new technologies and delivery mechanisms (see Chapter Chapter 5. on IO.4).

Overall conclusions on IO.1

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

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

a) Korea's network of LEAs use a broad range of financial intelligence and other relevant information to develop evidence and trace criminal proceeds.

b) KoFIU has access to a range of information online, through consultation with LEAs or entrusted agencies, or on request from other sources. KoFIU has a general process for operational analysis, including computerised analyses of reports received, basic analysis and in-depth analysis followed by dissemination to concerned competent authorities. This helps integrate a variety of intelligence and automated data cross-matching to identify high-risk STRs and to develop intelligence value. However, there is scope for KoFIU to enhance its operational and strategic analysis, particularly in relation to high-risk areas such as tax crimes.

c) Authorities make good use of KoFIU products, which largely support the operational needs of LEAs and supervisors. While statistics are not comprehensive, those that are available suggest LEAs use KoFIU information to pursue predicate offences and to some extent to pursue ML. The NTS is the greatest requester of KoFIU information which is consistent with Korea's risk profile and the high risk of tax crime. The SPO and the NPA are less actively using KoFIU products.

d) KoFIU has taken steps in recent years to improve the quality of reporting entities' STRs which has improved the overall quality of reports. Nonetheless, the quantity of financial intelligence available is limited by gaps in the reporting obligation (DNFBPs other than casinos are not covered).[23] Based on the relative importance of these sectors in Korea (see para.78), this gap has been given moderate weight.

e) The competent authorities have strong mechanisms in place to co-operate and exchange information, while protecting its confidentiality. KoFIU's structure comprising seconded officials from other government agencies supports access to financial intelligence and interagency collaboration. However, secondments are only posted to KoFIU for a short time, which may negatively impact its institutional knowledge and ability to undertake financial analysis.

23. The corresponding recommended action is covered in Chapter 5 on preventive measures as it relates to Recommendation 23.

Immediate Outcome 7

a) LEAs take a "follow the money" approach in their activities which allows for the effective identification and investigation of ML. Policy and operational changes since 2017 have strengthened the system and have had a positive impact on the number of ML prosecutions. Operational co-ordination among the relevant agencies works well and agencies are able to share resources and expertise.
b) Korea has made efforts to pursue ML in line with its risks. However, a significant gap in Korea's predicate offences seriously undermines these efforts by preventing Korea from pursuing ML in relation to most tax crime, which Korea recognises as its highest risk area and greatest proceeds-generating offence. Professional enablers are not a prominent feature in Korea's ML cases, but the increasing use of complex corporate structures means this typology may be an emerging risk. Korea has taken steps to prevent the use of accounts in borrowed names which continues to be a common typology for ML in Korea and is inherently difficult to investigate (see para.39).
c) Korea is effective in obtaining convictions in self-laundering cases. However, it is less clear that the authorities actively pursue standalone and third party ML. Cases of laundering based on a foreign predicate offence are extremely rare. Over the past decade, there have been no prosecutions of legal persons for ML.
d) Sanctions imposed for ML are generally low and courts do not use the full range of sanctions available. It does not appear that a ML conviction has a notable impact in terms of sentencing.
e) Korea pursues alternative measures in tax crime cases where it is unable to pursue ML due to gaps in its predicate offence list. In other cases, there is a limited range of available alternative criminal justice measures. While the authorities pursue the predicate offence and asset recovery, they generally do so regardless of whether or not it is possible to secure a ML conviction.

Immediate Outcome 8

a) Korean authorities robustly pursue asset recovery and take steps to deprive criminals of criminal proceeds or assets of equivalent value. Measures are in place to facilitate confiscation and ensure assets are not dissipated or subject to depreciation prior to confiscation, although these mechanisms have not always been systematically used. Asset recovery was designated a formal government priority in 2017. While asset recovery was pursued prior to this time, its enhanced status allows for increased resources and specialisation.
b) Authorities demonstrated their ability to confiscate a range of assets (both proceeds and assets of equivalent value), including in very high-profile cases. Case studies demonstrate that Korea is able to confiscate the proceeds of foreign predicates.
c) Between criminal asset recovery, tax levies, and restitution, Korea is able to deprive criminals of a reasonable value of proceeds. Further efforts are needed to increase the recovery of assets subject to confiscation

orders. Korea's recent operational and structural changes are enhancing its system and may help ensure a higher percentage of assets ordered for confiscation are recovered.

d) Recovery targets and outcomes are largely consistent with risk and national AML/CFT policies. Korea has had considerable recent success in confiscating virtual assets, which it identifies as a risk area. Tax procedures are actively used to recover the proceeds of tax crime, which is Korea's highest proceeds-generating offence. The proceeds of fraud, a higher-risk predicate offence, are recovered through victim restitution orders, although there may be limitations where the victims cannot be identified or where the proceeds exceed the harm caused to the victim.[24]

e) Authorities are aware of the risks and methodologies of cross-border movements of currency and BNIs. However, seizure and confiscation powers are used infrequently. Sanctions imposed are low, but appear to be somewhat dissuasive (at least for repeat offenders, given the relatively low level of recidivism).

Recommended Actions

Immediate Outcome 6

Korea should:

a) Enhance KoFIU's strategic and operational analysis to ensure deeper and more frequent analysis, including in high risk areas such as tax crimes.

b) Further enhance the STR filtering system, particularly at the early stages to ensure disseminations are of high value to receiving LEAs, including the SPO and the NPA.

c) Continue to upgrade KoFIU's IT resources and increase the number of permanent staff to ensure institutional knowledge is maintained within KoFIU.

d) Ensure KoFIU and supervisors undertake additional outreach on further improving the overall quality of STRs.

Immediate Outcome 7

Korea should:

a) As a matter of priority, amend the law to expand the range of tax crimes that are ML predicate offences (for example, to align this range of crimes with those that require STR reporting) to ensure Korea is able to prosecute ML based on tax crime.

b) Ensure it is actively investigating, prosecuting, and convicting a full range of ML cases, including by:

   i. Strengthening knowledge and expertise at the SPO and DPO level by providing training and guidance to prosecutors on the different

24. In August 2019, the Act on Special Cases Concerning the Confiscation and Return of Property Acquired Through Corrupt Practices was amended to permit the government to confiscate the proceeds (or assets of equivalent value) of fraud cases involving criminal organisations, unauthorised fund-raising, pyramid schemes, telecommunications or other similar cases, and return the proceeds to the victims. As this measure was not in force at the time of the on-site visit, it was not taken into account for the purposes of this evaluation.

ML types, to ensure that they systematically consider, prioritise and pursue all types of ML, including against legal persons where appropriate; and

ii. Continuing to enhance the investigatory and IT resources of the NPA's CPITs to ensure they continue to have sufficient capacity to investigate ML.

c) Develop guidance for the judiciary on sanctions for ML, including relevant aggravating and mitigating factors, to ensure that sanctions are imposed in a consistently effective, proportionate, and dissuasive manner.

d) Assess, at the national level, the risks and vulnerabilities posed by the accounting and legal sectors to ensure a robust understanding of the ML risks posed by professional enablers. In doing so, consider whether the emerging risks in the accounting and legal sectors (as identified in the NRA) are being impacted by the growing number of VASPs and the increasing use of corporate structures in ML and asset flight cases.[25]

e) Continue the positive efforts to pursue policy measures to prevent the use of accounts in borrowed names and explore tools to facilitate and enhance LEAs' ability to investigate and trace the movement of funds using such accounts.

Immediate Outcome 8

Korea should:

a) Expand the ability for authorities to confiscate fraud proceeds where compensation cannot adequately deprive the offender of the illegal assets, including if the victims cannot be identified or where the proceeds exceed the harm caused to the victim.

b) Continue exploring measures to promote the actual recovery of assets ordered for confiscation and systematically take advantage of available mechanisms and measures to facilitate confiscation and recovery.

c) Actively utilise seizure and confiscation powers in cases of cross-border currency and BNI movement and impose sanctions where appropriate.

d) Continue pursuing asset recovery in respect of foreign predicate offences.

e) Monitor the resources of the CARD teams at the national and district level to ensure that sufficient resources continue to remain available to handle the increased focus on asset recovery.

25. The NRA identifies emerging risks in Korea's growing legal and accountancy sectors, as these professionals begin to offer a wider range of services. To date, the most common ML typologies involving lawyers and accountants have been when CEOs/managers of larger conglomerates use the company's own in-house lawyers and accountants to set up complex legal structures to facilitate embezzlement, tax crime and/or related ML. The NRA also recognises the risks of virtual asset activity and the growing number of companies in Korea, which are VASPs. These companies are smaller and may be more likely to use external legal and accountancy services on an ad hoc basis (rather than keeping in-house lawyers and accountants permanently on staff). Korea should consider whether all of these factors could impact the ML/TF risks facing lawyers and accountants.

128. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32.

Immediate Outcome 6 (Financial Intelligence ML/TF)

Use of financial intelligence and other information

129. Korea's network of criminal justice and operational agencies all regularly use financial intelligence and other relevant information to develop evidence and trace criminal proceeds related to ML, associated predicate offences and TF. Additionally, Korea's supervisors use financial intelligence to inform their supervisory inspection cycles and focus.

130. These conclusions are based on: statistics and breakdowns on STRs; CTRs; case studies; and discussions with KoFIU, the NPA, the SPO, the NTS, the KSC, the KCG, the National Election Commission, the NIS, the FSS, the FSC and the entrusted agencies (see para.84).

131. KoFIU and LEAs obtain and analyse a wide range of financial, criminal and customs intelligence; regulatory, company, and land information; and other information. KoFIU can directly access different types of information online or obtain it on request (through warrants in some cases) or through consultation with LEAs and entrusted agencies (see Table 3.1 and Table 3.2). In some cases, the defined period for obtaining information is relatively long (e.g. for criminal records, import and export information, and family relation certificates). But in practice, this information can be obtained more rapidly where necessary or accessed directly by secondees working at KoFIU.

Table 3.1. Administrative information available to KoFIU

Information Type	Dissemination Institution	Collection Method	Obtaining Period	Legal Basis
Resident Registration	Ministry of the Interior and Safety	Online search	Real-time	Article 10-1, 2 of the *FTRA*
Arrivals and Departures (Koreans)	MOJ	Foreigner Information Network Environment[26] (fine.hikorea.go.kr)	Real-time	Agreement
Arrivals and Departures (Foreigners) Registered Foreigners				
Land Information	Ministry of Land, Infrastructure and Transport	Computerised file	1 day	Article 14-2 of the *Enforcement Decree*
Employment Insurance	Korea Employment Information Service	Computerised file	1 week	Negotiation
Criminal records	National Police Agency	Written paper, separately obtained	1-2 weeks	Article 10-1, 3 of the *FTRA*
Tax ledgers	National Tax Service	Computerised file	1 day	Article 14-1 of the *Enforcement Decree*
Import and Export Performance	Korea Customs Service	Computerised file	2 weeks	Article 14-2 of the *Enforcement Decree*

26. Only access by government-exclusive internal network.

Information Type	Dissemination Institution	Collection Method	Obtaining Period	Legal Basis
Family Relation Certificate	Supreme Court (local government)	Written paper, separately obtained	2-3 weeks	Article 10-1, 2 of the *FTRA*
Real Estate Register Corporation Register	Supreme Court	Public Information Sharing Center (share.go.kr)	Real-time	Agreement

Table 3.2. Credit information available to KoFIU

Information type	Dissemination institution	Collection method	Obtaining period	Legal basis
Financial transaction Personal loan Debt guarantee Delinquent transaction Commercial loan	Korea Credit Information services	Online	Daily	Article 14-2 of the *Enforcement Decree*
Enterprise	Korea Enterprise Data (CRETOP)	Online	Real-time	Commercial database

132. A key strength of Korea's system is KoFICS (Korea Financial Information Connect System), an online system that provides access to the main LEA and regulators' databases and the KoFIU database. KoFIU has established and managed KoFICS since 2013. KoFICS helps to integrate a range of intelligence and allows for automated data cross-matching to identify high-risk STRs and develop intelligence value. KoFICS also allows the following sharing of information between KoFIU and LEAs:

a) analysis spontaneously disseminated to LEAs by KoFIU;
b) information requested or provided to KoFIU by LEAs; and
c) feedback from each LEA about information disseminated by KoFIU.

133. KoFIU has 20 permanent staff managing its information systems, including KoFICS. These staff include 5 IT system managers and 15 IT system maintenance personnel. KoFIU's current IT system is effective, but is 17 years old which results in some limitations, including in handling large volumes of data. As a result, KoFIU is updating its system to further strengthen its financial intelligence function and ensure it remains an example of good practice.

134. Access to financial intelligence is further facilitated by KoFIU's structure comprising seconded public officials from eight government agencies (see Table 3.3). Around half of KoFIU's employees are secondees (typically highly experienced investigators and prosecutors) and are seconded for 2-3 years on average. This structure provides a number of advantages, including supporting the use of financial intelligence for investigations by strengthening interaction and feedback between intelligence producers and operational consumers; enhancing KoFIU and LEA expertise on AML/CFT matters, including operational risks, analysis and countermeasures; and ensuring a more comprehensive risk understanding by all relevant agencies. However, it also has limitations, such as the resulting regular staff turnover which can make it difficult to retain institutional knowledge that is vital to ensure deep and well-rounded analysis. The system could be strengthened by increasing the number of permanent KoFIU staff that operate alongside the secondees in order to protect and maintain institutional knowledge.

Table 3.3. KoFIU staff: organisation and number of staff

Organisation	FSC	FSS	MOJ / SPO (including prosecutors)	NTS	KCS	NPA & KCG	National Election Commission	Supreme Court (judges)	Total
Number of people dispatched	30	2	9	14	10	9	1	1	76

135. The statistics show that NTS is the greatest recipient of KoFIU's spontaneous disseminations, receiving 2.3 times more than the next highest recipient (the NPA) (see Table 3.7 below). This is consistent with Korea's risk profile as the NTS investigates tax crime, which is Korea's top proceeds-generating crime. The NTS is also the greatest requester of KoFIU information, which is equally consistent with Korea's risk profile (see Table 3.8 below). Nevertheless, the lower number of requests from other LEAs reinforces the concern that other LEAs are more focused on pursuing predicate offences than ML (see the section below on IO.7).

136. LEAs regularly use other non-KoFIU information to open and progress financial investigations. Depending on the nature of the case, asset scanning of bank, property, company and business information; inquiries into ownership structures; and obtaining personal records and travel information routinely occur in parallel financial investigations.

137. The KCS uses its Customer Database Warehouse (CDW), which contains customs information (e.g. import and export, freight, vessel, arrival and departure of flights and passengers, etc.), history of previous investigations, and history checks of licence plate numbers of vehicles owned by the Ministry of Land, Infrastructure and Transport.

138. The NTS uses a number of IT systems. NTIS (Neo Tax Integrated System) analyses and makes links between national tax information. FOCAS (FIU Financial and Other information Consolidated Analysis System) facilitates requests for and dissemination of KoFIU information, and improves analyses and management of information. ICAS (International Consolidated Analysis System) consolidates tax report data, administrative information, and financial statements of domestic and foreign companies to analyse international transactions. GIS (Geospatial Information System) contains recent maps and information on property owners. Finally, the E-Hanaro Civil Service System gives access to other administrative information necessary for investigations (e.g. arrival and departure information, vehicle registration, local tax payment certification, foreign registry certificates, building registers, etc.).

139. All LEAs and concerned regulators use DART (Data Analysis, Retrieval and Transfer System by the FSS), an accessible database of company information, including business reports, corporate conditions, financial statements, etc. LEAs use it actively for investigations into corporations (see Chapter 7 on IO.5).

140. LEAs and KoFIU use data from multiple sources to "follow the money" in cases of complex proceeds-generating crimes and ML and use financial intelligence to initiate investigations (see Box 3.1). Korea provided a limited number of cases related to ML, but was able to show its capacity to develop leads and unveil deeper layers of financial activity involving networks and funds flows within Korea and in some cases in several other jurisdictions. Korea has only one TF case, but was able to demonstrate its ability

to access and analyse a range of information, to trace funds and investigate matters related to TF. This is consistent with the low level of TF risk in Korea.

Box 3.1. Cases initiated by Korean LEAs using financial intelligence and other information

Case Study 1: A defence company's CEO's embezzlement and ML (case by the SPO)

Defence company D is a family-owned company with approximately 92% of shares held by the suspect, Person J, and his family members. The SPO received STRs, CTRs and financial transaction details on Company D from KoFIU. By comparing Company D's imports and shipping reports with import/export and foreign exchange trade statistics from the KCS and the Bank of Korea, the SPO detected that Person J had embezzled corporate funds by fraudulently altering the price of imports and illegally moving embezzled funds offshore. Criminal records from the NPA confirmed that Person J's eldest son-in-law and the executive director of Company D were under investigation for violating the *Defence Acquisition Program Act*. The SPO provided relevant information to the NPA and investigations confirmed that, from 19 to 28 March 2013, Person J and his children laundered and concealed embezzled and tax-evaded funds by purchasing highly expensive gold bars and savings insurance in the name of Person J's children.

Case Study 2: Composite Income Tax Crime via Borrowed-name Accounts (Case by NTS)

Person K failed to report KRW 5 billion (EUR 3.8 million) worth of income from his business by using a borrowed name account held under his spouse's name. The NTS reviewed taxation documents and CTR information from KoFIU on Person K's spouse confirming that Person K failed to report amounts that he had deposited as cash income. The NTS collected an additional KRW 2.2 billion (EUR1.7 million) in tax from Person K and imposed a penalty of KRW 1 billion (EUR 766 177).

Case Study 3: Illegally Moving Assets Offshore by Forging Trade (Case by KCS)

STRs and CTRs disseminated by KoFIU to the KCS prompted an investigation into Person C. The KCS collected evidence on Person C's financial transactions and sought information on Person C stored in the CDW database. This evidence showed that Person C and two other persons had illegally obtained and moved KRW 19.3 billion (EUR 14.8 million) in assets to the Philippines through forging trade documents. KRW 16.8 billion (EUR 12.9 million) was then transferred back into Korea. The KCS sent the case against Person C to the SPO in 2016 for suspicions of violating the *Act on the punishment, etc. of Specific Economic Crimes and Foreign Exchange Transactions*.

Reports received and requested by competent authorities

141. KoFIU receives a large number of STRs and CTRs from obliged entities (FIs and casinos). However, gaps in the scope of the reporting obligations (DNFBPs other than casinos are not covered) affect the financial information available. KoFIU also receives a monthly electronic report from the KCS on all cross-border declarations from the previous month (also see R.32). This information is disseminated to LEAs to support their investigations, and to supervisors to support their risk profiling of obliged entities. The authorities confirmed that reports received generally contain relevant information that is useful to their work.

142. These conclusions are based on statistics, and discussions with KoFIU, LEAs (the NPA, the SPO, the NTS, the KCS, the KCG, the National Election Commission and the NIS) and supervisory authorities (the FSS, the FSC and the entrusted agencies).

143. KoFIU receives different forms of financial information from reporting entities (mainly FIs, including banks, insurance companies, securities, the Korean Post and others, and casinos) and from foreign FIUs (see Table 3.4). No STRs have been filed by DNFBPs other than casinos, as these entities are not subject to reporting obligations (see R.23 and Chapter Chapter 5. on IO.4). KoFIU also obtains information directly from reporting entities through warrants and accesses open source information.

Table 3.4. Information sent to KoFIU

Information Type	Dissemination institution	Collection method	Obtaining period	*FTRA* legal basis
STR	Reporting entities	Online	Daily	Article 4
CTR	Reporting entities	Online	Daily	Article 4-2
Additional information	Reporting entities	Online	Daily	Article 10
Foreign FIUs' disseminated information	Foreign FIUs	ESW	Daily	Article 8

144. KoFIU can request data from reporting entities where necessary to undertake its analysis, to confirm a STR or CTR meets the legislative requirements, or to obtain foreign exchange data (see R.29). Information cannot be obtained from most DNFBPs. In addition, LEAs can directly access a broad range of information with a warrant. LEAs emphasised that financial intelligence information is much easier to access through KoFIU than through a warrant, and the reports provided have a significant amount of other relevant data and basic analysis.

145. KoFIU has taken steps to enhance the quality of the STRs it receives. It operates training programs designed to improve STR quality and gives lectures to reporting entities in this regard. It also provides reporting entities with feedback on STRs and ways to improve quality (either directly or through their entrusted agency). Table 3.5 below shows a significant reduction in the number of STRs filed between 2016 and 2017 and a fair level of disseminations, both spontaneous and upon request of LEAs. KoFIU explained that its outreach programs in 2016 significantly reduced the number of STRs (from 703 356 to 519 908), but increased their quality. Nonetheless, reporting entities indicated that TF-related STRs are still filed whenever there is a transaction or other interaction with a country with a high risk of terrorism. This suggests a level of over-reporting in this area where more outreach is needed (see R.34 and Chapter Chapter 5. on IO.4). In 2018, the number of STRs rose again (to 678 975), due to the new requirement for reporting entities to apply enhanced CDD to transactions involving virtual assets, and thereby be more observant of these types of transactions

and file STRs as needed.[27] KoFIU could consider additional measures to deal with the large number of STRs, for example, enhancing its outreach and education to reporting entities on when and how to report quality STRs. Korea should also continue its efforts to develop and enhance the STR filtering system at the early stages, to enable investigations to focus on more substantive cases.

Table 3.5. STR intelligence packages: overall dissemination & usage

	Overall STR (A)[28]	Spontaneous dissemination by KoFIU	**Upon LEAs'** request	Total of disseminated STR (use) (B)	Rate of use (B/A %)
2014	501 425	30 361	106 615	136 976	27%
2015	624 076	34 977	148 050	183 027	29%
2016	703 356	25 205	149 856	175 061	25%
2017	519 908	22 668	185 977	208 645	40%
2018	678 975	32 843	180 865	213 708	31%

146. STRs are stored in KoFIU's data system. This information is spontaneously disseminated to LEAs either as a STR-related intelligence packages or as general information packets. As indicated in Table 3.7 below, the NTS receives the largest share of KoFIU's spontaneous disseminations. This is consistent with the NRA which identifies tax crime as the number one predicate offence. The LEAs Committee (see Table 2. in Chapter 0) holds two rounds of meetings annually during which KoFIU receives opinions and feedback from LEAs. This demonstrates KoFIU's efforts to improve the effectiveness of information disseminated to each agency.

Box 3.2. KoFIU's use of cross-border currency/BNI reports

In February 2014, KoFIU detected suspicious activity as a result of its analysis of the KCS databases on cross-border currency/BNI reports. KoFIU identified a sum of cash that had been used to pay for business transactions with the intent of avoiding customs duties. The amount of foreign currency imported was larger than the amount exchanged into Korean won, leading to the detection of illicit foreign exchange transactions and tax crime by failing to report overseas revenue. Some of the cash was declared to the KCS as travel expenses or not declared, but was used to invest in virtual assets to take advantage of the high prices in Korea (the "kimchi premium"). KoFIU identified the suspicion, analysed available information, and disseminated the resulting information packed to relevant authorities.

Reports on cross-border currency and bearer negotiable instruments

147. Korea implements a declaration system for travellers arriving or departing Korea carrying more than USD 10 000 (EUR 8 800) of currency and/or BNIs. Declarations are made to the relevant KCS office. For mail and cargo, transports of more than USD 10 000 (EUR 8 800) must be declared to the relevant KCS office with documents proving the necessity and cause of the transportation (see R.32). All declaration reports are stored in the KCS database and KoFIU routinely cross checks STRs against these reports. This framework expands the data and information

27. These requirements came into force in January 2018.
28. Reports related to virtual assets (293 345 in 2018) were not included.

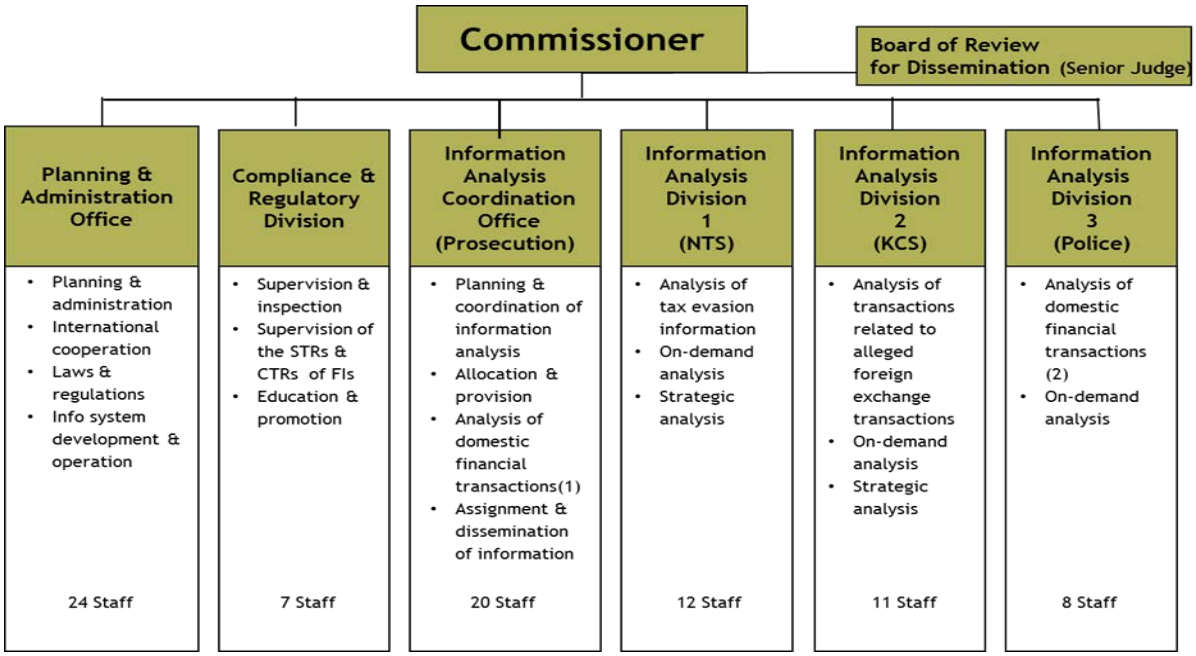
available to KoFIU, enhancing its foundation for operation and strategic analysis, and providing a solid foundation for Korea to detect suspicious activity (see Box 3.2 above).

Operational needs supported by FIU analysis and dissemination

148. KoFIU's financial analysis and dissemination supports LEA's operational needs to a large extent. KoFIU's efforts to increase disseminations are particularly notable as they occurred during a period of growing pressure where STR reporting increased in volume. LEAs generally spoke positively of KoFIU's operational analysis and the intelligence value of its disseminations. FIs also praised KoFIU for its open formal and informal channels of contact that enable questions about STRs to be discussed and addressed quickly before reports are submitted. KoFIU has a system in place to conduct regular strategic analysis. However, there is scope to increase operational and strategic analysis linked to high-risk proceeds-generating offences (particularly tax crimes).

149. These conclusions are based on statistics and discussions with KoFIU, LEAs (the NPA, the SPO, the NTS, the KCS, the KCG, the National Election Commission and the NIS) and supervisory authorities (the FSS, the FSC and the entrusted agencies).

Figure 3.1. KoFIU organisational chart



150. To deal with the recent growth of STRs, KoFIU increased its staff to 76 in 2018. KoFIU assigns almost half of its staff to STR analysis, and is considering increasing its operational staff in 2019/2020. KoFIU considers this staffing increase should be sufficient to meet its growing workload but it should continue to monitor its resources (particularly permanent staff) against operational requirements that are likely to continue to grow.

Operational analysis

151. KoFIU initially screens all reports to determine their urgency and check for missing information. KoFIU officers assess urgent STRs and CTRs immediately,

disseminating them as required, or contacting reporting entities to obtain missing information. Further automated checks and manual screening categorise STRs into low and high risk (excluding TF). Online STR access is a strong element of Korea's financial intelligence model as it allows users to tailor searches to any operational needs at early stages, for example, where investigators are considering a potential parallel financial investigation into proceeds-generating crimes. Extensive use of online STR searches highlights the value operational consumers of financial intelligence place on the system.

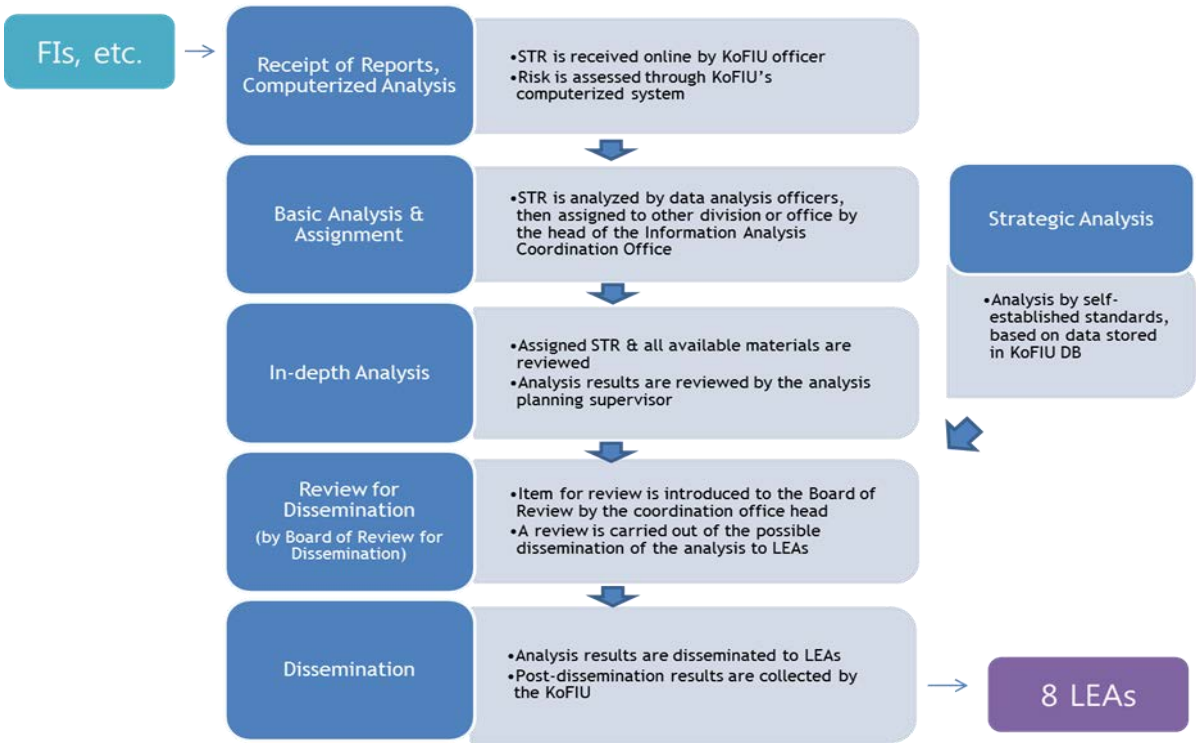
152. KoFIU has a general process to analyse information that consists of three stages: a computerised analysis of received reports, basic analysis, and in-depth analysis. These analyses are followed by dissemination to concerned competent authorities (see Table 3.6 and Figure 3.2).

Table 3.6. KoFIU's three levels of STR information analysis

	Computerised analysis	1st conservation	Basic analysis	2nd conservation	In-depth analysis	3rd conservation	Dissemination*	Dissemination**
2014	501 425	337 352	164 073	142 235	23 305	1 419	23 886	30 361
2015	624 076	461 596	162 480	114 941	30 854	1 267	29 587	34 994
2016	703 356	574 931	128 425	122 397	22 177	1 063	21 114	25 205
2017	519 908	410 031	109 877	68 588	19 767	1 239	18 528	22 634
2018	678 975	498 771	180 204	90 401	25 525	1 527	24 638	32 834
5-year total	3 027 740	2 282 681	745 059	538 562	124 268	6 515	117 753	146 037

* Net number of disseminated cases, excluding disseminations to multiple agencies.
** Total number of disseminations, including cases disseminated to multiple agencies and cases from information analysis.

Figure 3.2. KoFIU's general process for information analysis



153. During the first stage of operational analysis, the information system automatically performs computerised statistical analysis of each STR and classifies them by level of risk and type of transaction. This analysis takes into account the level of suspicion and ML risk, a search of the STR, and the frequency of STRs reported by the obliged entity. Depending on the result, STRs are selected as either requiring basic analysis by information analysis officers or requiring priority allocation. The other STRs are stored in the KoFIU database. Enhancements to KoFIU's IT system, particularly at the early stages of computerised analysis, would better ensure that disseminations are of high value and may increase the utility of disseminations, including to the SPO and the NPA (see para.156 and Table 3.7).

154. At the basic analysis stage, information analysis officers consider the results of the computerised analysis combined with previous data. If suspicion of a predicate offence (and to some extent ML) arises, the STR is assigned for detailed analysis.

155. At the detailed analysis stage, analysis officers seconded from each LEA perform analysis to identify links to specific predicate offences and to some extent ML activities. They consider overall information including financial transaction details such as STRs and CTRs in KoFIU's database and administrative business documents gathered from outside sources to figure out the transaction and capital flow characteristics, and determine if there is any link between the financial transaction and a predicate offence. The disseminated detailed analysis serves as a basis for investigation of predicates or ML and/or to trace the proceeds of crime.

156. If KoFIU finds any suspicion during its operational analysis, it spontaneously disseminates the resulting financial intelligence package on the associated predicate offenses and to some extent on ML to LEAs (see Table 3.7). Statistics are not comprehensive and do not distinguish between the number of STRs triggering or contributing to ML and TF investigations as opposed to predicate offences (see

Table 3.7). Of the 244 558 spontaneous disseminations to LEAs from 2002 to 2018, 132 019 cases were completed (i.e. considered and either used or not used). Of these, 42 457 (32.2%) were directly used by the LEA (e.g. to obtain new information or clues, to identify assets or fund flows, to identify other suspects, to expand the ongoing inquiry, or to identify other allegations) and another 62 831(47.6%) were indirectly used (to supplement existing investigative materials or verify existing information or facts). Approximately 20% were identified as "no suspicion", meaning they did not provide new information or information to support an investigation or inquiry (see Table 3.7. These figures suggest KoFIU's operational analysis and disseminations are generally useful and support the needs of LEAs. However, figures relating specifically to the SPO and the NPA suggest disseminations to these agencies are used to a lesser extent, with more than 50% of disseminations raising no suspicion. In addition, a large number of disseminations to the NPA remain in progress. KoFIU actively collaborates with these agencies to improve the utility of its disseminations, including through secondees and the LEAs Committee (see para.146). These efforts should be continued and further enhanced to increase the use of disseminations by the SPO and the NPA.

Table 3.7. KoFIU's spontaneous dissemination to LEAs and LEAs use of this information (2012-2018)

Agency	Disseminations received	In progress	Completed	(Of those completed)		
				No suspicion	Suspension of prosecution/ investigation	Prosecution/ indictment/ inquiry
Supreme Prosecutors Office (SPO)	15 702	1 873	13 829	8 822	986	4 021
National Police Agency (NPA)	60 656	48 283	12 373	6 954	2 388	3 031
National Tax Service (NTS)	139 400	52 303	87 097	6 488	50 328	30 281
Korea Customs Service (KCS)	27 297	9 150	18 147	4 205	9 124	4 818
Financial Services Commission (FSC)	1 174	927	247	154	5	88
National Election Commission	62	23	39	13	0	26
Korea Coast Guard (KCG)	260	23	283	91	0	192
National Intelligence Service (NIS)	7	3	4	4	0	0
TOTAL	244 558	112 539	132 019	26 731	62 831	42 457

157. LEAs may also request operational analysis from KoFIU. Since 2018, KoFIU has collected feedback on the utility of information disseminated to LEAs upon request. As of 2018, 72.2% of the feedback received indicated that the requested intelligence package was highly useful, serving as key investigative leads for investigations and inquiries as well as identifying asset and capital flows (see Table 3.8).

Table 3.8. KoFIU's dissemination of information to LEAs upon their request and LEAs use of this information (2018)

Agency	Information requested and received	In progress	Completed	(Of those completed)		
				Not used	Used to verify/supplement	Used to uncover new information
Supreme Prosecutors Office (SPO)	523	294	145	32	86	27
National Police Agency (NPA)	481	448	0	0	0	0
National Tax Service (NTS)	36 562	13 116	16 048	4 722	6 851	4 475
Korea Customs Service (KCS)	441	220	5	3	2	0
Financial Services Commission (FSC)	0	0	0	0	0	0
National Election Commission	5	4	0	0	0	0
Korea Coast Guard (KCG)	11	9	1	0	1	0
National Intelligence Service (NIS)	0	0	0	0	0	0
TOTAL	38 023	14 091	16 199	4 757	6 940	4 502

Note: Feedback on the use of KoFIU information prior to 2018 is not available, as this information was not sought from LEAs.

158. Korea provided several examples of cases demonstrating that KoFIU's operational analysis has proven useful in triggering and progressing investigations of predicate offences and related ML (see Box 3.3).

Box 3.3. Cases of investigations or inquiries initiated by KoFIU's information

Case Study 1: Embezzlement and Tax Crime Using a Company Account of a Virtual Asset Service Provider (VASP)

KoFIU received and analysed an STR involving the executive director of a VASP (Person A) that flagged high risks of ML and market manipulation between virtual asset dealers. Financial transaction patterns and problems in accounting transparency revealed the possibility of embezzlement, tax crime and mixing of funds. KoFIU traced transactions with another virtual asset exchange through the company's accounts and found large transfers to the private bank accounts of the CEO and Person A. KoFIU disseminated the STRs and its analysis to the SPO. The SPO's investigation revealed that two suspects (Persons A and K) who operated virtual currency exchanges had manipulated the computerised system to make it appear as if billions of KRW in cash had been deposited, thereby deceiving 7 060 victims and illegally acquiring about KRW 38.2 billion (EUR 29.4 million) worth of virtual assets in profit. The SPO supplemented the STR, CTR and basic analysis provided by KoFIU with direct evidence secured through search and seizure on relevant companies, financial intelligence, etc. The SPO prosecuted and detained Person K and others for violating the *Act on the*

Aggravated Punishment, Etc. Of Specific Economic Crimes and other charges in March 2018 and confiscated about KRW 4.5 billion (EUR 3.5 million) worth of criminal proceeds in bonds from Person K.

Case Study 2: Billions of KRW from an online gaming website

A bank reported an STR involving Person A who regularly deposited large sums of cash from unknown sources then wired the money to many unspecified persons and received wires from other peoples' bank accounts worth up to KRW 20 million (EUR 15 400). KoFIU conducted operational analysis of the STR and determined that Person A had made online gambling-related transactions. KoFIU disseminated the STR and its analysis to the SPO, including information on Person A's transactions and account information, Person A's criminal record, and suspicions regarding related account holders. The SPO traced the proceeds and confirmed that Peron A and others had opened online gambling websites worth KRW 34.4 billion (EUR 26.5 million) and made KRW 6.215 billion (EUR 4.7 million) of illegal profits. The SPO searched and seized the online gambling website's main headquarters, apprehended 12 staff members and confiscated KRW 22.6 billion (EUR 17.4 million) worth of assets. Person A and ten other perpetrators and accomplices were prosecuted. The investigation was conducted based on KoFIU's information that contained the suspects' financial transaction details and supported the allegations in the investigative documents. KoFIU's information also made it possible to estimate the scale of the online gambling market with the transaction details of the deposited and withdrawn funds.

Strategic Analysis

159. KoFIU undertakes strategic analysis to a certain extent. KoFIU has three teams that undertake strategic analysis focused on different areas (tax crime, customs-related offending, and other criminal activity). These teams include secondees from relevant agencies (the NTS, the KCS, and the prosecution service) that provide insight and expertise on these areas.

160. Strategic analysis is generally conducted in three stages. The first stage is intelligence collection and analysis. The relevant team gathers available information from a range of sources. This includes STR and CTR reports, currency exchange reports, discussions and information from relevant parties (e.g. reporting entities, supervisors, and LEAs), information provided by domestic or international counterparts or bodies, and media reports. This information is collected and reviewed through statistical analyses, keyword analyses, working reports, and case studies.

161. At the second stage (identification and utilisation of trends and patterns), the outcome of these preliminary analyses is reviewed and discussed with relevant agencies to identify ML/TF trends and patterns. Regular discussions also take place internally between KoFIU teams, the KoFIU Commissioner, and the Head of the Information Analysis Co-ordination Office (see Figure 3.1). Through this process, the teams develop themes of strategic analysis for dissemination to users.

162. Finally, the third stage involves the dissemination of strategic analysis and the receipt of feedback. KoFIU disseminates strategic analysis reports with specific

examples (case studies) related to the identified theme. This information is shared with LEAs to facilitate and guide the identification and investigations of ML and proceeds-generating offences and to identify priority areas and policy targets. Certain strategic analysis products are also disseminated to reporting entities and supervisors to serve as a basis for supervision and inspection plans and to ensure reporting entities are aware of risks. Strategic analysis also feeds into the NRA. KoFIU seeks feedback on its strategic analysis products through relevant committees (see Table 2.1. in Chapter 0).

163. KoFIU produces an annual ML/TF Trends Report, which is a product of its strategic analysis. The report provides a yearly analysis of ML/TF trends and patterns and the results of strategic analysis by each of the three subject teams. Korea provided a few other examples of strategic analysis, of varying depth (see Box 3.4). From the examples provided, the assessment team considered that LEAs, reporting entities, and policy-makers could benefit from deeper and more frequent strategic analysis, particularly in identified high-risk areas (such as tax crime).

Box 3.4. KoFIU strategic analysis on ML through casinos

A STR analysis by KoFIU in July 2018 identified a recurring ML typology through which a suspect would exchange the proceeds of investment fraud for a check issued by the casino, then leave without exchanging it into chips. In September 2018, KoFIU's analysis on this typology was shared with inspection agencies and LEAs, as well as with casinos. This enables the Jeju Provincial Policy Agency to identify ML related to a voice phishing operation. It was also incorporated into the inspection plan of the SGP casino supervisor.

Co-operation and exchange of information/financial intelligence

164. Korea has strong co-operation mechanisms in place that work well in practice. KoFIU and other competent authorities regularly co-operate and exchange information and financial intelligence, and have adequate measures to protect the confidentiality of information exchanged and used.

165. These conclusions are based on visit to the premises of KoFIU, and discussions with KoFIU, LEAs (the NPA, the SPO, the NTS, the KCS, the KCG, the National Election Commission and the NIS) and supervisory authorities (the FSS, the FSC and the entrusted agencies).

166. Informal co-operation effectively supports co-ordination and information sharing between agencies. KoFIU provides a sound platform to support this co-operation as well as share expertise between authorities and private sector. The KoFIU model, with its use of secondments, helps cross-match financial, police and customs intelligence, and also overcomes security restrictions that might otherwise constrain quick online access across different agency databases. KoFIU not only co-operates and exchanges information and financial intelligence with LEAs, but also engages with regulators to support AML/CFT supervision through its Inspection Agencies Committee (see Table 2.1. in Chapter 0).

167. To protect domestic information exchanged between KoFIU and other competent authorities, Korea uses KoFICS (see para.132) which has different security access levels. KoFIU and the NTS also have a separate additional channel of secure

direct information exchange (FOCAS, see para.138), which further assists in exchanging any urgent information related to tax crimes. Appropriate measures are in place to protect the confidentiality and security of KoFIU information and the KoFICS database (see R.29).

3

Overall conclusions on IO.6

168. **Korea is rated as having a substantial** level **of effectiveness for IO.6.**

Immediate Outcome 7 (ML investigation and prosecution)

ML identification and investigation

169. Korean LEAs take a "follow the money" approach in their law enforcement activity. Since 2017, policy and operational changes have been made to further strengthen Korea's framework on asset recovery (seethe section below on IO.8). While the goal of these changes was to increase asset recovery, rather than ML investigations, they nonetheless ensure the use of financial investigations by specialised teams which puts Korea in a strong position to investigate ML.

170. These conclusions are based on: case studies provided by Korea; available statistics on ML investigations; and discussions with LEAs and other relevant authorities, including the SPO, the NPA, the KCG, the NTS, the KCS, the FSS, and the FSC.

171. Investigation figures show that Korean LEAs have consistently pursued ML at a reasonable level. Since 2017, newly-established asset recovery teams work alongside primary investigative units to do financial investigations related to predicate offending, trace and recover assets, and investigate ML. The specialised asset recovery teams have had a measurable impact in terms of asset recovery (see the section below on IO.8) and have seen a dramatic jump in the number of ML prosecutions in 2018 (see Table 3.11 in 3.3. below). The overall number of ML investigations conducted by Korean LEAs has remained fairly steady (averaging 575 investigations annually from 2014-2018), which is reasonable in light of Korea's context and relatively low level of criminal offending (see Table 3.9). In coming years, these figures are expected to increase as a result of the procedural and operational changes made by Korea.

Table 3.9. Criminal ML investigations 2014 – 2018

	Cases Investigated	Persons Investigated
2014	523	839
2015	535	1 007
2016	675	1 323
2017	516	934
2018	626	1 312
TOTAL		5 417
AVERAGE	575	1 083

172. Parallel financial investigations are the most common detection source for ML cases with STRs, informants and media reports also serving as possible leads. Once detected, ML is investigated by the NPA (under the direction and supervision of a prosecutor) or by a prosecutor from the SPO or a DPO. Depending on the predicate offence involved, other LEAs may investigate the predicate offence and related ML (e.g. the KCS for customs offences).

173. In line with the government focus on asset recovery, the NPA piloted a specialised Criminal Proceeds Investigation Team (CPIT) from March 2018 at its national headquarters in Seoul. Following the 2018 NRA (which highlighted the risks of predicate offending and the resulting need for asset tracing), the NPA decided to expand the programme. In January 2019, it rolled out specialised CPITs to all 17 regional police offices. These teams work alongside predicate offence investigators to trace assets and investigate ML, and conduct standalone ML investigations.

174. Within the SPO, the Criminal Asset Recovery Division (CARD) was established in 2018 and operates at the national level, with similar teams in place in each DPO and Branch Prosecutors' Office. Prosecutors in these units are responsible for undertaking asset recovery actions, undertaking ML investigations and prosecutions, supervising ML investigations, and providing financial investigative support to investigations into proceeds-generating crimes. CARD's performance management system incentivises asset recovery and ML by positively acknowledging prosecutors who successfully pursue such investigations.[29] This new organisation and structure is a positive step although, as recognised by Korean authorities, it is a recent initiative, so it is too soon to assess its effectiveness. In addition to the NPA and the SPO, a range of other LEAs may also work with prosecutors on ML investigations (see Table 3.10).

Table 3.10. Authorities with responsibility for investigating ML

Agency	Team	Human Resources	Types of ML pursued
Prosecutors' Offices	1 Criminal Asset Recovery Division in the SPO, 1 Criminal Asset Recovery Department in the Seoul Central DPO, 17 Criminal Asset Recovery Sections in each of the 17 DPOs, and 40 Criminal Asset Recovery Sections in each of the 40 Branch Prosecutors' Offices	62 prosecutors 120 investigators	Supervise all investigations, and investigates and prosecutes of ML
NPA	17 regional stations each have a Criminal Proceeds Investigation Team	52 investigators (including with financial backgrounds and qualifications)	Investigates ML (under the direction of a prosecutor)
Korean Coast Guard	1 Criminal Intelligence Section at the headquarters; 5 Special Crime Squads in the regional offices; and 6 Intellectual Crime Investigation Sections in the regional stations.	8 investigators at headquarters; 30 in the regional offices; 26 in the regional stations	Investigation of offences occurring on the sea and related ML
National Tax Service (NTS)	7 regional offices; 125 district offices	4 237 investigators in total	Inquiries into tax offences (e.g. tax crime)
Korean Customs Service (KCS)	1 ML division in the headquarters; 20 ML teams in customs offices	11 ML investigators at headquarters;	Inquiries into customs offences (e.g. smuggling, asset flight) and related ML

29. The system only provides performance management incentives (not financial incentives which could carry corruption risks).

Agency	Team	Human Resources	Types of ML pursued
		113 in customs offices	
Financial Services Commission (FSC)	The Capital Market Investigation Unit	23 investigators	Inquiries into capital market offences (e.g. market manipulation) or offences by FI employees and related ML
Financial Supervisory Service (FSS)	3 Capital Market Investigation departments	81 investigators	Inquiries into capital market offences (e.g. market manipulation) and related ML

Note: The figures reflected above show the resources available to pursue ML, and do not reflect dedicated ML resources.

175. Investigating teams without in-house financial investigation expertise may seek help from the SPO or relevant DPO. For example, the SPO's CARD provides advice and assistance to other investigative teams (in any agency) to trace financial flows, analyse accounts and financial records, and seize corporate assets. The SPO also has a dedicated accounting analysis team that can provide assistance in corporate cases, including seizing and analysing corporate accounts. These teams have published manuals on asset-tracing and corporate accounting analysis. The SPO also aims to strengthen ML knowledge and expertise within the 18 DPOs and 40 Branch Prosecutors' Offices, and plans to provide extensive training. Enhancing ML knowledge at the district level may help Korea ensure that the authorities pursue and prioritise ML cases more effectively.

176. Across the LEA teams described in Table 3.10, a total of 62 prosecutors and approximately 4 700 investigators are available to pursue asset recovery and ML investigations, although the level of ML-specific training and expertise varies across agencies and teams (see paras.173-174 above). In general, LEA representatives considered these resources sufficient, although one representative noted that the NPA's CPIT could benefit from additional human and IT resources. Where resources are not sufficient, authorities have the useful ability to share and pool resources (e.g. to investigate a particularly complex case) by drawing resources from regional offices upon direction of the relevant head office or by conducting joint inter-agency investigations. Given the recent nature of the CPIT teams, and the expected increase in the number of ML investigations, additional resources may be required to ensure these teams continue to have capacity to effectively pursue ML.

177. LEAs have access to a range of investigative tools and techniques to investigate ML, and actively use information from KoFIU both as an investigative lead and to support ongoing investigations (see the section above on IO.6). LEA representatives estimated that KoFIU is able to provide information when requested about 50% of the time. In the remaining cases (e.g. where there is no related STR or CTR), the prosecutor would seek a court order to obtain the information directly from the relevant institutions. LEAs can obtain court orders promptly, typically within 1-2 days, and prosecutors are able to secure orders urgently, within hours, where necessary.

178. Even where information is obtained from KoFIU on the person(s) under investigation, investigators and prosecutors noted that in most cases, they also need information on related persons and accounts. This is particularly necessary in Korea due to the risk and prevalence of ML through accounts in borrowed names (see Chapter 1, para.39). In some cases, the requesting LEA is able to substantiate a request to KoFIU for information on related accounts (e.g. by providing information showing a suspicion of accounts in borrowed names). However, LEA representatives noted that in many cases they would not be able to obtain information from KoFIU and would

instead use a court order. Korea has taken a range of steps to prevent and improve detection of borrowed name accounts, and should continue these efforts to further help LEAs detect and trace accounts in borrowed names.

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

179. Korea has made efforts to pursue ML in line with its risk. However, a significant gap in Korea's predicate offences prevents the authorities from pursuing ML in its highest risk area (tax crime), which seriously undermines these efforts.

180. These conclusions are based on the 2014, 2016 and 2018 NRAs; other risk assessment and strategy documents provided by Korea; case studies; and discussions with the SPO, the NPA, the KCG, the NTS, the KCS, and the FSS. Based on the risks identified by Korea, and its own scoping exercise, the assessment team focused on Korea's pursuit of: ML stemming from tax crime, illegal gambling and financial fraud; cash-based ML; ML involving virtual assets; and ML using accounts in borrowed names.[30] Professional enablers are not a prominent feature in Korea's ML cases, but the increasing use of complex corporate structures means this typology may be an emerging risk.

181. Korea's 2018 NRA concluded that: the three highest-risk proceeds-generating offences were tax crime, illegal gambling and financial fraud;[31] cash and virtual assets posed particular vulnerabilities for ML; and banks were the highest risk institution. LEAs supported these findings noting that illegal gambling and fraud are common predicate offences seen in their day-to-day activities. In terms of common methods for ML in Korea, authorities all recognised and confirmed the use of cash, an increasing use of virtual assets and the likelihood of money moving through a Korean bank. LEAs consistently noted that the vast majority of ML schemes in Korea use bank accounts in borrowed names (either bought, or in the name of an associate or family member) (see para.39). Authorities agreed that using professional enablers was uncommon, but noted an increasing use of corporate structures, which may result in an increased use of professional enablers in the future. Authorities were not sensitive to this as an emerging risk.

182. Statistics provided by Korea show some alignment between identified risk areas and ML investigations and prosecutions, although there are some notable exceptions. The most significant issue is the lack of ML investigations and prosecutions of tax crime, despite this being the most significant proceeds-generating offence, because most tax crimes are not predicate offences for ML. There is a higher number of ML investigations and prosecutions into illegal gambling and financial fraud, which are Korea's other major proceeds-generating offences. However, compared to the total number of predicate offence investigations and prosecutions in these areas, the number of ML investigations and prosecutions remains low (generally less than 1%). Other identified risk areas, such as securities offences and asset flight, also see relatively low numbers of ML investigation and prosecution. Crimes not identified in the NRA, such as prostitution, see higher numbers of ML investigations and prosecutions, although such crimes likely involve much lower values (see Table 3.11).

30. Enquiries and research by the assessment team confirmed that drug-related offending and organised crime were not prevalent predicate offences in Korea (see Chapter 1, para.36).

31. Korea's NRA identifies seven major predicate offences for ML. The top three are reflected here. The remaining offences are corruption, market manipulation, asset flight, and embezzlement.

Table 3.11. Investigations and prosecutions of ML in Korea 2015-2018 broken down by representative charge*

	2015		2016		2017		2018	
	Investigations	Prosecutions	Investigations	Prosecutions	Investigations	Prosecutions	Investigations	Prosecutions
Proceeds concealment and disguise (ML)	70	27	64	23	60	7	430	532
Embezzlement-related ML	47	100	23	124	51	92	82	119
Illegal gambling-related ML	11	55	39	73	32	111	34	134
Financial fraud-related ML	29	80	25	70	30	45	47	127
Corruption-related ML	24	97	7	73	17	46	14	56
Trademark theft-related ML	11	20	7	31	13	18	3	23
Securities offences-related ML	3	1	24	13	9	8	6	15
Asset flight-related ML	17	7	19	7	9	18	6	9
Prostitution-related ML	3	5	11	38	5	25	0	10
Smuggling-related ML	37	33	22	25	3	6	2	9
Tax crime-related ML	0	0	0	0	0	2	1	8
Drug offending-related ML	2	2	0	5	0	2	1	1
ML related to other offences	281	-	434	10	287	-	0	0
TOTAL ML	535	373**	675	492	516	346**	626	1 043

*Each case under investigation or prosecution is entered into the system by "representative charge". This reflects the perceived more serious charge, although there may be several charges involved in one investigation or prosecution. The figures in the above table reflect the representative charges, which in some case may be ML and in other cases may be the relevant predicate offence. ML was pursued in all cases in the above table.

** In some cases, there may be duplication as one prosecution was registered by several representative charges. This means the total figure for some years does not equate to the registered representative charges.

Note: The figures in this table reflect the year an investigation or prosecution was opened (meaning each investigation or prosecution is counted only once, even if it spans several years. The number of prosecutions may be higher than the number of investigations because prosecutors may choose to file a ML charge based on the evidence available even where the investigation was not focused on ML.

183. **ML associated with tax crime:** Korea is very limited in its ability to investigate and prosecute ML related to tax crime due to severe gaps in its predicate offence framework. The vast majority of tax crimes are not considered predicate offences for ML. The only tax crime included within the scope of Korea's predicate offences is obtaining fraudulent tax rebates over KRW 500 million (EUR 378 422). LEA representatives estimated that this type of offending accounts for one in 100 tax crimes. As a result of this major shortcoming, Korea is very rarely able to pursue criminal investigations or prosecutions into ML related to tax offending (see Table 3.11). This is a particularly significant deficiency given Korea's identification of tax offending as its highest-risk proceeds-generating offence. Criminal prosecution is generally not pursued in tax offending cases, with Korea instead prioritising remediation (see the section below on alternative measures). Where a tax offence is detected, the NTS informs the offending natural or legal person and instructs them to pay the unpaid tax. The NTS may also impose a criminal penalty of up to five times the amount of tax evaded or refer the case to a prosecutor for prosecution. The case is generally recommended for prosecution only if the tax and penalty remain unpaid.

184. **ML associated with illegal gambling:** The NPA actively investigates illegal gambling, and to some extent, the associated ML. Illegal gambling has been consistently identified as a high-risk area since Korea's first NRA in 2014. As a result, annually since 2015, NPA has had special 'crackdowns' on illegal gambling which aim to raise public awareness of illegal gambling, enhance deterrence and identify cases. These crackdowns resulted in a notable increase in related ML investigations and prosecutions in 2016 and 2017. The total number remain low in comparison to the number of predicate offences investigated and prosecuted, suggesting an increased focus on asset recovery and predicate offending rather than ML (see Table 3.11). NPA representatives met at the on-site were well aware of the risk posed by illegal gambling, and were able to describe common ML methodologies and schemes associated with this offence, including ML through virtual assets (see Box 3.5).

185. **ML associated with financial fraud:** The NPA has dedicated Intelligent Crime Investigation Teams in all regions that focus on preventing financial fraud, including voice phishing, illegal private financing, and insurance fraud. Fraud has been a priority since 2016 and the NPA undertook special crackdowns in both 2016 and 2017. While these resulted in a number of arrests, there was no corresponding increase in the number of ML investigations and prosecutions related to this predicate which may be due to a focus on asset recovery and predicate offending rather than ML (see Table 3.11). The FSS has launched a call centre to encourage fraud reporting, with rewards of up to KRW 10 million (EUR 7 700) for those who report. Insurance companies operate similar channels to encourage clients to report insurance fraud. LEAs acknowledge financial fraud, particularly voice phishing, as a high risk.

186. **Cash-based ML:** Case studies and discussions with LEAs confirmed that most of Korea's ML cases are cash-based and relatively simple in their methodology. Authorities at both the regional and national levels are well equipped to pursue this type of ML, which tends to involve much simpler typologies.

187. **ML through virtual assets:** The 2018 NRA identifies virtual assets as a high risk for ML. Korea has actively responded to this risk, including at the law enforcement level. There have been a number of cases of ML through virtual assets in Korea. The authorities noted that this typology is particularly common for laundering proceeds of illegal gambling.

188. In addition to the risk areas identified above, Korea also demonstrated that it was taking action in respect of other areas identified in the NRA, including asset flight (see Box 3.13 below) and borrowed names (see Box 3.6 below). Given the ongoing prevalence of the use of borrowed name accounts for ML, Korea should continue its positive efforts to identify policy and operational measures to prevent and detect this typology.

Box 3.5. Illegal gambling case with money laundered through virtual assets

In August 2018, a local police station referred a case to the Suwon DPO *involving the theft of KRW 78 million (EUR 59 000) in gambling profits from the residence of Person A. The large amount of cash involved raised suspicions and, by looking into it further, the DPO found that the cash was the profits from an illegal gambling website operated by Person D (based outside Korea). Person A was arrested for receiving criminal proceeds, and her residence was searched resulting in the seizure of documentary evidence and KRW 57 million (EUR 43 140) in cash. The DPO traced Person A's funds and detected additional bank accounts used to conceal the proceeds, including links to Person B (D's brother-in-law). Both Persons A and B were receiving illegal proceeds and laundering the funds through investing in virtual assets. A total of over KRW 100 billion* (EUR 75.7 million) in profits were traced through various accounts, KRW 4.9 billion (EUR 3.7 million) of which was received and laundered by Persons A and B. The prosecution froze KRW 4.9 billion (EUR 3.7 million) of Person A and B's assets, including cash, bank accounts, virtual asset accounts, insurance, vehicles, and luxury goods (capturing proceeds and assets of equivalent value). Person A and B were both prosecuted for ML and the case is currently pending. An Interpol red notice has been issued for Person D.

Box 3.6. Korea's pursuit of ML in cases involving borrowed name accounts

ML through borrowed name accounts is widely recognised as Korea's most common ML methodology, regardless of the predicate offence involved. This issue is well understood by all LEAs. Korea criminalised the use of borrowed name accounts in 2014 in response to the identified risks in this area (*Electronic Financial Transactions Act*). Since 2014, the NPA has engaged in annual crackdowns to detect and prosecute the use of borrowed name accounts, including outside the ML context. These crackdowns have seen an average of 24 000 cases investigated and 14 500 persons prosecuted annually since 2014. Authorities utilise various investigative techniques and information sources to detect the use of borrowed name accounts, including requesting financial transaction information on related persons (including family and friends) from KoFIU, studying CCTV footage and online banking information, and obtaining information from informants and relevant networks. The NPA also has a professional analysis tool that helps officers to review a large volume of data and information in order to trace funds and detect the use of borrowed names. Identifying the use of bought name accounts is more complicated, although authorities are able to use various tools to detect this typology (e.g. access to CCTV or information from financial institution staff).

189. LEAs noted that they have witnessed an increasing number of complex corporate structures in the context of ML and predicate offending. Tackling ML via complex corporate structures may be complicated by issues in obtaining company information (see Chapter Chapter 7. on IO.5). In the cases seen to-date, authorities noted that these schemes have been set up using insider personnel, including legal teams and in-house accountants, rather than using professional enablers. Nonetheless, if this trend continues, professional enablers may become an emerging risk for Korea in the future. The use of professional enablers may also be impacted by the growing number of VASPs in Korea. Authorities are well aware of the risks posed by virtual assets (see Chapter 2. on IO.1) and LEAs have knowledge and expertise in legal and accounting issues. It may be timely for Korea to review the risks posed by professional enablers to determine if there are particular vulnerabilities in this area.

Types of ML cases pursued

190. While Korea was able to demonstrate that it has been able to prosecute and convict third party, standalone and self-laundering, the assessment team was not satisfied that the different types of ML were being prosecuted to a large extent. The majority of Korea's cases are self-laundering. Relatively few cases were provided of standalone ML, third party laundering, and laundering based on a foreign predicate.

191. These conclusions are based on case studies provided by Korea; available statistics on the types of ML pursued; and discussions with LEAs, including the SPO, the NPA, and the KCG.

192. Korea's "follow the money" approach leaves it well equipped to pursue cases of self-laundering. Discussions with authorities and case studies provided by Korea confirmed that self-laundering is the most common type of ML prosecutions and convictions. This is somewhat consistent with Korea's ML risk profile which sees offenders self-laundering proceeds through cash, virtual assets, and borrowed name accounts.

193. Standalone ML and third party ML are prosecuted to a lesser extent. Where standalone and third party ML are prosecuted, it is almost exclusively family members and associates with a connection to the principal offender laundering the money, rather than an unrelated person or professional enabler. This aligns with Korea's ML risks and the prevalence of laundering through borrowed name accounts which can be those of a family member or associate. Nonetheless, the low number of cases involving unrelated or removed third parties may suggest authorities are less equipped to pursue more complex ML schemes.

194. Prosecutions of ML relating to the proceeds of a foreign predicate appear to be extremely rare. Korea provided a handful of examples of prosecutions for the laundering of foreign predicates. While Korea's ML risks are largely domestic, the assessment team nonetheless expected to see additional and more recent examples of such cases.

Box 3.7. Korea's ability to pursue different types of ML

Standalone and third party ML: In 2016, Person K, the operator of an illegal gambling site, withdrew all proceeds from the site and deposited the cash into an account under a borrowed name. At the request of Person K, Person S (an acquaintance) withdrew KRW 5 million (EUR 3 784) in ten regular intervals between September and October 2016 to deliver a total of KRW 50 million (EUR 37 841) in cash to Person K. Person S was prosecuted and convicted of ML and sentenced to one year in prison.

Third-party ML: Between 2013 and 2015, Person K laundered KRW 1.4 billion (EUR 1 million) of illegal gambling proceeds through his bank account at the request of Person C. Person K either withdrew the money in cash and passed it to Person C, or transferred it to Person C's account via wire transfer. Person K was sentenced to 10 months in prison on charges of ML and aiding and abetting illegal gambling

Self-laundering: In 2008, Person G received bribes of KRW 100 million (EUR 75 683). Person G obtained an additional KRW 100 million (EUR 75 683) from his friend (person L) as an investment and used the total funds to purchase a bakery which he registered in L's name. L withdrew his investment in 2009 and transferred registration to G's mother. In 2012, part of the bakery was sold to G's sister, in return for KRW 150 million (EUR 113 525) which G invested, making a further profit. G was convicted of both bribery and ML, and sentenced to eight years in prison.

Self-laundering: Between 2011 and 2018, a ring of 54 persons launched, operated and participated in a network of illegal gambling sites. In May 2017, the NPA received a report from an informant and launched an investigation. A total of 82 warrants were obtained and executed for the search and seizure of financial accounts, premises, and communications. Transaction analysis traced the proceeds of the sites to borrowed name accounts and real estate investments in others' names. The NPA froze approximately KRW 13.1 billion (EUR 10.1 million) worth of real estate, real property, and bank accounts and arrested and indicted 140 persons. In January 2019, sentences were issued, ranging up to three years of imprisonment and KRW 7.5 billion (EUR 5.7 million) was ordered for confiscation

ML based on a foreign predicate: Upon receipt of an MLA request for enforcement of a confiscation order, Korea traced KRW 1.32 billion (EUR 890 195) in bribes that Person M been and hidden in Korean accounts. Korean authorities traced and returned KRW 679.8 million to the requesting state. While tracing the funds, the Korean authorities detected several individuals in Korea that had aided in laundering the money, including Person M's mistress, and confiscated various real property and funds worth KRW 450 million (EUR 340 577). Three individuals were prosecuted and convicted of ML and sentenced to imprisonment of between 6 and 10 months. Korea is currently working to recover the additional funds and, when recovered, will liaise with the requesting state as to next steps.

195. Case studies and discussions with LEAs showed that where legal persons have been involved in ML in Korea, they are usually shell companies or companies close to bankruptcy that are dissolved after the laundering is complete. As a result, prosecutions of legal persons for ML are extremely rare. Nonetheless, Korea provided one case study in which a company and its CEO laundered money through company accounts. The case resulted in a suspended sentence for the CEO, but the legal person was not prosecuted or sanctioned. No other case studies were provided to show the prosecution or conviction of legal persons for ML. In theory, the liability of legal persons is triggered when a representative of the company commits ML.

Effectiveness, proportionality and dissuasiveness of sanctions

196. Korea's ML sanctions are generally too low to be effective, proportionate and dissuasive for either natural or legal persons. This conclusion is based on: case studies provided by Korea showing sentencing practices; statistics on sentencing; and discussions with the SPO, the NPA, the KCG, and the MOJ.

197. On paper, ML sanctions are largely in line with similar offences in Korea, noting that Korea's criminal sanctions are generally low by global standards. The general ML offence under POCA is punishable by five years of imprisonment and/or a fine of KRW 30 million (EUR 23 500). The drug-specific ML offence has the same fine, with a higher prison sentence of seven years (see R.3). Korea explained that the policy rationale for the different imprisonment sentences is due to the drug-specific ML offence existing under a special enactment that was passed to respond to a particular threat, while the POCA offence is a general offence. Nonetheless, this discrepancy is out of line with Korea's risk areas (where drug offending is not considered a high-risk offence). These sanctions are comparable to those available under Korean law for embezzlement, breach of trust, insider trading and lower-level bribery (5 years in prison), but are lower than those for fraud, unfair trading and receiving higher-value bribes (10 years to life imprisonment). The fines available are particularly low for legal persons (see R.3).

198. In practice, sentences against natural persons are generally low. It is also difficult to measure the impact of the ML sentence as ML is typically prosecuted alongside a predicate offence and the sentence imposed will not distinguish between the separate charges. Between 2014 and 2017, the most common sentence imposed for a conviction including (but not limited to) ML under POCA was imprisonment for between one and three years, with the average being 33 months (2.75 years) (see Table 3.12). The fines imposed are similarly low, with over 88% of fines falling into the lowest bracket of under KRW 50 million (EUR 38 800) (see Table 3.13). The average fine varies considerably year to year—KRW 172.3 million (EUR 133 900) in 2017 and KRW 19.6 million (EUR 15 200) in 2016 (in addition to confiscation; see the section below on IO.8). Sentences against legal persons cannot be assessed in practice in the absence of any prosecutions or convictions.

199. Based on the case studies provided, sentences for standalone ML are rarely more than one year in prison, while stronger sentences are imposed where ML is sentenced alongside bribery (often 7 years in prison) or embezzlement (3-5 years in prison). This suggests the courts generally do not use the full range of sanctions available for ML. Sentences at the lower end of the scale may be appropriate where the launderer acts as a mule or merely provides an account (see Box 3.8). However, where a third party launderer was complicit in and/or benefited from the act, these sentences are unlikely to be proportionate.

Box 3.8. Sanctions imposed in cases involving a ML charge

Sentence of 10 months for high value ML: Person K laundered KRW 1.4 billion (EUR 1 million) of illegal gambling proceeds through his bank account at the request of Person C. Person K either withdrew the money in cash and passed it to Person C, or transferred it to Person C's account via wire transfer. Person K was sentenced to 10 months in prison on charges of ML and aiding and abetting illegal gambling.

Sentence of 5 years for ML and embezzlement: Person X was one of several executives at a savings bank who established special purpose companies in the names of the bank's employees and illegally gave loans to these companies while also embezzling KRW 139 million (EUR 105 200) on the pretext of giving pay checks to these employees. Person X was convicted of embezzlement and ML and sentenced to 5 years in prison.

Sentence of 7 years' for ML and bribery: Person M accepted a bribe of KRW 134.9 million (EUR 102 098) in return for demolishing a traditional market and building an apartment complex. The parties signed a false contract related to art installations to hide the bribe. Person M laundered the bribe by converting the money into cash and checks. He was convicted of ML and taking bribes and sentenced to 7 years in prison.

200. Representatives of LEAs largely considered that available sanctions were sufficiently effective, proportionate and dissuasive, but noted that there is significant judicial discretion resulting in a wide range of varied sanctions. Guidance for the judiciary (judicial sentencing guidelines) may help ensure Korea is able to impose sanctions in a consistently effective and proportionate manner.

Table 3.12. Number of prison sentences for ML offences

	< 6 months	6 months < 1 year	1 < 3 years	> 3 years
POCA	48	370	954	437
ASPIT	0	0	5	5

Table 3.13. Number of fines for ML offences

	< KRA 50 m	KRW 50 m < 100 m	KRW 100 m < 300 m	> KRW 300 m
POCA	121	12	2	2
ASPIT	0	0	0	0

Use of alternative measures

201. Korea has alternative criminal justice measures available for tax offending. For tax crime, Korea actively pursues tax levies and fines. Other actions (e.g. pursuit of the predicate offence and asset recovery) are generally pursued regardless of whether or not it is possible to secure a ML conviction, rather than as a true alternative to ML. These conclusions are based on case studies provided by Korea and discussions with the SPO, the NPA, the KCG, the NTS, and the KCS.

202. Indicting and prosecuting for ML is a prosecutorial decision. Where there is insufficient evidence for a ML charge, the prosecutor will pursue the predicate offence, which also enables confiscation of the criminal proceeds (based on a conviction for the predicate offending). While this action may sometimes be used as an alternative measure (where ML cannot be proven), this course of action is taken reasonably often in Korea (see Table 3.14) suggesting it is not always being pursued as a strict alternative to ML. This may change with Korea's new operational and procedural changes that incentivise the pursuit of ML (see above).

Table 3.14. ML investigations resulting in only predicate offence charges

	2015	2016	2017
Cases	221	237	198
Persons involved	386	377	284

203. In most cases of tax offending, Korea is not able to file ML charges due to limitations in the predicate offences (see para.183). The same limitation does not apply to STR reporting requirements, which extend to a broader range of tax crimes, meaning KoFIU receives a range of reports related to all types of tax offending. These reports are sought by and disseminated to the NTS for use in its tax audits. Where the NTS detects a tax offence, it will inform the offending natural or legal person and instructs them to pay the unpaid tax in addition to a monetary penalty. The case is generally recommended for criminal prosecution only if the tax and penalty remain unpaid.

Overall conclusions on IO.7

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

Immediate Outcome 8 (Confiscation)

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

205. Asset recovery is actively pursued as a policy objective across relevant LEAs. Since 2017, asset recovery (include freezing and confiscation of proceeds, instrumentalities, and property of equivalent value) has been formally designated as a high governmental priority which has further increased Korea's confiscation efforts.

206. These conclusions are based on: discussions with the SPO, the NPA, the KCG, the NTS, and the KCS; public and policy statements from the Korean government; and statistics and case studies provided by Korea.

207. Korea's criminal case management system, the Korea Information System of Criminal Justice Services (KICS) automatically identifies and flags cases with potential recoverable assets–either proceeds or property of equivalent value. This ensures asset recovery is systematically considered and that prosecutors pursue all available assets that could be subject to confiscation orders. In 2017, the Korean government formally identified confiscation as one of its top priorities. Discussions with authorities and statistics provided by Korea showed that Korea actively pursued asset recovery prior to 2017, but its enhanced status allows for increased resources and specialisation. Specific asset recovery teams have been established within the NPA and the prosecution service at both the national and regional level (see para.173-174). These teams have specific expertise in tracing assets and receive regular training on

recovering proceeds. Training is thorough, sometimes being held over a two-week period, and covers a variety of topics, including asset tracing methods, accounting analysis, how to read financial transaction information received from FIs, and financial statement analysis. Discussions with agencies confirmed that these new teams ensure asset recovery is now being considered systematically in all cases and that preservation of all available assets (including property of corresponding value) is prioritised to prevent asset-dissipation. Cross-agency teams were also established to leverage different expertise and powers. In some cases (e.g. with the SPO's CARD), pursuing asset recovery is incentivised by being reflected positively in performance reviews.

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

208. Korea actively confiscates the proceeds of domestic and foreign predicates, and pursues proceeds moved offshore. Between criminal confiscation efforts and tax levies, Korea is able to deprive criminals of a high value of proceeds. The legal framework is robust, ensuring that confiscation is straightforward and measures are in place to ensure assets are not dissipated, although these mechanisms have not always been systematically used. Early indicators suggest that Korea's recent operational and structural changes are further enhancing its system. In particular, these changes may help ensure a higher percentage of assets ordered for confiscation are recovered.

209. These conclusions are based on: discussions on asset recovery with prosecutors and other LEAs (particularly the KCS and the NTS); case studies; and statistics on confiscation.

210. Korea has a conviction-based regime for asset recovery that allows for value-based confiscation. Proceeds-generating offences and ML are investigated by a prosecutor or a LEA under the direction of a prosecutor (see the section above on IO.7). The prosecutor is responsible for making decisions relating to the asset recovery elements of the case, including freezing, seizure and confiscation. The case management system used by prosecutors ensures that potential asset recovery is automatically flagged and systematically considered in all relevant cases, and that prosecutors pursue all available assets, including assets of equivalent value.

211. From 2017, specialised teams were established in each prosecutors' office to focus on asset recovery and ensure confiscation is pursued in all cases involving proceeds-generating offences. Under these teams, 62 prosecutors and 120 investigators are now dedicated to asset recovery and ML which has had a very positive effect on the number of criminal preservation orders. Prior to the existence of these specialised teams, on average Korea was preserving KRW 520 508 million (EUR 402.5 million) and confiscating KRW 224 828 million (EUR 173.9 million) annually through the criminal process. These amounts are reasonable given Korea's context and relatively low levels of criminality. Since establishing the SPO's CARD, requests for freezing have increased by 90% with Korea preserving KRW 2 439 041 (EUR 1 886.2 million) in 2018 (see Table 3.15). These changes remain recent, but authorities expect this positive trend to continue. Authorities are currently well equipped and resourced to handle this work, but if these positive trends continue across all districts, Korea may need to monitor resources to ensure that the prosecutors' offices remain equipped to handle the growing number of cases.

212. Prior to conviction and confiscation, the relevant prosecutor will routinely apply for a preservation order to prevent dissipation of proceeds or assets of equivalent value. To obtain a preservation order, the prosecutor must demonstrate that, on the balance of probabilities (the civil standard of proof), a proceeds-generating offence has been committed. This threshold does not prove difficult to meet in practice. Prosecutors explained that available financial intelligence, including information from KoFIU, was generally deemed sufficient. Courts rarely refuse applications for preservation orders and typically issue preservation orders permitting the preservation of a high value of proceeds or assets of equivalent value, calculated on the basis of the prosecutor's application, which helps prevent the dissipation of assets. Preservation orders typically take between two days and two weeks to obtain, depending on the complexity of the case, the extent of financial intelligence available, and the urgency of the situation. Urgent preservation orders may be obtained to prevent the dissipation of assets. Since the SPO's CARD and the similar regional teams were created, there have been no cases of asset dissipation prior to preservation. Where this occurs, prosecutors can file a civil claim to recover and preserve the dissipated assets.

213. A strength of Korea's system is that a preservation order launches the confiscation proceedings. Once a preservation order is obtained, the confiscation aspects of the case can run alongside the predicate offence and/or ML investigation and prosecutions, meaning that a confiscation order can be granted immediately upon conviction without having to start a separate confiscation proceeding. Prior to the implementation of the new teams, this system was not systematically used resulting in slower confiscation results. Korea should ensure it takes advantage of these available efficiencies. Confiscation orders are calculated based on the value of criminal proceeds shown in the relevant case, meaning these will often be lower than the amounts initial sought for preservation by prosecutors. Value-based confiscation is actively used where the actual proceeds cannot be identified.

Table 3.15. Criminal proceeds preserved, confiscated and recovered

	Amount preserved		Amount ordered for confiscation		Amount recovered	
	KRW million	EUR million	KRW million	EUR million	KRW million	EUR million
2015	471 724	364.7	224 688	173.8	59 522	46.0
2016	540 635	418.1	213 896	165.5	55 105	42.6
2017	549 167	424.7	235 900	182.5	34 526	26.7
2018	2 439 041	1 886.2	103 935	80.4	10 188	7.9
TOTAL	4 000 567	3 094.8	778 419	602.2	159 341	123.2

214. The total amounts preserved, confiscated and recovered by Korea are reasonable, especially taking into account Korea's relatively low level of crime. The new asset-recovery teams have had a significant and impressive impact on the use of preservation orders, with an increase of almost KRW 2 trillion (EUR 1.5 billion) preserved (see Table 3.15). From 2015-2018, the amounts recovered are approximately 20% of those ordered for confiscation. In some cases, this is because the recovery process is ongoing meaning the assets have yet to be realised. In other cases, Korean authorities noted that preservation orders may not have been effectively used in the past resulting in the dissipation of assets. Given the new teams' focus on asset recovery and systematic use of preservation orders, prosecutors expected to see an increase in the amount of assets recovered in the future. The new teams have had considerable success in preservation; however, their impact on recovery figures has

yet to be seen. To further improve recovery efforts, Korea has implemented an IT system to monitor cases requiring or involving asset recovery, complete with an alert system to flag assets for confiscation and ensure these are promptly confiscated immediately upon conviction. Korea should continue pursuing efforts in this area to increase the proportion of assets recovered.

215. Case studies provided by Korea demonstrate the authorities' ability to seize and confiscate a wide range of proceeds, instrumentalities, and assets of equivalent value, including cash, gold bars, real property, bank accounts, insurance plans, high value assets (e.g. vehicles, jewellery, art, etc.) and even golf course memberships. Korea has also had considerable success confiscating virtual assets following a 2017 case in which the Court recognised the value of virtual assets and determined that they were subject to confiscation. Since then, virtual assets have been actively frozen and confiscated (see Box 3.9).

216. As confiscation is conviction-based, Korea has systems in place to manage and maintain assets prior to confiscation (see R.4). A particularly positive aspect of Korea's system is that it is able to liquidate preserved assets prior to confiscation in order to preserve their value and prevent depreciation. Korea should ensure it takes advantage of such opportunities to increase the percentage of confiscated assets recovered.

Box 3.9. Confiscation of virtual assets

In 2018, SPO detected that Person P was operating an illegal pornography website. Person B received payments in virtual assets (specifically Bitcoin). The SPO's digital forensics team was able to trace the movement of the virtual assets that were exchanged into other types of virtual asset in a virtual currency exchange before eventually being cashed out. The SPO was able to obtain a preservation order for approximately KRW 4.5 billion (EUR 3.4 million) that was imposed on the virtual currency exchange to freeze the virtual assets. A confiscation order for the preserved amount was given upon conviction.

217. Case studies show Korea is capable of confiscating the proceeds of foreign predicate offending, both on its own initiative and in the context of an international co-operation request (see IO.2).

218. Korea also provided several case studies demonstrating its ability to recover proceeds moved overseas (see Box 3.10). Asset flight is a major risk area for Korea and, as a result, the authorities are very sensitive to the possibility of assets moving offshore, particularly in tax crime cases. Korea has taken steps to address this risk, including establishing a specific task force focused on recovering tax crime proceeds located offshore (see Box 3.13 below).

Box 3.10. Recovery of criminal proceeds located offshore

Recovery from Mongolia: Between 2005 and 2008, Person A obtained KRW 4.6 billion (EUR 3.5 million) from running a large-scale illegal game

room. These proceeds were deposited into Korean accounts and KRW 1.7 billion (EUR 1.3 million) was subsequently transferred to a group of currency exchangers based in Mongolia. The proceeds were then used to invest in a hotel development in Ulaanbaatar with Person A obtaining a 35% stake in the development. Person A was arrested in January 2009 and convicted in November 2010 at which point confiscation proceedings commenced. The SPO liaised with the Mongolian authorities who were able to identify Person A's ownership stakes in the hotel. The SPO then requested MLA to recover the value of the proceeds. In response, Mongolian authorities seized and auctioned off the hotel. A total of KRW 365 million (EUR 285 000) (the equivalent of Person A's 35% share of the hotel) was returned to Korea by Mongolia.

Recovery from the U.S.: In October 2015, Person B paid USD 3.45 million out of company funds in exchange for favours from a sales director at a US. based company in relation to a contract worth USD 35 million. The SPO traced the funds to the U.S., and in December 2017, USD 3.2 million was recovered from the U.S. and preserved for confiscation.

219. Korea uses tax procedures to confiscate the proceeds of tax crime, which is Korea's highest proceeds-generating offence. Upon completing an inquiry into tax crime, the NTS will recalculate the tax owed and collect this amount in addition to a monetary penalty of up to five times the unpaid amount. The NTS actively pursues outstanding taxes in addition to imposing fines for non-compliance. Korea's effectiveness in this area is clear, with large amounts collected (see Table 3.16 and Box 3.11).

Table 3.16. Proceeds of tax offences recovered through tax levies

	Amount of proceeds of tax crime recovered through tax levies		Amount of additional tax penalties imposed	
	KRW million	EUR million	KRW million	EUR million
2015	1 039 014	802.9	12 855	9.9
2016	1 554 247	1 201.1	14 587	11.3
2017	1 092 987	844.6	13 596	10.5

Box 3.11. Use of tax levies to recover laundered proceeds of tax crime

Person P inherited an overseas slush fund account created by his father from payments from foreign trade partners. Person P moved the account into his own name and withdrew all the funds from the account prior to his father's death without disclosing the amount to the NTS, thereby concealing the money in order to avoid the inheritance tax. The NTS conducted an investigation and calculated the outstanding tax amount as KRW 25 billion (EUR 18.9 million). This amount and a further KRW 3 billion (EUR 2.3 million) of tax penalties was collected from Person P.

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

220. Korea has measures in place to detect and prevent cross-border movements of currency and BNIs. Available powers to seize and confiscate falsely or undeclared funds are used relatively infrequently. Sanctions imposed are low, but appear to be somewhat dissuasive (at least for repeat offenders).

221. These conclusions are based on discussions with the KCS and the KCG, statistics provided by Korea, and available case studies.

222. Relevant authorities, particularly the KCS and the KCG, were aware of possible risk areas and typologies. However, illegal currency/BNI movements are not perceived as a high risk in Korea, despite relatively high amounts being moved (see Table 3.17). Authorities confirmed that breaches of cross-border requirements occur most often in person, rather than with movements in mail or freight.

223. Korea has a legal framework in place to prevent and detect cross-border movements of cash whether on person or in freight or through the mail (see R.32). The KCS continually monitors cash declarations to identify irregularities or inconsistencies, and conducts random sampling and searches to screen for cash. Where border officers have any suspicion of offending, they are able to question suspects including asking about the source of funds and seeking information to verify the reasons for the fund movement. If necessary, the authorities can arrest the suspect and seize the funds. This step is rarely taken, which the KCS explained is because most of the cases they see in practice result from ignorance of the law or a misunderstanding of declaration requirements rather than an intent to smuggle cash into or out of Korea. Border officers are more likely to impose administrative fines that are low in comparison to the amounts uncovered (see Table 3.17).

Table 3.17. Discovery of illegal currency/BNI movements

	2015		2016		2017		2018	
Number of occurrences	1 064		1 002		1 221		1 913	
	KRW 100 million	EUR million	KRW 100 million	EUR million	KRW 100 million	EUR million	KRW 100 million	EUR million
Amount moved	665	50.3	449	34	506	38.2	810	61.2
Total administrative fines	0*	0	3	0.2	8	0.6	12	0.9
Total amount seized at the border	665	50.3	363	27.5	302	22.8	514	39

* Administrative fines for breaches in declaration requirements came into force in 2016.

224. The KCS noted that cash/BNI movement in freight is relatively rare, but movements through the mail are more problematic. All parcels entering or leaving Korea are scanned for cash to detect such movements, and KCS has established a unit that looks specifically at cash/BNI movements by mail to combat this identified vulnerability.

225. Sanctions for undeclared cash movement are generally low. Cases involving discrepancies of less than USD 30 000 (EUR 26 400) between the amount declared and the amount being moved are considered to be minor and are punishable by an

administrative fine of up to KRW 50 million (EUR 38 200) or 5% of the amount.[32] More serious cases involving a discrepancy of more than USD 30 000 (EUR 26 400) are punishable by one year in prison or a fine amounting to the higher of KRW 100 million (EUR 78 400) or three times the amount. On paper, these sanctions appear too low to be effective, proportionate and dissuasive (see R.32) and in practice sanctions being applied are often low (see Table 3.17) which may be a result of most cases lacking a malicious intent. Korea was able to provide case studies showing higher penalties for knowing and repeat offenders (see Box 3.12). The Korean authorities consider the sanctions are adequate and note that they have proven dissuasive given the relatively low number of recidivist offenders (only 0.5% of offenders reoffended since 2014).[33] However, there remains a risk that the level of sanctions may not deter first-time offenders.

Box 3.12. Cross-border currency movement to purchase virtual assets

In 2018, as part of its ongoing monitoring, the KCS detected that Person L was regularly transporting KRW 70-100 million (EUR 53 687 to 76 697) in cash across the border while reporting it as travel expenses. However, records showed his overseas stays were limited to 1-2 days. The KCS requested financial transaction information from KoFIU which showed several transactions with virtual asset exchanges. The KCS completed an investigation which showed Person L had been making false reports and was moving currency out of Korea to purchase virtual assets. The case was referred for prosecution, and Person L was sentenced to 10 months' imprisonment.

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

226. Korea's confiscation results are largely in line with its ML/TF risks and national AML/CFT policies and priorities. Korea could improve the system by expanding the power to confiscate in fraud cases and increasing the total amounts recovered from those ordered for confiscation.

227. These conclusions are based on discussions with the SPO, the NPA, and the NTS; case studies; and statistics on confiscation, tax levies, and compensation provided by Korea.

228. The 2018 NRA identifies tax offending, illegal gambling, fraud, asset flight, cash-based ML and virtual assets as major ML risk areas. LEAs identified these areas as high priority for confiscation. The statistics and case studies show that the authorities pursue confiscation in a manner that is largely in line with Korea's risk profile (see Table 3.16 and Table 3.18, and Box 3.9, Box 3.10, and Box 3.11). Korea could improve its efforts by enhancing its recovery of all assets ordered for confiscation (see para.214).

32. If it is the second such offence within two years, the fine may be increased to 7% of the amount (Enforcement Decree of the FETA, arts.40(2).

33. Korea's overall recidivism rate (i.e. offenders who commit a criminal offence and go on to commit the same criminal offence again) is 13.4%.

Table 3.18. Amount ordered for criminal confiscation by offence

	2015		2016		2017	
	KRW million	EUR million	KRW million	EUR million	KRW million	EUR million
Standalone ML	16 093	12.4	1 051	0.8	4 440	3.4
Illegal gambling	48 308	37.2	92 892	71.5	219 135	168.7
Securities offences	79 314	61.1	59 796	46.0	72 512	55.8
Asset flight	42 846	33.0	147 868	113.9	56 917	43.8
Corruption	74 815	57.6	100 924	77.7	54 083	41.6
Embezzlement	108 192	83.3	72 348	55.7	50 578	38.9
Prostitution	25 485	19.6	21 028	16.2	17 595	13.5
Smuggling	16 613	12.8	13 652	10.5	15 877	12.2
Trademark theft	8 174	6.3	4 464	3.4	8 758	6.7
Drug offending	988	0.8	607	0.5	1 696	1.3
Financial fraud*	417	0.3	14 982	11.5	1 667	1.3
Tax crime**	1 330	1.0	859	0.7	0	0

* The proceeds of fraud are generally recovered through restitution rather than criminal confiscation. See para.229.
** The proceeds of tax crime are recovered through tax levies rather than criminal confiscation. See Table 3.16 and paras.219 and 229.

Box 3.13. Pursuit of asset recovery for asset flight related to tax crime

In June 2018, the government launched the Illicit Asset Recovery Task Force, a multi-agency task force that focuses on the confiscation of tax crime proceeds located abroad. The taskforce comprising 14 investigators from the NTS, KCS, FSS and other relevant agencies. The purpose of the taskforce is to investigate offshore tax crime using tax havens, asset flight, shell companies, false trade deals, etc.

The Task Force has made inquiries into a number of cases, with positive results:

- Six cases were recommended to the prosecution for indictment. One has progressed to indictment, while the other remain under investigation.
- Seven cases were passed to the NTS and the KCS for further investigation.
- Two preservation orders were sought to freeze proceeds of KRW 5.1 billion (EUR 3.9 million).

The Task Force has also been active in MLA, with investigators travelling to foreign countries to seek co-operation and share information with authorities. Destination countries include the U.S., Germany, the Netherlands, Cambodia and Thailand.

229. The proceeds of tax offending and fraud are recovered through other measures rather than criminal confiscation. The proceeds of tax offences (Korea's highest risk proceeds-generating offence) are recovered through tax levies by the NTS (see para. 219 above). Fraud proceeds are subject to compensation and restituted to victims, as opposed to recovering them through criminal confiscation proceedings. In any case, these methods ensure that criminals are deprived of their proceeds, which is

one of the characteristics of an effective system under IO.8. At the time of the on-site visit, Korea was considering legislative changes to allow the government to confiscate the proceeds of certain fraud cases before returning it to the victims.[34] This system could be strengthened further by ensuring that confiscation can be pursued where compensation is not available (e.g., where the victim cannot be identified or where the amount of proceeds exceeds the amount of harm caused and subject to compensation).

Overall conclusions on IO.8

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

34. In August 2019, the Act on Special Cases Concerning the Confiscation and Return of Property Acquired Through Corrupt Practices was amended to permit the government to confiscate the proceeds (or assets of equivalent value) of fraud cases involving criminal organisations, unauthorised fund-raising, pyramid schemes, telecommunications or other similar cases, and return the proceeds to the victims. As this measure was not in force at the time of the on-site visit, it was not taken into account for the purposes of this evaluation.

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

a) Korea has no prosecutions or convictions for TF, which is consistent with its risk profile. Korea has assessed its terrorism and TF risk as low, which is reasonable given its context. The specific TF vulnerabilities identified in Korea's 2018 NRA are largely reflected in the instances where suspicions of TF have arisen in Korea (although, upon enquiry, such suspicions have not been substantiated and only one formal TF investigation has been pursued).

b) Despite only having one formal TF investigation, Korea has demonstrated its ability to identify and investigate TF. Various intelligence sources are used to identify TF. LEAs have made inquiries into potential TF in a number of cases, including in respect of Korea's only terrorism-related prosecution. Korea's risk profile means there is a lack of experience within investigative and prosecutorial authorities, which Korea works to mitigate through training.

c) TF investigations are integrated with national strategies at the operational level due to strong inter agency collaboration and the existence of formal working groups. TF elements are also reflected in national counter-terrorism policies, despite the scarcity of cases.

d) Available penalties would allow Korea to impose effective, proportionate and dissuasive sanctions on natural persons and Korea uses alternative measures where suspicions of potential TF cannot be substantiated. Deportation is actively used and in such cases, Korea collaborates closely with the receiving state to share information and intelligence relating to any suspicion.

Immediate Outcome 10

a) While there are some technical gaps, TF-related TFS in Korea are implemented without delay. The legal framework restricts FIs and casinos (but not other DNFBPs) from financial transactions, and prohibits them from making funds and other assets available to designated persons and entities resulting in a freezing obligation. This framework largely implements TFS for FIs and casinos, although, due to the lack of TFS-specific guidance on the freezing requirement, there are

concerns that incoming wire transfers will be rejected rather than frozen, which impacts the effectiveness of the system.

b) DNFBPs (other than casinos) are not subject to the TFS-specific prohibition, but only subject to the general prohibition (i.e. the TF offence).

c) FIs and casinos are supervised for compliance with TF-related TFS, but other DNFBPs are not as they are not subject to AML/CFT obligations.

d) Korea has undertaken assessments to identify at-risk NPOs, concluding that 137 NPOs are at risk of TF abuse due to their overseas operations and another slightly larger group are at risk based on one shared characteristic. This assessment could benefit from the involvement of NPOs themselves, and from further nuance regarding the particular activities and vulnerabilities that create this risk. While Korea has assessed the TF risks posed by Korean NPOs, it does not have a firm grasp on the overall makeup of its NPO sector.

e) Strong reporting and supervision measures are in place for the 137 at-risk NPOs operating abroad. These NPOs also have access to ongoing outreach and support programmes, which were widely praised by NPOs. Other NPOs, including the other group of NPOs identified as at-risk due to one particular characteristic, are subject to registration and some reporting measures (depending on their size and funding levels). However, these NPOs would benefit from active engagement and targeted guidance. A specific committee facilitates domestic co-operation on NPO issues, although its membership does not include all relevant parties and it is not clear how it feeds into the National Counter-Terrorism Commission.

Immediate Outcome 11

a) Korea has a strong focus on PF issues related to DPRK and implements sanctions on transactions with DPRK that go beyond UNSCR 1718. It also implements its requirements under UNSCR 2231 on Iran. Korea has made 198 domestic designations complementary to UNSCR 1718, and co-sponsored 11 designations. Korea has not frozen any funds under these regimes. Korea has inter agency meetings when there is a UN decision on designations, but there is no formal standing co-ordinating body on PF-related matters.

b) While there are some technical gaps with the obligations, PF-related TFS in Korea are implemented without delay for FIs and casinos. The gaps relate to the lack of an obligation to freeze the funds, or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

c) DNFBPs (other than casinos) are not subject to the TFS specific prohibition, but only subject to the general prohibition of PF-related matters.

d) FIs and casinos showed a generally good understanding of their TFS requirements. FIs and casinos are required to prohibit transactions with designated entities and persons, resulting in a freezing obligation.

However, due to the lack of TFS-specific guidance on the freezing requirements, in some cases this leads to funds being rejected (rather than frozen).

e) Supervisors monitor FIs and casinos for compliance with proliferation-related TFS and provide regular AML/CFT outreach, including on TFS elements.

Recommended Actions

Immediate Outcome 9

Korea should:

a) Enhance available training and guidance on TF for prosecutors to ensure they have access to the skills and expertise necessary to pursue TF cases.
b) Ensure that where authorities have suspicions of potential TF, they continue to conduct a thorough inquiry to determine whether there is evidence to substantiate TF and justify an investigation.

Immediate Outcome 10

Korea should:

a) Enhance its risk assessment of the NPO sector by: clearly identifying all NPOs within the FATF definition; taking into account a broader range of risk factors to better identify the specific threats and vulnerabilities of particular NPO groups; and seeking broader input from NPOs and other relevant parties (e.g. KOICA).
b) Expand its outreach and engagement efforts in the NPO sector to include other at-risk NPOs, smaller NPOs and those operating domestically, for example, by leveraging the experience of or pursuing partnerships with agencies or entities (e.g. KCOC) already operating in these areas.
c) Ensure NPO registrars have access to relevant information and strategies on TF, for example, by including more registrars in the NPO CFT Agencies Committee or developing mechanisms to ensure the Committee's discussions and activities are shared with registrars.
d) Ensure decisions and discussions are shared between the NPOs CFT Agencies Committee under the AML/CFT Policy Co-ordination Committee and the National Counter-Terrorism Commission.

Immediate Outcomes 10 and 11 (targeted financial sanctions)

Korea should:

a) Address the TC deficiencies under R.6 and R.7, and make all DNFBPs subject to TFS obligations and monitoring for TFS compliance by a designated supervisor.
b) Extend the current notification mechanism to all DNFBPs.
c) Issue more targeted and sector-specific guidance and outreach on how to implement TFS (e.g. around the management of funds and licensing regimes), including guidance on the freezing obligation related to incoming transfers, to ensure that funds are frozen rather than rejected,

and, in case of rejection, pursue available sanctions where funds are not frozen.

d) Ensure that registries screen against sanctions lists at the company formation stage and ensure ongoing checks of existing companies, consistent with the prohibition from dealing with terrorism-related and proliferation-related assets that applies to all natural and legal persons.

e) Consider making the legislative supervisory obligation in place for FIs and casinos more explicit on TF and PF-related TFS.

Immediate Outcome 11

Korea should:

a) formalise the co-ordination structures around PF-related TFS to ensure that all relevant bodies have the opportunity to meet and discuss PF objectives and strategies, and keep them under review.

231. 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

232. While Korea has no prosecutions or convictions for TF, this is largely consistent with its risk profile.

233. This conclusion is based on the 2018 NRA and other risk assessments (e.g. on NPOs), case studies, and discussions with the Office for Government Policy Co-ordination, the MFA, the MOJ, the NIS, KoFIU, LEAs, and NPOs.

234. Korea assesses its terrorism and TF risk as low, which is reasonable. Korea is not an international financial centre and is largely safe from violent crime and terrorist attacks (see also Chapter 1, paras.42-43). The 2018 NRA notes that "No terrorist groups have been found to be active in South Korea, and individuals, organisations or NPOs suspected of having links to terrorist groups or involved in TF activities have also yet to be found".[35] Nonetheless, the 2018 NRA and discussions with relevant authorities identified various instances in which the Korean authorities have identified and taken action against individuals with possible links to terrorist organisations, including at least one TF investigation and one terrorism prosecution. Thus, Korea acknowledges that while its terrorism risk may be low, it is not immune to TF risks.

235. The 2018 NRA identifies and analyses five vulnerabilities that could result in TF activities in Korea. These are:

a) a growing population of non-Korean residents (including on Jeju Island);
b) an increasing number of refugee applications and illegal residents;
c) an increase in the value of remittances being sent to countries with possible terrorist links;

35. Republic of Korea National AML/CFT Risk Assessment (November 2018), pg.122.

d) charity work by Korean NPOs in countries with possible terrorist links; and
e) complacency stemming from Korea's current state as a terrorism-free country.

236. Authorities had a good understanding of Korea's TF risks, with KoFIU, the NIS, and the NPA demonstrating a deeper awareness of the particular threats and vulnerabilities. Authorities appreciated the risk of both domestic and foreign TF, and consistently understood the distinction between terrorism risk and TF risk.

237. Korea has had no TF prosecutions or convictions, which is in line with its TF risk assessment and risk profile. There has been one TF investigation, which did not result in sufficient evidence to pursue to indictment and instead resulted in deportation (see Box 4.2). Korea has also had one terrorism prosecution for inciting terrorist acts. The NPA and the SPO looked for potential TF in this case, but were not able to find any evidence of this behaviour (Box 4.1).

Box 4.1. Terrorism investigation with TF inquiry

Korea has had only one case of terrorism. A Syrian individual, Person S, was prosecuted and convicted of inciting terrorism. During the investigation into the incitement aspect of the case, the NPA and SPO used their asset tracing capabilities to review Person S's fund movements to determine if a charge of TF could be substantiated. Information was sought from KoFIU, but there was very little bank account information available as Person S dealt mostly in cash. There was nothing to indicate TF and, as a result, no grounds to justify a formal TF investigation or charge. Person S was designated pursuant to UNSCR 1373 (see Box 4.3).

238. Korea sees the threat from home-grown terrorism as low. In line with this assessment and the vulnerabilities identified in the 2018 NRA (specifically (a) and (b) in para.235 above), most cases in which Korea has identified potential, unconfirmed links with terrorist groups have involved foreign nationals. Only four instances have involved Korean nationals suspected of contacting international terrorist groups. Korea's one TF investigation involved a foreign national remitting KRW 2 million (EUR 1 500) to a known terrorist fundraiser (see Box 4.2). This is consistent with the 2018 NRA's identification of the risk posed by remittance ((c) in para.235 above). There are no detected instances of Korean NPOs being abused for TF purposes.

TF identification and investigation

239. Despite a low number of cases, Korea was able to demonstrate that it is able to identify TF cases and to investigate them should they arise.

240. This conclusion is based on the limited number of available case studies and discussions with the NIS, KoFIU, the SPO and the NPA.

241. Korea identifies TF cases through various intelligence sources. The NIS houses the Terrorism Information Integration Centre (TIIC) which collects and analyses terrorism and TF-related information and intelligence. The Centre has a variety of methods through which intelligence is collected in Korea. The NIS shared with the assessment team information on the methods used, and the assessment team was satisfied that the NIS is actively collecting intelligence to detect TF in Korea should it arise. In addition to this domestic intelligence, the TIIC also receives and shares

information with overseas partners. Where the intelligence indicates the need for an investigation, the Centre will transfer the case to the NPA. The TIIC also shares information and discusses TF matters with the NPA, the KCS, military intelligence, and other relevant bodies, including by hosting 3-4 operational meetings every year.

242. Both the NIS and the NPA recognise TF-related STRs as a potential source of intelligence and a method for detecting TF. KoFIU screens STRs to identify any related to TF (primarily through keyword searches). The number of TF STRs submitted to KoFIU varied dramatically between 2013 and 2018, from 2 in 2014 to 416 in 2018. The peak in 2018 resulted from outreach by the NIS and KoFIU to reporting entities to increase their awareness of TF risk which resulted in an increase in STRs. All TF-related STRs undergo basic analysis at KoFIU, regardless of other factors. Where basic analysis indicates the STRs may be useful, they are disseminated to LEAs, including the NIS, the NPA and the SPO.

243. KoFIU does not disseminate most TF STRs due to a lack of evidence of TF. KoFIU explained that many are made solely on the basis that the transaction involved a country with high terrorism risk, but upon analysis by KoFIU, there are no additional red flags or indicators of TF. This is consistent with the findings in IO.4 that defensive reporting of TF STRs remains an issue (see para.359 in Chapter 5). On average, KoFIU made five TF-related disseminations per year between 2013 and 2018. All were investigated by the NIS, the NPA and/or the SPO, but no evidence of TF was detected. The NIS and NPA also occasionally seek information from KoFIU to support their inquiries and investigations (on average, seven times per year).

244. If TF was identified, a counterintelligence team in the NPA's Foreign Affairs and Security Section would investigate under the supervision and direction of the SPO's National Security Division (which has a specialist TF prosecutor) or the relevant DPO's Public Security Department. These authorities showed a strong commitment to pursuing TF, noting that they pursue any terrorism-related offending (including TF) as a priority. As Korea has had only one TF investigation and no prosecutions, the investigative and prosecutorial authorities lack practical experience in this area. To mitigate this, NPA provides regular, ongoing TF training for its investigators and intelligence officials that draws on foreign case studies to elaborate the methods and risks of TF and covering fund-tracing techniques. For prosecutors, the SPO provides training to the DPOs and Branch Prosecutors' Offices.

245. The NIS, NPA and SPO actively investigated Korea's sole TF investigation, but this did not result in sufficient evidence for a TF indictment to be pursued (Box 4.2). While Korea has had no other formal TF investigations, there have been inquiries into potential TF in a variety of cases, including in respect of Korea's one terrorism prosecution. Statistics from the NIS on the number of requests made for KoFIU information relating to TF suggest that, on average, seven such inquiries were pursued annually between 2016 and 2018. This supports the assessors' findings that Korean authorities are alert to the potential for TF and are actively looking for possible cases.

Box 4.2. Case study of a TF investigation in Korea

Person L, an Indonesian national, came to Korea in October 2007 on an employment visa, stayed after the visa expired and was arrested in November 2015 for overstaying their visa. At the time, Person L was also carrying an unauthorised sword and an imitation gun. In the course of the investigation, Person L's fund flows were analysed and it was determined that between 2014 and 2015, Person L had remitted a total of KRW 2 million / EUR 1 500 over 11 occasions to an individual in Indonesia who (according to NIS intelligence) may have been an associate of a terrorist organisation. Further investigations were conducted, bank account information was obtained and forensic analysis of communications data was undertaken. However, there was insufficient evidence to establish that the recipient of the funds had actual links to a terrorist group. However, the investigations did uncover that Person L had changed their name since entering Korea and had used a forged identity card to seek work and open bank accounts. The case was further complicated because the individual was arrested and in custody, meaning authorities had a limited time (20 days) in which to decide whether to indict. In this context, more time-consuming investigative techniques (e.g. international co-operation) could not be fully utilised. As a result, SPO determined that Person L could not be indicted for TF, but could be charged with illegally overstaying in Korea, carrying an unauthorised sword and imitation gun, and using a bank account in someone else's name. Person L was sentenced to 8 months' suspended imprisonment. Upon conviction, Korea deported Person L to Indonesia in April 2016 and shared with Indonesia the information obtained in the course of the investigation. This enabled Indonesia to designate the individual pursuant to UNSCR 1373.

246. Korea has had other instances in which individuals appeared to support terrorist groups, raising suspicions of possible links with these groups. Between January 2010 and September 2018, 86 such individuals were deported (approximately ten per year). In each case, the relevant authorities conducted an inquiry, including collaborating informally with international partners to obtain information on the relevant individuals. These enquiries did not produce any evidence that the individuals had actual links to terrorist groups or had been involved in TF, so formal TF investigations were not opened. As a result, Korea instead resorted to deportation as an alternative measure (see the section below on alternative measures). Case studies and discussions with relevant authorities reassured the assessment team that these suspicions were thoroughly considered by Korean authorities, that evidence of TF was robustly pursued but was not found, and that deportation (with appropriate collaboration with the receiving state) was therefore a suitable alternative.

TF investigation integrated with and supportive of national strategies

247. Korea's TF investigations are integrated with national strategies at an operational level. TF elements are also reflected in national counter-terrorism policies, despite the scarcity of cases.

248. These conclusions are based on a review of Korea's counter-terrorism strategies and oversight bodies and discussions with the Office for Government Policy Coordination, the NIS, KoFIU and other LEAs.

249. Counter-terrorism policy and issues in Korea are overseen by the National Counter-Terrorism Commission and implemented by the National Counter-Terrorism Centre. The Commission is a regular Ministerial-level meeting led by the Prime Minister that brings together 21 relevant agencies, including from the NIS, KoFIU, the NPA, and several other bodies also represented in the AML/CFT Policy Co-ordination Committee. A working-level committee below the Commission meets every 1-2 months to discuss counter-terrorism policy and ongoing investigations, including TF investigations. These discussions feed into the Commission's counter-terrorism guidelines and policies, including its National Counter-Terrorism Plan which is reviewed and updated on an annual basis. The Plan identifies three areas for prioritisation in 2019: prevention measures, strengthening counter-terrorism capacity, and future development of Korea's counter-terrorism strategy. Combating TF is identified as a goal within the prevention area.

250. The National Counter-Terrorism Plan also recommends that where terrorism is investigated "there should always be a parallel financial investigation". Korea was able to demonstrate that inquiries into TF are well integrated into terrorism investigations at the operational level (see Box 4.1). This is aided by the role of the NIS' TIIC which collects intelligence at a general level, although its focus on financial flows could be strengthened. The regular operational meetings held by the TIIC and the working-level arm of the National Counter-Terrorism Commission also help ensure terrorism and TF information is shared between relevant agencies.

251. TF in Korea is punishable by up to ten years in prison or a fine of up to KRW 100 million (EUR 77 800) (see R.5). These penalties are relatively high in the context of Korea's legal system. By way of comparison, serious bodily harm and extortion are also punishable by ten years of imprisonment. The range of penalties for TF would allow Korea to apply effective, proportionate and dissuasive sanctions for natural persons. The sanctions are likely too low to be effective for legal persons, although the risk of legal persons (such as NPOs) being used for TF is low (see the section on IO.10).

252. As there have been no convictions for TF, no sanctions have been imposed in practice, which is not unreasonable given Korea's low risk for TF. In the absence of sanctions imposed in practice, the effectiveness of TF sanctions in Korea cannot yet be fully assessed.

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

253. Korea appropriately uses other measures to achieve the objective of IO.9 where it is not practicable to secure a TF conviction. Korea's use of alternative measures tends to occur where a suspicion of TF cannot be substantiated despite thorough enquiries.

254. These conclusions are based on discussions with the NIS, the NPA, the SPO and KoFIU; available case studies; and information in Korea's 2018 NRA.

255. In line with Korea's risk assessment, many of its suspected potential terrorism or TF cases involve foreign nationals (see para.235). In such cases, Korea actively uses

deportation where there is insufficient evidence to pursue terrorism or TF charges. The suspicion may arise based on intelligence from the NIS or the NPA. Agencies collaborate closely, as well as with the SPO, KoFIU and foreign counterparts, to determine if there is any evidence of information that could provide grounds for formally pursuing a TF investigation. Korea demonstrated that these enquiries were thorough and that all necessary measures were taken to determine whether sufficient evidence existed to open a TF investigation. Thus far, sufficient evidence has been found in only one case (leading to Korea's one TF investigation). This results in a lack of practical TF investigative and prosecutorial expertise, although Korea is making efforts to counteract this gap (see para.244 above). Where insufficient evidence exists to open a TF investigation, the LEAs will provide information to the Immigration Service within the MOJ to determine if there are grounds for deportation (e.g. for over-staying a visa).

256. Korea has deported 86 individuals between 2010 and 2018 in response to suspected possible links to terrorist groups. Discussions with LEAs confirmed that the authorities would make necessary inquiries in such cases to determine whether there was information to justify opening an investigation and would resort to deportation only where such information could not be found. When Korea decides to pursue deportation (as opposed to investigation and prosecution), the authorities inform the individual's home country (to which the individual is deported) of their suspicions in order for them to continue monitoring for potential terrorism-related offending. Korea shares information and intelligence to the extent possible, including through NIS' secure channels. NIS also has ongoing communication with the receiving country to provide further assistance and support to any investigations or monitoring.

257. In addition to deportation, Korea also makes use of other immigration measures to prevent and disrupt terrorism (such as blocking a citizen's passport, thereby preventing them from travelling). Immigration systems help identify high-risk individuals and allow Korea to prevent cross-border movements. This step is taken in respect of Korean individuals for whom deportation is not an option.

Overall conclusions on IO.9

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

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of TF-related targeted financial sanctions without delay

259. Korea has a basis for implementing terrorist-related TFS without delay, and has frozen funds. Korea uses the legal framework described in R.6 to implement TFS pursuant to UNSCRs 1267/1989, 1988 and its successor resolutions (collectively referred to as UNSCR 1267), and UNSCR 1373. Korea has co-sponsored designations at the UN and has made domestic designations, including giving effect to foreign requests for domestic designations. The technical shortcomings in the scope and depth of the TFS obligations undermine effectiveness to a large extent. Korea's implementation of TFS relies on a combination of TFS-specific and TF prohibitions, and ongoing account monitoring obligations that result in a freezing obligation. However, the lack of TFS-specific guidance raises serious concerns that incoming funds/assets will be rejected or turned away to avoid violating the financial transaction prohibitions, rather than freezing them as required by R.6. Additionally, DNFBPs, except for casinos, are only subject to general prohibitions on providing funds and other assets (i.e. the TF offence),

but not subject to TFS-specific prohibitions on funds and other assets of designated persons and entities.

260. These conclusions are based on: a review of Korea's legal framework; case examples provided by Korea; statistics on designations and actions taken to implement TFS; discussions with relevant competent authorities (the MFA, the Ministry of Finance and Economy, the MOJ, the NIS, the SPO, the NPA, the FSC and KoFIU); and discussions with FIs and DNFBPs.

Implementation of the Designation Obligation

261. The FSC is the authority responsible for identifying and proposing new targets for designation, and giving effect to foreign requests. In most cases, this authority is delegated to KoFIU. Prior to deciding on a potential designation, the FSC or KoFIU consults relevant ministries, including getting approval from the MFA, the Ministry of Finance and Economy and the MOJ. The consultation process generally takes no more than one week. If a designation is urgent and a matter of national security, the FSC can obtain post-designation approval (see R.6 for more details).

262. Korea has demonstrated the ability to make designations itself and give effect to foreign requests. Korea has co-sponsored 11 designations pursuant to UNSCR 1267. Korea made its first designation pursuant to UNSCR 1373 in January 2019 (see Box 4.3). Additionally, Korea has given effect to foreign requests made pursuant to UNSCR 1373 relating to 338 persons and 149 entities, equally subject to Korea's freezing mechanism.

263. Unlike other areas co-ordinated through the AML/CFT Co-ordination Committee or its working groups, it is not clear how Korea co-ordinates TFS at the national level on a regular basis. The system would benefit from either designating an existing committee or establishing a new mechanism to co-ordinate TFS measures and keep TFS policies up-to-date.

Box 4.3. Korea makes a designation pursuant to UNSCR 1373

A Syrian national, Person S, is a former employee of a car factory in Korea. He became sympathetic to ISIL groups and began inciting people around him and online to join ISIL. Upon receiving a report about Person S and his behaviour, the Incheon Metropolitan Police Agency investigated his acquaintances and others, and online posts published on his social media accounts and other places, and then sent the case for prosecution. On 6 December 2018, the Incheon District Court convicted Person S of incitement to joint terrorist groups pursuant to the *Anti-Terrorism Act* and sentenced him to three years of imprisonment. The investigative authorities also conducted a financial investigation into Person S, but concluded that he was not involved in any TF activities. However, the authorities remained concerned about his potential involvement in terrorist-related activities and, on that basis, Korea designated Person S domestically pursuant to UNSCR 1373 on 16 January 2019. On the same day, Person S' bank account (containing EUR 1 512) was also frozen. The timeline from identifying Person S as a potential target for designation to the designation itself was less than one month, consistent with the

requirement for the authorities to make prompt decisions on designations.[36]

Implementation of targeted financial sanctions

264. Implementation of TFS occurs without delay. The designation mechanism is automatic and requires no human interaction (see R.6 for further details). Korea implements TFS related to UNSCRs 1267, 1373 and successor resolutions through the PFOPIA, its Enforcement Decree and (since June 2019)[37] by updating its Designation Notice (which has immediate force and effect) with the relevant designations. Upon updating the Designation Notice, the Ministry of Government Legislation is also notified in order to reflect the amendments in the National Law Information Centre.

265. The FSC and KoFIU communicate new designations and de-listings to FIs and casinos by email to all sector associations and by posting the updated Designation Notice on their webpages. Usually this is done within one business day, but minor improvements are needed to address the occasions when a designation is made on a Friday, Saturday or public holiday, which leads to the notification being made within three calendar days.

266. Larger FIs and casinos have a good understanding of their TFS obligations and generally have good controls and preventive measures in place to detect designated persons and entities. Software providers are often used to screen customers. From the information provided, only smaller FIs (e.g. one-man currency exchangers) are not using watch-list services providers. However, these smaller institutions are required to keep books of all transactions and provide these to the KCS, which screens the records for matches with any listed person or entity. Supervisors and private sector representatives interviewed advised that no positive identity match had been identified during this post-monitoring process.

267. The AML/CFT framework does not cover DNFBPs (other than casinos). While DNFBPs are subject to the general prohibition on making funds and other assets available (i.e. the TF offence), this does not include the TFS-specific prohibitions on dealing with designated persons and entities. Nevertheless, some DNFBPs, primarily those which are part of an international group subject to AML/CFT obligations in other countries, demonstrated some knowledge about TFS and the prohibitions on making funds or other assets available to designated persons. However, there are no measures in place to monitor or sanction uncovered DNFBPs and, therefore, their level of implementation is difficult to assess. Based on the relative importance of the different non-covered DNFBP sectors (see para.78), this deficiency is considered major rather than fundamental for the purpose of assessing IO.10. This area needs major improvement.

268. All supervisors of FIs and mainland casino operators supervise these sectors for compliance with their TFS obligations. However, it is not clear whether the SGP casino supervisor is supervising for TFS compliance (see Chapter Chapter 6. on IO.3

36. The requirement of identifying a potential target for designation and designating the individual person/entity "promptly" differs from the requirement to implement TFS "without delay". In Korea, TFS are immediately and automatically implemented upon designation at both the UN and domestically meeting the requirement of "without delay", which is interpreted to be no more than 24 hours.

37. Prior to amending the regime, UNSCR 1373 designations were implemented within 4-10 days (including 3 days for publication in the Official Gazette) which is not without delay, as required.

for further details). No sanctions have been imposed to date for violation of the TFS obligation under the PFOPIA, its Enforcement Decree or the Designation Notice. Korea would benefit from designating an AML/CFT supervisor for the uncovered DNFBP sectors.

269. Sanctioned persons and entities are not prevented from setting up companies in Korea, as the company registry does not carry out checks against the sanctions lists (see Chapter 7 describing the company registries). Korea should add a requirement for registries to screen against sanctions lists at the company formation stage and ensure ongoing checks of existing companies. This would enhance implementation of the prohibitions from dealing with terrorist-related assets that apply to all natural and legal persons.

270. The legal framework to implement TFS in Korea consists of:

a) a general prohibition on providing or making funds and other assets available to designated persons or entities, which applies to all natural and legal persons;
b) specific prohibitions on carrying out transactions for or to designated persons or entities, which apply to all financial institutions and casinos; and
c) ongoing account monitoring obligations for FIs and casinos aimed at identifying whether they are holding funds/other assets related to designated persons/entities.

271. Together, these provisions create a freezing obligation for FIs and casinos when an existing customer becomes a designee because no further transactions are allowed (unless licensed under specific circumstances, as provided for under UNSCR 1452). This mechanism has been tested successfully in practice. FIs and casinos are required to report frozen funds and other assets to KoFIU.

272. Korea has frozen a total of KWR 272 million (EUR 206 666) under UNSCR 1373. Most recently in January 2019 Korea froze KRW 2 million (EUR 1 512) based on its first designation pursuant to UNSCR 1373. The majority of the assets frozen (KRW 270 million), relating to three legal persons and five bank accounts, have been frozen since 2008. In 2008, KoFIU allowed deductions from the accounts to pay for contracts entered into prior to the designation, in line with the exemptions provided for under UNSCR 1452. No deductions have been allowed since 2008.

273. Despite the existence of a freezing obligation, without TFS-specific guidance the assessment team has concerns about how FIs and casinos will exercise these provisions in respect of incoming transfers—whether by wire transfer or through some other means, such as a designated person or entity arriving at a branch to open an account. In such cases, the lack of guidance raises serious concerns that institutions faced with incoming funds or assets will reject or turn away the funds or business to avoid violating the financial transaction prohibitions, rather than go beyond the letter of the law and freeze them as required by R.6. This concern is especially relevant in Korea's context where the financial sector appears to be particularly risk averse and concerned with reputational risk. Rejecting incoming transfers would result in the funds or assets moving elsewhere, rather than being stopped as is envisaged by IO.10 (see Box 4.4 below).[38] This concern was confirmed by the FIs the assessment team met

38. The case study relates to U.S. sanctions, not UN sanctions, but the private sector representatives confirmed during the on-site, that they would reject incoming transfers from designated persons and entities similarly to the case study.

during the on-site, and supported by the low number of TFS-related STRs being filed (two in 2016 and four in 2018). In conclusion, this suggests that FIs and casinos may not be implementing their TFS obligations effectively.

Box 4.4. Transaction rejected by bank

Company A, a corporate banking customer, has maintained financial transactions with Bank X since 1995. Company A has performed transactions including foreign exchange (outward remittance), trade financing (payment guarantee, opening of letter of credit), management funds lending, KRW account, etc. In May 2018, Company A requested modifications in the conditions of a letter of credit for export of Company B. Company C, the beneficiary of the transaction, was identified as being a positive identity match with the U.S. sanctions list as contained on Korea's consolidated watch list which includes the names of designated persons and entities. The watch list contained information that Company C had links to group X (a terrorist organisation subject to U.S. sanctions). The transaction was subsequently rejected. No STR was filed with the Korean authorities.

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

274. Korea's overall risk of TF abuse through NPOs is low. Korea has undertaken assessments to identify at-risk NPOs, although these could benefit from further nuance regarding the particular activities and vulnerabilities that pose the highest threat. Strong mitigation measures and ongoing outreach and support programmes are in place for NPOs operating abroad which were identified as higher risk. More limited measures are in place for other NPOs, including other at-risk NPO groups.

275. These conclusions are based on: discussions with the MFA, NPOs, KCOC and KOICA; the 2016 and 2018 NRAs; and NPO guidance and outreach documents.

276. Korea's NPO sector comprises 14 033 NPOs. While Korea has assessed the TF risks posed by Korean NPOs, it does not have a firm grasp on the overall makeup of its NPO sector (see R.8). Korea categorises NPOs into those operating domestically, those operating abroad and those with religious affiliations. Based on intelligence from LEAs, Korea considered that domestic NPOs are low risk.

277. Korea undertook NPO-specific risk assessments alongside the 2016 and 2018 NRAs. Academics carried out the 2016 assessment using open source information and interviews with NPOs. The review was brief and lacked depth due to insufficient data. KoFIU undertook a more comprehensive review in 2018 to feed into the 2018 NRA. The 2018 review drew on a mix of qualitative and quantitative information including remittance and immigration statistics, meetings with government agencies, input from the KCOC (a forum of development aid NPOs) and an interview with an organisation representing Christian missionary groups. The NRA could have benefited from involving other NPOs (to ensure input from all categories of higher risk NPOs) and KOICA, which works closely with NPOs operating abroad.

278. Korea concluded that 137 NPOs are at risk of TF abuse due to their overseas operations. These NPOs dispense overseas development aid (ODA) and are members of the KCOC. Within this group, 22 NPOs were identified as being at particularly high risk due to their operations in high-risk countries. The risk assessment identified general vulnerabilities of these NPOs, with limited consideration of the specific threats and methodologies for potential TF abuse. Christian missionary groups were deemed low risk on the basis that their fund transfers were minimal, despite the fact that they have sometimes been a target of terrorist acts so could feasibly also be targeted as a funding source. Korea's focus on KCOC-member ODA organisations may risk overlooking other NPOs operating abroad but outside the ODA context or which are not KCOC members. This risk was noted by individuals working in Korea's NPO sector who considered the assessment was driven primarily by geographical considerations, and could benefit from further detail and nuance (e.g. on the types of projects or persons that may be at risk).

279. The 137 ODA agencies are subject to stringent supervision and monitoring, and receive ongoing outreach and education, including on TF issues. All are registered with the MFA and are members of the KCOC.[39] Most (87%) also receive funding from KOICA which means they are subject to comprehensive and rigorous reporting requirements (see R.8). NPOs confirmed that these requirements were strict, almost to the point of being overly burdensome. Nonetheless, they acknowledged their effectiveness in terms of maintaining transparency and accountability in the ODA NPO community. Korea expressly prohibits KOICA-funded NPOs from starting programmes in high-risk countries (as determined by the MFA). NPOs met during the on-site confirmed that they are conservative with operations in high-risk countries, and if a country were to become high-risk during a project, they would consider ways to withdraw safely. NPOs which are KCOC members are also subject to some due diligence upon joining the KCOC to ensure the NPO is of good standing.

280. The 22 particularly at-risk ODA NPOs have not been publicly identified or notified, so do not benefit from additional formal outreach or resources (such as specific guidance). However, they are subject to closer examination by the KCOC and KOICA. These NPOs are also subject to discussion by relevant government agencies that form Korea's NPOs CFT Agencies Committee (see para.286 below).

281. KOICA and the KCOC are active in their outreach to their member NPOs. The KCOC has an extensive education programme, including on issues relating to good governance and accountability. The programme was widely praised by NPOs. With the help of KoFIU, the KCOC has expanded the programme to cover TF issues. KOICA is also working to build TF understanding and awareness. Each year, KOICA holds an education session that is compulsory for all NPOs receiving or planning to seek funding from KOICA. In 2018, KOICA held this event jointly with the KCOC and covered TF issues, distributed a booklet on TF risk, and discussed guidance and best practices. Trainers drew on case studies to highlight particular risks (e.g. due diligence on local hires). These outreach efforts are very positive and could usefully be expanded to include other at-risk NPOs, smaller NPOs and those operating domestically.

282. In addition to the 137 ODA agencies, another slightly larger group of NPOs has also been identified as being at higher risk of TF abuse based on one shared characteristic. The risk analysis on these NPOs was blunt and based on the relevant

39. To qualify for membership in the KCOC, NPOs must have two years' experience in international development work, have a budget of at least KRW 100 million (EUR 76 795) and be headquartered in Korea.

NPOs having one particular attribute in common. It could have benefited from more depth to identify the specific types or characteristics of NPOs within this group that were particularly at risk. Like all NPOs, NPOs in this group must register with one of 22 central government agencies or one of 77 local governments depending on their location and activities. No single registrar has visibility over these at-risk NPOs. Registrars do not share information or consider they have a CFT role. Outreach and support has been very limited.

283. Most domestic NPOs are deemed lower risk based on intelligence from LEAs. This is a reasonable assessment in the current context, but Korea's focus on two very specific groups of NPOs may limit the identification of emerging threats or risks. Domestic NPOs are subject to registration requirements and 9 164 larger NPOs are supervised by NTS for tax purposes (see R.8). This group includes most ODA NPOs, but does not include other at-risk NPOs.

284. Outreach for domestic NPOs and the donor community is limited. In mid-2019, KoFIU produced a booklet on NPO TF abuse risks and guidelines developed by specialists with both academic and practical expertise in the NPO sector. The Guidelines include best practices for addressing TF risks and vulnerabilities drawing on (foreign) case studies and examples. The Guidelines are a very positive step, but have had little time to be circulated and socialised. Korea could benefit from including NPOs themselves in the development of future guidance, as well as from expanding its outreach programme. Participants in the on-site visit felt that outside the ODA sector, outreach and education was limited, and that smaller NPOs could benefit from further support.

285. Korea has sanctioned NPOs for failing to comply with disclosure requirements, but the authorities acknowledge that available sanctions for NPOs are not strong (see R.8).

286. Korea has a strong structure in place to co-ordinate on TF-related NPO issues. In 2018, Korea established a NPOs CFT Agencies Committee (the NPO Committee) as a sub-committee of the AML/CFT Policy Co-ordination Committee. The NPO Committee brings together some relevant government agencies (including KoFIU, KOICA, the NIS and the NTS), but does not include all NPO registrars meaning registrars do not receive updates on TF risk. KCOC is not represented on the Committee as it is not a government body. The Committee meets on an ad hoc basis as needed to discuss and co-ordinate on TF issues relating to NPOs. The Committee's meetings have included discussions on how to better-supervise NPOs' foreign currency remittances and the risks posed by certain NPO groups. The meeting discussions resulted in KoFIU issuing the NPO Guidelines described above. The authorities can also share information on at-risk NPOs through the TIIC (see para.241).

Deprivation of TF assets and instrumentalities

287. Korea has a legal framework in place to deprive individuals of TF assets and instrumentalities via its criminal process in the context of TF investigations and prosecutions, although this is subject to some shortcomings.

288. These conclusions are based on relevant statutory provisions and discussions with KoFIU, the SPO, and the MOJ (see also the sources listed under IO.8). However, the lack of TF and terrorism cases in Korea made it difficult to assess the effectiveness of Korea's framework in this area.

289. Korea can freeze and confiscate proceeds and instrumentalities related to terrorism and TF under its criminal law. The authorities can obtain a preservation order even prior to indictment to prevent offenders from moving or dissipating the assets. The confiscation proceedings then runs alongside the criminal proceedings, allowing the court to order confiscation immediately upon conviction (see Chapter 3 on IO.8). These powers can be executed on behalf of a requesting foreign state (see Chapter Chapter 8. on IO.2 and R.38). No TF or terrorism assets or instrumentalities have been preserved or confiscated under these provisions to date, which is reasonable given Korea's risk profile and the low number of TF and terrorism cases. Although Korea has not yet had the opportunity to test these legal authorities and powers in the TF context, it has successfully tested them in the ML context (see Chapter 3 on IO.8). Korea has also frozen funds in relation to UNSCR 1373 (see Chapter 4 and para.272).

Consistency of measures with overall TF risk profile

290. Korea's measures to prevent terrorist, terrorist organisations and terrorist financiers from raising, moving and using funds, and from abusing the NPO sector are consistent with Korea's overall TF risk profile in some (but not all) cases. Korea has a legal basis for implementing TFS and has frozen funds on this basis. However, the lack of TFS-specific guidance raises serious concerns, despite Korea's low risk TF profile. Korea's measures to mitigate the risks of NPOs being abused for terrorist purposes do not adequately cover all NPOs identified as being at higher risk. In the context of TF investigations and prosecutions, Korea has implemented adequate measures to take provisional measures and confiscate terrorist-related assets and instrumentalities.

291. These conclusions are based on a review of the legal framework and implementation of TFS (see R.6 and above), the sources listed above in the other parts of this chapter; and the sources listed under Chapter 2 on IO.1.

292. Korea is effectively making and giving effect to TFS designations in line with its risks. However, the lack of TFS-specific guidance raises serious concerns.

293. While Korea's approach to the NPO sector could benefit from further refinement, the steps it has taken are positive given the overall low risk in this sector. Korea has demonstrated that it is endeavouring to take a risk-based approach to its monitoring of and outreach to NPOs. Nonetheless, certain at-risk NPOs could benefit from further engagement and Korea should ensure it has visibility of the broader NPO sector to enable the detection of emerging and evolving risk areas.

294. Korea's powers to preserve and confiscate TF or terrorism-related assets or instrumentalities under its criminal regime have yet to be tested, but this is in line with Korea's low risk TF profile and have been used successfully in the ML context (see Chapter 3 on IO.8).

Overall conclusions on IO.10

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

Immediate Outcome 11 (PF financial sanctions)

296. Korea uses the same legal framework for implementing TFS related to the proliferation of WMDs, as it does for implementing TFS related to terrorism. Korea implements TFS without delay and has made numerous domestic designations complementary to UNSCR 1718. However, DNFBPs (other than casinos) are not subject

to the TFS-specific financial transaction prohibitions but only to the general prohibition (i.e. the TF offence) which covers PF-related matters, but does not in itself result in freezing action. Moreover, the lack of TFS-specific guidance raises serious concerns that FIs and casinos will reject or turn away incoming funds/assets to avoid violating the financial transaction prohibitions, rather than freezing them as required by R.7.

297. The conclusions under IO.11 are based on: a review of Korea's legal framework; case examples provided by Korea; statistics on designations; discussions with relevant competent authorities (the MFA, the Ministry of Finance and Economy, the Ministry of Trade Industry & Energy, the Ministry of Unification, the NIS, the FSS, the FSC and KoFIU); and discussions with FIs and DNFBPs.

Implementation of targeted financial sanctions related to proliferation financing without delay

298. Due to Korea's geographical proximity to DPRK, the Korean authorities have an increased focus on PF-related TFS regarding DPRK. Korean authorities are aware of PF-sanctions related to Iran, though there is a higher focus on DPRK. Korea and Iran have economic ties in the form of trade between the two countries and branches of Iranian banks in Korea, although these branches are shut down for business by the Korean authorities, which is being enforced by ongoing enhanced oversight. The assessment team identified no violations. The Korean government is very aware of its PF obligations and co-ordinates on PF matters. This co-ordination is achieved through ad-hoc inter agency working level meetings. Korea advised that the AML/CFT Policy Co-ordination Committee can also discuss PF-related matters, but this was not evidenced. Korea would benefit from a standing whole-of-government committee, meeting regularly, to discuss PF-related matters.

299. Korea's legal framework for implementing proliferation-related TFS pursuant to UNSCR 1718 (on DPRK) and UNSCR 2231 (on Iran) and their successor resolutions is the same as for implementing terrorism-related TFS. As for terrorism-related TFS under IO.10 (see earlier in this chapter), there are a number of TC gaps with the scope of the freezing obligations and DNFBPs (other than casinos) are not subject to the TFS-specific prohibition (only the general prohibition of making funds and other assets available).

300. The FSC is the responsible authority for identifying and proposing new targets for designation. Prior to deciding on a potential designation, the FSC will consult relevant ministries, as described in IO.10 (see the section above). Additionally, Korea has its own domestic mechanism in place for identifying and designating persons and entities complementary to UNSCRs 1718 and 2231, which goes beyond what the FATF and UN standards require. Between March 2016 and December 2017, Korea designated 108 persons and 90 entities domestically (all located in DPRK) complementary to UNSCR 1718, and published them on the Designation Notice as restricted persons (see R.7). The designations were made domestically and not at the UN level, but are subject to the same freezing requirement.

301. Through its legal framework, Korea implements a freezing obligation for FIs and casinos through a TFS-specific prohibition on transactions, and the general prohibition on making funds and other assets available (i.e. the TF offence) when an existing customer becomes a designee. However, as described above in IO.10, the lack of TFS-specific guidance to FIs and casinos on how to implement their TFS obligations,

including the freezing obligation, creates serious concerns that incoming funds or assets will go unfrozen (see the section above on IO.10 for a full description).

302. Designations pursuant to UNSCR 1718 and 2231 take immediate effect in Korea and are communicated to FIs and casinos (but not other DNFBPs) through the same mechanisms described in IO.10 (see the section above) and criterion 6.5d. Communication to FIs and casinos usually takes one day, but on rare occasions may take up to three days. De-listings and other changes to the lists are communicated to FIs and casinos the same way.

303. Other DNFBPs are subject to the general prohibition on providing or making funds and other assets available (i.e. the TF offence). However, they are not monitored for compliance with this obligation, are not made aware of designations or changes to the lists, and are not subject to the TFS-specific prohibitions on carrying out transactions for or to designated persons or entities.

304. Korea has not frozen funds or other assets related to UNSCR 1718 or 2231. Consequently, Korea's licensing regime for governing access to funds for basic and extraordinary expenses has not been tested in relation to proliferation-related TFS. However, the same licensing regime also applies to terrorism-related TFS and has been successfully tested once in that context (see the section on IO.10 above), albeit some time ago.

305. The lack of frozen funds or other assets related to UNSCR 1718 and 2231 does not seem to be wholly in line with Korea's immense international trade flows, geographical proximity to DPRK or the large number of proliferation-related designees that it has designated domestically (beyond the persons and entities designated at the UN level) (see para.37 and 55).

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

306. FIs and casinos, except for smaller one-man FIs, use commercial software for screening new and existing customers against the Iran and DPRK sanction lists. FIs and casinos are required to report to the FSC if they are holding funds of a designated person or entity. This includes potential sanctions breaches and frozen funds. However, other DNFBPs are not subject to these requirements.

307. Similar to the assessment under IO.10 (see the section above), the lack of TFS-specific guidance raises major concerns, particularly if a designee is not an existing customer. In such cases, FIs and casinos are more likely to reject the funds in line with the prohibitions (rather than freezing them), resulting in the funds going back into the global financial system (see Box 4.4).

308. Three cases of violating other types of sanctions to combat proliferation have been identified in Korea since 2016 (e.g. sanctions relating to goods exports to DPRK). Although these cases are not related to TFS, they demonstrate Korea's ability to identify proliferation-related breaches. One case was sent to the prosecutor's office in January 2019 (see Box 4.5). The other two cases resulted in guilty verdicts in the court of first instance and have been appealed by the defendants.

Box 4.5. Disruption of import in violation of DPRK prohibition

Korea's intelligence network was aware of a vessel carrying coal. After receiving information from a third country in October 2017 that coal from DPRK had arrived in Korea in violation of the UN Security Council sanctions, the Korean authorities held a series of meetings to deliberate on how to implement the related UN Security Council sanctions against DPRK. The KCS (which is responsible for export controls, including on PF matters) reviewed and examined the import history, including of importers previously identified as having smuggled coal from DPRK, and confirmed that DPRK coal and pig irons had illegally arrived in Korea. This triggered an investigation into imports of DPRK coal by the SPO that is currently ongoing.

309. The KCG, which has investigative powers in Korea, is monitoring vessels on an ongoing basis. In particular, the KGC has the ability to do real-time monitoring of vessels subject to prohibition, including any attempt to trade coal, USD or oil with DPRK. Since the above case arose, Korea has enhanced its focus on co-operation and monitoring of vessels potentially involved in crime, has enhanced its vessel inspections, and now undertakes immediate investigation when a suspicion arises.

FIs and DNFBPs' understanding of and compliance with obligations

310. Larger FIs and casinos have a good understanding of their PF-related TFS obligations and use commercial software to screen for matches on the DPRK and Iran sanctions lists as part of their CDD for new and existing customers. False positives do arise, particularly in relation to persons designated on the DPRK sanctions lists who have Korean names. However, the institutions interviewed indicated that Korea's national registration system, ID numbers, and real-name system make it relatively easy to distinguish between North Koreans designated on the watch lists, South Korean citizens or residents with the same or similar names, and clear false positives. None of the institutions interviewed reported ever having had an identity match with a designated person or entity, but advised that if a match were identified, they would not execute the transaction or make funds available to designated persons/entities. In the absence of TFS-specific guidance, this implies that incoming funds or assets might be turned away rather than frozen as is required by R.7.

311. The institutions interviewed and the case studies provided demonstrate that the private sector has a generally good awareness of proliferation and PF issues (particularly in relation to DPRK) and a focus on complying with TFS obligations. Although it does not involve a designated person/entity, the following case study (Box 4.6) is an example which demonstrates Korea's ability to detect a suspicious transaction and possible attempt to evade sanctions with Iran in the context of trade financing, apply EDD and classify the customer as high-risk. No information was provided on whether the bank followed up on the suspicion and/or filed an STR.

Box 4.6. Attempted transaction to Iran

On January 2019, Customer A, a limited company, requested Bank Branch B to wire USD 3 000 worth of remittance to Turkey-based Company C for the purpose of making an advance and submitted documents in support of the trading payment. However, Bank B detected a discrepancy between information submitted by Customer A in the supporting documents and information given to one of its employees during a consultation. Bank B subsequently requested further information about the trading transaction. After careful review of the additional documents provided, Bank B determined that Customer A was attempting to transfer the remittance through Turkey because it was impossible to trade U.S. dollars with Iran-based companies. Bank B subsequently rejected the request for remittance and recorded that Customer A had attempted to carry out roundabout transactions and should be more carefully handled in future when requesting further foreign exchange transactions. Bank B also registered Customer A on its filtering database system as a suspicious company for Iran roundabout transactions, and adopted measures to deny any requests to perform transactions with Company C (the Turkey-based company).

312. Smaller FIs, including one-man FIs (e.g. sole proprietor currency exchangers), have a reasonable understanding of their PF-related obligations. They are aware of the prohibition to make funds available or conduct transactions for or to designated persons and entities. However, their compliance is hindered by not using software to screen customers and transactions. Only some one-man FIs perform manual checks on the sanctions lists. Others do not. However, this gap is mitigated to some extent by the post-transaction screening performed by the currency exchangers' respective banking connection[40] and the KCS.

313. Other DNFBPs are not subject to the AML/CFT framework, but are subject to the general prohibition that no natural or legal person is allowed to make funds available to designated persons and entities. Despite not being subject to the AML/CFT framework, the DNFBPs met with by the assessment team showed a reasonable understanding of the PF-related prohibitions to DPRK and Iran, and some advised that they did perform screening of new and existing customers against the DPRK and Iran lists. However, none of these DNFBPs are subject to any STR reporting obligations and none do so in practice. Consequently, it is not known to what extent such DNFBPs may have detected funds or assets related to designated persons or entities.

314. KoFIU has provided proliferation training covering missile sanctions and missile components to obliged entities. Additionally, a three-day training program covering both CFT and counter-PF is provided by the KCS. Korea advised that they have an increased focus on providing guidance and training to the private sector. However, understanding of proliferation-related TFS obligations could be enhanced, particularly for smaller FIs and uncovered DNFBPs. Korea should increase training for FIs and DNFBPs in this area and provide more targeted guidance, e.g. in relation to the

40. Currency exchangers are not allowed to have more than one business relationship with one bank, providing currencies.

management of frozen funds and licensing regimes to support the understanding of TFS obligations.

Competent authorities ensuring and monitoring compliance

315. KoFIU and its entrusted agencies supervise FIs and casinos for compliance with proliferation-related TFS obligations, however, as with terrorism-related TFS (see the section above on IO.10), the legal supervisory obligation could benefit from being made more explicit. Supervision is undertaken as part of FIs' and casinos' obligation to undertake a self-assessment that feeds into KoFIU's IT-RBA system (prior to 2018, this system was not an IT system, see Chapter Chapter 6. , para.390-391 for further description). Supervision also takes place as part of the supervisors' on-site and off-site inspections. The private sector confirmed that they were supervised for compliance with TFS obligations, although it was not clear to the assessment team whether TFS compliance is an integrated part of all inspections.

316. There is no monitoring of DNFBPs (other than casinos) as they are not subject to the specific prohibitions on financial transactions as part of the framework. Korea needs to make a major improvement in its system by making all DNFBPs part of the legal framework for TFS implementation, and designating a supervisor for monitoring compliance.

317. Breaches of TFS obligations are identified through supervisors' on-site and off-site inspections of FIs and casinos. Additionally, the KCS receives all ledgers, including information on transfers in foreign currency, and screens them against relevant sanctions lists, including for DPRK and Iran. Based on the information provided, there have been no cases of breaches of PF-related TFS obligations involving FIs or casinos.

318. The sanctions available for non-compliance with PF-related TFS and prohibitions to make funds available are proportionate and dissuasive (see c.7.3). However, the effectiveness of the sanctions available for TFS-related breaches is untested because no violations of the TFS obligations have been detected.

Overall conclusions on IO.11

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

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

a) FIs and casinos are subject to a comprehensive legal framework covering most elements of AML/CFT preventive measures. The most important gaps are the lack of: coverage of all DNFBP sectors (except for casinos); guidance on implementing TFS, including incoming transfers; and requirements on domestic PEPs and PEPs of international organisations.
b) Larger FIs and most casinos have a sound understanding of national, sectorial and institutional ML/TF risks, and their AML/CFT obligations, due to vigorous efforts by Korean authorities (including outreach, training, supervisory activities and the RBA System). Smaller FIs and some casinos demonstrated a reasonable understanding of the ML/TF risks, but not all undertake institutional risk assessments. Uncovered DNFBP sectors demonstrated a basic understanding of ML/TF risks but are not subject to the AML/CFT framework.
c) The most important sectors (including banks, securities companies and insurance companies which dominate the financial sector) have a sound understanding and implementation of AML/CFT obligations, including CDD, BO, TFS, new technologies and PEPs (including domestic PEPs even though this is not a legal requirement in Korea). FIs have clear procedures for assessing ML/TF risks, both in relation to new technologies, and at an institutional level in general. It is not clear to what extent smaller FIs implement these requirements.
d) The prevailing use of borrowed name accounts presents challenges for FIs in undertaking on-going CDD and transaction monitoring. Though Korea has implemented mitigating measures through the *Real Name Act,* the use of borrowed names remains a concern.
e) Most FIs and casinos comply with their obligation to report STRs promptly. Korea has made efforts to improve the quality of reported STRs which have been successful, and resulted in a decrease in the amount of STRs. However, improvements could be made to reporting by smaller institutions (both in terms of number and quality), and by all obliged entities in relation to TF-related STRs.

Recommended Actions

a) Korea should expand the scope of AML/CFT obligations to cover all DNFBP sectors.
b) Korea should require FIs and DNFBPs to apply enhanced CDD for domestic PEPs and PEPs of international organisations, and ensure

accurate implementation of the TFS obligation, in particular for incoming transfers, by issuing guidance and provide outreach to obliged entities.

c) Korea should continue its efforts to enhance FIs' and casinos' understanding of ML/TF risk at an institutional level, and their knowledge of applying adequate risk mitigating measures.

d) Korea should continue to provide outreach, guidance and specific awareness-raising programs to the private sector, particularly for smaller FIs, casinos and uncovered DNFBP sectors to improve understanding of ML/TF risks and AML/CFT obligations, particularly in relation to STR reporting.

320. 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)

321. Based on their relative importance and Korea's risks, context and materiality, implementation issues have been weighted most heavily for the banking sector, heavily for important sectors (securities/investment, casino, and insurance), moderately heavy for dealers in precious metals and stones, and less heavily for less important sectors (currency exchange, remittance, accountants, lawyers, and real estate). See Chapter 1, para.78 for more detail about the weighting, and paras.74-77 for a description of each sector's types of activities.

322. Meetings with the private sector did not reveal any serious concerns about the implementation of preventive measures. Overall, the important sectors demonstrated good awareness and implementation of preventive measures. FIs and casinos are required to file STRs and CTRs. In addition, in 2018, after the Kimchi premium scandal (see Box 2.2 in Chapter 0), Korea required obliged entities to file transaction reports when dealing with virtual assets, whether suspicious or not. Despite DNFBPs (other than casinos) not being subject to AML/CFT preventive measures, these sectors demonstrated a reasonable awareness of ML/TF risks and the AML/CFT framework.

323. The conclusions under IO.4 are based on interviews with a range of private sector representatives, statistics and case examples of enforcement actions, and input from the supervisors (KoFIU, the FSC, the FSS and other entrusted agencies), including on their findings during supervisory activities.

Understanding of ML/TF risks and AML/CFT obligations

324. All covered sectors were involved in developing Korea's 2018 NRA, including to some extent those DNFBPs not covered by the AML/CFT framework (see also Chapter 2, para.99). After publishing the 2018 NRA, KoFIU communicated the findings to the private sector through a series of seminars. All private sector representatives, including some from the non-covered DNFBP sectors, demonstrated a good knowledge of the 2018 NRA and the risks and vulnerabilities it identified.

325. A particularly good feature in Korea is the IT-RBA System and KoFIU's sector-specific comprehensive assessments (see Chapter Chapter 6. , paras.384, 390-391), which provides a basis for continuously enhancing the obliged entities' risk understanding. When FIs and casinos provide information about their implementation

of AML/CFT requirements, they receive feedback including areas for improvement and increased focus. Private sector representatives find this feedback to be of great value in strengthening their systems.

326. Larger FIs, particularly banks, have a sound understanding of the ML/TF risks and AML/CFT obligations applicable to their respective sectors. At an institutional level, larger FIs undertake individual firm-specific risk assessments that consider different factors, including customer base, geographical factors, products, services and delivery mechanisms. Additionally, before introducing a new product, service or delivery mechanism into the market, the launching FI will do a risk assessment. FIs reported that if they identify higher risks and cannot find adequate mitigating measures, they close down the new product, service or delivery mechanism and do not introduce it into the market.

327. Some FIs incorporate AML/CFT compliance into their annual employee performance reviews. In such cases, if an employee has not performed well in terms of AML/CFT compliance, this has a negative impact on the employee's review and could potentially result in a pay cut.

328. Smaller FIs (e.g. sole proprietor currency exchangers) and some casinos have a reasonable understanding of the ML/TF risks and their AML/CFT obligations. They mainly follow the NRA results and the risk factors listed in the AML/CFT Regulation (including the higher risk categorisation of customer, countries, products and services) and have undertaken individual institutional risk assessments to a lesser extent.

329. Casinos in general have a good understanding of the national ML/TF risks. The understanding of sector-specific ML/TF risk is more varied; some casinos demonstrated a good understanding, while others need to increase their understanding. This varied level of understanding equally extends to casinos' understanding of AML/CFT obligations, including the application of EDD in higher risks cases, where improvements are needed by some casinos.

330. DNFBPs other than casinos are not covered by the AML/CFT framework and, therefore, do not undertake a risk assessment at the institutional level.

Application of risk mitigating measures

331. Korea's 2018 NRA identifies virtual assets as posing a high risk. On this basis, KoFIU issued Guidelines on Virtual Assets imposing requirements on all obliged entities when dealing with customers involved in virtual assets, including the requirement to apply EDD to any customer relationship involving virtual assets.

332. Obliged entities are required to assess the ML/TF risks of each customer based on their geography, customer characteristics, product and services, and to apply mitigating measures commensurate with the risks, including applying EDD for high-risk customers. Customer risk assessments are required to be updated on an ongoing basis, particularly when there is a change in the customer profile, provided services etc. The AML/CFT Regulation provides a list of non-exhaustive factors posing higher risk. The factors for customer-specific risks include foreign PEPs, non-resident customers and cash intensive customers. The private sector representatives interviewed demonstrated a clear understanding of their responsibilities in applying risk mitigation measures commensurate with the ML/TF risk of individual customers.

333. Concerning new technology, obliged entities apply clear procedures to identify, assess and mitigate risks. During the process of developing new products, the

respective AML compliance unit participates in the process with input on risk assessment and provides their opinion for approval. For online banking and electronic payment service providers, the private sector representatives demonstrated good knowledge of risk mitigating measures taken, commensurate with the risks.

334. The NRA identifies cash transactions as a high-risk area. To mitigate this risk, Korea requires all obliged entities to make CTRs to KoFIU if they take part in a cash transaction over KRW 10 million (EUR 7 637), or file an STR with KoFIU if they observe split transactions aimed at avoiding the CTR obligation.

335. Larger FIs have a strong focus on applying mitigating measures. For example, the FSS highlighted that one bank, where breaches had been identified, had gone beyond the requirements of the action plan to ensure a higher level of protection against ML/TF abuse.

336. Smaller FIs (e.g. sole proprietor currency exchanger) mainly follow the results of the 2018 NRA and are not in all cases completing an institutional-specific assessment of the risks. For some smaller FI sectors, their main exposure is captured by the NRA findings. However, the NRA does not cover all factors (e.g. geographical higher-risk customer types). Korea should review the need to provide training and further guidance to these sectors.

337. Overall, there is an increase in obliged entities' level of compliance, as demonstrated by the results of an annual sector-specific comprehensive assessment undertaken by KoFIU (see Chapter 6, para.384 and Table 6.7). However, major improvements are needed in some areas.

Application of CDD and record-keeping requirements

338. FIs demonstrated an overall sound understanding and implementation of CDD and record keeping requirements, including on-going monitoring. The number of monetary sanctions applied for breaches of the CDD requirements has decreased, which is consistent with the private sector's increased understanding and application of CDD. Nevertheless, supervisors are still identifying breaches of the CDD requirements. On this basis, adequate implementation of CDD requirements remain a focus area for KoFIU and the entrusted agencies.

339. While many casinos have a good understanding and implementation of CDD and record-keeping requirements, including on-going monitoring, others have only a basic understanding of the AML/CFT obligations, which should be increased.

340. For record keeping, no major issues emerged during interviews with the authorities and private sector representatives. All obliged entities met with indicated that they scan and digitally preserve all material obtained through the CDD process, transaction records or investigations of suspicious behaviour. KOFIU and LEAs also indicated that no major issues have been identified with regard to the quality of the material and information preserved by obliged entities.

341. FIs and casinos are required to apply CDD on all customers, whether natural or legal persons or legal arrangements. All identity information must be verified using an independent and reliable source. A strong feature in Korea's system for verifying the identity of natural persons is the national registration system. All residents in Korea receive a resident registration number which is issued by the government at

birth.[41] Foreign nationals residing in Korea for over 30 days are also required to register with the relevant district office within 14 days after the determination of their domicile. When any resident turns 17 years old, they are required to obtain a resident registration card and carry it at all times.

342. Up until June 2019, FIs and casinos were only required to terminate a financial transaction if CDD could not be completed (and were not required to terminate the business relationship). However, in practice, the private sector representatives interviewed indicated that if they cannot complete CDD, they terminate the business relationship and refuse financial transactions, as demonstrated by the case below in Box 5.1. This appears consistent with the financial sector's relatively risk-averse nature and high sensitivity to reputational risks (see also Chapter 1, para.54).

Box 5.1. Termination of business relationship

Stock Company X is a game software development company established in 2012. It opened an account at Bank Branch A on 9 May 2018, explaining that the purpose of opening the account was to receive proceeds from exporting game software abroad. Branch A was unaware of any high-risk conditions, performed CDD assuming the company was an ordinary entity and opened the account. The next day, the AML/CFT Division of Bank A discovered that the company was a VASP and requested the relevant branch to confirm additional information. Branch A reviewed the details of the company's business and performed enhanced CDD, which included confirming the fact that the company had recently established a virtual asset service. The customer responded by saying that it would manage the company's working capital and would not manage any virtual assets through the bank, but refused to provide additional information or co-operate with Branch A's AML/CFT risk control policies. Complying with Korea's *Guidelines on Virtual Assets*, Branch A limited transactions on the customer's account, continuously reported the current status of monitoring to the AML/CFT Business Council and the Financial Crime Risk Committee, and ultimately closed the customer's account and terminated the business relation on 24 August 2018.

343. The use of borrowed names is a common typology for ML and tax crime in Korea (see Chapter 1, para.39). In an effort to mitigate the ML/TF risks of using borrowed names, Korea adopted the Real Name Act, under which FIs and casinos should only provide services (including account opening) in the actual customer's name. However, concerns remain in terms of ongoing CDD where the actual customer opens an account and later "sells" it or gives it away. LEAs confirmed this concern, indicating that borrowed name accounts are opened in real names, but are abused by third parties for illegal purposes. Additionally, supervisory agencies confirmed that a black market on borrowed names exists. Korea should increase its efforts to combat this issue (see Chapter 3, para.188 and Box 3.6).

344. DNFBPs (other than casinos) are not covered by the AML/CFT framework and therefore are not required to perform CDD or keep records. Nevertheless, real estate agents do the basic customer identification and verification required to file all real

41. Based on the 1962 Resident Registration Act.

estate sales contracts with the relevant authority, and are prohibited from registering real estate rights in the name of another person. Real estate agents must keep these records for five years. However, the obligations on real estate agents are not sufficiently detailed to meet the FATF requirements. Overall, it is crucial for Korea to regulate all DNFBP sectors, in particular the DPMS sector where an underground black market exists.

Application of EDD measures

Politically exposed persons

345. The 2018 NRA identifies corruption as one of Korea's main risks. Private sector representatives (particularly larger FIs and most casinos) demonstrated a strong understanding of the risks posed by PEPs. There has been an increased focus on PEPs, including domestic PEPs since the corruption scandals of two former Korean Presidents (see also Chapter 1, para.54).

346. FIs and casinos are not required to undertake EDD when dealing with domestic PEPs or PEPs of international organisations (see R.12). Nevertheless, the private sector representatives all demonstrated that they do not differentiate between foreign, domestic or international organisation PEPs, and apply enhanced CDD on all PEPs. During the CDD process, FIs and casinos use commercial software providers to screen new and existing customers and beneficial owners during on-going monitoring to check for PEP status. If PEP status (foreign, domestic or international organisation) is confirmed, EDD is applied, and the customer is given a high-risk rating. There have been cases where on-going EDD has revealed increased risks, and the FI has consequently terminated the business relationship

Box 5.2. Termination of customer relationship related to PEPs

On 23 March 2012, Foundation X opened two accounts and established a business relationship with Bank A. At the time of the account opening, Foundation X categorised the customer as a PEP-related entity after confirming through the CDD process that family members and close friends of a former President had substantial authority to operate the foundation. Consequently, EDD was applied. The amount of funds operated through the accounts amounted to approximately KRW 2 billion (EUR 1.5 million). In 2016, negative news reports emerged with suspicions of how Foundation X was using its proceeds for asset management, instead of for providing scholarships. On this basis, additional monitoring was undertaken by Bank A. At the beginning of 2018, further news reports emerged about serious criminal acts by Foundation X, including how it was involved in major proceeds-generating crimes such as bribery, embezzlement, breach of trust and tax crime, and that the authorities had issued an arrest warrant. In March 2018, Bank A's Financial Crime Risk Committee discussed Foundation X and decided to end the business relationship on the basis that the risks arising from maintaining such a relationship were not an acceptable risk level for the bank.

Correspondent banking

347. The legal AML/CFT framework applicable to cross-border correspondent banking relationships is fully compliant with the FATF Standards. The FIs interviewed have clear procedures on managing the ML/TF risks posed by correspondent banking relationships. This includes assessing new and existing correspondent relationships and taking appropriate action, as needed (e.g. closing a correspondent relationship). When making such an assessment, the following factors are considered: the respective countries of the correspondent bank; the FATF Public Statement and Compliance Document (generally referred to as the "black" and "grey" lists); and other open-source information (see Box 5.3). As part of its supervision, the FSS uncovered a few breaches in 2014 where new correspondent banking relationships had been approved by heads of departments, who are not part of senior management. However, in general the FSS finds FIs to be in compliance with the obligations related to correspondent banking relationships.

Box 5.3. Review of correspondent banking relationship

Bank X conducted a complete inspection of 5 035 correspondent banking relationships established by its head office and 20 overseas branches from June to July 2018. The aim of the inspection was to assess the adequacy of CDD procedures performed on these relationships. The inspection results showed that all of its branches with correspondent banking arrangements had completed the CDD procedures. Bank X also completed EDD on 364 respondent institutions (more specifically, 343 institutions with depositary arrangements and 21 higher-risk institutions) through September 2018. In August 2018, Bank X began to terminate over 27 of its correspondent banking relationships. None of the terminated relationships were based on violations of the U.N. sanctions, but based on the U.S. OFAC list.

348. Small value remitters and Korea Post (including its post offices) do cross-border remittance through banks, and do not establish direct cross-border relationships.

349. In addition to the AML/CFT regime, Korea's currency control regime (managed by the KCS) facilitates monitoring of correspondent banking activities. The KCS regularly checks data on all cross-border and foreign currency transactions.

New technologies

350. Obliged entities have a good understanding and management of risks associated with new technologies, particularly virtual assets. For new technologies in general, interviewed FIs and the majority of casinos have clear procedures in place to identify, assess and mitigate the risks. When developing new products, FIs and casinos consider AML/CFT compliance and take into account input from their relevant AML/CFT department.

351. Having assessed virtual assets as high risk in the 2018 NRA, Korea requires all obliged entities to apply EDD when dealing with them. Additionally, KoFIU published Guidelines on Virtual Assets in January 2018 to guide FIs in effectively implementing their AML/CFT requirements when dealing with virtual assets. During the on-site visit,

private sector representatives confirmed their increased focus when dealing with customers involved in virtual assets (see Box 5.1 above and Box 5.4 below).

Box 5.4. Suspension of accounts related to VASPs

On 13 September 2018, the internal control manager of a bank branch detected a suspicious transaction related to moving funds in the current account of Company Y, a VASP. The account was opened on 24 August 2018 and received around 5 200 transfers of funds worth KRW 10.8 billion (EUR 82 million) from multiple unspecified individuals during the period from 7 to 13 September 2018. The bank asked Company Y to provide documents necessary for CDD and for verifying the source of the funds for EDD. The representative director of Company Y refused to provide the requested documents. On this basis, the bank immediately gave Company Y notice of account suspension and suspended transfers of funds into the account on 17 September 2018, effectively blocking the account. The bank further blocked Company Y from opening new accounts or transferring funds to an overseas account. The bank also suspended the additional accounts held by nine other VASPs who failed to provide requested information and were suspected of tunnelling funds using virtual assets. Between 1 January and 31 December 2018, the bank suspended these accounts and filed an STR on each of them.

Wire transfer rules

352. All private sector representatives met during the on-site had a sound understanding of the wire transfer rules covering all situations, whether a FI is the originator, intermediary or beneficiary institution. The obliged entities demonstrated a strong knowledge of their obligations in cases where a wire transfer is missing some of the required information, and are legally required to have procedures in place for when to reject, execute or suspend a transaction. However, FIs are not legally required to have procedures in place for follow-up actions, and it was not clear whether such procedures are developed at the FI-level.

353. Although the AML/CFT framework is largely in place in Korea, there is a technical deficiency, as no requirements are in place for wire transfers below KRW 1 million (EUR 760), which impacts the effectiveness of the system.

Targeted financial sanctions relating to TF

354. The private sector representatives met during the on-site demonstrated a clear understanding of their obligation to implement TFS. The majority of the obliged entities (except for small FIs, such as sole proprietor currency exchangers) use commercial software to screen new and existing customers against the sanctions lists.

355. All FIs and casinos (including smaller FIs not using commercial screening software) are required to keep books of all transactions and provide these to the KCS. The KCS screens the records for matches with any designated person or entity. The assessment team was informed that no positive identity match has ever been identified during this post-monitoring process. However, the system's effectiveness is hindered

by the lack of TFS-specific guidance. FIs and casinos are prohibited from performing financial transactions for or to designated persons and entities, which results in a freezing obligation. However, in some cases (e.g. where the person is not an existing customer or in the case of occasional wire transfers), the FIs and casinos are prohibited from "taking" the funds, resulting in a rejection of the customer or transfer (see Chapter 4, Box 4.4). As funds in practice are not being frozen in such cases, this is a major concern.

Higher-risk countries

356. The FIs and casinos met during the on-site have clear knowledge and awareness of higher-risk countries that they are legally required to consider when risk rating their customers. They referenced both the FATF and European Union (EU) lists, and highlighted that a regular check of the lists was common practice. Additionally, FIs have a conservative approach towards customers from listed countries, generally refusing to establish such customer relationships.

DNFBPs other than casinos

357. As they are not covered by the AML/CFT framework, there are no requirements for DNFBPs other than casinos to undertake enhanced measures in higher risk situations, as described above in this section.

Reporting obligations and tipping off

358. The FIs and casinos met during the on-site demonstrated a strong commitment to filing STRs promptly, including on attempted transactions. The larger FIs and the majority of casinos have a sound understanding and implementation of their reporting obligations, whereas smaller FIs seemed to put in less effort in obtaining information to substantiate STRs. KoFIU confirmed that for smaller FIs there was a need to deepen the understanding of the practical aspects of the reporting obligation.

359. Despite larger FIs having a generally sound understanding of their reporting obligations, improvements are needed for smaller entities. KoFIU has a focus on improving this area. In 2013, Korea removed the STR reporting threshold, which naturally resulted in an increase in STRs reported. KoFIU provides feedback to obliged entities, including feedback on specific STRs reported, feedback through its comprehensive assessment and feedback in an annual report on the overall level of STRs reported. Additionally, in November 2016, KoFIU undertook a successful outreach program/training focused on improving the quality of STRs. Based on this training, the number of reported STRs dropped significantly in 2017 (Table 5.1) and KoFIU confirmed that it had received better quality STRs after the training. However, the assessment team noted potential over-reporting for all obliged entities regarding TF-related STRs, as these are filed solely on the basis that a transaction involved a country with high terrorism risk (see Chapter 4, para.243).

Table 5.1. STRs filed by sector

Sector	2014	2015	2016	2017	2018
Banks	433 695	522 036	458 244	333 798	484 160
Securities	8 727	9 169	8 735	7 397	8 955
Insurance	3 892	5 870	7 152	7 790	7682
Savings banks	1 361	2 974	11 727	15 852	16 845
Community credit co-op.	25 642	29 643	98 718	36 958	29 728
Credit co-op.	1 022	4 507	12 426	9 643	6 408
Agriculture co-op.	12 693	31 045	84 065	89 357	105 943
Fisheries co-op.	503	367	531	675	802
Forestry co-op. Association	49	69	34	45	31
Credit card companies	1 610	4 796	7 150	8 393	9 323
Post offices	11 221	11447	13 259	8 543	7 015
Casinos	440	802	471	675	1 118
Instalment loan companies	547	399	570	543	676
Merchant banks	-	-	-	-	-
Leasing companies	3	44	124	132	150
Real estate trust companies	-	-	-	1	-
New technologies	-	-	2	3	4
Korea security deposit	-	-	-	5	8
Small value remitters	-	-	-	2	73
Currency exchangers	19	2	2	1	-
Future companies etc.	1	6	146	95	54
Total	501 425	624 076	703 356	591 908	678 975

360. In addition to filing STRs, Korea requires obliged entities to file CTRs and virtual asset transaction reports, whether suspicious or not. This is consistent with the government's increased focus on virtual assets, including the published guidance and the "Kimchi Premium" (see Chapter 0, Box 2.2).

361. Overall, Korea has increased its efforts to ensure better quality STRs from obliged entities. However, more outreach is needed both for the larger FIs and casinos and, in particular, for the smaller FIs. This outreach should cover the obligation to report STRs related to TFS in cases where a customer or transaction relates to a designated person or entity (see Box 4.4where a transaction was rejected by a bank based on TFS compliance, but no TFS-related STR was filed subsequently).

362. The Korean legal framework includes stringent confidentiality requirements and protects reporting entities, including their employees. Both supervisory authorities and interviewed institutions reported that they had not seen a case of tipping-off about the fact that an STR had been considered or filed. However, FIs and

casinos have a lesser focus on preventing tipping-off during the investigation of a suspicious customer or transaction. Based on several case studies provided, there is a risk that FIs and casinos continue with the CDD process, even where this process might tip-off the customer, without considering whether to stop the CDD process and file a STR instead. This is because, prior to June 2019, the legal framework did not provide a basis for discontinuing CDD if there was a risk of tipping-off, which is consistent with the case studies provided. Korea should provide adequate outreach and guidance, to ensure accurate implementation of the new requirement.

Internal controls and legal/regulatory requirements impending implementation

363. The make-up of the Korean financial banking sector (with its very large branch network) makes internal controls particularly important. Korea has 19 licensed banks with a total of 6 971 domestic branches across the country, and to a lesser extent, foreign branches and subsidiaries abroad (see Chapter 1, Table 1.1. FIs conducting the financial activities covered by the FATF Recommendations

364. Korea only recently (in June 2019) established a legal requirement to implement group-wide measures, which sets out a general requirement for FIs and casinos, but does not include all of the elements specifically required by FATF Recommendation 18 (see c.18.2). Despite this, the private sector representatives met during the on-site demonstrated strong internal controls, including at a group-wide level and in relation to domestic branches. The material provided in relation to supervisory activities confirmed that the supervisors check internal controls during inspections, including for domestic branches. This focus might be impacted by the significant fine imposed on a Korean bank's foreign branch by a foreign regulator in December 2017.

365. There are no regulatory requirements impeding the sharing of information within financial groups. However, the private sector representatives indicated that they do not share information within their group, including on STRs. In this context, it was highlighted that all FIs and casinos are required to undertake their own CDD and, on that basis, would detect all suspicious customers and transactions.

Overall conclusions on IO.4

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

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

a) The FSC generally applies robust licensing, registration and screening measures to prevent criminals and their associates from abusing FIs and casinos. However, there is no explicit requirement to assess beneficial owners who otherwise exercise control.

b) The FSS and other entrusted agencies maintain an overall good understanding of the ML/TF risk profiles of their respective sectors and at the individual institution level.

c) KoFIU, the FSS and other entrusted agencies have a good supervisory framework to monitor AML/CFT compliance. The quality and quantity of monitoring is largely in accordance with the RBA. However, given the very large branch network (noted under IO.4), KoFIU and the FSS would benefit from additional human resources for supervision.

d) The SGP, responsible for supervising casinos in Jeju since March 2019, demonstrated only a basic understanding of ML/TF risks in the casino sector and at the individual institution level, and does not apply a RBA to supervision.

e) Supervisors take effective remedial action. The FSS and other entrusted agencies may impose administrative sanctions on supervised entities or on a specific employee, while KoFIU is responsible for imposing monetary sanctions for most violations, except for violating the wire transfer requirements. These sanctions appear to be effective and dissuasive, but not proportionate in all cases which might be due to the recent increase in the maximum amount for monetary sanctions and the lack of direct applicability of sanctions to violations of wire transfer requirements.

f) KoFIU provides guidance and conducts a range of outreach activities, including joint trainings and seminars with other competent authorities, to raise supervised sectors' awareness of ML/TF risks and mitigation measures.

g) DNFBPs other than casinos are not subject to the AML/CFT framework or monitored for compliance.

Recommended Actions

a) Korea should subject all DNFBPs to AML/CFT requirements and supervision.
b) The SGP casino supervisor should enhance its understanding of ML/TF risks (both at the sector and institutional levels) and implement a RBA to supervision.
c) KoFIU should review its current sanctioning regime to consider whether the monetary sanctions are being used adequately, and extend the ability to apply monetary sanctions for violations of wire transfer requirements (which are currently not directly subject to monetary sanctions).
d) Korea should revise the licensing requirement for obtaining a casino license to include a fit and proper test for beneficial owners.
e) KoFIU and the FSS should receive additional human resources for AML/CFT supervision.
f) KoFIU should continue to refine its IT-RBA system, including the accuracy of the information held, and update the system if needed.

367. 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)

368. Positive and negative aspects of supervision were weighted most heavily for the banking sector, heavily for important sectors (securities/investment, casino and insurance), moderately heavy for DPMS, and less heavily for less important sectors (currency exchange, remittance, accountants, lawyers and real estate). This weighting is based on the relative importance of each sector and Korea's risks, context and materiality. See Chapter 1, para.78 for more detail about the weighting, paras.74-77 for a description of each sector's types of activities and volume of business in Korea's context, and paras.83-86 for a description of Korea's supervision arrangements.

369. KoFIU is the designated authority for supervising FIs. KoFIU has delegated its supervisory powers to 11 entrusted agencies,[42] including the FSS, which is the main supervisor for the financial area, covering the banking, securities and insurance sectors among others.[43] Currency exchangers are supervised by the KCS. Two supervisors are responsible for supervising the casino sector: KoFIU and the SGP.[44] DNFBPs (other than casinos) are not subject to the AML/CFT framework and have no designated AML/CFT supervisor.

42. The FSS, National Agricultural Co-operatives Federation, National Federation of Fisheries Co-operatives, National Forestry Co-operation Federation, Central Credit Co-operatives Association, Credit Community Co-operative Federation, Ministry of Science and ICT, Ministry of Interior and Safety, Ministry of Small and Medium Sized Enterprises and Start-ups, the KCS and the Jeju SGP (see

Table 1.5. Agencies assigned AML/CFT inspection responsibilities by KoFIU

43. The FSS also supervises some of the financial supervisors, including: National Agricultural Co-operatives Federation, National Federation of Fisheries Co-operatives, National Forestry Co-operation Federation, Central Credit Co-operatives Association, Credit Community Co-operative Federation.
44. The supervisory authority for casinos on Jeju was recently transferred from KoFIU to the SGP in March 2019.

370. The conclusions in IO.3 are based on: statistics and examples of supervisory actions provided by Korea; guidance issued by the competent authorities; a demonstration of Korea's RBA System; and discussions with KoFIU, the FSC, the SGP supervisor, the FSS, the KCS, a range of entrusted agencies, and FI and DNFBP sector representatives.

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

Financial institutions

371. Korea has imposed government restrictions on access to the financial market (see Chapter 1, para.73). For example, to obtain a banking licence, the applying entity's business plan has to distinguish itself from existing banks. In this context, Korea has only issued two new banking licence since 1992[45]—to internet banks which (unlike other Korean banks) only operate online.

372. Korea has a sound licensing regime for the banking, securities/investment and insurance sectors. This regime includes fit and proper checks of directors, auditors, executive directors and operating officers prior to their appointment. In this process, an assessment is also made of shareholders holding more than 5% of the shares. The fit and proper regime includes criminal record checks, vetting with domestic LEAs and checks against commercial databases. However, there is no explicit requirement to assess beneficial owners who otherwise exercise control or criminal associates.

373. The FSC has the authority to license or register most FIs including in the banking, credit co-operative, securities/investment, insurance and remittance sectors (but not currency exchangers). The remittance sector comprises electronic financial services providers and small value remitters. There is no requirement to obtain FSC approval when establishing a new domestic branch under an existing licence. The FSC has delegated to the FSS the authority to check FI's compliance with the licencing requirements on an ongoing basis, including fit and proper check of senior management and major shareholders every six months. Credit co-operatives are subject to the same licensing regime as banks. Their applications are assessed by their respective federation (which is also the direct supervisor) and approved by the Minister of Interior.

374. The licensing regime is generally a two-step approach covering the preliminary process and the final authorisation. The preliminary process is voluntary and assesses whether the applicant complies with most of the requirements (although at this initial early stage in the process, the institution does not yet have to have an operational IT system or hired staff in place). If the committee within the FSC approves the preliminary application, it will move to the final approval stage. Before final approval, the institution's IT system has to be operational, employees hired and adequate offices in place.

375. In the past five years, the FSC has not rejected any applications for FI licences after the preliminary licensing stage. The FSC explained that this is because only viable applications have been put forward during that time. As an example, in May 2019, the FSC rejected three applications during the preliminary licensing stage based on a lack of innovation or security aspects. In the context of the government restrictions on new FIs, companies undertake prior consultation with the FSC before starting the two-step

45. This does not include branches of foreign banks in Korea.

licensing process to understand whether they have a basis for obtaining a licence or not. If the consultation reveals no basis for obtaining a licence, the company does not formally apply.

376. To be viable, an applying FI must have the following requirements in place to obtain a licence: a corporate structure; viable business plan; capital requirements; IT systems; experienced employees; and a fit and proper assessment of the management, shareholders etc. This applies to both applying non-FIs and established FIs applying for a licence to provide new or other financial services (e.g. an insurance company seeking a banking licence).

377. Remittance providers are required to register with the FSC. The registration requirements are less extensive than the licencing requirements. Nevertheless, the FSS does a simplified proper test (including a criminal record check) prior to registration on all applicants, directors and shareholders.

378. From 2016, currency exchangers have been required to register with the KCS. The KCS undertakes simplified proper checks before registering currency exchangers (similar to those the FSS does for remittance providers). From 2017 to June 2019, the KCS received 949 applications for registration as currency exchangers, of which 69 were rejected based on not meeting the requirements for obtaining a registration. Rejected applicants are inspected by the KCS to identify if any operations are being conducted in violation of the rejection. Additionally, a database of rejected applicants is kept with the KCS.

379. Credit specialised companies (credit cards, hire-purchase companies, leasing and new technology venture capital companies) are required to register with the FSC. Korea Post is a part of the Ministry of Science and ICT and thereby not required to register, but is still subject to AML/CFT requirements.

380. Several mechanisms are in place to identify entities operating without a licence or registration. This includes intelligence from several agencies, including LEAs, supervisors etc., and a hotline for the public to provide such information. Additionally, through Korea's currency control system, the KSC has access to all transactions and can identify if an entity is operating without a licence or registration, and take appropriate action. The KCS detected two cases of unregistered currency exchangers (one in 2017 and one in 2018). These cases were transferred to the prosecution service for breach of the registration requirement.

DNFBPs

381. The licensing regime for casinos is largely in place, but only the person applying for a casino licence is subject to a fit and proper test. This requirement does not extend to beneficial owners or shareholders, which raises major concerns considering the relative importance of the casino sector.

382. Lawyers, accountants, notaries and real estate agents have professional and continuing ethical and professional accreditation requirements (see c.28.4), but are not subject to any specific fit and proper criteria. There are no requirements in place for DPMS.

Supervisors' understanding and identification of ML/TF risks

383. As one of the key authorities responsible for developing the 2018 NRA, KoFIU has a sound understanding of the ML/TF risks across all of the financial and casino

sectors, and co-operates closely with the entrusted agencies to help ensure a consistent understanding of risk. The FSS (which was also deeply involved in the 2018 NRA) and the other entrusted agencies (which participated) all use the NRA's results to inform their understanding of risk, and almost all demonstrated a good knowledge of the ML/TF risks facing Korea and the sectors they supervise.[46] The exception was the SGP, which was not involved in the NRA and demonstrated only a basic understanding of the ML/TF risks.

384. KoFIU relies on regular outreach (including various training and seminars to the financial sector) and its RBA System to strengthen its understanding of potential ML/TF risks continuously. Through its RBA System, KoFIU analyses self-assessment information from FIs and casinos against objective information to result in a risk rating for each individual institution. All FIs (other than currency exchangers) and casinos are legally required to provide self-assessment information against 175 indicators to KoFIU on a quarterly basis. Of these indicators, 96 are operational risk indicators applicable to all sectors and covering STR and CTR reporting, CDD, internal controls, group control policies and risk management. The remaining 79 indicators are inherent risk indicators, not all of which apply to all sectors. The inherent indicators cover the characteristics of customers, cross-border activity, products and services, delivery channels and entities. In general, each FI is subject to approximately 145 indicators. The IT-RBA system is a very strong feature in the Korean system. Based on the information received, KoFIU ranks the relative risks of each institution, assigning each a risk rating. Additionally, KoFIU undertakes an annual sector-specific comprehensive assessment that analyses the self-assessment information against objective information (e.g. supervisory results, STR reporting data, etc.) to deepen understanding of the sectoral and individual institution risks.

385. KoFIU provides the annual sector-specific comprehensive assessment to all of its entrusted agencies. The results are also communicated to the individual FIs and casinos with feedback on what areas need improving or strengthening.

386. The FSS uses the self-assessments, the comprehensive assessment, the NRA and the results of its own supervisory activities to inform its application of the RBA approach to supervision. This gives the FSS a strong understanding of the individual FIs' risk of abuse for ML/TF and the relative risks of the different sectors it supervises.

387. Other entrusted agencies of small sectors base their risk understanding on the same sources and have a good understanding of the ML/TF risks in the smaller financial sectors they supervise. The entrusted agencies all have a good understanding of their different sectors and co-operate closely on AML/CFT matters, both at the sectoral and individual levels. This understanding is particularly clear where the entrusted agencies are also the sector-specific federation(s). All entrusted agencies are required to share the results of their AML/CFT inspections with KoFIU and on this basis have regular exchanges.

388. Almost all supervisors have a good understanding of the relevant risks. The exception is the SGP supervisor, which applies a rules-based approach to supervision. Though the overall TF risk for Korea is low, the NRA noted that Jeju Island may be more

46. National Agricultural Co-operatives Federation, National Federation of Fisheries Co-operatives, National Forestry Co-operation Federation, Central Credit Co-operatives Association, Credit Community Co-operative Federation, Ministry of Science and ICT, Ministry of Interior and Safety, Ministry of Small and Medium Sized Enterprises and Start-ups, and the KCS.

vulnerable to TF activities.[47] No information was provided to suggest that the SGP supervisor has undertaken a specific risk assessment of its casino sector or has an understanding of the ML/TF risks posed by individual casinos on Jeju Island which comprise 16.9% of the casino sector in Korea. This might be explained by the fact that the SGP supervisor only assumed the supervisory responsibility for casinos on Jeju in March 2019.

389. DNFBPs (other than casinos) are not covered by AML/CFT obligations and therefore do not have a designated supervisor. KoFIU has some understanding of the ML/TF risks in these sectors, which it included in the NRA to some extent. However, KoFIU is not equipped with a risk understanding at the individual firm level. As these sectors are not subject to AML/CFT obligations, these sectors are also not subject to the requirements to provide annual input to KoFIU's comprehensive assessment. This hinders the authorities from deepening their understanding of the ML/TF risks in these sectors.

Evolution of Korea's RBA System into an IT-based RBA System

390. In 2014, KoFIU began developing an IT system to support the RBA System. The banking sector was the first sector covered by the IT-RBA System. KoFIU added more sectors each year and, since 2016, all of the important sectors have been included. Only currency exchangers remain outside the scope of the IT-RBA System, which has been fully operational since the end of 2018. Through the IT-RBA System, FIs and casinos provide self-assessment information on their respective indicators directly into the IT system that then automatically generates the inherent risk for each institution.

391. The IT-RBA System is a very positive feature, but the accuracy of its risk ratings relies on institutions entering their self-assessment data accurately. This raises concerns about the veracity of the self-assessment information. As self-assessment information is the basis upon which individual institutions are risk-rated, there should be incentives for them to provide accurate information, even if that may lead to a higher risk rating and consequent higher likelihood of being subject to on-site inspection. Both the authorities and all private sector entities interviewed were consistent in answering that they could get sanctioned for providing incorrect information, and their incentives were to improve the system if it was needed in certain areas. Some private sector representatives indicated that if they entered information inaccurately into the IT-RBA System, their internal audit systems will detect the inaccuracy and take action, and the FSS will sanction any inaccuracies it finds. However, it is not clear whether the internal audit systems of all FIs and casinos focus on detecting potential inaccuracies in IT-RBA System reporting or how regularly the FSS supervises and sanctions for breaches of this requirement. Despite this being an important issue because inaccurate information will skew the results and lead to an incorrect risk understanding, this is mitigated to some extent by the cross-checking of information held in the system with information obtained through inspections and open-sources. Nevertheless, Korea needs to review these issues to ensure that all obliged entities consistently provide accurate information through the self-assessment scheme.

47. Jeju Island, which is also a special visa zone, is more vulnerable to TF risks arising from an increasing number of illegal immigrants from jurisdictions at risk of TF, than other parts of Korea. Officials estimated in 2015 that the number of travellers whose whereabouts were unknown after their entry into Jeju Island was 4 353 (see p.126 of the 2018 NRA).

Risk-based supervision of compliance with AML/CFT requirements

392. All supervisors (with the exception of the SGP supervisor) apply a RBA to supervision. The entrusted agencies (including the SGP supervisor), in co-ordination with KoFIU, annually make their inspection plans for supervisory activities the following year. If emerging risks or major concerns arise, KoFIU has the ability to undertake ad hoc or thematic inspections (e.g. on CDD, STR reporting, etc.).

393. All supervisors (except for the KCS and the SGP supervisors) use KoFIU's comprehensive assessment as one of the components of the RBA to identify the annual priority areas for inspection. The other components are the results of the NRA and weight of the financial industry (i.e. the materiality of each sector). Each sector's risk rating is calculated by taking the NRA results (given 70% weight) and the comprehensive assessment results (given 30% weight), multiplied by the financial industry weight.

394. When the level of sector-specific risks has been identified, the FSS and other entrusted agencies, in co-ordination with KoFIU, choose the individual FIs in each sector that should be subject to on-site inspection. Table 6.2. FSS on-site inspections

Table 6.1. RBA, annual inspection plan 2019.

Sector	NRA Result (A)	FIU Comprehensive Assessment Result (B)	Weighted Risk Level (A*0.7+B*0.3=C)	Financial Industry Weight (D)	Final Risk Level (C*D)	Risk Rating	# of Institutions subject to Inspection	Inspection Resources (No. of days × examiners × institutions)
Banking	5	1	3.8	54.5%	2.07	**High**	6	216
Insurance	3	3	3.0	20.7%	0.62	**Moderate**	4	128
Savings banking	2	4	2.6	12.7%	0.33	**Moderate**	2	56
Financial Investment	4	2	3.4	7.5%	0.26	**Moderate**	2	56
Specialized Credit Finance*	1	5	2.2	4.6%	0.10	**Low**	2	56

395. The individual FIs and mainland casinos are chosen based on their individual results in the comprehensive analysis, previous inspection information and open-source information. A high amount of regulatory effort is allocated to supervising institutions with higher risk exposure and greater vulnerability to ML/TF risks (see Table 6.2. FSS on-site inspections

Table 6.2. FSS on-site inspections

	2014	2015	2016	2017	2018
Examination Records (total)	30	34	30	41	33
Specialised Examination	14	22	23	26	20
Banks	6	4	7	7	12
Financial Investment Companies	-	6	4	5	2
Insurance Companies	4	4	4	5	4
Specialised Credit Companies	2	2	2	2	-
Savings banks	2	3	6	7	2
Federation of Co-operative banks	-	3	-	-	-

	2014	2015	2016	2017	2018
Concurrent Examinations[48]	16	12	7	15	13
Banks	6	5	5	7	6
Financial Investment Companies	3	1	1	2	4
Insurance Companies	4	5	1	6	3
Specialised Credit Companies	1	1	-	-	-
Savings Companies	2	-	-	-	-

396. In addition to the planned on-site inspections, the FSS and other entrusted agencies carry out follow-up inspections, off-site inspections and ad hoc inspections as needed (e.g. if concerns about a specific institution or one of its branches arise). The AML/CFT supervisors generally advise FIs of planned inspections one week in advance, but also sometimes do inspections without prior notice. For the FSS, an on-site inspection takes on average two weeks for high risk FIs. This includes a prior documents check, the on-site inspection itself, and meetings with the executive managers and compliance officers.

397. If the prudential supervisors identify any potential AML/CFT breaches during a prudential inspection, they refer these to the specialised AML/CFT unit within the FSS. There is a focus on training prudential supervisors in AML/CFT matters, so they are better equipped to identify AML/CFT breaches.

398. Currency exchangers are the only FI sector not covered by KoFIU's RBA system. The KCS is responsible for registering and supervising currency exchangers and has its own Currency Exchange Management System (RBA system), where all transactions are received and considered based on a number of risk factors.[49] The KCS performs concurrent examinations of currency exchangers covering both prudential and AML/CFT compliance. In addition, through Korea's currency control system, the KCS conducts ongoing off-site monitoring of their CDD compliance (identification and verification) by reviewing all ledgers of currency exchangers (including customers and transactions).

48. Both prudential and AML/CFT system is inspected during a "concurrent examination".

49. Such risk factors are: a) transactions with persons on watch lists, b) inconsistency between the time of exchange and the time of departure/arrival, c) frequent large-volume exchanges with the same customers, d) high-value exchanges without filing CTRs, e) frequent transactions with FATF non-co-operative countries, etc.

Table 6.3. Other Entrusted Agencies' on-site inspections for 2018

	Agricultural Co-op.	Fishery Co-op.	Forestry Co-op.	Credit Union	Community Co-op.	Post office	KCS	Total
Institutions subject to examination	1 122	90	137	888	1 307	1 (2 586 agencies)	1 677	7 807
Executed examination	553	36	83	386	349	3 634	115	5 156
Specialized examination	-	1	12	15	13	-	-	41
Concurrent examination	553	35	71	371	336	3 634	115	5 115
Examination execution rate	49.3	40	60.6	43.5	26.7	100	6.9	66.1

399. The SGP supervisor applies a rules-based (not risk-based) approach to supervision. It advised that all casinos on Jeju are subject to weekly on-site visits. However, this was not confirmed by the private sector, which advised that annual on-site inspections were carried out. In any event, the SGP supervisor did not demonstrate an understanding or application of RBA supervision. Korea explained that the basis for the applied approach to supervision by the SGP supervisor was the recent transfer of the supervisory responsibility, and thereby the need for the SGP supervisor to understand the business of the casinos they supervise, which was supported by the annual inspection plan for 2019.

400. DNFBPs other than casinos are not covered by the AML/CFT framework nor monitored for AML/CFT matters.

Remedial actions and effective, proportionate, and dissuasive sanctions

401. All supervisors have a range of remedial measures they can impose on FIs and casinos for non-compliance. DNFBPs other than casinos are not subject to the AML/CFT framework and therefore are not monitored or subject to sanctions.

402. KoFIU's delegation of its supervisory authority to the FSS and other entrusted agencies (including the SGP supervisor) includes delegation of administrative sanctioning powers. The entrusted agencies have the powers to issue corrective orders, give warnings or cautions to a FI or casino, and partially or fully suspend a licence. Additionally, the entrusted agencies can apply administrative sanctions to senior management (reprimand warning, cautionary warning and caution) and employees (removal, suspension, salary reduction, reprimand and caution).

Table 6.4. Sanctions imposed by FSS[50]

	2014	2015	2016	2017	2018
On-site Correction Measures	23	64	33	32	29
Call for Management Attention	2	1	1	1	4
Improvement Order	29	58	40	47	56
Requirement of Voluntary Measures	4	4	-	1	8
Caution	-	1	-	3	14

50. Monetary sanctions are imposed by the KoFIU, see Table 6.6.

	2014	2015	2016	2017	2018
Reprimand	3	-	-	-	-
Notification on Violation of Retirees	-	-	-	-	2
Total no. of sanctions	61	128	74	84	113

Table 6.5. Sanctions imposed by other Entrusted Agencies 2017

	Agricultural Co-op.	Fishery Co-op.	Forestry Co-op.	Credit Union	Community Co-op.	Post office	KCS	SGP [51]	Total
On-site Correction Measures	-	36	174	297	55	676	5	31	1 274
Administrative fines[52]	N/A	N/A	N/A	N/A	N/A	N/A	19	N/A	19
Improvement, Correction, Caution	146	24	12	47	332	353	11	-	922
Reprimand, etc.-	-	-	-	1	-	-	-		

403. Entrusted agencies do not have the ability to impose monetary sanctions, but KoFIU can impose them upon request by the entrusted agencies. Monetary sanctions can be (and are) applied concurrently for each identified violation. With the recent increase in the level of monetary sanctions, each violation can be penalised by KRW 100 million (EUR 77 044). This means if 100 counts are identified for breaching CDD requirements the maximum monetary fine can be KRW 100 million multiplied by 100 counts, i.e. KRW 10 billion (EUR 7.7 million). The assessment team found no evidence of serious AML/CFT deficiencies in Korea's financial sector or mainland casinos. However, the supervisors do not apply monetary sanctions frequently, only using them in cases of severe or repeated violations, which is of concern. Additionally, monetary sanctions cannot be directly applied for violation of the record keeping or wire transfer requirements.

Table 6.6. Monetary sanctions applied by KoFIU 2014-2018

Entity	Date	KRW 1 million (EUR 763)	No. of breaches	Violation
Bank	22 May 2014	24	1	Failure to make STR
Bank	10 April 2015	1 994	299	Failure to perform CDD Failure to make STR
Bank	10 April 2015	3	1	Failure to perform CDD
Savings bank	14 June 2016	509	139	Failure to make STR
Community Credit Co-operative	19 April 2017	5	1	Failure to make STR
Savings bank	Prior notification	4.8	3	Failure to perform CDD
Savings bank	Prior notification	21.6	9	Failure to perform CDD
Bank	Prior notification	9.6	9	Failure to perform CDD
Bank	Prior notification	3.2	1	Failure to perform CDD

51. The SGP was only entrusted with the responsibility of supervising casinos on Jeju as of March 2019. On this basis, the numbers in this column of the table are from March until 18 July 2019.

52. Monetary sanctions imposed on FIs, except for currency exchangers, is shown in table 6.5XX, as these are imposed by the KoFIU.

404. The entrusted agencies (including the FSS) communicate their inspection results to the institutions' management and relevant staff at exit meetings, and apply administrative sanctions and take remedial actions where they have identified shortcomings and regulatory breaches. If the deficiencies relate to AML/CFT controls, the entrusted agencies continue to monitor the correcting actions by the institution, which is obliged to submit an action plan for addressing the deficiencies and report on measures taken. The reporting time depends on the severity of the identified violation(s), but may be required on a monthly basis. The entrusted agencies arrange high-level meetings with the institution's management if the institution does not complete remedial actions in a timely manner.

405. Co-ordination between KoFIU and the entrusted agencies on supervisory activities has proven effective. The entrusted agencies report to the Commissioner of KoFIU about breaches and other findings identified during inspections, and request KoFIU to apply monetary sanctions in serious cases.

406. In most cases where sanctions are applied, the sanction and the violating entity's name are made public. This is a strong deterrent in the Korean context, where the primary concern of obliged entities (especially larger FIs) is the reputational damage following publication of the applied sanctions. Concerns about reputational damage may be particularly acute in the Korean context where recent high-level corruption cases have generated a certain amount of public sensitivity to behaviour suggestive of corruption (see Chapter 1, para.54). In this context, the remedial actions applied to larger FIs are usually effective and dissuasive. However, there remain concerns about whether sanctions have been proportionate in all cases, including the application and size of monetary sanctions when compared to specific sector size, especially in the banking sector. Korea recently (in January 2019) increased the applicable monetary sanction tenfold from KRW 10 million (EUR 7 714) to KRW 100 million (EUR 77 145). All banks and other large FIs interviewed indicated that although monetary sanctions applied to date may seem low compared to other countries and are not applied in all cases, the overall sanctioning regime where monetary sanctions are all publicised can cause significant reputational damage to an institution. This appears to be the main concern both at the sectoral and individual institutional level.

407. On the other hand, smaller FIs interviewed stressed that the level of monetary sanctions were sufficiently high from their perspective, to the extent that applying a monetary sanction at the higher end of the available range could cause their businesses to close. As many of these entities have very small business volumes and much more limited profit margins, even low-level monetary sanctions may be dissuasive. In this context, remedial actions are effective, proportionate and dissuasive.

Impact of supervisory actions on compliance

408. Supervisory actions undertaken by KoFIU and its entrusted agencies have had a positive effect on compliance. Feedback from all FIs and casinos interviewed evidenced that, based on the supervisory actions, there has been increased AML/CFT awareness and resources applied across all sectors. Additionally, the supervisory actions on AML/CFT compliance have resulted in an increased focus by the management of FIs and mainland casinos, which is a very positive result.

409. The average sector score in KoFIU's annual comprehensive assessment also evidences the improvements made across all financial sectors (see Table 6.7). The data in the table is based on each institution's self-assessment and supervisory findings,

both on-site and off-site inspections. The percentages in the table demonstrate a gradual increase in the level of compliance by each sector (i.e. a higher percentage means a higher level of compliance). No sector has reached 100% compliance (which is not to be expected), but all sectors have demonstrated improvements over the years.

Table 6.7. Average score for comprehensive assessment

Sector	No. of institutions	2014 (%)	2015 (%)	2016 (%)	2017 (%)	2018 (%)
Banks	18	61.3	60.2	65.3	67.3	70.4
Cards	8	49.4	56.8	57.8	59.6	68.2
Life insurance	24	43	54.8	53.3	55.5	59
Fisheries Co.op	90	38	32.9	48.6	52.7	57.5
Savings banks	79	22.9	43.7	40.1	48.6	57
Securities	36	41.3	52	47.3	47.2	56.9
Casinos	14	28.1	41.2	51.9	44.1	52.7
Branches of foreign banks	39	38.8	39.3	45.7	43.7	54
Community Co.op	1 309	26.8	12.3	32	42.3	48.9
Forestry Co.op	137	30.3	27.3	38.7	42	42.6
Foreign securities	20	36.9	44.4	35.4	40.1	52.1
Agricultural Co.op	1 124	45.6	12.9	29.4	39.3	43.5
Leasing	42	29.2	23.4	22.8	38	44.1
Non-life insurance	19	31.6	41.4	27.1	37.7	35.1
Credit union	888	18.4	14.9	29.9	31.1	37.7
New tech venture capital	38	N/A	24.9	22	26.3	36
Futures	6	6	N/A	21.5	28.3	24.8
Real estate trusts	11	11	N/A	N/A	8.3	21

410. An example of a particularly positive action is the proactive work undertaken by KoFIU in November 2016 to raise the overall understanding by FIs and casinos on STR reporting obligations which led to improvements in the quality of STRs. However, as noted in Chapters 3 and Chapter 5. , additional work in this area is needed.

411. Due to previously inadequate supervision of the currency exchange sector, the supervisory responsibility was transferred from the Bank of Korea to the KCS in 2016. There has been a focus by the KCS on ensuring compliance by currency exchangers, which has led to several currency exchangers being de-registered or having their registration suspended. The KCS reported that the enhanced focus on the sector, including the supervisory actions, has increased the level of compliance in the sector. This is supported by the statistics provided, where fewer sanctions have been imposed in 2018 compared to a relatively high number in 2017. The KCS noted that there have been no cases of repeated offenders.

412. The supervisory responsibility of casinos in Jeju was only recently transferred to the SGP supervisor (in March 2019).[53] On this basis, the assessment team cannot conclude on the impact of the SGP supervisor's supervisory actions.

413. DNFBPs other than casinos are not subject to the AML/CFT framework, monitored or subject to AML/CFT supervisory actions.

Promoting a clear understanding of AML/CFT obligations and ML/TF risks

414. KoFIU provided a number of guidance papers, outreach and trainings (including seminars on the 2018 NRA) to obliged entities on understanding ML/TF risks and complying with AML/CFT obligations. During the seminar on the 2018 NRA, its findings were explained to obliged entities and the identified risks and vulnerabilities were highlighted.

415. Through the comprehensive assessment, KoFIU has analysed the main shortcomings among the different sectors. On this basis, KoFIU has conducted a range of outreach activities (e.g. seminars and training) to raise attention on common shortcomings and raise awareness of higher risk areas. When new and emerging risks arise, KoFIU does seminars and outreach, as it did with virtual assets. One type of specialised outreach was on CFT when specific regions were assessed as having increased exposure to TF. In this instance, KoFIU and other relevant authorities provided specialised training in the relevant regions to increase the obliged entities' understanding of TF and importance of complying with TFS.

416. Korea has established mandatory annual cyber-training (Table 6.8) and collective AML/CFT trainings to further ensure obliged entities' understanding of ML/TF risks and AML/CFT obligations. These trainings cover several topics, including the FATF Recommendations, the 2018 NRA, STRs, etc. However, as identified under IO.4 (see Chapter 5), supervisors should increase their efforts to decrease the level of defensive reporting by providing further guidance and training to obliged entities.

Table 6.8. AML/CFT cyber training 2014 – 2018 (no. of trainees)

Course	2014	2015	2016	2017	2018
Understanding of the AML/CFT System	1 644	3 673	4 719	2 901	4 220
Understanding of the AML/CFT System for the Management	-	-	-	637	7 855
AML/CFT Examination and Cases	1 028	2 617	902	1 795	825
How to write STRs	2 517	3 418	576	986	691
Types of STR by Sector	797	2 837	3 891	992	878
CDD Course for Bank Tellers	-	-	2 885	3 083	6 347
Construction of the AML Risk Assessment System	-	16	95	82	65
Understanding of the FATF Recommendations	-	12	64	100	110
Total	5 986	12 573	13 132	10 576	20 991

417. In an effort to enhance AML/CFT capabilities and raise awareness of executive officers and employees in obliged entities who are in charge of AML/CFT matters, the government introduced the AML/CFT certification system in 2017. Since the introduction of the system a total of 589 specialised officers and 3 287 general AML/CFT officers have been certified as having passed the course.

53. Prior to March 2019, casinos on Jeju were supervised by KoFIU.

418. For DNFBPs other than casinos no guidance has been provided and no outreach has been undertaken.

Overall conclusions on IO.3

419. **Korea 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) Korea has a growing understanding of the risks associated with legal persons, and has identified specific types of legal person at risk of ML/TF abuse. However, the authorities do not yet have a clear understanding of the specific characteristics and features that make these types of entities vulnerable to ML and it is not clear that Korea is effectively mitigating the specific ML risks posed by these types of entities. Nonetheless, authorities have taken steps to prevent the misuse of legal entities in general.

b) Basic and legal ownership information is publicly available through a wide network of registries that allow competent authorities to trace BO relatively easily, unless foreign ownership or a particularly complex corporate structure is involved. However, registry information is not always accurate or up-to-date. Where the legal person has a relationship with a FI or casino, the authorities can also obtain BO information directly from this source, although there are some issues with accuracy and up-to-dateness. In some cases, this channel will require a warrant meaning it cannot always be used at the intelligence-gathering stage.

c) Sanctions for legal entities failing to comply with reporting and record-keeping obligations are limited which reduces their ability to be effective, proportionate, and dissuasive.

d) The risks of commercial trusts in Korea are largely mitigated, as such entities are highly regulated and administered by licensed FIs. Very little information is available on civil trusts, which appear to be rare to non-existent, and limited information is available on foreign trusts, which have been seen in cases of tax crime and asset flight.

Recommended Actions

Korea should:

a) Deepen its understanding of the ML methodologies involving legal persons and the specific vulnerabilities of identified at-risk legal persons in order to implement effective mitigation measures for these entities.

b) Use the risk assessment to develop a co-ordinated plan for mitigating the risks and vulnerabilities posed by legal persons and arrangements to ensure mitigation actions are focused and comprehensive.

c) Adopt mechanisms to ensure the accuracy of the basic and BO information available on the various registers, such as by verifying information at the time of registration, conducting post-registration

testing of records, and encouraging users (especially FIs and casinos) to report errors.

d) Where appropriate, impose sanctions on both natural and legal persons who breach reporting requirements, make an inaccurate report or fail to report.

e) Obtain further information on the existence of civil and foreign trusts to confirm and quantify the risks in this area.

420. 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.[54]

Immediate Outcome 5 (Legal Persons and Arrangements)

421. The types of legal persons and arrangements in Korea are described in Chapter 1 (paras.81-82) and the technical compliance annex (see c.24.1 and c.25.1).

Public availability of information on the creation and types of legal persons and arrangements

422. Information on the creation and types of legal persons in Korea is widely available on-line. Publicly available information on legal arrangements is more limited, but these are less common.

423. These conclusions are based on a review of public websites and databases and discussions with register authorities and the MOJ.

424. Information on the creation and types of legal persons is publicly available in Korea on several free public websites. The Ministry of Government Legislation manages the Easy to Find, Practical Law site (www.easylaw.go.kr), available in 13 languages including Korean, English, Chinese, Japanese and Arabic. The Ministry of Small and Medium Sized Enterprises and Startups manages the Government for Business site (www.g4b.go.kr), available in Korean and English. The Korea Trade-Investment Promotion Agency (www.investkorea.org) manages the Invest Korea site, available in Korean, English, Chinese and Japanese. All three websites are easy to access and navigate. The legislative requirements for setting up a legal person are also set out in the Civil Act and Commercial Act, which are publicly available online.

425. Some information is available on specific types of trusts (e.g. commercial real estate trusts: www.koreanlii.or.kr, available in Korean and English).[55] This information is relatively easy to find online, but in most cases is limited to the legislative requirements for establishing and maintaining a trust, as found in various acts (such as the Trust Act) which are also publicly available.

54. The availability of accurate and up-to-date basic and BO 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.

55. Two types of trusts may be created under Korean law: commercial trusts, which are administered by a professional trustee which must be a licensed and regulated financial investment business approved by the FSC, and civil trusts, which are administered by a trustee (either a natural or legal person). Foreign trusts are also recognised and subject to the same requirements as civil trusts.

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

426. Korea has a growing awareness and understanding of the risks associated with legal persons. Authorities could benefit from a deeper understanding of ML methodologies involving legal persons and the specific vulnerabilities of identified at-risk legal persons. The focus on legal persons, as opposed to legal arrangements, is in line with Korea's risks.

427. These conclusions are based on: risk assessment documents provided by Korea; case studies; and discussions with register authorities, the MOJ, KoFIU, the SPO, the KCS and the NTS.

428. In January 2019, Korea completed its first specific risk assessment focused on the vulnerability and scope of abuse of Korean legal entities (both persons and arrangements) for ML/TF. Based on the specific legal entity risk assessment (LERA), Korea has concluded that the risk of ML/TF abuse through legal persons and arrangements is not significant. Nonetheless, LEAs (particularly the SPO, the KCS and the NTS) noted that corporate structures have been misused for ML, tax crime and asset flight, and they are seeing an increasing number of such cases. To date, such cases have usually involved in-house lawyers and accountants rather than professional enablers, although this is a risk that may emerge in future (see Chapter 3, para.189).

429. The LERA identifies two types of legal persons that are particularly open to ML abuse: offshore shell companies (that house Korean assets and have Korean beneficial owners) and domestic special purpose companies. These findings are based on public information, including detailed press releases on specific cases, many of which are included in the assessment. The vast majority of the case studies in the LERA relate to tax crime, followed by asset flight. The ML aspect of the cases is not always analysed, which makes it difficult to draw conclusions on how legal entities are being used for ML (as distinguished from the predicate offending). In this respect, the LERA could have benefited from drawing on more detailed case information, beyond what is publicly available. This reflects the assessors' general concern that ML is often seen as secondary to higher-risk proceeds-generating offences, especially tax crime or asset recovery (see Chapter 3 on IO.7). The use of offshore shell companies in asset flight cases was also picked up in the 2018 NRA.

430. In discussions, LEAs supported the LERA's findings, acknowledging the risks posed by special purpose and shell companies. However, the risk assessment does not analyse in detail the particular vulnerabilities of these types of companies that leave them open to ML abuse nor were LEAs able to clearly identify these vulnerabilities. The LERA also notes cases of public interest corporations (i.e. associations or foundations performing activities in the public interest) being used for tax crime schemes. However, again, the specific ML aspects are not covered nor are the vulnerabilities explained.

431. The ML risk assessment of offshore shell companies, special purpose companies and public interest corporations does not give a clear sense of the extent and depth of these risks. This may be due to a lack of data on the extent to which these entities have been misused (e.g. to establish the number of ML cases involving misuse of corporate structures, the proportion of asset flight cases involving offshore shell companies or the proportion of tax crime cases using public interest corporations).

432. One factor the LERA identifies as mitigating the risk of ML/TF through legal entities is the cultural climate in Korea where legal persons and arrangements are used

in a traditional sense (to establish businesses and chaebols) and are not widely used to move wealth, manage tax obligations, etc. as they are in other jurisdictions. Various government representatives echoed this sentiment during the on-site visit. Nonetheless, discussions with LEAs highlighted that corporate vehicles are increasingly being misused for ML and predicate offence crimes.

433. On the TF side, the LERA is brief, noting that Korea's overall TF risk is low and that there have been no cases of TF through legal entities. Accordingly, Korea has concluded that the risk of TF through legal persons is low.

434. Korea's LERA also considers the risks posed by legal arrangements, which goes beyond what the FATF Standards require. Broadening the scope of the LERA to include legal arrangements is a positive feature and an example of good practice. The risk assessment notes that there is almost no data on the misuse of trusts (either civil or commercial), but flags a potential risk of commercial trusts being abused for tax crime purposes. LEAs concurred with this conclusion, noting that they had not observed the misuse of trusts for ML, with the exception of foreign trusts occasionally seen in tax crime cases. Certain authorities were sensitive to potential risks from trusts, with one agency noting that an increase in civil trusts was feared after Korea changed rules on nominee accountholders, but in practice, this did not occur.

Mitigating measures to prevent misuse of legal persons and arrangements

435. Korea has taken steps to prevent the misuse of legal persons and arrangements. General registration requirements for legal persons are strong, although additional steps could be taken to mitigate the specific risks identified for particular types of legal persons.

436. These conclusions are based on information about relevant legal and operational measures taken by Korea and discussions with regulators and LEAs.

437. Korea has taken a variety of steps in recent years to strengthen transparency, mitigate identified vulnerabilities, and respond to weaknesses posed by legal persons and arrangements in general (see Table 7.1). These measures are positive and could be further strengthened through a co-ordinated plan to mitigated the specific risks and vulnerabilities identified in Korea's recent risk assessment.

438. Korea has implemented some measures in respect of each of the higher-risk legal persons identified in its LERA: offshore shell companies; special purpose companies; and public interest corporations. However, these measures are not clearly aimed at mitigating the ML risk. For offshore shell companies, Korea's foreign exchange controls may help mitigate the risks as cross-border movements of funds are reported to the Bank of Korea and the FSS, enabling fund flows to be tracked (see Chapter 1, para.37). Nevertheless, such companies continue to be seen in tax crime and ML cases. For special purpose companies, Korea has tightened their loan requirements following a number of cases in which such companies were used in fraudulent loan schemes. However, these measures are unlikely to address the ML risk posed by these entities and the LERA identifies that there remain risks in this area. For public interest corporations, the NTS set up special teams to monitor these entities; however, this is aimed more at detecting tax crime rather than preventing misuse.

439. All legal persons in Korea are subject to a registration and reporting framework that helps increase transparency and prevent misuse, although a lack of verification of the information on some registers undermines the utility of this system (see R.24 and Box 7.2 below).

440. Mitigation and preventive measures for trusts are largely in line with risks. Discussions with various government and private sector representatives confirmed that commercial trusts were much more common than civil trusts. A total of KRW 873.5 trillion (EUR 659.7 million) is held in commercial trusts across 56 commercial trust providers.[56] There have been some instances of commercial trusts being misused, although generally for tax crime rather than for ML. Commercial trusts must be administered by a licenced and authorised security provider (i.e. acting as the trustee). The trustees are therefore supervised by the FSC, which also supervises for their compliance with the Trust Act. As financial investment companies, they are also obliged to comply with Korea's AML/CFT obligations, including conducting CDD on trust parties.

Box 7.1. Recent legislative measures to mitigate misuse of legal persons and arrangements[57]

- November 2018 amendments to the *Act on External Audit of Stock Companies* introduced a new audit system, requires external audits for certain public companies and requires listed companies to use registered auditors.
- January 2016 amendments to the *FTRA* tightened CDD requirements, requiring FIs and casinos to obtain BO information relating to legal persons.
- May 2014 amendments to increase the penalties for the use of borrowed names, including by legal persons.
- May 2014 amendments to abolish bearer shares due to the risks they posed and their lack of transparency. This was a positive step to mitigate potential risks that Korea took, despite having no evidence that Korean companies used bearer shares in practice. Korea also prohibits the use of nominee shares and nominee directors.

441. Civil trusts in Korea are extremely rare. Of the many government and private sector representatives questioned on this topic, none was aware of any civil trusts operating in Korea (either currently or in the past). Korean authorities had made enquiries and undertaken research to try to determine the number of such trusts with no success. Quantitative data in this area would help Korea to confirm these anecdotal findings.

442. Foreign trusts are permitted in Korea and authorities confirmed these have been seen in cases of tax crime and asset flight. Korea's strict foreign exchange controls provide some mitigation of the risks in this area (see Chapter 1, para.37). Additional data is necessary to ensure a better understanding of the extent of any risks.

56. As of December 2018.

57. In September 2019, Korea introduced an electronic securities system that requires electronic registration for all shares (the Electronic Securities Act). As this measure was not in force at the time of the on-site visit, it was not taken into account for the purposes of this evaluation.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

443. Korean competent authorities use a variety of sources and mechanisms to obtain basic and BO information on legal persons. Used together, the available channels largely allow authorities to access adequate information on most Korean legal persons although this information may not always be accurate and up-to-date. Obtaining BO information is more difficult where the corporate structure is particularly complex or involves foreign ownership.

444. These conclusions are based on: a review of the available registry information; and discussions with registry authorities, LEAs, FIs and DNFBPs.

Information from financial institutions and casinos

445. Competent authorities explained that their first step for obtaining BO information is typically to request the information from KoFIU. When KoFIU receives a request for BO information, or wishes to obtain such information for its own purposes, it reviews the information on its STR database or approaches the FI or casino directly if it is able to do so (i.e. provided there is a related STR, CTR or foreign exchange report). Information must be provided within 15 days which is likely sufficient for most investigations, but may be problematic where there is an urgency (e.g. where authorities need to act quickly to trace and restrain assets before dissipation). FIs and casinos demonstrated a good understanding and implementation of their CDD and BO requirements, and information obtained through this channel is generally accurate (see Chapter Chapter 5. on IO.4). However, while the information is updated at various intervals (see R.10), this is based on materiality and risk so the information may not always be up-to-date.

446. If the information is not available through KoFIU (e.g. because KoFIU had not received any reports relating to the relevant legal person), competent authorities will seek the information directly from a FI or casino. The NTS and the FSC can request this information without a warrant where the information is required for tax-related purposes (for the NTS) or foreign exchange matters (for the KCS). Other authorities, including the SPO and the NPA, will require a court warrant. Warrants can be obtained quickly, generally within 1-2 days, or within hours where the request is particularly urgent. While this mechanism can provide timely access to largely accurate information, LEAs can only obtain warrants during an investigation and cannot obtain them for intelligence gathering purposes.

447. Obtaining BO information from FIs or casinos, either through KoFIU or directly, is dependent on the legal person having a relationship with a FI or casino. This is not guaranteed, especially in Korea's context in which professional intermediation is rare. In additions, it may be problematic where the requesting authority cannot link the legal person to a particular reporting entity.

Public legal person registers

448. Where information cannot readily be obtained from FIs or casinos, competent authorities can seek basic and legal ownership information from Korea's system of registers (see Box 7.2). Most LEAs did not report using this system themselves, but instead seek information from KoFIU. When KoFIU receives such a request, it will use register information (in addition to information from FIs and casinos) to provide a response back to the requesting authority. While Korea's registration system is wide-

ranging, a lack of verification of some register information undermines the utility of this system.

Box 7.2. Korea's public registries for legal persons

Legal Person Register

The Legal Person Register contains **basic information** on all 760 000 companies in Korea, including the purpose, company address, and director and representative information. Information is required to be accurate and to be updated within weeks of a change (see R.24). While registrars have the power to examine registry data, there is no formal and systematic verification process for register information. Instead, the information is largely entered as provided by the company. Registration officers from the National Court Administration are authorised to conduct inquiries and request corrections if errors are detected, but it is not clear how errors would be detected in the absence of formal verification procedures or a requirement on users to report inaccuracies. Providing inaccurate information is subject to penalties. The register is freely available online, including to all domestic and foreign authorities (www.iros.go.kr). The public nature of the registry allows some scrutiny that may aid accuracy.

Korea Enterprise Data (CRETOP)

CRETOP contains **basic information** (drawn from the Legal Person Register), **legal ownership information** (obtained via NTS), information on management and related persons, and credit information on all 760 000 companies in Korea. Information on shareholders (including foreign shareholders) includes personal information, percentages of shares held, changes to shareholdings, and information on natural and legal persons who have a special relationship with the shareholder or senior management. Links between CRETOP and the Legal Person Register ensure basic information is updated when the Legal Person Register is updated (i.e. within weeks of a change). Shareholder information is updated through the NTS, which receives such information on an annual basis from companies and conducts a desk-based review to check for accuracy (see R.24). Information on CRETOP is checked by 400 CRETOP staff who cross-check against various sources (e.g. Korea Credit Information Sources, Korea Technology Financial Corporation) and conduct 30 000 on-site, interview and desk-based examinations annually. CRETOP is legally required to be accurate and up-to-date with sanctions for inaccuracies. CRETOP is an online database that can be accessed by all relevant competent authorities and private sector entities (including FIs and DNFBPs) for free, and can be bulk downloaded by any member of the public for a fee.

Data Analysis, Retrieval and Transfer System (DART)

DART contains **major shareholder information** for public companies and large non-public companies (with over 500 shareholders) (there are approximately 74 000 such companies in Korea). This information is reported to the FSS for publication on the DART database

(www.dart.fss.or.kr). Shareholder information is included on DART where the total amount of the shares held by the principal person and any related persons amounts to 5% or more. Information includes percentages of shares held, changes to shareholdings, and information, and shareholding terms. DART also includes information on the person with the largest equity share and who exercises de facto control over the company. Information on the register is updated quarterly. There is no formal verification process, but FSS staff cross-check DART against information provided in the Legal Person Register. DART is freely available online, including to all domestic and foreign authorities. This allows public scrutiny which may aid accuracy.

Fair Trade Commission Information System

The Fair Trade Commission's Information System contains **company representative** and **shareholder information** (including governance and structuring information) for large conglomerates, meaning business groups with over KRW 5 trillion (EUR 3.8 million) in assets (there are 59 such groups in Korea encompassing 2 104 affiliate companies). Shareholder information includes the extent of shareholdings across a business group and information on related persons. The information is updated annually or where the business group reports a change. From 2018, the Fair Trade Commission started inspecting all reports for compliance with relevant disclosure requirements and is authorised to request additional material from a business group where a potential inaccuracy is detected. The Information System is freely available online, including to all domestic and foreign authorities (www.groupopni.ftc.go.kr) which also allows public scrutiny.

NPO Information System

The NTS' NPO Information System contains **management information** on public interest corporations (i.e. associations and foundations performing work in the public interest), covering 9 164 of Korea's 14 033 NPOs (65%). Information is updated annually (see R.24). There is no formal verification process, but there are tax levies for failing to provide information and the NTS is authorised to audit corporations that provide false documents. The Information System is freely available online, including to all domestic and foreign authorities (www.hometax.go.kr), which allows public scrutiny that may aid accuracy.

449. These registers provide comprehensive legal ownership information on all companies in Korea and allow authorities to trace BO relatively easily where no foreign ownership or control is involved and provided the corporate structure is not overly complex. Korean authorities and private sector entities (who also use the registers) considered that the databases would generally allow them to trace legal ownership to a natural person, including foreign shareholders. Including information on natural and legal persons with a special relationship to shareholders or management is a particularly positive step given Korea's risks around borrowed name accounts (see Chapter 1, para.39). However, it is not clear how these persons are identified and whether this information is verified.

450. In terms of accuracy, the registers are largely unverified and based on the assumption that companies will provide accurate information (as it is an offence not to do so; see R.24). The exception is CRETOP which reviews information through its examination process. This is positive, but does not amount to the systematic verification of BO information. There are also some concerns that the information may not be up to date. The shareholder information feeding into CRETOP and the NPO Information System is based on NTS data which is only required to be updated on an annual basis (see R.24) while DART is updated quarterly. The NTS conducts monitoring and inspections for tax compliance which may help detect out-of-date information. However, this is not systematic and there is no requirement or specific mechanism in place to ensure that the information remains current creating a risk that information on these registers may not be up-to-date. Implementing systematic verification and ensuring a feedback loop on the registers (e.g. from FIs or casinos where they detect inaccurate information in their CDD checks) would help ensure accuracy.

451. The utility of the system of registers is limited where BO is particularly complex or involves foreign persons or arrangements. Korea's foreign exchange controls require foreigners investing in Korea to report their information and investments to the NTS, so competent authorities may be able to obtain information on a foreign investor from the NTS (directly, in relation to tax crime investigations, or with a warrant for other investigations). However, this requirement will not automatically capture all foreign beneficial owners. In other cases involving foreign beneficial owners, a more time consuming process must be used involving requests to foreign counterparts.

Information from the NTS

452. The NTS maintains an internal database of corporate tax information, which includes basic and shareholder information on legal persons, based on tax reporting. The NTS also actively monitors for shareholders in fictitious or borrowed names through an information analysis system that cross-checks against long-term shareholding and tax data. Legal persons are only required to update their information on an annual basis (see R.24). Tax compliance inspections by the NTS may help detect out-of-date information, but the lack of a specific verification requirement or mechanism means the data may not be entirely up-to-date. As with the register information, tracing BO using the NTS database may be difficult where complex or foreign structures are used. To overcome this difficulty, the NTS can access information on foreign investments (see Chapter 1, para.37), use its network of liaison officers posted abroad or request information from its foreign counterparts (see Chapter 8 on IO.2). Information on the NTS register can only be accessed by other competent authorities in relation to tax crime investigations, or with a warrant in the context of other investigations.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

453. Access to basic and BO information on legal arrangements depends on the type of legal arrangement involved. Information on commercial trusts is generally available from the trustee (which is a licensed FI) within several days, while information on civil trusts, which are much rarer, and on foreign trusts is harder to obtain.

454. These conclusions are based on: a review of the available registry information; and discussions with registry authorities, LEAs, FIs and DNFBPs.

455. Commercial trusts must be administered by a financial investment business (acting as a professional trustee) appointed and licensed by the FSC. These entities are therefore directly subject to AML/CFT requirements, including the requirement to identify and verify the beneficial owner (see R.10). This requirement is well understood and implemented by the financial sector (see Chapter 5 on IO.4). Competent authorities are therefore able to access BO information on commercial trusts directly from the trustee. Obtaining this information generally requires a warrant (depending on the agency and the offending involved) and is therefore available only during the investigative stage. Warrants can typically be obtained and executed quickly (usually within 1-2 days). Commercial trusts are also subject to reporting obligations, which include reporting the trustee and beneficiaries to the NTS (see R.25). LEAs can therefore access information on trustees and beneficiaries in a timely manner from the NTS, but generally only with a warrant during an investigation.

456. Special purpose trusts (which are a type of commercial trust utilised for a special purpose and licensed by the MOJ) are subject to public disclosure requirements. Information on the trustors, trustees and beneficiaries of special purpose trusts is publicly available on the MOJ website.

457. Limited information is maintained on civil and foreign trusts. Where parties to such trusts interact with FIs or casinos, information on the trust that is collected during CDD processes can be obtained through this channel as set out in para.445-446. Civil and foreign trustees are required to maintain some information and make it available to competent authorities (see R.25). Civil trusts are very rare and as the competent authorities met by the assessment team had never encountered such entities, they have never had to seek basic or BO information on them in practice. Obtaining information on foreign trusts will generally require a more time-consuming process involving requests to foreign counterparts.

Effectiveness, proportionality and dissuasiveness of sanctions

458. Sanctions available for legal persons and arrangements that fail to comply with reporting obligations are somewhat limited, which reduces Korea's ability to impose proportionate and dissuasive sanctions. The FSS and the Fair Trade Commission have regularly imposed sanctions.

459. These conclusions are based on statistics on the use of sanctions, case studies on sanctioning and discussions with register authorities.

460. Failing to provide information or providing false information to the company registry (for the Legal Person Register) is punishable by up to five years in prison or a fine of KRW 10 million (EUR 7 500). While the imprisonment penalty is high, the fine is reasonably low which may limit Korea's ability to apply proportionate sanctions. In addition, no sanctions are available for the legal person itself (see R.24) which limits the dissuasiveness of sanctions. While late filings are easily monitored, the lack of verification of register information may make it difficult to detect inaccurate filings.

461. Listed companies that fail to provide shareholder information to the FSS (for the DART database) are liable for sanctions of up to three years in prison or a fine of up to KRW 100 million (EUR 75 500). Providing inaccurate shareholder information is subject to sanctions of five years of imprisonment or a fine of KRW 200 million (EUR 154 000) (see R.24). Sanctions may be imposed on both natural and legal persons. The FSS also has administrative sanctions available, such as the revocation of licences. The FSS has imposed sanctions regularly for failure to provide information

(see Table 7.1). It uses a range of sanctions, depending on the seriousness of the violation. For example, in 2018, 20 violations were sanctioned by fines (totalling KRW 1.05 billion (EUR 796 800)), and 3 by licence restrictions.

Table 7.1. Sanctions by the FSS for failure to provide shareholder information

	2014	2015	2016	2017	2018
Sanctioned companies	46	98	93	56	57
Violations	63	126	185	108	65

462. Conglomerates failing to provide information or providing false information to the Fair Trade Commission (for its Information System) are liable to a fine of up to KRW 100 million (EUR 75 500) (see R.24). The Fair Trade Commission began inspecting reports for compliance in 2018. Its 2018 inspection detected 194 violations by 139 affiliate companies resulting in a total of KRW 2 333.2 million (EUR 177 2800) in fines. Sanctions in practice appear to be low (see Box 7.3).

Box 7.3. Imposition of sanctions for provision of inaccurate shareholder information by Fair Trade Commission

Between 2012 and 2015, Companies A, B and C, affiliates of Business Group A, falsely reported to the Fair Trade Commission that their shares were owned by incumbent and former executives if Group A. In reality, Person L was the beneficial owner of Group A and the shares. The Fair Trade Commission detected this inaccuracy following an NTS audit and issued a warning to Group A's affiliates, requiring them to provide shareholder information. Upon receipt, the Fair Trade Commission identified multiple other instances in which the affiliates had falsely reported shareholder information. The Fair Trade Commission issued a warning to Person L and Group A's three affiliates. The three affiliates were also fined a total of KRW 58 million (EUR 43 870). The low penalties were considered justified given certain mitigating measures, including that Group A had no history of violations and the shares involved accounted for less than 1% of the total company value.

463. Public interest corporations failing to provide management information to NTS (for the NPO Information System) are subject to additional tax and a fine of up to KRW 20 million (EUR 15 100). Sanctions do not apply to natural persons and no specific sanctions are available for providing inaccurate information. This limits the ability of the NTS to impose effective, proportionate and dissuasive sanctions.

464. As of 1 July 2019, commercial trustees are subject to a fine of KRW 10 million (EUR 7 500) for failing to obtain relevant information. This penalty is too low to be dissuasive. Civil and foreign trustees have no specific sanctions related to record-keeping beyond a general liability for negligent bookkeeping (see R.25). No sanctions have been imposed on legal arrangements in practice, which is in line with the relatively limited use of these entities in Korea.

Overall conclusions on IO.5

465. **Korea is rated as having a moderate level of effectiveness for IO.5.**

CHAPTER 8. INTERNATIONAL CO-OPERATION

Key Findings and Recommended Actions

Key Findings

a) Korea has an effective legal and operational framework for seeking and providing MLA and extradition, including asset recovery and repatriation. Korea can provide assistance promptly and its requests and responses are generally of good quality. Co-operation under one of its 74 MLA treaties or 77 extradition treaties is generally faster and more frequent, but Korea can and has sought and provided MLA and extradition on the basis of reciprocity. Domestic co-operation to execute MLA and extradition requests is sound, and agencies collaborate and communicate regularly. Further streamlining domestic co-operation could help ensure rapid execution of requests in all cases.

b) A strength of Korea's system is the range of mechanisms it has established to streamline MLA and extradition with major partners, including regular bilateral meetings, videoconferences and teleconferences. Korea has not yet extended these measures to new and emerging partners, such as countries frequently implicated in tax crime cases.

c) At the individual agency level, strong channels are in place to exchange and share information with foreign counterparts. Contact points exist in counterpart agencies abroad and almost all LEAs post foreign liaison officers in strategically important countries to facilitate both formal and informal international co-operation.

d) KoFIU is making and receiving an increasing number of requests to and from foreign FIUs, including on behalf of other domestic agencies. If this trend continues, its current staffing arrangements may n be sufficient to manage the number of requests.

e) Korea's level of international co-operation is largely in line with its risk profile. However, given the identified risks in terms of asset flight and offshore tax crime, the assessment team expected to see a higher level of co-operation from the KCS and the NTS to obtain BO information. KoFIU is not always able to provide BO information in response to requests and does not systematically refer requesting parties to alternative information sources where a request is rejected.

Recommended Actions

Korea should:

a) Expand its mechanisms for facilitating co-operation (e.g. bilateral meetings, video and teleconferences, liaison officers) to new and emerging partners with whom Korea needs ongoing co-operation in light of its risks, particularly countries that are regularly involved in Korea's tax crime and asset flight cases.
b) Ensure that KoFIU:
    a. provides both basic and BO information where this information can be obtained using available domestic sources in response to a request for information on a legal person; and
    b. has sufficient staff to handle incoming and outgoing requests for information, especially should the number of requests continue to increase, and to increase the number and range of spontaneous disseminations to foreign partners.
c) Actively use international co-operation tools in asset flight and offshore tax crime cases, including using co-operation mechanisms available to the KCS and the NTS, especially to seek BO information.
d) Streamline the process for receiving MLA requests to ensure that requests are rapidly submitted to the SPO for execution (e.g. by developing guidance with suggested timeframes for each stage in the process).
e) Explore measures to facilitate extradition to ensure that all cases progress in a timely manner.

466. 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)

467. Korea's criminal context is largely domestic although it does face risks from asset flight and offshore tax crime which are highlighted in the 2018 NRA. LEAs noted that Korea can be a transit country for drug trafficking and smuggling, but these are not major predicate offences. Korea is not a financial centre and strict foreign currency and remittance controls make it difficult for funds to move through Korea (see Chapter 1, para.37). In this context, more weight was given to Korea's outgoing co-operation.

Providing constructive and timely MLA and extradition

468. Korea has an effective system for providing constructive and timely MLA and extradition, including asset repatriation. While co-operation can be provided on the basis of either a treaty or reciprocity, case studies indicated that co-operation was generally stronger and more timely with treaty partners. Korea has 74 MLA treaties and 77 extradition treaties, and should continue to pursue such relationships. Measures are in place to facilitate co-operation with frequent partners, and Korea should continue expanding access to these mechanisms. Domestic co-operation is sound, but could benefit from further streamlining to ensure the rapid execution of requests.

469. These conclusions are based on: case studies and statistics provided by Korea; feedback from FATF and FSRB delegations on the extent and adequacy of Korea's international co-operation; and discussions with the MOJ, the MFA, the SPO, the NPA, the KCG, the KCS and the NTS.

Mutual legal assistance

470. The MFA receives MLA requests and transmits them to the MOJ which assesses whether the request meets the statutory or treaty requirements. If so, the MOJ sends the request to the SPO's International Co-operation Centre which forwards it to the relevant DPO or other agency (e.g. the NPA) for execution. Close co-operation and communication between authorities streamlines this process. Officers in MOJ's International Co-operation Team monitor requests through the case management system and liaise with the SPO through a secure, online messaging service to ensure prompt execution of requests. Discussions with the MOJ and SPO confirmed that co-operation and communication between the authorities is ongoing and constructive.

471. Typically, Korea executes requests in a timely manner and delegation feedback did not suggest issues with delays. Korea estimates that requests are typically executed in one month. In general, requests are processed in the order in which they are received, but the MOJ and SPO are able to prioritise requests where required (e.g. where requested by the requesting country or when necessary to meet the statute of limitations). Korea can apply a simplified process for requests from certain key countries (sending the request directly to MOJ and bypassing MFA). Currently, 20 countries are able to use this system based on Korea's frequency of co-operation and mutual recognition.

472. Korea does not receive a high number of MLA requests, which is in line with its risk and context. The number of MLA requests has been steadily increasing from 80 in 2014 to 195 in 2018 (see Table 8.1). Most requests received are for readily available information (e.g. criminal records data) and are straightforward and quick to execute. Requests for bank account information can take longer as this information may not be available from KoFIU (depending on whether or not there is a related report), in which case the authorities need to secure and execute a warrant. Nonetheless, warrants can be obtained urgently where necessary. Requests to obtain witness statements (which account for most of Korea's requests–32%) also typically take longer to execute due to difficulties locating witnesses or securing their participation. Korea rarely refuses requests. Refusals are usually due to the nature of the offending (e.g. a politically motivated offence) or lack of information. In such cases, Korea reaches out to the requesting country prior to refusal, asking for further information to see if there is a way to grant the request.

Table 8.1. MLA requests received by Korea

	2014	2015	2016	2017	2018
Requests received	80	111	137	160	195
Relating to ML	*7*	*7*	*5*	*9*	*5*
Relating to TF	*0*	*0*	*0*	*0*	*1*
Requests executed	79	110	133	152	146
Relating to ML	*6*	*3*	*4*	*8*	*3*
Relating to TF	*0*	*0*	*0*	*0*	*1*
Requests denied	1	4	1	1	0
Relating to ML	*1*	*4*	*1*	*1*	*0*
Relating to TF	*0*	*0*	*0*	*0*	*0*
Requests ongoing	0	0	0	0	2
Relating to ML	*0*	*0*	*0*	*0*	*2*
Relating to TF	*0*	*0*	*0*	*0*	*0*

Note: The figures in the table reflect total annual information. A request may be received in one year and executed in another year.

473. Korea takes active steps to facilitate MLA and promote positive international co-operation with its major partners. Regular bilateral meetings on international co-operation are held with Korea's key partners—Japan, the U.S. and (from 2019) China—to discuss ongoing cases (see Box 8.1). Korea selected these partners based on the number of requests and level of co-operation, and they are consistent with Korea's risk and context (see Chapter 1, para.49). For other major partners (or where necessary), Korea actively uses ad hoc bilateral meetings, conference calls and video conferences to advance ongoing requests. Korea holds around 50 such meetings every year with a range of partners, including the U.K., Australia, Thailand and Sri Lanka. These measures are a good practice. It would be useful to extend them to other partners with which Korea needs ongoing co-operation based on its major ML/TF risks (e.g. offshore tax havens).

Box 8.1. Bilateral meetings on international co-operation

Between 2017 and 2019, Korean held several regular meetings with its key partners. These include the U.S., Japan, and China. The MOJ characterises the meetings as a frank, open discussion of ongoing cases. The meetings cover ongoing MLA and extradition requests involving the relevant parties, including the status of cases, outstanding information and any foreseen difficulties.

In addition, Korea held 19 *ad hoc* bilateral meetings with other jurisdictions to discuss ongoing cases and outstanding requests. This included meetings with Australia, Cambodia, India, the Philippines, Sri Lanka, and Thailand.

474. Case studies and discussions with Korean authorities confirmed that authorities understand the importance and value of MLA. For example, in one case, the Seoul Northern DPO detected potential smuggling in the course of an ongoing embezzlement investigation. The DPO proactively reached out to the relevant foreign

authorities to share this information and encourage them to pursue a MLA request for the relevant evidence.

475. Korea has specific procedures and legislation for sharing the recovered proceeds of corruption offending. For the proceeds of other offences, while no specific legislation is in place, Korea is able to share recovered assets and does so upon the request of the relevant foreign jurisdiction (see R.38). Korea provided several case studies demonstrating its ability to provide MLA in asset recovery cases and successfully repatriate the confiscated assets.

Box 8.2. MLA and asset repatriation

On 5 July 2013, the U.S. requested that Korea execute a U.S. confiscation order for USD 1.25 million (EUR 1.1 million). The money had been paid to the defendant (Person M) as bribes in return for awarding military procurement contracts. Person M laundered the money through a Korean company and transferred it to a third party (Person L) who used it to purchase property and other assets in Korea. The MOJ assessed the request and transmitted it to the Seoul Central DPO for execution. In executing the MLA request, the DPO uncovered separate violations of Korea's ML offence, which led them to open a domestic investigation encompassing Person M, Person L and another individual (Person R). Search and seizure orders were executed which uncovered additional assets for confiscation. In total, between February and September 2014, the DPO obtained six confiscation orders for assets totalling KRW 1.1 billion (EUR 848 267). Of this, KRW 140 million (EUR 107 961) was recovered and repatriated to the U.S. Korea confiscated the remaining KRW 1 billion (EUR 771 152) as part of the Korean investigation and secured criminal convictions against Person M, Person L, and Person R, resulting in prison sentences of 10 months. To facilitate execution of the request, the MOJ discussed the case with relevant officials from the U.S. Department of Justice during one of the regular Korea/U.S. meetings on international co-operation.

Extradition

476. Extradition requests are received by the MFA, assessed by the MOJ and executed by the SPO which seeks the arrest warrant and represents Korea in the court proceedings to decide on extradition. Korea receives a relatively small number of extradition requests (approximately eight per year) which is generally consistent with its risk profile and context. Of the 39 requests received between 2014 and 2018, 17 (44%) were executed. In some cases, individuals were deported rather than extradited to take advantage of this faster process. The receiving state was then able to arrest the person upon their arrival. In other cases, the requesting country was not able to provide supplementary information required by Korea, leading Korea to close the case. Five cases (13%) were rejected due to the requested person not being located in Korea, withdrawal of the request by the requesting state, or an ongoing indictment in Korea. Of the five ML/TF-related extradition requests received from 2014-2018, none have been executed. Three were rejected on the basis that the requested individual was not

present in Korea or was deceased, one is under review, and the fifth is on hold until the requested individual finishes serving a sentence in Korea.

Table 8.2. Extradition requests received by Korea

	2014	2015	2016	2017	2018
Requests received	8	4	5	14	8
Relating to ML	*0*	*0*	*0*	*0*	*1*
Relating to TF	*0*	*0*	*0*	*2*	*2*
Requests executed	4	2	1	1	9
Relating to ML	0	0	0	0	0
Relating to TF	0	0	0	0	0
Requests denied	0	0	0	1	4
Relating to ML	0	0	0	0	0
Relating to TF	0	0	0	0	2
Requests ongoing	7	3	3	3	1
Relating to ML	0	0	0	0	1
Relating to TF	0	0	0	2	0

Note: The figures in the table reflect total annual information. A request may be received in one year and executed in another year.

477. Case studies provided by Korea show that it can execute requests rapidly (see Box 8.3). Simplified procedures are available under certain treaties that permit Korea to make a provisional arrest prior to receipt of a formal request (which is not possible for requests granted on the basis of reciprocity). For requests from key partners (China, Japan and the U.S.), extradition can take as little as four months. Statistics suggest that in other cases, requests will take significantly longer and can take several years to execute. Korea would benefit from exploring measures to reduce these delays, to ensure that timely extradition can be provided to all requesting countries.

Box 8.3. Extradition request showing Korea's ability to rapidly provide extradition

In June 2017, the MFA received an extradition request from the U.S. for a Korean American individual (Person L) who had fraudulently obtained loans amounting to USD 3.2 million (EUR 2.9 million). The MOJ assessed the request, and in August 2017, transmitted it to the SPO for action. The SPO reviewed the request, sought an arrest warrant, and commenced a search for the requested individual. Person L was located and arrested in December 2017 and court proceedings commenced the same day. The Seoul High Court granted extradition on 8 January 2018. The MOJ approved extradition on 1 February 2018. Korea extradited Person L to the U.S. on 23 February 2018 (eight months after receiving the extradition request).

478. To facilitate extradition, the MOJ has points of contact with competent authorities in the requesting country with which it has regular communication on

ongoing cases. Korea also uses its regular key-partner meetings on international co-operation (see para.473).

Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

479. As Korea's 2018 NRA identifies asset flight and offshore tax crime as major predicate offences, international co-operation is an essential tool for Korean authorities. Authorities are aware of the importance of international co-operation and use it regularly to pursue ML and associated predicates and recover proceeds located overseas. Korea could benefit from strengthening relationships with certain partners in line with its risk areas.

480. These conclusions are based on: case examples provided by Korea which demonstrated its effectiveness; statistics on MLA and extradition requests by Korea; feedback from FATF and FSRB delegations; and discussions with the MOJ, MFA and LEAs.

MLA

481. Korea makes active use of MLA, making approximately 240 requests per year. This number has increased from 184 in 2014 to 320 in 2018 (see Table 8.3). Requests are made to a range of countries, with the U.S., China and Japan (Korea's primary trading partners) as Korea's key recipients. Korea could benefit from seeking to establish closer co-operation channels with other countries commonly reflected in case studies (particularly on tax crime and asset flight) to facilitate smoother and more regular co-operation in line with its risk profile. The majority of Korea's MLA requests are for witness statements (30%), documents/information (18%), internet-related information (e.g. IP addresses, domain name, email account data, etc.) (15%) and asset recovery (14%). The relatively high number of asset recovery requests is in line with the government's focus on and prioritisation of confiscation (see Chapter 3 on IO.8). By comparison, the number of MLA requests relating to ML is relatively low (see Table 8.3). This highlights authorities' focus on asset recovery and predicate offending as opposed to ML (see Chapter 3 on IO.7). Case studies also show Korea's ability to successfully request MLA for asset freezing, confiscation and repatriation (see Box 8.4).

Box 8.4. Request to Mongolia for asset seizure and confiscation

From 2005 to 2008, Person A ran an illegal gaming house in Seoul, concealed the proceeds by sending KRW 4.8 billion (EUR 3.6 million) to Mongolia and used this money to build a hotel. In November 2010, the SPO commenced a financial investigation and by February 2011 had traced the proceeds to the hotel in Mongolia. In March 2011, the SPO made a MLA request for Mongolia to freeze the assets. Korea provided further information in support of the request in June 2011. In August 2011, the hotel was frozen. In October 2014, Person A was sentenced to 2.5 years of imprisonment for illegal gambling and ML, and a confiscation order of KRW 4.8 billion (EUR 3.6 million) was imposed. Korea made a subsequent request for confiscation and repatriation, and Mongolia repatriated the hotel proceeds to Korea.

Table 8.3. MLA requests sent by Korea

	2014	2015	2016	2017	2018
Requests sent	184	236	220	240	320
Relating to ML	*0*	*2*	*1*	*2*	*3*
Relating to TF	*0*	*0*	*0*	*0*	*0*
Requests executed	168	215	196	193	236
Relating to ML	*0*	*2*	*1*	*2*	*3*
Relating to TF	*0*	*0*	*0*	*0*	*0*
Requests denied	4	3	8	12	15
Relating to ML	*0*	*0*	*0*	*0*	*0*
Relating to TF	*0*	*0*	*0*	*0*	*0*
Requests ongoing	12	18	16	35	69
Relating to ML	*0*	*0*	*0*	*0*	*0*
Relating to TF	*0*	*0*	*0*	*0*	*0*

Note: The figures in the table reflect total annual information. A request may be received in one year and executed in another year.

482. To facilitate the execution of Korea's MLA requests, Korea utilises its regular conferences and meetings with key partners to discuss cases and exchange information (see para.473). For countries dealing with Korea on a regular basis, the MOJ has a contact point in the counterpart agency which can be used to follow up on outstanding requests. Korea also has a network of prosecutors posted abroad that can be used to follow up on requests, make inquiries with foreign counterparts and identify relevant contact points in foreign agencies. Korea decides where to post these officers, based on the level of co-operation with the foreign counterpart (ten such prosecutors are posted in various countries, including China, Germany, the Netherlands and the U.S.). Korea could usefully strengthen this co-operation network by expanding these channels to cover more recent and emerging partners in line with Korea's risk assessment. For example, there are several countries commonly reflected in Korea's tax crime cases with which Korea does not yet have such systems in place.

Extradition

483. As with MLA, the decision to seek extradition is made by the prosecutor leading the case. Korea provided a large number of case studies showing prosecutors are willing to seek extradition in predicate offence cases, as well as ML cases, although to a lesser extent (nine requests since 2009). Korea has never requested extradition for TF, which is consistent with its identified low TF risk (see Table 8.4).

Table 8.4. Extradition requests sent by Korea

	2014	2015	2016	2017	2018
Requests sent	28	19	49	53	49
Relating to ML	*0*	*2*	*1*	*1*	*1*
Relating to TF	*0*	*0*	*0*	*0*	*0*
Requests executed	13	12	8	15	15
Relating to ML	0	1*	0	0	0
Relating to TF	0	0	0	0	0
Requests denied	4	4	9	7	4
Relating to ML	0	0	0	1	0
Relating to TF	0	0	0	0	0
Requests ongoing	7	6	22	30	29
Relating to ML	0	1	1	0	1
Relating to TF	0	0	0	0	0

* The individual returned voluntarily.
Note: The figures in the table reflect total annual information. A request may be received in one year and executed in another year.

484. Korean prosecutors actively use simplified mechanisms where available. For example, Korea provided case studies in which it had sought the provisional arrest of requested persons prior to providing a formal extradition request (see Box 8.5). Korea tends to be prompt in requesting extradition where the suspect's location is known. In several cases, a formal extradition request was sent within days of the suspect departing Korea. To locate offenders, Korea makes use of Interpol mechanisms, including alert notices. As with MLA, Korea facilitates extradition through conference calls, in-person meetings, contact points in foreign counterparts and prosecutors posted abroad. This simplifies the submission of additional information and supplementary documents.

Box 8.5. Korea's use of simplified mechanisms to facilitate extradition

Between 2012 and 2016, an individual (Person J) with links to a former Korean president committed a range of crimes related to her education record, including falsifying documents, committing fraud, receiving bribes and concealing the proceeds. Person J fled to Denmark. Korea issued an Interpol red notice against Person J, and the Danish authorities consequently alerted Korea to Person J's location. On 2 January 2017, Korea requested the provisional arrest of Person J and within days followed up with a formal extradition request. Korea established a hotline between the Korean MOJ and the counterpart authorities in Denmark to ensure the case progressed rapidly and smoothly. This facilitated providing supplementary information throughout early 2017, including an updated arrest warrant. In June 2017, Denmark approved the extradition request. A Korean escort team of two prosecutors and three investigators flew to Denmark to accompany the offender back to Korea.

Seeking and providing other forms of international cooperation for AML/CFT purposes

485. Korean authorities have strong systems in place to co-operate and share information with foreign counterparts. Most authorities strategically post liaison officers abroad in major partner countries to provide valuable assistance from within the foreign country. While co-operation with certain major partners is strong, Korea could usefully expand its co-operation channels with more recent and emerging partners, in line with its risk assessment.

486. These conclusions were based on: case studies on co-operation; and discussions with the SPO, the NPA, the KCG, the NTS, the KCS, KoFIU; the FSS; and the FSC.

Law enforcement agencies (LEAs)

487. The SPO and NPA regularly co-operate with counterpart agencies. The SPO has been especially active in this area by establishing networks and conferences to facilitate co-operation in areas of particular interest consistent with government priorities, although not necessarily in line with Korea's risks (see Box 8.6). In February 2018, the International Co-operation Centre (ICC) was established within the SPO to facilitate and encourage informal co-operation. It is also Korea's contact point for the Camden Asset Recovery Network (CARIN) and is the Secretariat for the Asia Pacific Asset Recovery Network (ARIN-AP). All international co-operation by prosecutors is centralised through the ICC to leverage relationships and contact points, and ensure quality and consistency in requests for information. The SPO also has prosecutors posted abroad to facilitate both formal and informal co-operation (see para.482).

Box 8.6. Forums for co-operation by the SPO

Anti-Drugs Liaison Officials' Meeting for International Co-operation

Since 1989, the SPO has held a regular annual conference of narcotics control officials from countries in the Asian region. The Anti-Drug Liaison Officials' Meeting for International Co-operation is a platform to discuss trends in international drug cases, identify potential joint investigations and consider avenues for improved co-operation. As of 2018, 23 countries, 7 international organisations, and 13 Korean authorities participate.

The ARIN-AP

In November 2013, Korea established a network of asset-recovery contact points in the Asia Pacific region to improve co-operation and information exchange through training and by providing a platform for making contact. The ARIN-AP comprises 22 member states and 8 observer international organisations, with Korea's SPO serving as its secretariat.

488. The NPA's International Affairs Division co-operates with SPO ICC on international co-operation, and makes active and effective use of Interpol at a level consistent with Korea's risk and context (see Box 8.7). The NPA has 60 officers dispatched to 49 countries, including key partners, to facilitate and aid in international co-operation. The KCG has ten dispatched officers that perform the same role and

functions for the KCG, in addition to an officer posted an Interpol. The KCG is also a member of the North Pacific Coast Guard Agencies Forum, which provides a platform for co-operation and information sharing between coast guards from strategic partners (Canada, China, Japan, Korea, Russia and the U.S.).

Box 8.7. NPA co-operation through Interpol

On 19 March 2018, Corporation J made a cross-border wire transfer of KRW 4 billion (EUR 3 million) to a Bulgarian bank account after receiving emails from a person fraudulently claiming to be a client. The case was promptly reported to the NPA on 20 March 2018. On the same day, the International Affairs Division of the NPA made an urgent request via Interpol to the Bulgarian police. That evening, the Bulgarian police froze the beneficiary account and transferred the money back to Korea. Corporation J was able to recover the money the following day.

489. The KCG has experience in joint investigations, while the SPO and the NPA prefer parallel and collaborative investigations. In most cases, this is not problematic. Case studies indicated such investigations were effective and relevant information could be shared, including on a spontaneous basis. Nonetheless, Korea may wish to consider pursuing joint investigations where cases may benefit from broader information and evidence sharing (e.g. TF investigations).

490. The KCS is able to co-operate and exchange information with partner countries through multilateral channels (e.g. the World Customs Organisation), through 34 bilateral memoranda of understanding (MOUs), or under the principle of reciprocity. Korea used these mechanisms 288 times in 2017-2018, of which 219 were requests to the KCS for information. The vast majority of these requests were promptly executed with information provided. The remaining 69 cases were instances of the KCS requesting assistance from abroad. In light of the risk of asset flight (which falls within the KCS' mandate), the KCS may benefit from seeking co-operation more actively. Discussions with authorities confirmed that one of the aims of a new Illicit Asset Recovery Task Force is to strengthen and increase international co-operation in asset flight cases. The Task Force has already made active use of informal co-operation channels since its establishment in 2018 (see Box 3.13 in Chapter 3). To facilitate co-operation and information sharing, the KCS has customs attachés posted abroad.

Table 8.5. KCS information exchange with foreign counterparts

	Requests received by KCS		Requests made by KCS	
	Total requests	Requests executed*	Total requests	Requests executed*
2017	71	44	9	6
2018	148	135	60	34
Total	219	179	69	50

* In certain cases, KCS did not have available information, so had a nil response to the requesting country.

491. The NTS' International Affairs Division co-operates through a range of multilateral and bilateral agreements covering 139 countries. Korea has also implemented the OECD Common Reporting Standard Multilateral Competent

Authority Agreement that allows the automatic exchange of financial account information with 102 countries (as at 2019). The NTS noted that co-operation with certain countries can be challenging and available agreements do not always include countries frequently seen in Korea's tax crime cases which can limit the extent and utility of international co-operation.

KoFIU

492. KoFIU is able to exchange information through 69 MOUs with foreign counterparts or via the Egmont Group. KoFIU actively uses these channels to share and seek information for its own purposes or on behalf of domestic authorities. The number of requests KoFIU makes through Egmont varies dramatically from year to year (e.g. 125 in 2014 compared to 449 in 2018), but appears to be increasing (see Table 8.6). KoFIU confirmed that it is actively seeking more requests for co-operation to trace assets in support of the government's focus on asset recovery (see Chapter 3 on IO.8). Outreach to the SPO on the information available through KoFIU has also seen an increase in the SPO's use of KoFIU as a source of information from foreign jurisdictions. KoFIU is able to share information with counterparts on a spontaneous basis, although this has been rare in the past. Recent figures suggest KoFIU may be enhancing its efforts in this area and it should continue in this regard (see Table 8.6).

493. KoFIU executed requests received in a reasonably timely fashion, despite having low human resources (within 49 days on average). It has three people working on international co-operation: a division head, one international co-operation officer and one translator. This is a low number of people given the number of requests made and received by KoFIU, and the recent increase in requests. KoFIU intends to add additional translators, but may also benefit from additional analysis staff to support international co-operation. Additional resources (both analysts and translators) may also permit KoFIU to increase its spontaneous information sharing.

Table 8.6. KoFIU information exchange with foreign FIUs

	Egmont requests made by KoFIU	Egmont requests received by KoFIU	Spontaneous provision of information to KoFIU	Spontaneous provision of information by KoFIU
2014	125	65	27	0
2015	251	57	31	0
2016	174	47	25	0
2017	234	45	48	0
2018	449	69	39	7

494. KoFIU can share information it holds and obtain information for a foreign counterpart where there is a related STR, CTR, or foreign exchange report or for the purpose of its financial transaction analysis (see R.29). Where KoFIU does not hold or cannot obtain the information, KoFIU declines the request but does not systematically inform the requesting party of other channels for obtaining the requested information (e.g. seeking MLA to execute a court warrant on the institution) which may hamper the requesting countries' efforts. Feedback from delegations on Korea's international co-operation identified this as a concern.

Supervisors

495. The FSC, including KoFIU (in its supervisory capacity) and the FSS, is able to share information relevant to supervisory powers (e.g. on licensing and registration)

and can carry out joint inspections (see Box 8.8). KoFIU and the FSS have MOUs with 79 foreign counterparts and are working to expand this list. Information can be shared in the absence of a MOU on the basis of reciprocity, but may be subject to certain restrictions (e.g. privacy limitations on personal information). In practice, information sharing is generally limited to certain countries, reflective of Korea's key partners (China, Japan, the U.K. and the U.S.). Information exchanges typically relate to licensing and registration issues. Requests received are executed promptly (generally within one week) and are rarely refused. Delegation feedback on co-operation with supervisors was positive. There are also FSS officers located in major partner countries (including China, Japan, the U.K. and the U.S.) to enable closer co-operation with key partners and to follow up on outstanding requests.

Box 8.8. Co-operation between the FSS and a foreign country's supervisor

In early 2018, the FSS conducted an on-site AML/CFT inspection of a foreign branch of Korean Bank A. During the inspection, the FSS team visited the foreign country's supervisor and shared findings from the inspection of Bank A's branch. The FSS later requested that the foreign supervisor provide examination documents on foreign branches of Korean banks. Several months later, the foreign supervisor requested documents held by the FSS relating to the inspection of Bank A's branch. The FSS readily provided these documents within one week. All the requests and document exchanges were made under a bilateral MOU between Korea and the foreign country.

International exchange of basic and beneficial ownership information of legal persons and arrangements

496. Korea's experience in exchanging basic and BO information on legal persons and arrangements varies significantly across agencies. The NTS and KoFIU regularly receive requests for such information, although outgoing requests are less common. Other agencies, including supervisors, are less familiar with such requests.

497. These conclusions are based on discussions with KoFIU, the NTS, the KCS, the NPA, the KCG, the SPO, the FSS and the FSC.

498. KoFIU regularly receives requests for information on legal persons that typically include basic and BO information. Authorities estimated that 20% of requests received included requests for information on legal persons. In responding to such requests, it follows the same process as it would for a domestic request, obtaining information from a relevant FI or casino (where possible) or from company registries (see Chapter 7 on IO.5). Case studies provided by Korea and feedback from delegations suggest that basic information is more easily and readily provided than BO information, which is not always included in KoFIU's response (see Box 8.9). Nonetheless, BO information can be provided to the extent it is available in Korea (see IO.5). Outbound requests for BO information are less common, which is in line with Korea's risk profile (the misuse of legal entities is not a prevalent feature in Korea's criminal cases). Nonetheless, LEAs identified a growing use of complex corporate structures, the offshore corporate structures and foreign trusts in ML, tax crime and

asset flight cases, and Korea should ensure BO information is pursued in such cases (see Chapter 3 on IO.7 and Chapter 7 on IO.5).

Box 8.9. KoFIU response to request for information on legal persons

Country A was investigating a case of potential ML involving a company suspected of illegally exported beer to Country B via Country C, in breach of Country A's prohibitions on exporting goods to Country B. Proceeds were transferred to accounts in Korea and Country C. The FIU of Country A asked KoFIU for information on the suspect company and their trade counterparts. In response, KoFIU was able to provide information on the suspect company, including basic information (the name, registration number, date of establishment, representative, contact, and address). Korea did not provide BO information.

499. The NTS also commonly receives requests for information on companies linked to tax collection or tax crime. The NTS deals with such requests in the same manner as domestic requests, using the NTS register to identify basic and legal ownership information (see Chapter 7 on IO.5). The NTS stated that it would generally not make requests for BO information. Instead, it would request basic company information, make its own domestic inquiries to identify the individual believed to be the beneficial owner, and then request information on this person. In such cases, a parallel request for BO information may be useful to confirm or cross-check the information detected by the NTS.

500. Other agencies were not familiar with requests for BO information. The MoJ, the SPO and the FSS stated they had received no such requests.

501. No agency had experience seeking or providing basic or BO information on trusts. This is largely consistent with Korea's risk profile, although LEAs did note the use of foreign trusts in ML and tax crime cases that may necessitate outgoing requests for information on these structures.

Overall conclusions on IO.2

502. **Korea is rated as having a substantial level of effectiveness for IO.2.**

TECHNICAL COMPLIANCE ANNEX

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.

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 2009. This report is available here.

Recommendation 1 – Assessing risks and applying a risk-based approach

Criterion 1.1 – Korea identifies and assesses its ML/TF risks through its NRA process. While there is no regulatory requirement to undertake a NRA, three NRAs have been published to date in 2014, 2016 and November 2018. There is an informal government consensus to update the NRA every 2-3 years. The 2018 NRA was developed over a twenty-month period using qualitative and quantitative information from a range of sources and involving most relevant agencies and stakeholders, including the private sector. The 2018 NRA identifies nine major ML/TF risks.[58]

Criterion 1.2 – The AML/ CFT Policy Co-ordination Committee is responsible for co-ordinating Korea's actions to assess its ML/TF risks (*Regulations on the Establishment and Operation of the AML/CFT Policy Co-ordination Committee, etc.*, arts.3, 5). The 2018 NRA is a product of this Committee. The Committee consists of 12 relevant agencies chaired by the Commissioner of KoFIU.[59] Five sub-committees exist at the working-level to implement the Committee's decisions in relevant areas (policy implementation, law enforcement, supervision, NPOs, and private sector consultation) (*Regulations on the Establishment and Operation of the AML/CFT Policy Co-ordination Committee, etc.*, art.9). The AML/CFT Policy Co-ordination Committee reports to Cabinet and a National Counter-Terrorism Committee (a committee of 21 Ministers led by the Prime Minister, which is responsible for assessing and co-ordinating Korea's response to TF (*Anti-Terrorism Act*, art.5)).

Criterion 1.3 – Korea has kept its ML/TF risk assessments up-to-date. Since 2014, three NRAs have been conducted at regular two-year intervals (2014, 2016 and 2018). The 2018 NRA is the most thorough in terms of scope and input from relevant agencies and stakeholders. These are supplemented by regular meetings of the committees responsible for ML/TF risk assessment which discuss ongoing developments in Korea's ML/TF risks.

58. Seven of these risks relate to predicate offences: tax crime, illegal gambling, financial fraud, corruption, unfair trading, asset flight and embezzlement. The other two risks relate to high-risk vulnerabilities: the abuse of cash transactions and virtual assets.

59. KoFIU, the MOJ, Ministry of Economy and Finance, the MFA, the NIS, the National Election Commission, the SPO, the NPA, the NTS, the KCS, the KCG, and the FSS.

Criterion 1.4 – Korea has mechanisms to provide information on the results of its risk assessments to relevant public and private sector agencies and entities. All three NRAs were published online.[60] The 2018 NRA is an official government document and was reported to Cabinet upon completion in November 2018. It was shared with relevant public sector institutions through the AML/CFT Policy Co-ordination Committee and with supervisory entities through its sub-committee, the Inspection Agencies Committee. It was also shared with 635 representatives of FIs and casinos through six seminars between December 2018 and February 2019. Sharing mechanisms were also in place for the 2014 and 2016 NRAs, although to a more limited extent.

Risk mitigation

Criterion 1.5 – Korea largely applies a risk-based approach to allocating resources and implementing AML/CFT measures, although measures tend to be general (rather than responding to specific risks) and actions are particularly limited for TF risks. In 2014, following the first NRA, Korea formulated the *AML/CFT System Development Strategy*, which set out a three-phase work programme from 2014 to 2016 to respond to the identified risks. Specific measures in response to the 2014 NRA included: providing LEAs with broader access to KoFIU information, enhancing KoFIU human resources, establishing a Capital Markets Investigation Unit within the FSC, and assigning KRW 12 billion to develop an AML/CFT risk assessment framework for the private sector.

Following the 2016 NRA, the *AML/CFT System Development Strategy* was reviewed by a working-level Joint Task Force for Mutual Evaluation which was established based on key principles including prioritising vulnerabilities. The Task Force identified seven areas of focus aimed more closely on improving compliance with the FATF Standards than addressing the specific risks identified in the 2016 NRA.

The areas of focus of the *AML/CFT System Development Strategy* were reviewed again after the 2018 NRA. KoFIU identified three key tasks to best respond to the risks identified in the 2018 NRA: building an advanced AML/CFT Framework, efficient use of financial information, and capacity building in the private sector. These tasks are very high-level and general. Nonetheless, practical measures have been taken to respond to certain identified risks, including: increasing FSS supervisory staff to improve inspections of the mutual finance sector; lowering the CTR threshold; and increasing LEA resources for tracing criminal proceeds, undertaking TF investigations, and investigating high risk proceeds-generating offences (such as tax crime and illegal gambling). Activities are largely focused on ML risk with more limited action in response to identified TF risks.

Criterion 1.6 – Korea has not imposed the FATF Recommendations on DNFBPs, except for casinos.

(a) The lack of coverage of DNFBPs is not based on a proven low risk.

(b) (Not applicable) No financial activity is exempted.

Criterion 1.7 – FIs and casinos are required to apply EDD when conducting business listed as high risk under the categories of country, customers, products or services (*AML/CFT Reg.*, arts.29-31, 106-109) in order to manage and mitigate risks. FIs and

60. The 2014 and 2016 NRAs are available at www.prism.go.kr. The 2018 NRA is available at: www.fsc.go.kr/info/ntc_news_view.jsp?bbsid=BBS0030&page=2&sch1=subject&sword=&r_url=&menu=7210100&no=32811 and www.kofiu.go.kr/index.jsp.

casinos must do a risk assessment of a customer relationship and apply EDD for high risk customers which are not listed as high risk in arts.29-31 and 106-109 of the *AML/CFT Regulation*, but present a high risk (*AML/CFT Reg.*, arts.56, 122).

Criterion 1.8 – FIs and casinos are allowed to apply SDD for customers, products or services assessed as low risk for ML/TF in arts.29-31, 106-109 of the *AML/CFT Regulation* (*AML/CFT Reg.*, arts.20(2), 102(2)). Additionally, FIs and casinos are allowed not to verify the identity of the ultimate owner or controller of the following: the state or a local government; an exhaustive list of public organisations; other financial companies, etc. (excluding casino operators and persons identified as high risk of ML/TF by the KoFIU), and; a corporation which shall submit and annual report pursuant to art.159(1) of the *Financial Investment Services and Capital Markets Act* (*Enforcement Decree of the FTRA,* art.10-5(5)). All exemptions are based on a proven low risk.

Criterion 1.9 – KoFIU and the entrusted agencies (see Chapter 1, para.84) are designated to ensure that FIs and casinos implement their obligations under R.1, and have powers to do so.

Risk assessment

Criterion 1.10 – FIs and casinos are required to take steps to identify, assess and understand their ML/TF risks for customers, countries or geographic areas, and products, services, transactions or delivery channels (*FTRA,* art.5; *AML/CFT Reg.*, art.19). This includes requirements to: (a) document the risk assessment; (b) consider all relevant risk factors; (c) keep the assessments up-to-date; and (d) have appropriate mechanisms to provide risk assessment information to the KoFIU or entrusted agencies.

Risk mitigation

Criterion 1.11 – FIs and casinos are required to:

(a) have policies, controls and procedures, which are approved by management (although not senior management as is required), to enable them to mitigate the risks that they have identified;

(b) have independent audits, and monitor compliance with internal policies, control and procedures of risk management and risk mitigation controls, including enhancing these if necessary (*AML/CFT Reg.*, art. 19(2)); and

(c) apply EDD in situations where there is an increased risk for ML/TF, including management and mitigation of the risks identified (refer to c.1.7).

Criterion 1.12 – FIs and casinos are allowed to apply SDD for lower risks customers, services and products (refer to c.1.8). FIs and casinos are not allowed to conduct SDD if a transaction is suspicious or poses an increased risk for ML or TF (*AML/CFT Reg.*, art.20).

Weighting and Conclusion

Korea has implemented the main aspects of R.1, with only three deficiencies, which have been assessed minor in the Korean context:

(a) The approach to allocating resources and implementing AML/CFT measures does not specifically respond to risk, and actions are particularly limited for TF risks.

(b) FIs and casinos are not required to have their AML/CFT policies, controls and procedures approved by senior management (only management level approval is required).

(c) Korea's AML/CFT measures have a scope issue, as they do not apply to DNFBPs, except for casinos. In the Korean context, the non-covered DNFBPs have been given less weight than other sectors which are more important, both materially and in terms of risk (see Chapter 1, para.78).

Recommendation 1 is rated largely compliant.

Recommendation 2 - National co-operation and co-ordination

In its 3rd MER, Korea was rated largely compliant with requirements on national co-operation and co-ordination. The main technical deficiency was limited feedback from KoFIU to supervisory authorities. Several of the main co-ordination bodies continue to operate, but some co-operation mechanisms have changed and new developments have occurred since 2009.

Criterion 2.1 – Korea's national AML/CFT policy is set by the AML/CFT Policy Co-ordination Committee. The strategy is based around three key tasks, with the overarching goals of building "a transparency and credible society". Korea's AML/CFT strategies are regularly reviewed, but are not always clearly informed by identified risks. An *AML/CFT System Development Strategy* set out a work programme for 2014-2016 to respond to risks identified in the first NRA. This was updated following the 2016 NRA and seven areas of focus were identified, but these relate more to improving compliance with the FATF Standards than the risk areas identified in the NRAs. These areas of focus were further refined in response to the 2018 NRA and narrowed to three key tasks which are broadly framed and do not strictly respond to the identified risks. See c.1.5 for further details.

Criterion 2.2 – The FSC has authority for AML/CFT policies, although in practice much of this authority is delegated to KoFIU which is housed within the FSC (*PFOPIA*, art.3). AML/CFT policies are co-ordinated through the AML/CFT Policy Co-ordination Committee which reports to Cabinet and the National Counter-Terrorism Committee on TF matters (*Anti-Terrorism Act*, art.5).

Criterion 2.3 – The AML/CFT Policy Co-ordination Committee and its sub-committees provide a mechanism for co-operation between relevant AML/CFT authorities, including policy-makers (the MOJ, the Ministry of Economy and Finance, the MFA), KoFIU, LEAs (the NIS, the National Election Commission, the SPO and other prosecutors' offices, the NPA, the NTS, the KCS, the KCG, and the FSS), and supervisors (the FSS, KoFIU and entrusted agencies). Five working-level sub-committees promote co-operation and information-sharing at the operational level (Policy Implementation Committee, LEAs Committee, Inspection Agencies (i.e. supervisors) Committee, Private Sector Consultation Committee, and NPOs CFT Agencies Committee)

(*Regulations on the Establishment and Operation of the AML/CFT Policy Co-ordination Committee, etc.*, art.9; *Regulations on the Examination of Financial Institutions' AML/CFT Activities*, art.29). The National Counter-Terrorism Committee reviews and takes decisions on TF policies (see c.1.2). KoFIU also provides a practical forum for co-operation as it comprises secondees from ten other agencies.

Criterion 2.4 – Korea does not have a standing mechanism to ensure general domestic co-operation and co-ordination on PF at either the policymaking or operational levels. Such co-operation may occur through the AML/CFT Policy Co-ordination Committee, although this is not its central role. *Ad hoc* reactionary meetings are also held when issues arise.

Criterion 2.5 – Korea has co-operation and co-ordination mechanisms in place to ensure AML/CFT requirements comply with data protection and privacy rules. The FSC is the competent authority for both AML/CFT and data protection which facilitates co-operation between the relevant units (KoFIU, the Financial Industry Bureau, and the Financial Innovation Bureau). Korea also operates a Personal Information Protection Commission which co-ordinates privacy policy and ensures compliance with data protection rules. This includes reviewing AML/CFT legislation for consistency with privacy requirements. The FSC seconds staff to the commission.

Weighting and Conclusion

Korea has a framework for national co-operation and co-ordination which is broadly in line with the FATF Standards. Only two minor deficiencies remain. First, Korea's AML/CFT strategies are not always clearly informed by identified risks. Second, there is no standing mechanism to ensure general domestic co-operation and co-ordination on PF at the policymaking or operational levels (although co-operation and co-ordination may occur through the AML/CFT Policy Co-ordination Committee or *ad hoc* meetings).

Recommendation 2 is largely compliant.

Recommendation 3 - Money laundering offence

In the 3rd round, Korea was rated largely compliant with the requirements on the ML offence due to gaps in the coverage of designated predicate offences (terrorism, TF, and environmental crimes were not predicate offences and an inadequate range of copyright and fraud offences were included) and the limited availability of conspiracy in ML cases. Korea was rated partially compliant with the ML offence sanction requirements on the basis that sanctions for legal persons were not sufficiently effective and dissuasive and the sanctions imposed on natural persons were not effectively implemented. Since 2009, Korea has amended its ML offence and FATF revised its Standards to make some tax offences predicate offences for ML.

Criterion 3.1 – Korea criminalises ML through several offences: general ML and receiving offences under the *Proceeds of Crime Act* (*POCA*, art.3(1)) and specific ML and receiving offences for the proceeds of drug trafficking (*Act on Special Cases Concerning the Prevention of Illegal Trafficking in Narcotics* (*ASPIT*), art.7). These offences are consistent with the Vienna and Palermo Conventions and cover converting, transferring, disguising or concealing the nature, location, acquisition, disposition, or origin of criminal proceeds, and the acceptance of criminal proceeds. The 'possession' or 'use' of criminal proceeds are not explicitly criminalised, but are covered through the broad interpretation of 'acceptance' (Supreme Court

#2005DO3045; *Interpretive Note to POCA*). The specific offence for ML relating to drug trafficking includes a purposive element; however, this requires only proof of knowledge that the laundered property was criminal proceeds, which is in line with the Conventions (Supreme Court #2008DO10004).

Criterion 3.2 – The predicate offences for ML cover most serious offences and most relevant offences in each of the FATF Standard's designated categories of offences. The scope of predicate offences has been extended to include TF offences, environmental crime, breach of trust, aggravated embezzlement, and copyright offences (*POCA*, art.2). However, only a very limited range of tax offences (claiming false tax rebates over KRW 500 million (EUR 381 250)) are included despite Korea's identification of tax crime as its highest-risk proceeds-generating offence. The majority of tax crimes are not included as a predicate offence.

Criterion 3.3 – Korea does not apply a threshold approach.

Criterion 3.4 – Korea's ML offences apply to "property" generated, directly or indirectly, from offending (*POCA*, art.2; *ASPIT*, art.2). "Property" is interpreted broadly to cover all benefits with economic value in society including assets of all kinds, corporeal and incorporeal, moveable and immoveable, tangible and intangible (Supreme Court #2018DO3619; Suwon District Court #2017NO7120). There is an inconsistency in terminology between the two ML offences: the *POCA* ML offence applies to the laundering of "criminal proceeds" (*POCA*, art.2) while the specific drug trafficking ML offence applies to the laundering of "illegal profits"; however, both terms are defined with reference to "property".

Criterion 3.5 – It is not necessary that a person be convicted of a predicate offence to prove that property is the proceeds of crime (Supreme Court #2006DO5288).

Criterion 3.6 – Both ML offences extend to predicate offences committed outside of Korea provided the predicate offence was an offence in both Korea and the foreign country (*Criminal Act*, art.3; *POCA*, art.2(1); *ASPIT*, art.12).

Criterion 3.7 – Both ML offences apply to any person, including those who commit the predicate offence (Supreme Court #2004DO5652; Supreme Court #2005DO6079).

Criterion 3.8 – The *mens rea* of the ML offences (knowledge that the laundered property is the proceeds of crime) can be inferred from objective factual circumstances (Supreme Court #2005DO2709).

Criterion 3.9 – The sanctions for the ML offences are broadly in line with the sanctions for similar offences in Korea; however, they are too low to be sufficiently dissuasive, particularly the available monetary sanctions. The *POCA* ML offence (and its attempt) is punishable by 5 years of imprisonment or a fine of KRW 30 million (EUR 23 500) or both (*POCA*, art.3). The specific drug trafficking ML offence (and its attempt) is punishable by 7 years of imprisonment or a fine of KRW 30 million (EUR 23 500) or both (*ASPIT*, art.7).

Criterion 3.10 – Legal persons can be liable for ML where the legal person's negligence resulted in an employee, representative or agent committing the offence (*POCA*, art.7; *ASPIT*, art.18). The legal person's liability will not prejudice the liability of the natural person (Supreme Court #87DO1213). The fines available are the same as for natural persons (a fine of up to KRW 30 million (EUR 23 5000)). These sanctions are too low to be proportionate or dissuasive.

Criterion 3.11 – A range of ancillary offences are available for ML, including participation in (*Criminal Act*, art.30), conspiracy (*POCA*, art.3(3); *ASPIT*, art.7(3)), attempt (*POCA*, art.3(2); *ASPIT*, art.7(2)), aiding and abetting (*Criminal Act*, art.32), and inciting (*Criminal Act*, art.31).

Weighting and Conclusion

Korea criminalises ML in a manner broadly in line with the FATF Standards, however, minor deficiencies remain. The range of tax offences included as predicate offences is too narrow. This is weighted more heavily given Korea's identification of tax crime as a high-risk proceeds-generating offence. The sanctions for ML for both natural and legal persons are too low to be sufficiently dissuasive (or proportionate for legal persons), although this deficiency is considered minor as, in Korea's context, criminal sanctions often tend to be relatively low for financial and other types of crimes.

Recommendation 3 is largely compliant.

Recommendation 4 - Confiscation and provisional measures

In its 3rd MER, Korea was rated partially compliant with the confiscation requirements. In addition to effectiveness deficiencies, the main technical compliance deficiency was that confiscation powers were not available for the ML offences where the predicate offence was terrorism, TF, or environmental crime (due to scope issues with the ML offence). Since this time, Korea has expanded the scope of its ML offence although the range of tax offences covered remains limited (see R.3).

Criterion 4.1 – Korea has measures that enable confiscation of the following provided that a conviction is obtained in relation to the offending:

(a) Laundered property (*POCA*, art.8(1) para.1; *ASPIT*, art.13(1) para.1);

(b) Direct or indirect proceeds of offending or instrumentalities used or intended for use in ML or predicate offences (*POCA*, art.8(1) para.2-5; *ASPIT*, art.13(1) para.2-5l; *Criminal Act*, art.48(1));

(c) Property that is the proceeds of, or used in, or intended for use in TF or terrorism offences (*POCA*, art.8(1) para.2-5; *Criminal Act*, art.48(1));

(d) Property of corresponding value (*POCA*, art.10(1); *ASPIT*, art.16(1); *Criminal Act*, art.48(2)).

Property may be confiscated from third parties provided the parties had knowledge that the property was criminal proceeds (*POCA*, art.9(1); *ASPIT*, art.15(1); *Criminal Act*, art.48(1)). Property can include any benefit with economic value in society, including virtual assets (Supreme Court #2018DO3619; Suwon District Court #2017NO7120). Korea is not able to exercise its confiscation powers for ML offences relating to most cases of tax crime (due to the limited scope of the ML offence, see R.3), but would be able to confiscate the proceeds of this offending on the basis of a conviction for the proceeds-generating conduct, which is criminalised.

Criterion 4.2 – Korea has some measures in place to enable its competent authorities (specifically the SPO, the DPOs and branch prosecutors' offices) to:

(a) Identify, trace and evaluate property subject to confiscation through search, seizure and inspection orders, demands for documents or information, and orders

for financial, transaction, or taxation information, all of which are available with a warrant (*Criminal Procedure Act*, art.215; *POCA*, art.10(3)).

(b) Obtain a preservation order to prevent the disposal of property subject to confiscation (*ASPIT*, arts.33, 34; *POCA*, art.12).

(c) Void actions that would prevent the seizure or confiscation of property subject to a preservation order (*ASPIT*, art.36; *POCA*, art.12). Even if the property is not subject to a preservation order, if it is knowingly transferred to a third party, a confiscation order may be imposed on the third party. If the third party acquires the property rights unknowingly, value-based confiscation can be pursued against the offender.

(d) Take other investigative actions as set out in R.31.

Criterion 4.3 – A third party's rights to property subject to confiscation are protected provided the third party acquired the rights before commission of the relevant offence or unknowingly acquired the rights after commission of the offence (*POCA*, art.9(2); *ASPIT*, art.15(2)).

Criterion 4.4 – Money acquired through confiscation is transferred to the Treasury. Physical assets are maintained and auctioned by the relevant prosecutors' office or, for assets confiscated in value, by the Korea Asset Management Corporation. Auction proceeds revert to the Treasury.

Weighting and Conclusion

All criteria are met.

Recommendation 4 is compliant.

Recommendation 5 - Terrorist financing offence

In the 2009 MER, Korea was rated partially compliant with these requirements. The key technical deficiencies were: the TF offence did not adequately cover provision/collection of funds for an individual terrorist or terrorist organisation; TF was not a predicate offence for ML; and conspiracy to commit TF was only available where the TF offence was committed. Since this time, Korea has amended its TF offence, passed the *Anti-Terrorism Act 2016*, and expanded the scope of its ML offence. The requirements have also been updated to cover foreign terrorist fighters (FTFs).

Criterion 5.1 – Korea's TF offence largely criminalises TF on the basis of the TF Convention. The TF offence covers directly or indirectly providing or raising property or funds with the intention they should benefit an individual, corporation or organisation, being aware that this individual, corporation or organisation performs or intends to perform a terrorist act (*PFOPIA*, art.5-2(1)). 'Benefit' has been interpreted broadly by the courts and does not require a clear or specific intent (Supreme Court #82DO1450). A terrorist act covers a range of violent acts, including those covered in the treaties listed in the annex to the TF Convention. Under Korea's offence, a terrorist act must be committed for the purposes of interfering with a state, local, or foreign government or international organisation exercising its right, forcing it to perform an act, or threatening or endangering the public (*PFOPIA*, art.2(1)). While this intent may be proved by inferring from the circumstances, this nonetheless is an additional mental element which goes beyond art.2(1)(a) of the TF Convention. Korea's constitution also allows the direct application of treaties, although this has not been tested in a criminal case (*Constitution*, art.6(1)).

Criterion 5.2 – Korea's TF offence covers providing funds or property, directly or indirectly, with the intention that they should be used to carry out a terrorist act or provided to a terrorist organisation or individual terrorist for any purpose (*PFOPIA*, art.5-2(1)) The indirect collection of funds is not clearly covered. While the offence does not explicitly cover the provision or collection of funds in full *or in part* for the benefit of the terrorist(s), there is nothing in the legislation to suggest this restriction would be read into the text. Similarly, while "property" is not defined, under Korean law is understood and regularly used to cover all movable and immovable assets (see c.3.4 and c.4.1).

Criterion 5.2bis – Korea's TF offence covers financing for the benefit of an individual or group that intends to commit terrorist acts (*PFOPIA*, art.5-2(1)). While Korea does not explicitly cover the conduct outlines in c.5.2bis, "benefit" has been interpreted broadly (see c.5.1) meaning this conduct is likely covered. However, the offence has not been tested in practice.

Criterion 5.3 – Korea's TF offence extends to "funds" and "property" (*PFOPIA*, art.5-2(1)). These terms are interpreted broadly to cover all assets regardless of their source.

Criterion 5.4 – Korea's TF offence does not require that the funds or property were actually used to carry out or attempt a terrorist act, or were linked to a specific terrorist act. It is sufficient that the property was for the purpose of benefiting a person or group that performs or intends to perform a terrorist act (*PFOPIA*, art.5-2(1)).

Criterion 5.5 – Korea's legal principles allow intent to be proved through indirect or circumstantial facts (Supreme Court #2016DO15470).

Criterion 5.6 – The TF offence is punishable by up to 10 years of imprisonment with labour or a fine of KRW 100 million (EUR 78 000) (*PFOPIA*, art.6(1)). Attempting or aiding and abetting TF is subject to the same penalty, although the sentence may be mitigated by half (*Criminal Code*, art.25(2)). Conspiracy to commit TF is penalised by three years of imprisonment or a fine of up to KRW 30 million (EUR 23 500) (*PFOPIA*, art.5). While the fines are low, the imprisonment penalties ensure the penalties are proportionate and dissuasive.

Criterion 5.7 – Legal persons can be liable for TF where the legal person's negligence resulted in an employee, representative or agent committing the offence (*PFOPIA*, art.6(7)). The legal person's liability will not prejudice the liability of the natural person. The fines available are the same as for natural persons (a fine of up to KRW 100 million (EUR 78 000)). These sanctions are too low to be proportionate or dissuasive.

Criterion 5.8 – It is an offence under Korean law to:

(a) attempt to commit the TF offence (*PFOPIA*, art.6(4));

(b) participate in a TF offence or attempted offence (*Criminal Act*, arts.30, 32);

(c) organise or direct other to commit a TF offence or attempted offence (*Criminal Act*, art.31); and

(d) contribute to the commission of one of more TF offence(s) or attempted offence(s) by a group of persons with a common purpose (*PFOPIA*, art.6(5)).

Criterion 5.9 – Korea's TF offence is designated as a predicate offence to ML (*POCA*, art.2(2); *PFOPIA*, arts.6(1), (4)).

Criterion 5.10 – The TF offence applies regardless of the location of the financer or the terrorist/terrorist organisation (*PFOPIA*, art.5-2). Standard jurisdictional rules apply meaning there must be some connection between the TF offence and Korea (i.e. Korea does not have universal jurisdiction).

Weighting and Conclusion

Korea criminalises TF, but there are several minor deficiencies. The offence incorporates an additional mental element which goes beyond the TF Convention. Until the offence is tested in practice, it cannot be confirmed that it clearly covers the indirect collection of funds or the financing of FTFs which are minor deficiencies. The FTF issue is given less weight in Korea's unique risk context because it has not yet had any FTFs.[61] The sanctions for legal persons are not proportionate or dissuasive, which is a deficiency, but is given less weight as Korea's TF risk profile is largely focussed on individual activity (which would be subject to adequate sanctions).

Recommendation 5 is largely compliant.

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

In its 3rd MER, Korea was rated partially compliant with these requirements on the basis of the following technical deficiencies: lack of requirement to freeze terrorist funds (only restriction of transactions); not all funds are required to be frozen; and not all natural and legal persons are required to freeze assets.

Criterion 6.1 – For designations under UNSCRs 1267/1989 and 1988 (UN "sanctions regime"):

(a) The MFA is the competent authority for proposing designations to the 1267/1989 Committee and 1988 Committee.

(b) The FSC is responsible for deeming whether an individual, legal person or entity is related to any of the terrorist activities set out in art.2(a) of PFOPIA and meets the other conditions for designation set out in art.4 of *PFOPIA*. Where the FSC intends to propose a designation, it shall obtain prior consent of the Minister of Strategy and Finance, the Minister of Foreign Affairs and the Minister of Justice (*PFOPIA*, art.4(2)). Where prior consent is not obtained, it must obtain their consent within 48 hours of the designation or else the designation will lose its effect (*PFOPIA*, art. 4(3)). Additionally, Korea has an explicit mechanism for identifying targets for designation (*PFOPIA* art. 4(8)).

(c) An evidentiary standard of proof of "reasonable basis" is applied when deciding whether or not to make designations (*Administrative Procedures Act*, arts.4(1), 23(1)). Proposals for designations are not conditional upon the existence of a criminal proceeding.

(d) The FSC follows the procedures and standard forms for listings as adopted by the relevant Committee (1267/1989 or 1988 Committee).

61. Korea's NRA identifies 16 individuals who once been in Korea but in each of those cases, the individuals status as a foreign terrorist fighter (FTF) arose well after the individual had ceased to be in Korea.

(e) A request for listing is accompanied by as much relevant information as possible on the proposed name, including: date of birth; identity; passport/national ID number; terrorist organisation affiliation; violation of international law/UNSCR; active years; affiliated terror attacks/TF; active region; Interpol co-operation; statement of case and (in the case of proposing names to the 1267/1989 Committee), specify whether their status as a designating state may be made known.

Criterion 6.2 – Korea implements designations pursuant to 1373 through national mechanisms set out in the *PFOPIA*, as follows:

(a) The FSC is the competent authority for making designations pursuant to UNSCR 1373 as put forward on Korea's own motion (*PFOPIA* art. 4). This extends to examining and giving effect to, if appropriate, the request of another country.

(b) When the FSC receives information on restricted persons from relevant agencies such as the NPA, the NIS and the SPO, or from foreign countries through the MFA, it determines whether the designation criterion in UNSCR 1373 is met. Where necessary, the FSC may request further co-operation, material or opinions from those parties (*PFOPIA*, art. 4(8)).

(c) When receiving a request for designation the FSC consults the Ministry of Finance and Economy, MOJ and MFA, to determine whether they are satisfied that the request is supported by a reasonable basis to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373. In cases of emergency, where the FSC receive requests through the MFA, the FSC has the ability to immediately make the determination and designate, if the request is supported, and obtain a post-designation agreement. The designation takes effect when the updated *Designation of Persons Subject to Restrictions on Financial Transactions, etc.* (the *Designation Notice*) is posted on the FSC's and KoFIU webpages which is done immediately upon designation. The Ministry of Government Legislation is subsequently notified to reflect the amendments in the National Law Information Centre.

(d) An evidentiary standard of proof of "reasonable basis" is applied when deciding whether or not to make designations (*Administrative Procedures Act*, arts.4(1), 23(1)). Proposals for designations are not conditional upon the existence of a criminal proceeding.

(e) When requesting another country to give effect to the actions initiated under the freezing mechanism, Korea is able to provide identifying information and specific information supporting the designation, including personal information (*Personal Information Protection Act*, art.18(2)(6)).

Criterion 6.3 –

(a) The FSC, as the competent authority for making designations, has the legal authority to collect and solicit information when necessary to designate a person (*PFOPIA*, art.4(8)).

(b) The FSC has legal authority and mechanisms to operate *ex parte* against a person or entity who has been identified and whose (proposal for) designation is being considered. This stems from the FSC's authority to act *ex parte* when an urgent disposition is necessary for the safety and welfare of the general public or where reasonable grounds exist to acknowledge that hearing of an opinion is highly impractical or clearly unnecessary in view of the nature of the relevant disposition (*Administrative Procedures Act*, art.21(4)1, 3).

Criterion 6.4 – Korea implements TFS without delay. Designations by United Nations Security Council (UNSC) Committees, including pursuant to UNSCRs 1267 (1999), 1989 (2011), 2253 (2015) and 1988 (2011), are immediately effective in Korea. The legal basis is the *Designation Notice* which applies immediately by referring to any person designated by a UNSC Committee or pursuant to these UNSCRs. Likewise, designations pursuant to UNSCR 1373 are given effect without delay by posting an updated *Designation Notice* on the webpages of the FSC and KoFIU. Korea then subsequently notifies the Ministry of Government Legislation so the amendments may be reflected in the National Law Information Centre.

Criterion 6.5 – The FSC is the competent authority for implementing TFS in Korea. The following standards and procedures apply to implementing and enforcing TFS:

(a) FIs and casinos[62] are prohibited[63] from undertaking "financial transactions" (which is broadly defined under the *Financial Transactions Reporting Act*, art.2) with a designated person (*PFOPIA*, art.5(1)). Additionally, all natural and legal persons are prohibited from providing transfers, gifts, etc. of movable assets, immovable assets, bonds, or other property or property rights, and other acts of disposal (the TF offence; *PFOPIA*, art.5-2). Together, these comprehensive prohibitions effectively create a freezing obligation that meets the definition of "freeze" according to the FATF Standards, as they prohibit the transfer, conversion, disposition, or movement of any funds or other assets that are owned or controlled by designated persons or entities, including proceeds of these funds or other assets. Since they also require the entity to immediately refrain from performing any action, the "freeze" applies without delay and without prior notice. However, DNFBPs (other than casinos) are not required to implement the freezing obligation, as the TFS-specific prohibition to provide financial transactions does not apply to them, only the general prohibition (i.e. TF offence) does.

(b) The freezing obligation (see c.6.5(a)) covers (i) all funds and other assets that are owned or controlled by the designated person or entity (not just those that can be tied to a particular terrorist act, plot or threat). However, it does not extend to (ii) funds and other assets which are indirectly owned or controlled by listed natural and legal persons, including joint ownership, or (iii) funds or other assets derived or generated therefrom, as well as (iv) funds and other assets of other persons and entities acting on behalf, or at the direction, of designated persons.

(c) All natural and legal persons in Korea are prohibited from making funds and other assets, economic resources, or financial services available to an individual, legal person or entity (*PFOPIA*, art.5-2) (the TF-offence). However, this prohibition does not refer to designated persons and entities, and does not extend to funds and other assets made available indirectly or controlled jointly or by entities acting on behalf, or at the direction, of designated persons. Korea does, however, criminalise any person and entity knowingly providing funds and other assets to designated persons and entities, which applies to FIs, DNFBPs and any other person (*PFOPIA*, arts. 4, 6(2)3). However, by requiring "knowledge" these provisions are not adequately implementing TFS which should be implemented unconditionally.

(d) Korea has several mechanisms in place to communicate designations to FIs and casinos. Designations pursuant to UNSCR 1373 are communicated through the *Public Notice*. Other designations are communicated through the official gazette, and also

62. "Financial institutions etc." is defined in the FTRA art.2(1). This definition covers casinos, but not other DNFBPs.
63. "Restriction" is the term used in the Korean legislation.

posted on the webpages of the National Law Information Centre (www.law.go.kr) and Korea FIU (www.kofiu.go.kr) for reference. Additionally, such designations are notified through email to financial sector and casino associations which distribute the information to their members. However, there is no mechanism in place to communicate designations to DNFBPs other than casinos. Moreover, no clear guidance is provided to FIs and casinos that might be holding targeted funds or other assets, on their obligation to take action under the restricted transactions mechanism.

(e) FIs and casinos are required to report to competent authorities any actions taken to comply with the freezing obligation and prohibitions relating to the relevant UNSCRs (*PFOPIA*, art. 5(2); *FTRA*, art.4(1)-3), which includes attempted transactions. No requirements apply to other DNFBPs.

(f) Measures are in place to protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under R.6 (*PFOPIA*, art. 6(7)).

Criterion 6.6 – The following de-listing, unfreezing and access procedures apply:

(a) The procedures to submit de-listing requests to the relevant UN Sanctions Committee in the case of designated persons and entities who do not or no longer meet the criteria for designation pursuant to UNSCR 1267/1989 or UNSCR 1988 are provided in the *Designation Notice*.

(b) The procedures and mechanisms to de-list or unfreeze the funds or other assets of persons and entities designated pursuant to UNSCR 1373 that no longer meet the criteria for designation are listed in the *Designation Notice*.

(c) For designations pursuant to UNSCR 1373, where an objection to the designation has been denied by the FSC, a request for review of the designation decision can be filed as an administrative lawsuit to the court.

(d) The procedures to facilitate review by the 1988 Committee for designations pursuant to UNSCR 1988, in accordance with any applicable guidelines or procedures adopted by the 1988 Committee, including those of the Focal Point mechanism established under UNSCR 1730, are listed in the *Designation Notice*.

(e) For designations on the Al-Qaida Sanctions List, the procedures for informing designated persons and entities of the UN Office of the Ombudsperson pursuant to UNSCRs 1904, 1989 and 2083 to accept de-listing petitions are listed in the *Designation Notice*.

(f) The *Designation Notice* includes procedures to unfreeze the funds or other assets of persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), upon verification that the person or entity involved is not a designated person or entity.

(g) The same mechanisms are used for communicating listings and de-listings to FIs and casinos (see analysis under c.6.5(d)). No specific guidance has been provided to FIs or casinos on their obligations to respect a de-listing or unfreezing action. There is no mechanism in place to communicate designations to DNFBPs other than casinos.

Criterion 6.7 – The FSC can authorise prohibited financial transactions (as defined in *FTRA*, art.2) subject to TFS on a case-by-case basis for purposes prescribed by law (*Enforcement Decree of the PFOPIA*, art.2(3)) in accordance with the procedures set out in UNSCR 1452. The same procedure applies to designations pursuant to UNSCR 1373.

Weighting and Conclusion

Korea has a regime for implementing TFS, but there are moderate shortcomings. The most serious is that the freezing obligation does not extend to DNFBPs other than casinos. The freezing obligation (for FIs and casinos) and the general prohibition (for all natural and legal persons) do not apply to funds and other assets indirectly owned or controlled (including joint ownership) or where persons or entities act on behalf of or at the direction of designated persons, and the additional measure, for criminalising all natural and legal persons providing funds and other assets, is conditional upon a level of knowledge. There is no mechanism in place to communicate designations, delistings and unfreezings to DNFBPs other than casinos. No guidance has been issued to FIs and DNFBPs on how to meet their TFS obligations or specifically on respecting delisting or unfreezing actions.

Recommendation 6 is partially compliant.

Recommendation 7 – Targeted financial sanctions related to proliferation

This is a new Recommendation which was not assessed in Korea's 3rd MER

Criterion 7.1 – Korea implements proliferation-related TFS without delay. The relevant legal framework consists of the *PFOPIA* and the *Designation Notice* which is its enforcement rule (public notice). The TFS of the *PFOPIA* apply to all designated individuals, legal persons and entities. The *Designation Notice* applies immediately by reference to all persons designated by the UNSC pursuant to, *inter alia*, UNSCRs 1718(2006) on DPRK and 2231(2015) on Iran, and any other designation made by a UNSC Committee, thereby also covering successor resolutions.

Criterion 7.2 – The FSC is the competent authority for implementing TFS in Korea.

(a) The same freezing obligations described under c.6.5(a) apply to PF-related TFS and suffer from the same deficiencies.

(b) The same deficiencies described under c.6.5(b) apply to the scope of the freezing obligation.

(c) All natural and legal persons in Korea, and Korean nationals abroad, are prohibited from making funds and other assets, economic resources, or financial services available, whether directly or indirectly (*PFOPIA*, art.5-2(1) and (2) (the TF offence)). Additionally, Korea is criminalising any person and entity who knowingly provided funds and other assets to designated persons and entities, which applies to both FIs, DNFBPs and any other person (*PFOPIA*, arts. 4, 6(2)3). However, by requiring "knowledge" these provisions are not adequately implementing TFS which should be implemented unconditionally.

(d) Korea uses the same mechanisms described under c.6.5(d) to communicate designations to FIs and casinos, but there is no mechanism in place to communicate designations to DNFBPs other than casinos. No specific guidance has been provided to FIs or DNFBPs on their obligations.

(e) FIs and casinos are required to report to competent authorities any actions taken in compliance with the prohibition of the requirements of the relevant UNSCRs (*PFOPIA*, art.5(2)), including attempted transactions. No requirements apply to other DNFBPs.

(f) Measures are in place to protect the rights of bona fide third parties acting in good *faith when implementing the obligations under R.7 (PFOPIA, art.6(7)).*

Criterion 7.3 – FIs and casinos are being monitored for compliance with the obligations set out in the *PFOPIA*, but there are no measures in place for monitoring other DNFBPs. Any person failing to comply with the *PFOPIA* (providing, raising, transporting or keeping funds for a designated person) is punishable by criminal sanctions of imprisonment with labour for not more than 10 years or a fine not exceeding KRW 100 million (EUR 78 000) (*PFOPIA*, art.6). Criminal sanctions can be applied to FIs and casinos, but only if an employee has made a financial transaction or received a payment involving a designated person (*PFOPIA*, art.7, cf. art.5(1)). This does not extend to when the employee has opened an account or provided financial services not covering a transaction or receiving payment. DNFBPs who have any type of transactions with designated persons or entities are subject to not more than 3 years' imprisonment or a fine of KRW 30 million (EUR 23 088) (*PFOPIA*, art.6(2)).

Criterion 7.4 – The FSC is responsible for de-listing individuals who are no longer related to PF (*PFOPIA*, art.4(6)).

(a) Anyone may petition the FSC with a de-listing request. The publicly known procedures to submit de-listing requests to the FSC for de-listing established pursuant to UNSCR 1730, or submitting information on designated persons or entities to petition the FSC, are provided for in the *Designation Notice*.

(b) The *Designation Notice* contains publicly known procedures to unfreeze the funds or other assets of persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by the restriction to funds mechanism (i.e. a false positive), upon verification that the person or entity involved is not a designated person or entity.

(c) The FSC can grant designated persons access to funds or other assets, on a case-by-case basis in conjunction with other ministries, however, it is not explicit that the FSC must determine that the exemption conditions set out in UNSCRs 1718 and 2231 are met before authorising access (*PFOPIA*, art.4(4)).

(d) The same mechanisms are used for communicating listings and de-listings to FIs and DNFBPs (see analysis under c.7.2(d)). No specific guidance has been provided to FIs or DNFBPs on their obligations to respect de-listing or unfreezing actions.

Criterion 7.5 – With regards to contracts, agreements or obligations that arose prior to the date on which accounts became subject to targeted financial sanctions:

(a) There is no legal basis to prohibit/permit addition to frozen accounts pursuant to UNSCRs 1718 or 2231 for interests and other earnings 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.

(b) There is no legal basis to allow designated persons or entities to make payments due under contracts entered into prior to the listing of such person or entity, from funds or other assets frozen pursuant to UNSCRs 1737 and 2231.

Weighting and Conclusion

Korea has a regime for implementing targeted financial sanctions, however the following moderate shortcomings exist:

(a) The freezing obligation does not extend to DNFBPs (other than casinos), as the prohibition on financial transactions does not apply to them; the freezing obligation does not extend to funds or other assets indirectly owned or controlled (including joint ownership) or where persons or entities act on behalf of or at the direction of designated persons, the additional measure, for criminalising all natural and legal persons providing funds and other assets, is conditional upon a level of knowledge; no mechanism in place to communicate designations, de-listings and unfreezings to DNFBPs other than casinos, and; no guidance has been issued to FIs and DNFBPs on how to meet their obligations in this area.

(b) No measures exist to ensure compliance by DNFBPs other than casinos.

(c) De-listing, unfreezing and access procedures have the following deficiencies: it is not explicit that authorising access to funds must be based on a determination that the exemption conditions set out in UNSCRs 1718 and 2231 are met; and no specific guidance has been provided to FIs or DNFBPs on their obligations to respect de-listing or unfreezing actions.

(d) No legal basis to prohibit/permit addition to frozen accounts pursuant to UNSCRs 1718 or 2231 and no legal basis to allow designated persons or entities to make payments due under contracts.

Of these shortcomings, deficiency (a) above was weighted most heavily.

Recommendation 7 is partially compliant.

Recommendation 8 – Non-profit organisations

In its 3rd MER, Korea was rated partially 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) Korea has not clearly identified which of its 14 033 registered NPOs fall within the FATF definition of NPO.[64] Korea considers that its definition of 'public interest corporation' aligns with the FATF definition of NPO. Korea estimates that 9 164 public interest corporations exist, but this number captures only larger public interest corporations that are subject to a duty of disclosure, and excludes smaller NPOs that may nonetheless fall within the FATF definition. In addition, Korea's definition of 'public interest corporation' does not strictly align with the FATF definition. A 'public interest corporation' is a legal person "conducting activities concerning aid or payment of school expenses, scholarships or research expenses, sciences and charities in in order to contribute to the general interest of society" (*Act on the Establishment and Operation of Public Interest Corporations*, art.2). The definition of 'public interest corporation' does not clearly extend to religious, cultural or social

64. Recommendation 8 provides that "NPO refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of 'good works'."

charities, and Korea confirms that it does not cover organisations raising funds for religious purposes. It also would not capture organisations that are raising, but not yet providing, funds; or NPOs founded as a legal arrangements (not a legal person) (noting that this would be rare in Korea).

In any case, Korea has identified the features and types of NPOs across its entire NPO population (14 033 entities) which may be at risk of TF abuse. To do so, Korea categorised its NPOs as those operating domestically, those operating abroad, and those with certain religious affiliations. NPOs operating domestically were identified as lower risk based on intelligence from law enforcement. A group of 137 NPOs which form the KCOC implement development and aid projects and were identified as being at potential risk due to their operations abroad. Within this group, Korea identified 22 specific NPOs as being at higher risk of TF abuse due to their operation within jurisdictions with a high risk of terrorism. A further 147 NPOs are considered at higher risk based on one specific shared characteristic.

This assessment is included within the 2018 NRA and was based on research reports which fed into the 2016 NRA, meetings of the NPOs CFT Agencies Committee (a sub-committee of the AML/CFT Policy Co-ordination Committee), outreach to KCOC and its NPOs,[65] immigration statistics, wire transfer data, analysis of the few TF-related incidents in Korea (none were related to NPOs), and information on the activities conducted by NPOs in conflict areas. However, as is recognised in a specific NPO TF risk assessment which fed into the 2016 NRA, "there is insufficient accumulated data regarding the risk of NPOs being abused for terrorist financing, which makes it difficult to predict related risks in the future." Limitations in oversight and reporting requirements for certain NPOs (see c.8.3) may also impact Korea's ability to identify at-risk NPOs.

(b) Korea has made efforts to identify the nature of TF threats posed to at-risk NPOs and how terrorist actors could abuse those NPOs based on discussions with NPOs, intelligence, and case studies from other countries. For example, the 2018 NRA identifies the threat of false fundraising by religious institutions. However, some of the threats identified are very general (e.g. the diversion of funds to terrorist groups) with little focus on how Korean NPOs could be abused based on the services offered. KoFIU's *Guidelines on Combating TF Abuse of NPOs* provide some information for NPOs on TF threats and vulnerabilities, however, this is largely based on international studies and reports and could benefit from insight into the particular threats and characteristics of relevance for Korean NPOs.

(c) KoFIU has undertaken three reviews (in 2006, 2016, and 2018), to varying levels of detail, of the adequacy of Korea's measures to prevent TF abuse of at-risk NPOs. The legislative framework was considered adequate and risk-based. The results of the reviews were discussed in the NPOs CFT Agencies Committee and fed into the KoFIU *Guidelines on Combating TF Abuse of NPOs*. The review also led to practical changes to manage risk, such as requiring certain NPOs' financial reports and other data to be made public by the NTS (see c.8.3).

(d) Korea has periodically reassessed the NPO sector to review up-to-date information on its vulnerabilities. The TF risks in the NPO sector were first assessed in 2006, were covered in the 2016 NRA, and were considered again in the 2018 NRA

65. Outreach involved an August 2018 meeting between KoFIU and KCOC members to discuss their activities, financing, expenditures, understanding of TF abuse, supervision and controls, etc., and a November 2018 education session held by KoFIU and KCOC on potential TF abuse risks.

to take into account new information. Korea's NPOs CFT Agencies Committee was established in 2018 to discuss the risks and vulnerabilities of the NPO sector on an ongoing basis. The NPOs CFT Agencies Committee meets on an *ad hoc* basis to discuss issues as they arise, including new information on risks and vulnerabilities.[66]

Criterion 8.2 –

(a) KOICA within the MFA is responsible for Korea's international development aid and has issued general guidance to NPOs it works with on accountability, transparency, and record-keeping. This guidance is relevant to the 137 at-risk NPOs that form KCOC, although not all KCOC members receive KOICA funding. The other group of at-risk NPOs are not KCOC members nor do they receive KOICA funding. For other NPOs, including the other group of at-risk NPOs, KoFIU developed its *Guidelines on Combating TF Abuse of NPOs* which include brief guidance and case studies on some governance and integrity issues. However, the Guidelines are not comprehensive. Certain NPOs are also subject to measures and obligations that aim to increase transparency and accountability and prevent TF (see c.8.3).

(b) Korea has undertaken some outreach for NPOs to increase the understanding of potential TF vulnerabilities and measures to protect against such abuse. KoFIU, the FSC, and KCOC held an educational session in November 2018 for the NPOs identified as at-risk due to their activities abroad (i.e. the 137 development aid NPOs that form KCOC). The session aimed to raise awareness and share best practices on maintaining integrity, conducting due diligence, ensuring transparency and accountability, and monitoring internal controls. Limited outreach has been undertaken for other NPOs identified as at-risk. These NPOs received a government letter requesting that they consider the risk of TF abuse in implementing policies. They also have access to the KoFIU Guidelines. No measures have been undertaken to provide information to donor communities on the TF vulnerabilities of NPOs.

(c) The KoFIU Guidelines include best practices for addressing TF risks and vulnerabilities. The Guidelines were developed by specialists with experience and academic backgrounds in NPOs and drew from overseas experiences. NPOs themselves were not involved in the development or refinement of the Guidelines, although there are plans to involve NPOs in future work.

(d) All NPOs are required to use regulated financial channels and provide information on their accounts to the NTS (Inheritance Tax and Gift Tax Act, art.50-2). The 137 development aid NPOs are also subject to additional requirements to conduct transactions through certified bank accounts or regulated financial channels (*Korea International Cooperation Agency Act*, art.22-2).

Criterion 8.3 – Korea takes some steps to promote supervision and monitoring of NPOs to demonstrate that the measures applied to NPOs are risk-based. However, half of Korea's higher-risk NPO population are not subject to adequate measures.

NPOs are required to register with one of 22 central government agencies or one of 77 local governments. Most of the 137 overseas development NPOs Korea identified as at higher-risk of TF abuse are registered with the MFA. Those that receive KOICA funding to provide development aid must comply with certain requirements. Upon creation, they must submit to KOICA: their purpose and objectives; information on

66. E.g. The Committee met in August 2018 to discuss NPO supervision and the risks posed by wire transfers; in October 2018 to discuss NPOs operating overseas and the management of religious NPOs in Korea; and in January 2019 to discuss the outcomes of the National Counter-Terrorism Committee meeting and the TF risk assessment.

their directors, officers and assets; and the methods they use for contribution and fundraising (*Civil Act*, art.49; *Regulations on Establishment and Supervision of NPOs*). They must also submit annual business reports and expense records (*Assistance for Non-profit, Non-governmental Organisations Act*, arts.8, 9). Public interest corporations must be approved for operation by the relevant registrar and are required to submit a business plan and report, have standing rules, appoint directors, be audited and supervised, and publish financial statements (*Act on the Establishment and Operation of Public Interest Corporations*, arts.3, 5, 6, 10, and 12). Larger public interest corporations[67] are also subject to tax disclosure obligations, including an annual audit and publishing financial statements and lists of donations on the NTS website (*Act on the Establishment and Operation of Public Interest Corporations*, arts.10, 12; *Corporate Tax Act*, art.112-2; *Inheritance Tax and Gift Tax Act*, art.50-3). This information is made public through Korea's GuideStar website (www.guidestar.or.kr). For NPOs that are not public interest corporations, which includes half of the NPOs identified as higher-risk by Korea, there are no similar disclosure or reporting obligations.

Criterion 8.4 –

(a) Korea has some systems in place to monitor its NPOs for compliance with the requirements of R.8. All Korean NPOs are required to register with one of 22 central government agencies or one of 77 local governments. The MFA is the registrar for most of the 137 at-risk overseas development NPOs. Many of these entities receive KOICA funding and are therefore subject to ongoing and strict scrutiny to prevent misuse of public funds, including through TF. Not all 137 members of KCOC receive funding from KOICA meaning some higher-risk NPOs are not subject to this monitoring. Public interest corporations are subject to some annual monitoring by their registrar or the NTS. While this monitoring is not focused specifically on TF, it aims to prevent the misuse of funds, including through TF. However, this monitoring does not apply to all the NPOs identified as higher risk. Other at-risk NPOs are monitored by LEAs with the goal of preventing criminal offending, including TF. This surveillance is not strictly focused on R.8 requirements, but contributes to TF prevention. Korea also has strong co-ordination mechanisms, such as the NPOs CFT Agencies Committee (see c.8.1 and Table 2. in Chapter 0) which permits relevant agencies to share information on NPOs to monitor for TF. Korea's monitoring and supervisions systems are generally consistent with Korea's risk, although monitoring of certain at-risk NPOs could be more focused on R.8 requirements.

(b) Korea has some ability to apply effective, proportionate and dissuasive sanctions for violations of the requirements applicable to NPOs. Registrars are able to deregister NPOs for breaches of their financial reporting obligations, including the requirement to submit to an audit or publish financial statements (*Civil Act*, art.38; *Act on the Establishment and Operation of Public Interest Corporations*, art.16). The NTS can also sanction such breaches by imposing additional tax. No sanctions are available for the NPO's officers. The government can revoke subsidies from NPOs that receive subsidies where they fail to comply with their financial and reporting obligations. Where a NPO collects donations outside its specified collection plan, the NPO or its officer(s) can face imprisonment of up to three years or a fine of KRW 30 million (EUR 23 500) (*Act on Collection and Use of Donations*, art.4, 10, 16).

67. NPOs that fundraise over KRW 300 million / EUR 228 667 or have activities valued at over KRW 500 million / EUR 381 095.

Overall, the range of sanctions available is relatively limited which may reduce Korea's ability to impose proportionate sanctions.

Criterion 8.5 –

(a) Korea ensures co-operation and co-ordination between authorities with information on NPOs through the NPOs CFT Agencies Committee which was established in 2018 and meets on an *ad hoc* basis depending on need. The Committee comprises some relevant agencies (such as the NTS, the NPA, and the FSS) but does not include all registrars which limits its ability to act as a platform for information-exchange (see Table 2. in Chapter 0). The Counter-Terrorism Committee provides another platform for potential co-operation and information-sharing on TF abuse of NPOs, but also does not include all NPO registrars.

(b) The NPA, the SPO and other prosecutors' offices are competent to carry out investigations into NPOs suspected of TF abuse, actively monitor at-risk NPOs to increase their expertise and have capacity to investigate potential TF.

(c) The NPA is able to obtain information on the administration and management of NPOs through various channels. It has the power to request or demand this information from the relevant NPO registrar or the NPO itself (*Criminal Procedure Act*, art.199(2)). Tax and financial information is available publicly on the NTS and GuideStar websites (www.guidestar.or.kr). Information on financial transactions can be obtained through KoFIU or via a warrant (*FTRA*, art.7; *Criminal Procedure Act*, arts.215-217). Other investigative powers are also available as set out in R.31.

(d) The NPOs CFT Agencies Committee and Counter-Terrorism Committee provide mechanisms for sharing suspicions of NPO abuse with relevant authorities, including the NPA for investigation. NPO registrars are aware of the TF risks in the sector, in part due to outreach on this topic, and know to report any suspicions to the NPA. While registrars do not have specific mechanisms in place for such reporting, they have an obligation to implement systems and conditions to prevent terrorism, which may serve as encouragement to report (*Anti-Terrorism Act*, art.3).

Criterion 8.6 – International requests for information regarding particular NPOs suspected of TF abuse are dealt with in the same was as any other request for information. KoFIU, the NPA or other competent authorities can informally provide information as described in R.40. Where one agency receives a request for information relevant to another agency, the NPOs CFT Agencies Committee provides contact points through which such requests can be shared. Foreign parties may also obtain public financial or administrative information through GuideStar or the NTS.

Weighting and Conclusion

Korea has a framework in place for preventing TF abuse through NPOs, however, there remain some deficiencies. Korea has not fully identified which of its NPOs fall within the FATF definition. This is a minor deficiency as it is mitigated by Korea's identification of at-risk NPOs, although its identification of TF threats to NPOs remains very general. There are policies aimed at promoting accountability, integrity and public confidence, although there are not comprehensive policies for all NPOs including at-risk NPOs. Outreach efforts have not included certain high-risk NPOs or donor communities and the largest group of identified at-risk NPOs are not subject to relevant reporting or disclosure requirements. These are considered moderate deficiencies and given more weight due to the risks identified by Korea. NPOs themselves have not been involved in the development of relevant guidance.

Monitoring of NPOs takes place, but for certain at-risk NPOs, monitoring is focused on criminal activity rather than ensuring compliance with R.8 requirements. The range of sanctions for breaching R.8 requirements is relatively limited. Finally, information-sharing on NPOs is limited as co-ordination committees do not include all NPO registrars.

Recommendation 8 is partially compliant.

Recommendation 9 – Financial institution secrecy laws

In its 3rd MER, Korea was rated largely compliant on financial secrecy. The technical deficiency was that a financial secrecy provision limited the sharing of customer identification information between financial institutions in a way that impeded full implementation of FATF requirements.

Criterion 9.1 –

There are no financial institution secrecy laws inhibiting implementation of AML/CFT measures. The duty of confidentiality (*Act on Real Name Financial Transactions and Confidentiality*, art.4) can be waived in the following situations:

Access to information by competent authorities: KoFIU as the financial supervisor can request information from FIs (*FTRA*, art.10). The authority to supervise FIs has been delegated to entrusted agencies, who equally can request information from FIs. Additionally, transaction information can be obtained by the FSC and the Governor for the FSS without a court order for AML/CFT purposes when the information is needed to co-operate with foreign counterparts (*Act on Real Name Financial Transactions and Confidentiality*, art.4.6).

Sharing of information between competent authorities: When information is deemed necessary for a criminal investigation related to criminal proceeds, illegal gains, ML/TF etc. the Commissioner of KoFIU shall make the relevant information available to the competent authorities (*FTRA*, art.7, cf. *FTRA*, art.12). Different supervisory authorities can exchange information where the information is necessary for investigating insider trading, financial misconduct etc. (*Act on Real Name Financial Transactions and Confidentiality*, art.4(2) and (3)).

Sharing of information between FIs: FIs can share STR related information with other FIs in the same financial group to prevent ML/TF (*FTRA*, art. 4(6)). Additionally, FIs can exchange transaction information when this is necessary for internal business (*Act on Real Name Financial Transactions and Confidentiality*, art.4(5)), thereby not inhibiting sharing of transaction information related to R.13, 16 and 17. However, based on the definition of "financial transaction" (*FTRA*, art.2(2)), the ability to share information does not extend to CDD information in cases where this information is unrelated to a transaction.

Weighting and Conclusion

Bank secrecy laws are in place in Korea which generally do not inhibit AML/CFT implementation, although limitations exist in relation to sharing of information which is unrelated to a transaction between FIs (e.g. other CDD information).

Recommendation 9 is largely compliant.

Recommendation 10 – Customer due diligence

In its 3rd MER, Korea was rated partially compliant with these requirements. The technical deficiencies related to: when FIs should undertake CDD; customers who are legal persons or arrangements (no requirement to verify if a natural person is authorised to act; to obtain information on the nature of its business, ownership and control structure, legal form and powers; or to identify and verify beneficial owners unless there is a ML/TF suspicion); no requirement to obtain information on the purpose and intended nature of the business relationship or to keep CDD information up to date; no prohibition on doing business when CDD is not complete and no requirement to mitigate the risks or consider filing an STR in such cases; no requirement to conduct CDD on existing customers or consider terminating a business relationship or filing an STR if CDD cannot be completed; and exemptions for some smaller FIs, money exchangers and investment-related companies.

Criterion 10.1 – There is no explicit requirement in law to prohibit anonymous accounts, however, FIs are required to identify the customer and verify the information before opening an account (*FTRA*, art.5-2(1)).

Criterion 10.2 – FIs are required to undertake CDD when:

(a) establishing a business relationship (*FTRA*, art.5-2(1));

(b) carrying out "isolated" (occasional) financial transactions or through several transactions by the same person within a seven day period above the threshold of USD 10 000 (EUR 8 799) for transactions in foreign currency, and KRW 15 million (EUR 11 691) for transactions in domestic currency (*Enforcement Decree of the FTRA,* art.10-3; *AML/CFT Reg.*, art.23), which is slightly above the threshold of maximum USD/EUR 10 000;

(c) carrying out a wire transfer above the designated threshold of KRW 1 million (EUR 787) (*FTRA*, art.5-2(1)-1, *Enforcement Decree of the FTRA*, art.10-3(1)2; *AML/CFT Reg.*, art.23);

(d) a customer presents a suspicion of ML or TF (*AML/CFT Reg.*, art.24-1); and

(e) there are concerns as to the adequacy and veracity of previously obtained customer identification data (*AML/CFT Reg.*, art.24-2).

Criterion 10.3 – FIs are required to identify permanent and occasional customers. For natural persons the following identification information is required: name; date of birth and gender (only for non-residents); identification number; country of residence (only for foreigners), and; address and contact information (*AML/CFT Reg.*, art.38(1)). For legal persons and arrangements the following identification information is required: name; identification number; address and place of headquarters and offices; information on the representative or senior management officials; business type; purpose of establishment, and; identification information on the settlor, trustee, administrator and beneficiary (only relates to legal arrangements) (*AML/CFT Reg.*, art.38(2)). All identity information (for natural or legal persons and legal arrangements) must be verified by using reliable and independent documents, data, information etc. (*FTRA*, art.5-2(1)1; *Enforcement Decree of the FTRA*, art.10-4; *AML/CFT Reg.*, art.37).

Criterion 10.4 – FIs are required to identify any person carrying out transactions or opening an account on behalf of another natural or legal person or legal arrangement and verify that this person is authorised to do so (*AML/CFT Reg.*, art.38-3). However,

this does not extend to acting in other ways, e.g. approving new services to an existing account.

Criterion 10.5 – FIs are required to identify who ultimately owns or controls the customer by using reliable documents (*Enforcement Decree of the FTRA*, art.10-5; *AML/CFT Reg.*, art.41).

Criterion 10.6 – FIs are required to obtain information on the purpose and intended nature of the business relationship (*AML/CFT Reg.*, art.37(2)).

Criterion 10.7 – FIs are required to conduct ongoing due diligence on the business relationship (*AML/CFT Reg.*, art.34(1)) including by:

(a) examining transactions to determine if they are consistent with the FI's knowledge of the customer, the customer's business, risk profile and source of funds, and

(b) reviewing the existing records of higher risk categories of customers or transactions to ensure that the documents, data and information obtained through CDD are up-to date and adequate.

Criterion 10.8 – FIs are required to understand the nature of the business relationship, ownership and control structure of customers who are legal persons or legal arrangements (*AML/CFT Reg.*, art.37(3)).

Criterion 10.9 – FIs are required to identify and verify the identity of legal persons and legal arrangements through the following information (*AML/CFT Reg.*, art.40):

(a) name of the entity, business type and identity number,

(b) obtain information on the powers that regulate the legal person or legal arrangement or the names of representatives and persons having a senior management position, and

(c) the address and place of its headquarters and offices.

Criterion 10.10 – For customers that are legal persons (*AML/CFT Reg.*, art.41):

(a) FIs are required to verify the identity of the natural person(s) who ultimately has a controlling ownership interest (the beneficial owner) in a legal person,

(b) if the FI is unable to verify the identity of the beneficial owner, it shall verify the identity of one of the following: (i) a shareholder who holds the largest portion of shares, considering the number of issued and remaining voting shares; (ii) a shareholder who has appointed a majority of representatives, managing partners, or executives; or (iii) a person who substantially controls the legal person, if this person is clearly different from the shareholders and thereby not covered under (i) and (ii),

(c) where no persons can be identified under (a) or (b), FIs shall identify the senior managing official.

Criterion 10.11 – For customers that are legal arrangements, FIs are required to identify and verify the identity of the beneficial owners, including:

(a)–(b) for trusts and other legal arrangements, the identity of the settlor, trustee(s), the trust administrator and the beneficiary. However, there is no requirement to identify any other natural persons exercising effective control over the trust (*AML/CFT Reg.*, art.38(2));

Criterion 10.12 – FIs are required to perform CDD measures for customers of life insurance and investment related products, including the person who signed the contract and the beneficiaries (*AML/CFT Reg.*, art.20(4)), and the beneficial owner(s) (*AML/CFT Reg.*, art.41). For beneficiaries, FIs are required to perform the following CDD measures when the beneficiary is designated and at the time of pay-out (*AML/CFT Reg.*, art.33):

(a) for a beneficiary which is identified as a specifically named natural or legal person or arrangement, the name;

(b) for beneficiaries listed by characteristics or by class or other means, FIs are required to obtain sufficient information to satisfy the FI that it will be able to establish the identity at the time of pay-out;

(c) for both (a) and (b) above, the verification of the identity of the beneficiary must occur at the time of pay-out.

Criterion 10.13 – FIs are required to include the beneficiary of a life insurance policy as a relevant risk factor in the customer relationship (*AML/CFT Reg.*, art.20(4), cf. *Enforcement Decree of the FTRA*, art.10-6).

Criterion 10.14 – FIs are required to conduct CDD prior to executing a transaction (*AML/CFT Reg.*, art.32), except in cases where the Commissioner of KoFIU approves a delayed verification (*Enforcement Decree of the FTRA*, art.10-6), provided that:

(a) FIs are required to complete CDD, including verification, as soon as reasonably possible (*AML/CFT Reg.*, art.33(1)1).

(b) the delayed verification is essential not to interrupt the normal conduct of business (*AML/CFT Reg.*, art.33(1)3).

(c) FIs effectively manage ML/TF risks when approving a delayed verification.

Criterion 10.15 – FIs are required to establish and implement procedures to manage and control ML/TF risks that might arise from conducting delayed verification (*AML/CFT Reg.*, art.33(2)).

Criterion 10.16 – FIs shall conduct CDD on customers existing prior to the entering into force of the amended *FTRA* and its *Enforcement Decree* (December 2008) at appropriate times. Appropriate times refers to: (i) when a significant transaction takes place; (ii) when customer documentation standard change substantially; (iii) when there is a material change in the way that an account is operated; or (iv) when there are doubts about the adequacy of customer identification previously obtained (*AML/CFT Reg.*, art.25(2)).

Criterion 10.17 – EDD must be applied when there are increased ML/TF risk covering a range of customer types, and factors of risk, services and geography as listed in the *AML/CFT Reg.* (arts.29-31). Additionally, FIs are required to undertake a risk assessment of a customer relationship (*AML/CFT Reg.*, art.28) and apply EDD if higher risks for ML/TF have been assessed (*AML/CFT Reg.*, art.56).

Criterion 10.18 – FIs are permitted to apply simplified CDD measures by not verifying the identity of the ultimate owner or controller of the following: the state or a local government; an exhaustive list of public organisations; other financial companies, etc. (excluding casino operators and persons identified as high risk of ML/TF by the KoFIU), and; a corporation which shall submit and annual report pursuant to art.159(1) of the *Financial Investment Services and Capital Markets Act*

(*Enforcement Decree of the FTRA*, art.10-5(5)). Simplified CDD is not permitted in cases involving customers if there is a suspicion of ML/TF or in a higher risk scenario.

Criterion 10.19 –

(a) FIs are required to reject a customer's request for opening a bank account or transaction, and terminate a transaction if they are unable to conduct CDD (*FTRA*, art.5-2(4)). However, where relevant CDD measures cannot be complied with for existing customers, FIs are not required to terminate the business relationship, but can only reject the existing customer's transaction requests.

(b) If CDD measures cannot be complied with, FIs are required to consider making an STR in relation to the customer (*AML/CFT Reg.*, art.44-2).

Criterion 10.20 – FIs are permitted to not conduct CDD and file an STR where there is a reasonable possibility of tipping-off the customer (*AML/CFT Reg.*, art.44-2).

Weighting and Conclusion

CDD measures are largely in place in Korea. In the Korean context, the following deficiencies have been assessed minor:

(a) The threshold (domestic currency) for FIs to apply CDD when carrying out occasional transactions is slightly above USD/EUR 10 000.

(b) Acting on behalf of another person only covers performing a transaction or account opening, not e.g. approving new services to an existing account.

(c) For legal arrangements, FIs are not required to identify all natural persons exercising effective control over the legal arrangement.

(d) FIs are not required to terminate a business relationship with an existing customer if CDD cannot be complied with.

Recommendation 10 is largely compliant.

Recommendation 11 – Record-keeping

In its 3rd MER, Korea was rated largely compliant with these requirements on the basis of the following technical deficiencies: no specific requirement for FIs to keep transaction records sufficient to permit reconstruction of individual transactions; and no requirement to ensure that the information is available to the competent authorities on a timely basis.

Criterion 11.1 –FIs are required to retain all necessary records on transactions, both domestic and cross-border, for at least five years following completion of the transaction (*FTRA*, art.5-4).

Criterion 11.2 **–**FIs are required to keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction (*FTRA*, art.5-4; *AML/CFT Reg.*, art.85).

Criterion 11.3 – FIs are required to keep transaction data (*AML/CFT Reg.*, art.85).

Criterion 11.4 – FIs are required to provide any data retained upon request from the Commissioner of KoFIU or the head of a designated inspection body, in a timely manner (*AML/CFT Reg.*, art.86(4)).

Weighting and Conclusion

All criteria are met.

Recommendation 11 is compliant.

Recommendation 12 – Politically exposed persons

In its 3rd MER, Korea was rated non-compliant with these requirements based on the following technical deficiencies: no requirement for FIs to determine if a customer is a foreign PEP; to obtain senior management approval before establishing or continuing business relationships with PEPs; to establish the source of wealth and funds of customers and beneficial owners identified as PEPs; or to conduct enhanced ongoing monitoring of business relationships with PEPs. Since its last evaluation, the FATF Standards in this area have been expanded to also include domestic PEPs.

Criterion 12.1 – In relation to foreign PEPs, in addition to performing CDD (see R.10), FIs are required to:

(a) establish appropriate procedures to determine whether a customer or a beneficial owner is a PEP (*AML/CFT Reg.*, art.65);

(b) obtain the approval of senior management to open an account or continue a business relationship with an existing customer (*AML/CFT Reg.*, art.66);

(c) apply enhanced CDD and establish the source of funds by taking appropriate actions to obtain additional information, including the identity of family members and close associates authorised to undertake transactions on the account, and information on any business entity or organisation connected to the PEP (*AML/CFT Reg.*, art.67); and

(d) undertake enhanced transaction monitoring on established foreign PEPs (*AML/CFT Reg.*, art.68(2)). However, there is no requirement to undertake enhanced ongoing monitoring of the relationship otherwise (e.g. to ensure that the customer's risk profile has not changed due to a change of geographical location).

Criterion 12.2 – There are no requirements covering domestic PEPs or persons entrusted with a prominent function by an international organisation.

Criterion 12.3 – FIs are required to apply enhanced CDD to family members and close associates of foreign PEPs as referenced under c.12.1 (*AML/CFT Reg.*, art.64). However, this does not extend to the family members and close associates of domestic PEPs or PEPs of international organisations.

Criterion 12.4 – There is no requirement for FIs to determine whether the beneficial owner of a beneficiary of a life insurance policy is a PEP.

Weighting and Conclusion

Korea has implemented most requirements for foreign PEPs except for the requirement to undertake enhanced ongoing monitoring (other than transaction monitoring) and no requirement to determine whether a beneficial owner of a beneficiary of a life insurance policy is a PEP. There are no requirements for domestic PEPs or PEPs of international organisations.

Recommendation 12 is partially compliant.

Recommendation 13 – Correspondent banking

In its 3rd MER, Korea was rated non-compliant with these requirements on the basis of the following technical deficiencies. FIs were not required to: determine whether a respondent institution has been subject to ML/TF enforcement action; assess the adequacy of the respondent's AML/CFT controls; require senior management approval before establishing the relationship; or document the respective AML/CFT responsibilities of each institution.

Criterion 13.1 – FIs which are authorised to enter into a correspondent-banking and similar relationship are: small value remitters (*Foreign Exchange Transaction Act* (*FETA*), art.8) and banks (*Banking Act*, art.27). Cross-border correspondent banking relationships are listed as high risk situations to which EDD must be applied prior to establishing a new relationship (*AML/CFT Reg.*, arts.31(3), art.55), including the following measures:

(a) understand the nature of the respondent institution's sales and business operations, and determine the reputation of the respondent institution from publicly available information and the quality of supervision, including whether the respondent has been subject to a ML/TF investigation or regulatory action (*AML/CFT Reg.*, art.59(1)1-2);

(b) assess the respondent institution's AML/CFT controls and measures against ML/TF (*AML/CFT Reg.*, art.59(1)-3);

(c) obtain senior management approval (*AML/CFT Reg.*, art.60); and

(d) document in writing the respective AML/CFT responsibilities of each institution (*AML/CFT Reg.*, art.59(1)-4))

Criterion 13.2 – FIs providing payable-through-accounts to respondent institutions must satisfy themselves that the respondent:

(a) has performed CDD on customers with direct access to accounts of the correspondent institution (*AML/CFT Reg.*, art.59(2)); and

(b) is able to provide relevant CDD information upon request to the correspondent institution (*AML/CFT Reg.*, art.59(2)).

Criterion 13.3 – FIs are not allowed to enter into or continue a correspondent-banking relationship with a shell bank (*AML/CFT Reg.*, art.58(2)), and should satisfy themselves that the respondent FI do not permit their accounts to be used by shell banks (*AML/CFT Reg.*, art.58(3)).

Weighting and Conclusion

All criteria are met.

Recommendation 13 is compliant.

Recommendation 14 – Money or value transfer services

In its 3rd MER, Korea was rated partially compliant with these requirements on the basis of technical deficiencies relating to limitations identified with regards to CDD and EDD requirements, record keeping, third party reliance, correspondent banking, PEPs, regulation and supervision of FIs, high risk countries and sanctions.

Criterion 14.1 – Licensed FIs (e.g. banks) can provide money or value transfer services (MVTS) without a separate license. In addition, three types of MVTS providers exist: small value remitters; electronic financial services providers; and Korea Post. These are required to register as either electronic financial services providers with the FSC (*FETA*, art.28), or as small value remitters with the Minister of Economy and Finance (*FETA*, art.8). No new post operators can be established.

Criterion 14.2 – Electronic financial services providers operating without a registration are punishable with up to three years of imprisonment or a fine up to KRW 20 million (EUR 15 617). Small value remitters carrying out MVTS without a registration are subject to criminal sanctions including imprisonment of up to three years or a fine up to KRW 300 million (EUR 234 259) (*FETA,* art.27-2). Small value remitters and Korea Post can make cross-border wire transfers not exceeding an amount corresponding to USD 3 000 (EUR 2 697) a day and a maximum of USD 30 000 (EUR 26 973) per person per year (*Foreign Exchange Transaction Reg.*, arts.3-4). Electronic financial services providers are only allowed to do domestic transfers. On this basis, the sanctions available for small value remitters and electronic financial services providers are proportionate and dissuasive. The Korean authorities are aware of the risk posed by MVTS providers operating without a registration. Several authorities have taken measures to identify un-registered operators including the NTS, the KCS, etc.

Criterion 14.3 – All MVTS providers are supervised by the FSS (*FTRA*, art.11(6); *Enforcement Decree of the FTRA*, art.15).

Criterion 14.4 – This criterion is not applicable, as Korea does not allow for MVTS providers to use agents.

Criterion 14.5 – This criterion is not applicable, as Korea does not allow for MVTS providers to use agents.

Weighting and Conclusion

All criteria are met.

Recommendation 14 is compliant.

Recommendation 15 – New technologies[68]

In its 3rd MER, Korea was rated compliant with these requirements.

Criterion 15.1 – Korea has identified and assessed the risks related to new technologies. Korea has assessed the ML/TF risk of virtual assets as high in its 2018

68. The FATF revised R.15 in October 2018 and its interpretive note in June 2019 to require countries to apply preventive and other measures to VASPs and virtual asset activity. This evaluation does not assess Korea's compliance with revised R.15 because, at the time of the on-site visit, FATF had not yet revised its assessment Methodology accordingly. Korea will be assessed for technical compliance with revised R.15 in due course, in the context of its mutual evaluation follow-up process.

NRA and has subsequently discouraged use of virtual assets. Korea also assessed the risks of non face-to-face CDD through online banking when opening accounts and executing transactions as being high risk.

FIs are required to assess the risks of ML/TF prior to making new products and business practices or services available, including risks emerging from new delivery mechanisms, or the use of new or developing technologies for both new and existing products (*AML/CFT Reg.*, art.17).

Criterion 15.2 – FIs are required to (*AML/CFT Reg.*, art.17):

(a) establish and implement procedures to conduct a risk assessment prior to the launch or use of a new product or service; and

(b) manage and mitigate risks posed by new technologies and apply EDD to mitigate risks when higher risks have been identified (*AML/CFT Reg.*, art.56).

Weighting and Conclusion

Both criteria are met.

Recommendation 15 is compliant.

Recommendation 16 – Wire transfers

In its 3rd MER, Korea was assessed partially compliant with these requirements as there were no requirements: for ordering FIs to include full originator information in messages accompanying cross-border or domestic wire transfers; for each intermediary or beneficiary institution in the payment chain to transmit all originator information accompanying a wire transfer; or for beneficiary institutions to adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information. Since Korea's last evaluation, the FATF Standards have been strengthened to require FIs to include beneficiary information with wire transfers.

Criterion 16.1 – FIs are required to ensure that all cross-border wire transfers of or above USD/EUR 1 000 are accompanied by (a) required and accurate originator information (name, account number or unique reference number and address and resident registration number or passport number/registration number for foreign persons), and (b) required beneficiary information (name and account number) (*FTRA*, art.5-3).

Criterion 16.2 – FIs are required to ensure that batch files contain required and accurate originator information and full beneficiary information (*AML/CFT Reg.*, art.47(2)).

Criterion 16.3 – There is no requirement to include required originator and beneficiary information for wire transfers below USD/EUR 1 000.

Criterion 16.4 – There is no requirement to obtain and verify customer information for wire transfers below the threshold.

Criterion 16.5 – Ordering FIs are required to ensure that domestic wire transfers are accompanied by originator information as indicated for cross-border wire transfers (*AML/CFT Reg.*, art.47(1)).

Criterion 16.6 – This criterion is not applicable because ordering FIs are required to include full originator and beneficiary information on all domestic wire transfers (see c.16.5).

Criterion 16.7 – Ordering FIs are required to maintain all originator and beneficiary information collected, in accordance with R.11 (*FTRA*, art.5-4).

Criterion 16.8 – Ordering FIs are not prohibited from executing a wire transfer if it does not comply with the requirements specified above at c.16.1-16.7.

Criterion 16.9 – Intermediary FIs are required to ensure that all originator and beneficiary information is retained with the wire transfer (*AML/CFT Reg.*, art.48(1)).

Criterion 16.10 – Intermediary FIs are required to keep a record of originator and beneficiary information received with a wire transfer where technical limitations prevent the required originator information or beneficiary information accompanying a cross-border wire transfer (*AML/CFT Reg.*, arts.48(1), 50).

Criterion 16.11 – Intermediary FIs are required to take reasonable measures, including monitoring, to identify wire transfers that lack required originator or required beneficiary information (*AML/CFT Reg.*, arts.48(2)).

Criterion 16.12 – Intermediary FIs are required to have risk-based policies and procedures for determining when to execute, suspend or reject a wire transfer lacking required originator or beneficiary information (*AML/CFT Reg.*, art.48(3)). However, there is no explicit requirement covering appropriate follow-up actions.

Criterion 16.13 – Beneficiary FIs are required to take reasonable measures, including monitoring, to identify cross-border wire transfers lacking required originator or beneficiary information (*AML/CFT Reg.*, art.48(2)).

Criterion 16.14 – Beneficiary FIs are required to undertake CDD when carrying out a wire transfer above KRW 1 million (EUR 787) (*FTRA,* art.5-2(1)-1, *Enforcement Decree of the FTRA*, art.10-3(1)-2; *AML/CFT Reg.*, art.23), and maintain this information in accordance with R.11.

Criterion 16.15 – Beneficiary FIs are required to have risk-based policies and procedures for determining when to execute or reject a wire transfer lacking required originator or beneficiary information (*AML/CFT Reg.*, art.48(3)). However, there is no requirement covering appropriate follow-up actions.

Criterion 16.16 – MVTS providers are required to comply with all of the relevant R.16 requirements in Korea. No Korean MVTS providers operate in other countries, and no agents are allowed.

Criterion 16.17 – MVTS providers controlling both the ordering and the beneficiary side of a wire transfer, are not required to:

(a) take into account all the information from both the ordering and the beneficiary sides in order to determine whether an STR has to be filed; or

(b) file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to KoFIU.

Criterion 16.18 – FIs are prohibited from making financial transactions for, and funds available to, designated legal and natural persons (*PFOPIA*, art.5) (see R.6 and R.7).

Weighting and Conclusion

Korea has measures in place applicable to the ordering FI, the intermediary FI and the beneficiary FI with regards to wire transfers. Some minor deficiencies have been identified related to: wire transfers below USD/EUR 1 000 (no requirement to include required originator and beneficiary information, or obtain and verify customer information); ordering FIs are not prohibited from executing wire transfer not complying with R.16; no explicit requirement for intermediary and beneficiary FIs to have risk-based policies and procedures for determining the appropriate follow-up action, and; no requirement applicable to MVTS providers controlling both the ordering and the beneficiary side of a wire transfer.

Recommendation 16 is largely compliant.

Recommendation 17 – Reliance on third parties

In its 3rd MER, Korea was assessed non-compliant with these requirements as there were no requirements for FIs relying on a third party: to perform CDD; to immediately gain from the third party the necessary CDD information; to take adequate steps to satisfy themselves that copies of identification data and other relevant CDD documentation will be made available from the third party upon request without delay; to satisfy themselves that the third party is regulated, supervised and has measures in place to comply with CDD requirements; and to take into account whether third parties in foreign countries adequately apply the FATF Recommendations.

Criterion 17.1 – FIs are allowed to rely on third parties to conduct CDD (*AML/CFT Reg.*, art.53). When doing so, the ultimate responsibility remains with the relying entity (*AML/CFT Reg.*, art.54), which is required to:

(a) obtain immediately the necessary information about the CDD measures (*AML/CFT Reg.*, art.53(1));

(b) satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available by the third party without delay (*AML/CFT Reg.*, art.53(2)); and

(c) satisfy itself that the third party is regulated and supervised for, and has measures in place for complying with AML/CFT requirements, including CDD and record-keeping requirements in line with Recommendations 10 and 11 (*AML/CFT Reg.*, art.53(3)).

Criterion 17.2– FIs can rely on third parties located outside of Korea if the country in question has adopted and implemented the FATF Recommendations effectively (*AML/CFT Reg.*, art.53(4)).

Criterion 17.3 – As the *AML/CFT Regulation* does not differentiate between reliance on third parties from within a financial group and other third parties (c.17.1), this criterion is not applicable.

Weighting and Conclusion

Recommendation 17 is compliant.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In its 3rd MER, Korea was rated partially compliant with these requirements. The deficiencies were no requirements for FIs to: communicate internal AML/CFT procedures, policies and controls to employees; appoint compliance officers at a management level; have audit committees test compliance with AML/CFT procedures, policies and controls; have screening procedures to ensure high standards when hiring employees; have foreign subsidiaries and branches observe AML/CFT measures consistent with Korean requirements; pay special attention to the application of AML/CFT measures in branches and subsidiaries located in jurisdictions which insufficiently apply the FATF Recommendations; and where the home and host country requirements differ, apply the higher of the two standards wherever possible.

Criterion 18.1 – FIs are required to implement the following internal controls (*Act on Corporate Governance of Financial Companies*, art.24(1); *Regulation on the Supervision of the Corporate Governance of Financial Companies*, art.11(2)6):

(a) appoint a compliance officer at management level (*Act on Corporate Governance of Financial Companies*, art.25(2));

(b) screen and perform identity checks on employees prior to hiring or continuing to employ directors, officers and employees (*AML/CFT Reg.*, art.10);

(c) implement education and training of management and employees to prevent ML/TF (*FTRA*, art.5(3)); and

(d) have an independent audit function to test the system (*AML/CFT Reg.*, art.13).

Criterion 18.2 – Although there is a general requirement for FIs to establish, implement, and evaluate internal controls for AML/CFT at group-level (*AML/CFT Reg.*, art.5(2)1), there are no explicit requirements for them to implement the specific measures set out in c.18.1 and c.18.2(a)-(c) at the group-wide level.

Criterion 18.3 – FIs are required to ensure that their foreign branches or subsidiaries comply with the AML/CFT requirements (*AML/CFT Reg.*, art.27(1)). Where the regulation of the home and the host country differs, the stricter rule-set shall be applied to the extent laws and regulation of the host country permits. If the host country does not permit proper implementation of the AML/CFT measures, the FIs must notify KoFIU (*Financial Transaction Report and Supervisory Reg.*, art.2(3)). However, in these cases, the FIs are not required to take appropriate additional measures.

Weighting and Conclusion

Korea generally has measures in place regarding internal controls including group-wide measures for foreign branches and subsidiaries. Two minor deficiencies have been identified. There is no explicit requirement for financial groups to implement the measures set out in c.18.1 and c.18.2(a)-(c) at the group-wide level, which has been weighted minor considering the overall requirement to implement group-wide measures is in place. FIs are not required to take appropriate additional measures when the host country does not permit proper implementation of the AML/CFT measures.

Recommendation 18 is largely compliant.

Recommendation 19 – Higher-risk countries

In its 3rd MER, Korea was rated non-compliant with these requirements on the basis of the following technical deficiencies. There was no requirement for FIs: to pay special attention to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations; or, where transactions have no apparent economic or lawful purpose, to examine the background and purpose of the transactions, set forth findings in writing and make them available to assist competent authorities. The only possible counter-measure was application of EDD.

Criterion 19.1 – FIs are required to pay special attention and apply EDD to business relationships and transactions with natural or legal persons, FIs etc. from countries for which this is called upon by the FATF (*AML/CFT Reg.*, arts.70, 72). FIs are also required to establish and implement procedures to assess the ML/TF risks associated with customers from these countries.

Criterion 19.2 – FIs are required to apply countermeasures upon request from the KoFIU (*AML/CFT Reg.*, art.72(2)), including when called upon to do so by the FATF. However, it is not explicit that these measures should be applied proportionate to the risks.

Criterion 19.3 – KoFIU sends official notices to FIs advising them when changes are made to the *FATF Public Statement* and *Ongoing Compliance Document*. Additionally, KoFIU highlights in the official notices whether counter measures or EDD should be applied.

Weighting and Conclusion

There is no explicit reference to apply countermeasures proportionate to the risk.

Recommendation 19 is largely compliant.

Recommendation 20 – Reporting of suspicious transaction

In its 3rd MER, Korea was rated partially compliant with these requirements on the basis of the following technical deficiencies. STR requirements did not apply to the proceeds of all required predicate offences or to transactions below the threshold of KRW 20 million (EUR 15 419) (for transactions in KRW) or USD 10 000 (EUR 8 989) (for transactions in foreign currencies).

Criterion 20.1 – FIs are required to report suspicious transactions to KoFIU without delay (*FTRA*, art.4-1). "Suspicious transaction" includes transactions where there is reasonable grounds to suspect that the asset is the proceeds of an offence, illegal gains or of ML/TF.

Criterion 20.2 – FIs are required to report suspicious transactions, including attempted transactions, regardless of their amount (*FTRA*, art.4(1)).

Weighting and Conclusion

Both criteria are met.

Recommendation 20 is compliant.

Recommendation 21 – Tipping-off and confidentiality

In its 3rd MER, Korea was rated compliant with these requirements.

Criterion 21.1 – FIs and their directors, officers and employees are protected against criminal and civil liability when disclosing information as part of filing a STR with KoFIU (*FTRA*, art.4(7)). This protection covers STRs filed as suspicion of "illegal assets", ML or TF and is not limited to cases where the underlying criminal activity was known at the time of filing the STR.

Criterion 21.2 – FIs and their directors, officers and employees are prohibited from disclosing the fact that they intend to or have filed an STR to the KoFIU (*FTRA*, art.4(6)). This ban does not inhibit FIs and their directors, officers and employees from sharing the fact that they intend to or have filed a STR with FIs in the same financial group to prevent ML/TF or to share the information with foreign FIUs (*FTRA*, art.4(6)).

Weighting and Conclusion

Both criteria are met.

Recommendation 21 is compliant.

Recommendation 22 – DNFBPs: Customer due diligence

In its 3rd MER, Korea was rated non-compliant with these requirements because no AML/CFT obligations applied to DNFBP sectors, except for casinos.

Criterion 22.1 – The CDD requirements set out in R.10 (which are subject to the same technical deficiencies noted in R.10) are required to be applied in the following situations:

(a) By casinos when customers engage in financial transactions of KRW 3 million (EUR 2 264).

(b) Real estate agents when they are involved in transactions for a client concerning the buying or selling of real estate are required to file the real estate sales contract, including the price to the relevant authority (*Act on Report on Real Estate Transactions etc.*, art.3(1) and (3)). Additionally, it is prohibited to register the rights to real estate in the name of another person (*Act on Registration of Real Estate under Actual Titleholder's Name*, art.3). However, these measures do not comply with most of the detailed CDD requirements under R.10.

(c)-(e) DPMS, lawyers, notaries, accountants and TCSPs are not required to apply CDD in line with R.10.

Criterion 22.2 – Casinos are required to comply with the same record keeping requirements as FIs under R.11.

All companies, including DNFBPs, are required to keep trade books and other documents relating to business for a period of ten years (*Commercial Act*, art.33). However, this does not cover all required records which must be kept pursuant to R.22.

Criterion 22.3 – Casinos are required to comply with the same PEPs requirements as FIs under R.12 and are subject to the same technical deficiencies. Other DNFBPs are not required to comply with the PEPs requirements under R.12

Criterion 22.4 – DNFBPs are not required to comply with the new technologies requirements under R.15.

Criterion 22.5 – DNFBPs are not required to comply with third party reliance requirements under R.17.

Weighting and Conclusion

Casinos are subject to the same technical deficiencies as FIs with regards to CDD and record keeping requirements under R.10 and R.12 and are not required to comply with the requirements under R.15 and R.17. For real estate agents, only limited CDD requirements and record keeping requirements apply. For DNFBPs other than casinos, only limited record keeping requirements and none of the requirements of R.10, R.12, R.15 and R.17 apply which is the most heavily weighted deficiency.

Recommendation 22 is partially compliant.

Recommendation 23 – DNFBPs: Other measures

In its 3rd MER, Korea was rated non-compliant with these requirements because no AML/CFT obligations applied to DNFBP sectors, except for casinos.

Criterion 23.1 – Casinos are required to comply with the same STR requirements as FIs under R.20. Other DNFBPs are not required to file STRs.

Criterion 23.2 – Casinos are required to comply with the same internal control requirements as FIs under c.18.1(b). There is no requirement for casinos to appoint a compliance officer as required by c.18.1(a). Other DNFBPs are not required to comply with the internal control requirements of R.18.

Criterion 23.3 – Casinos are required to comply with the same higher-risk countries requirements as FIs under R.19 and are subject to the same technical deficiency. Other DNFBPs are not required to comply with the higher-risk countries requirements of R.19.

Criterion 23.4 – Casinos are required to comply with the same tipping-off and confidentiality requirement as FIs under R.21. Other DNFBPs are not required to comply with the tipping-off and confidentiality requirements of R.21.

Weighting and Conclusion

Casinos are subject to the same technical deficiencies as FIs on R.19 (higher-risk countries). There is no requirement for casinos to appoint a compliance officer. Other DNFBPs are not subject to any of these requirements which is the most heavily weighted deficiency.

Recommendation 23 is partially complaint.

Recommendation 24 – Transparency and beneficial ownership of legal persons

Korea was rated not compliant with these requirements in its last MER. The technical deficiencies identified were: a lack of legislation establishing transparency of BO and control of legal persons; competent authorities were not able to obtain BO information; and no measures to prevent the misuse of bearer shares. Since then, the

FATF Standards in this area were significantly strengthened and Korea has amended and enacted a range of legislating relating to legal persons.

Criterion 24.1 – Korea has mechanisms in place to identify and describe the different types, forms, and basic features of legal persons. Korea has five types of company (partnership companies, limited partnership companies, limited liability companies, stock companies, and limited companies) and two types of non-profit corporations (associations and foundations). Information on the features and process for establishing the different types of legal persons (companies, associations and foundations) is publicly available online on the *Government for Business* site managed by the Ministry of SMEs and Start-ups (www.g4b.go.kr), the *Easy to Find, Practical Law* site managed by the Ministry of Government Legislation (www.easylaw.go.kr), and the *Invest Korea* site managed by the Korea Trade-Investment Promotion Agency (www.investkorea.org). However, these sites do not include information on the processes for obtaining and recording BO information. Information on recording basic and BO is available in the relevant legislation.

Criterion 24.2 – In January 2019, Korea finalised an assessment of the ML/TF risks associated with the types of legal persons created in Korea. The assessment was undertaken by a Korean law firm in co-operation with relevant government agencies including KoFIU, the MOJ, the NTS, and the KCS.

Basic Information

Criterion 24.3 – All companies, associations and foundations operating in Korea, including foreign companies, must be registered in order to operate (*Commercial Act*, art.172; *Regulation on Registration of Corporations under the Civil Act and Special Corporations*, art.6). To register, each legal person must submit certain information to the registry office administered by the Supreme Court (*Commercial Registration Act*, art.11; *Civil Act*, art.49; *Regulation on Registration of Corporations under the Civil Act and Special Corporations*, art.6). There are different registers for the different entity types.[69] Inclusion on the register serves as proof of incorporation. Each registry records the entity's name, address, a list of directors, rules relating to shareholdings and company representation, and partner/representative information (*Commercial Act*, arts.180, 183, 269, 271, 287-5, 317, 549, 549-2). The register information is publicly available at the registry office or on the registry website (www.iros.go.kr) (*Commercial Registration Reg.*, arts.26, 29).

Criterion 24.4 – Companies are required to maintain registry information at the principal office (i.e. the company's registered address) and at each branch office for stock and limited companies (see c.24.3; *Commercial Act*, arts.33, 266(1), 396, 566). It is not clear if a similar requirement exists for associations and foundations. Companies are required to maintain a register of shareholders and the name and categories of shares they hold and submit this information to the NTS (*Commercial Act*, arts.352, 396; *Corporate Tax Act*, art.119). Associations and foundations must keep a list of members (*Civil Act*, art.55).

Criterion 24.5 – Korea has some requirements in place to ensure basic and shareholder/member information is accurate and up-to-date. It is a criminal offence to provide inaccurate basic information to the register (*Criminal Act*, art.228) and

69. There are 11 company registries in Korea for: trade names, incompetent persons, legal representatives, managers, limited partnerships, general partnerships, joint-stock companies, limited liability companies, stock companies, limited companies, and foreign companies. For information on NPO registries, see R.8.

shareholder/member information must be accurate (*Commercial Act*, art.635; *Civil Act*, art.55). The registrars are empowered to examine the information submitted to the registry, but are not required to systematically verify the submitted information (see Chapter 7 on IO.5) (*Rule on Examination of Commercial Registration*, art.54). Korea requires legal persons to update any changes to basic registry information within two weeks (for companies) or three weeks (for associations and foundations) (*Commercial Act*, arts.183, 269, 287-5(4), 317(4), 549(4); *Civil Act*, art.52). Associations and foundations are required to update their list of members upon a change (*Civil Act*, art.55). Companies, associations and foundations are required to advise the NTS if there is a change to shareholdings or membership on an annual basis, which does not ensure the shareholder information is up-to-date (*Corporate Tax* Act, art.119). This information may be updated by the NTS as part of its ongoing tax monitoring, but such updates are not systematic (*Regulation on Handling of Corporate Tax*, arts.88-94).

Beneficial Ownership Information

Criterion 24.6 – Korea has three mechanisms in place that may allow competent authorities to obtain BO information, although this is not always available in a timely manner and some mechanisms are more focused on legal ownership rather than BO.

(a) Companies are required to obtain and hold a range of legal ownership information which may allow tracing of the beneficial owner where ownership is straightforward. Shareholder registry requirements (see c.24.4) require that companies maintain information on the "real holders" of stocks and provide this information to the NTS (*Enforcement Decree of the Corporate Tax Act*, art.161(6)). However, the concept of "real holders" is not defined in the legislation, so it is not clear that companies are keeping BO information in line with the FATF definition. Listed companies must maintain and submit to the FSC information on: executives, officers, and employees; significant shareholders (those with de factor control over company management); and shareholders owning over 5% between themselves and related persons (e.g. relatives or dependents) (*Capital Markets Act*, art.173; *Enforcement Decree of the Capital Markets Act*, arts.2, 125, 141, 147). Associations and foundations maintain information on their members. LEAs can obtain any of this information directly from the company, but only with a warrant meaning such information cannot be accessed during the intelligence phase of an inquiry (*Criminal Procedure Act*, art.199). While warrants can be obtained in a timely fashion (1-2 days), obtaining BO information in this way would require authorities to exercise multiple warrants at each layer of ownership, which is unlikely to allow timely access to the information. In addition, where foreign ownership is involved, authorities would need to resort to international co-operation methods, which may be time-consuming.

(b) Legal ownership information is also available through a comprehensive system of company registries that hold shareholder and investor information (see Chapter 7 on IO.5). Registry information is obtained either directly from the company or through the NTS. Competent authorities may access this information directly from the registries and could use it to trace BO through layers of legal persons, provided that BO aligns with legal ownership. This may be relatively timely where the ownership structure is comprised solely of Korean companies. However, where foreign companies are involved, the authorities will have to resort to less timely methods of acquiring BO information (e.g. obtaining MLA, as foreign companies are not subject to relevant disclosure requirements). Tracing BO information through the registers may also be more difficult where the corporate structure is particularly complex, and

involves entities not included in the registry (e.g. civil trusts, associations or foundations). Registry information is not systematically verified for accuracy (see c.24.7).

(c) There are requirements on FIs and casinos (but not other DNFBPs) to identify beneficial owners as part of CDD (see R.10, 22). Competent authorities can request this information through KoFIU where there is a related STR, CTR or foreign exchange transaction. FIs and casinos are required to respond to a KoFIU request for information without delay (*AML/CFT Reg.*, art.86). Alternatively, the NTS and the KCS are able to obtain information from FIs directly without a warrant (*Real Name Financial Transactions Act*, art.4). Other LEAs may obtain this information with a court warrant which can be obtained and executed urgently, but is generally less timely and is only available where there is an investigation (i.e. a warrant cannot be obtained for intelligence purposes). Obtaining BO information through this channel is dependent on the legal person having a relationship with a FI or casino, which is not guaranteed, especially in Korea's context in which professional intermediation is rare.

Criterion 24.7 – To the extent BO information is kept (see c.24.6), it is somewhat accurate and up-to-date.

Legal ownership information held by legal persons must be kept up-to-date but there are gaps as shareholder information held by the NTS need only be updated annually (*Corporate Tax Act*, art.119(1)). This information may also be updated by the NTS through ongoing tax monitoring, but such updates are not systematic. For publicly-traded companies, any changes in management, significant shareholders, or shareholders over 5% must be submitted to the FSC within five days (*Financial Investment Services and Capital Markets Act*, art.147).

Information on the registries is obtained from companies themselves. Some registries have verification processes but many are not systematically verified, so risk being inaccurate. In addition, the information on the registries is often updated infrequently (e.g. annually or quarterly) meaning the information is not consistently up to date (see Chapter 7 on IO.5).

FIs and casinos are required to obtain BO information at various intervals (see R.10, 22). However, these updates are based on materiality and risk, and may not ensure the BO information is always up-to-date.

Criterion 24.8 – Korea ensures companies co-operate with competent authorities to the fullest extent possible in determining the beneficial owner by requiring each company to have a designated company representative or executive that is obliged to co-operate with competent authorities on company matters (*Commercial Act*, arts.201, 269, 287-12). The company must record the representative's address in the company register (*Commercial Act*, arts.207, 269, 287-19, 408-4, 562, 614). However, there is no requirement that the company representative be resident in Korea which limits the utility of this requirement. Associations and foundations are required to have directors, but it is not clear that these representatives have explicit obligations to co-operate with competent authorities on determining beneficial ownership (Civil Act, art.57-59).

Criterion 24.9 – Korea has in place record-keeping rules for most of the entities and information referred to above. Basic information (c.24.3), including shareholder/membership information (c.24.4), on legal persons is maintained by the registry for at least five years, although the requirement to retain this information after the legal person ceases to exist is not explicitly clear (*Commercial Registration*

Rule, art.25; *Framework Act on National Taxes*, art.85-3; *Regulation on Registration of Corporations under the Civil Act and Special Corporations*, arts.3, 6). Legal persons and liquidators are required to maintain this information for ten years (*Commercial Act*, arts.33, 266, 269, 287-45, 541, 613). For BO information (c.24.6), FIs and casinos must maintain BO information obtained as part of CDD for at least five years (*AML/CFT Reg.*, art.84).

Other Requirements

Criterion 24.10 – Competent authorities, including supervisors, the NTS and LEAs, can obtain basic information on legal persons from the various company registries at any time. Access to BO information is somewhat limited by what is available (see c.24.6).

LEAs can obtain basic and legal ownership information directly from a company, although for most authorities this will require a warrant meaning such information cannot be accessed during the intelligence phase of an inquiry (see c.24.6; *Criminal Procedure Act*, art.199). Tracing the beneficial owner in this way may require multiple warrants, which is unlikely to be timely. Where foreign ownership is involved, more time-consuming international co-operation will be required.

Obtaining shareholder, membership, and investor information from relevant databases (see Chapter 7 on IO.5) is straightforward and timely and can allow authorities to trace BO relatively easily. However, more time-consuming international co-operation would be required where foreign ownership is involved. This method may also be problematic where the corporate structure was particularly complex (e.g. involving an association or civil trust). Information on the registries is largely unverified, so may not be accurate (see c.24.7).

Information on the executives, officers, and employees of publicly-traded companies, their significant shareholders (those with *de facto* control over company management), and shareholders with more than a 5% interest between themselves and related persons (e.g. relatives or dependents) is publicly available online and can be accessed by competent authorities (*Capital Markets Act*, art.173; *Enforcement Decree of the Capital Markets Act*, arts.2, 125, 141, 147).

LEAs can access BO information from FIs and casinos through KoFIU provided there is a related report. FIs and casinos must provide the information to KoFIU without delay, but there is no set timeframe for KoFIU to transmit the information to the requesting authority (*AML/CFT Reg.*, art.86). The NTS and the KCS are able to obtain information from FIs directly without a warrant (*Real Name Financial Transactions Act*, art.4). Other LEAs must obtain a warrant which can be done urgently, but is not available during the intelligence-gathering stage.

Criterion 24.11 – Korea no longer allows legal persons to issue bearer shares (*Commercial Act*, art.357 was abolished in May 2014). No bearer shares exist in Korea.

Criterion 24.12 – Neither nominee shareholders nor directors are permitted in Korea (*Real Name Financial Transaction Act*, art.6; *Punishment of Tax Evaders Act*, art.11).

Criterion 24.13 – Failing to register a company and provide the required information will result in the company not being formed (*Commercial Act*, art.172). If the basic information provided is not accurate and up-to-date, criminal sanctions of five years of imprisonment or a fine of up to KRW 10 million (EUR 7 800) may be imposed on

the person responsible for filing (*Criminal Act*, art.228). Sanctions are not available for the legal person itself.

For unlisted companies, failure to provide shareholder information to the NTS is punishable by a fine of 1/100th of the face value of the shares (*Corporate Tax Act*, art.75-2). There is no clear sanction for providing inaccurate information. For publicly-traded companies, failing to provide shareholder information to the FSS is punishable by up to three years in prison or a fine of up to KRW 100 million (EUR 75 500). Providing in accurate information is subject to sanctions of five years of imprisonment or a fine of KRW 200 million (EUR 154 000) (*Financial Investment Services and Capital Markets Act*, art.444). This fine may be imposed on an individual or the corporation.

No information was provided on the sanctions on legal persons or liquidators for failing to maintain records, or on the sanctions for failure to co-operate with competent authorities in determining the beneficial owner.

Using nominee shares is punishable by five years of imprisonment or a fine of KRW 50 million (EUR 37 300). Acting or using a nominee director is punishable by two years of imprisonment or a fine of KRW 20 million (EUR 15 600) (*Punishment of Tax Evaders Act*, art.11).

Criterion 24.14 – Korea can provide international co-operation in relation to basic and BO information, to the extent it is available in Korea:

(a) Basic information on company registries is accessible online (in Korean), and can be accessed by foreign authorities. Where authorities do not speak Korean, this information can be provided on request by KoFIU or LEAs (R.40).

(b) Korean authorities can exchange information on shareholders with foreign counterparts through formal MLA as well as through informal co-operation (see R.37 and R.40).

(c) Authorities' investigative powers can be used to obtain information where necessary (see R.37 and R.40).

Criterion 24.15 – Korea has systems in place to monitor requests for assistance received, including for basic and BO information. There is no formal system to monitor the quality of assistance provided in this regard, but this is done to some extent through Korea's generic case monitoring frameworks.

Weighting and Conclusion

Korea's legal framework on the transparency and BO of legal persons has a number of shortcomings in its framework relating to legal person transparency. Information is not publicly available on the processes for obtaining and recording BO information (c.24.1). It is not clear if associations and foundations are required to maintain registry information (c.24.4). The requirement for registers to maintain basic information following dissolution of a company is not explicitly clear (c.24.9). Competent authorities have the powers to obtain access to BO information during an investigation, but not always at the intelligence gathering phase, and access is not always timely particularly if international co-operation is needed (c.24.10).Sanctions for failing to ensure accurate and up-to-date basic information are not available for the legal person and it is not clear there are satisfactory sanctions for: failure to maintain an accurate and up-to-date register of shareholders or members; failing to maintain records; or failure to co-operate with competent authorities in determining

the beneficial owner (c.24.13). There is no formal system to monitor the quality of international assistance in obtaining basic and BO information beyond Korea's generic case monitoring frameworks (c.24.15).

There are moderate deficiencies with the availability of BO information. Korea has some mechanisms in place to make BO information available to competent authorities, although the information is not always available in a timely manner (c.24.6). Legal persons are not clearly required to keep shareholder and membership information held by the NTS up-to-date and registry information is not systematically verified for accuracy (c.24.5). Available BO information is somewhat accurate and up-to-date (c.24.7). Associations and foundations are not required to have a representative that is obliged to co-operate with competent authorities and company representatives do not have to be resident in Korea (c.24.8). These deficiencies are weighted more heavily in light of the number of ML and predicate offence cases which involve beneficial owners.

Recommendation 24 is partially compliant.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

In its 2009 MER, Korea was rated not compliant with these requirements. The technical deficiencies were: a lack of legislation establishing transparency of BO and control of legal arrangements; limited available information for competent authorities to obtain on the BO of legal arrangements; and failure to subject TCSPs to AML/CFT obligations. Since then, the FATF Standards in this area were strengthened.

Trusts in Korea are primarily governed by the *Trust Act*. This Act defines a trust as "a legal relation that a person who creates a trust (hereinafter referred to as "truster") transfers a specific piece of property (including part of business or an intellectual property right) to a person who accepts the trust (hereinafter referred to as "trustee"), establishes a security right or makes any other disposition, and requires the trustee to manage, dispose of, operate, or develop such property or engage in other necessary conduct to fulfil the purpose of the trust, for the benefit of a specific person (hereinafter referred to as "beneficiary") or for a specific purpose, based on a confidence relation between the truster and the trustee." (art.2). The *Trust Act* prescribes that a trust may be created by contract, by will, or by declaration.

Under the *Financial Investment Services and Capital Markets Act*, commercial trusts are designated as financial investment businesses and therefore qualify as a FI (art.6). Such trusts are therefore subject to relevant AML/CFT obligations.

Criterion 25.1 – Two types of trust exist in Korea: commercial trusts are administered by a professional trustee who must be approved by the FSC and must be a financial investment business (*Financial Investment Services and Capital Markets Act*, arts.6, 8, 11, 12), while civil trusts may be administered by any person. Civil trusts are extremely rare –no public or private sector representatives met during the on-site visit were aware of the existence of any civil trusts. Korea also recognises foreign trusts, which Korea confirmed are subject to the same requirements as civil trusts (*Trust Act*, art.2; *Act on Private International Law*, art.7). Foreign trusts are not common, but Korean authorities are aware of such structures operating in Korea.

(a) Commercial trustees are subject to Korea's AML/CFT requirements. They must submit to the NTS a declaration form identifying the settlor, trustee, beneficiary and

beneficial owner of the trust (*Inheritance Tax and Gift Tax Act*, art.82(4); *Enforcement Decree of the Inheritance Tax and Gift Tax Act*, art.84(4); *Inheritance Tax and Gift Tax Act Enforcement Rule*, art.24 and Annex 21; Trust Act, art.79). Civil and foreign trustees are only required to identify the beneficiary (*Trust Act*, arts.39, 79). Korean law does not recognise the concept of a protector of a trust.

(b) Commercial trustees are required to hold basic information on regulated agents or service providers to the trust (*Enforcement Decree of the Financial Investment Services and Capital Markets Act*, art.62(1)). There is no such requirement for civil or foreign trustees.

(c) All trustees (including those of civil and foreign trusts) must preserve trust information for at least five years (*Trust Act*, art.39; *Enforcement Decree of the Trust Act*, art.3; *AML/CFT Reg.*, art.84; *FTRA*, art.5-4; *Capital Markets Act*, art.60(1); *Enforcement Decree of the Capital Markets Act*, art.62(1); *Framework Act on National Taxes*, art.85-3).

Criterion 25.2 – Information held by commercial trustees must be accurate and updated quarterly (*Enforcement Decree of the Inheritance Tax and Gift Tax Act*, art.84(4); *Criminal Act*, art.231; *FTRA*, arts.11, 17). Civil and foreign trustees have no specific obligation to keep information accurate and up-to-date beyond a general prohibition on negligent bookkeeping (*Trust Act*, art.146).

Criterion 25.3 – All trustees are obliged to "disclose their status to financial institutions, etc." when forming a business relationship or carrying out an occasional transaction (*AML/CFT Reg.*, art.20(5)).

Criterion 25.4 – To the extent that the information is available, trustees are not prevented from providing competent Korean authorities with any information relating to the trust, whether in relation to a domestic matter or as part of an MLA request. Nor are trustees prevented from providing FIs or DNFBPs with any information relating to the BO or control or assets of the trust, provided they have such information.

Criterion 25.5 – Competent authorities, including LEAs, are able to access information held by trustees, including on BO, the residence of the trustee, and the trust assets, to the extent that this information is available (*Financial Investment Reg.*, art.4-13; *Trust Act*, art.40). Commercial trustees must provide such information within three days, but civil and foreign trustees are not subject to a specific timeframe. Where such information is available, KoFIU and supervisors are able to access BO information from FIs and casinos although KoFIU's ability to access such information is limited (see R.9 and R.29) (*FTRA*, arts.4(5), 10(3); *Capital Markets Act*, art.419(5)). Alternatively, the NTS and the KCS are able to obtain information directly from commercial trustees without a warrant (*Real Name Financial Transactions Act*, art.4). Other LEAs must obtain a warrant which can be done quickly, but cannot be used for intelligence gathering.

Criterion 25.6 – Korea can provide international co-operation in relation to trust information, including BO information, where this information is available (see R.37 and 40).

(a) There is no register of trusts in Korea, although information on assets held by commercial trustees is publicly available. Some information on trusts is maintained by the NTS (see c.25.1). This can be obtained by domestic authorities and shared with

foreign authorities but only with a warrant and pursuant to a MLA request (*Framework Act on National Taxes*, art.81-13).

(b) Competent authorities are able to exchange information on trusts that is available domestically with foreign counterparts.

(c) Authorities' investigative powers can be used to obtain BO information on trusts to the extent it is available (see R.40).

Criterion 25.7 – There is no general liability for Korean trustees that fail to perform their duties. Commercial trustees are subject to an administrative fine of KRW 100 million (EUR 78 400) for failure to obtain and maintain information on the settlor, trustee, beneficiary and beneficial owner of the trust (*FTRA*, art.17). If basic information is inaccurate, commercial trustees are subject to imprisonment of less than five year or a fine or up to KRW 100 million (KRW 75 250) (*Enforcement Decree of the Inheritance Tax and Gift Act*, art.84(4); *FTRA*, arts.11, 17). Failure to obtain and maintain beneficiary information is penalised by an administrative fine of KRW 5 million (EUR 3 900) for civil and foreign trustees, which is not proportionate or dissuasive, or up to three years of imprisonment and a fine of up to KRW 100 million (EUR 75 250) for commercial trustees (*Trust Act*, art.146(1); *Capital Markets Act*, art.445(11)). It is not clear that adequate sanctions are in place for civil and foreign trustees who fail to: maintain information on regulated agents (c.25.1(b)); keep basic information accurate (c.25.2); or disclose their status (c.25.3).

Criterion 25.8 – For a commercial trustee, failing to provide trust information to supervisory authorities is punishable by an administrative fine of KRW 100 million (EUR 75 250) (*FTRA*, art.17(1)). The same breach by civil trustees is punishable by KRW 5 million (EUR 3 900). This is too low to be dissuasive or to allow proportionate fines.

Weighting and Conclusion

Korea's legal framework for the transparency of legal arrangements has minor shortcomings, particularly in the framework for civil or foreign trustees. These trustees are only required to identify the beneficiary to a trust; are not required to hold information on regulated agents or service providers; have no explicit obligation to ensure trust information is accurate and up-to-date; and are not subject to a specific timeframe for providing information to competent authorities. Sanctions available for these trustees are not dissuasive or proportionate. These deficiencies are given less weight due to the rarity of civil trusts within Korea and the relatively limited use of foreign trusts. Trust information is often (but not always) available in a timely manner.

Recommendation 25 is largely compliant.

Recommendation 26 – Regulation and supervision of financial institutions

In its 3rd MER, Korea was rated partially compliant with these requirements on the basis of technical deficiencies relating to inadequate supervision, including the intensity and frequency of inspections of core principles institutions and other FIs.

Criterion 26.1 – KoFIU is the designated authority ultimately responsible for supervising FIs' compliance with AML/CFT requirements (*FTRA*, art.11(1)). KoFIU has the ability to entrust other authorities to be responsible for supervising one or more financial sectors (*FTRA*, art.11(6); *Enforcement Decree to the FTRA*, art.15). On

that basis, KoFIU has designated 11 other agencies (entrusted agencies) with responsibility for supervising the financial sectors (see Chapter 1).

Criterion 26.2 – Korea requires all FIs to be licensed or registered (Core Principles FIs must be licensed[70]) (*Banking Act*, *Financial Investment Services and Capital Markets Act*, *Insurance Act*, *Credit Co-operatives Act*, *FETA*, *Electronic Financial Transactions Act*, etc.). There is no explicit prohibition on the establishment, or continued operation, of shell banks, however, the licensing regime ensures that no shell banks are established.

Criterion 26.3 – Korea takes regulatory measures to prevent criminals or their associates from holding a significant or controlling interest, or holding a management function, in a FI. Korea requires fit and proper tests of "executive officers", including, directors, auditors, executive directors and operating officers, prior to appointment (*Act on Corporate Governance,* arts.5-7). However, the requirement does not explicitly extend to beneficial owners.

Criterion 26.4 –

(a) Core principle FIs are subject to regulation and supervision by the FSS in line with the Core Principles, including the application of consolidated group supervision.

(b) Small value remitters, electronic financial services providers, Korea Post and currency exchangers are subject to supervision for AML/CFT compliance (*FTRA*, art.2).

Criterion 26.5 – The frequency and intensity of on-site and off-site AML/CFT supervision of FIs is decided by the head of the relevant entrusted agencies (c.26.1). Inspections are required to be conducted on a risk sensitive basis (*Regulation on Examination of FIs AML/CFT Activities,* art.4), and include the following factors:

(a) the ML/TF risks and the policies, internal controls and procedures associated with the institution's or group's risk profile;

(b) the ML/TF risks present in the country; and

(c) the characteristics of the FIs or groups, in particular the diversity and number of FIs and degree of discretion allowed to them under the RBA.

Criterion 26.6 – KoFIU annually carries out a comprehensive assessment of FIs implementation of AML/CFT measures (*AML/CFT Reg.*, art.18). Additionally, KoFIU or the entrusted agencies are required to review FIs' risk assessments when major events or developments occur (*AML/CFT Reg.*, art.19(7)).

Weighting and Conclusion

All FIs are required to be licensed or registered. Criminals are prevented from holding a significant or controlling interest, but are not explicitly prevented from being the beneficial owner.

Recommendation 26 is largely compliant.

70. The Korea Development Bank, the Korea Industrial bank and the Korea Export-Import Bank are established and subject to requirements under the Korea Development Bank Act, the Export-Import Bank of Korea Act, and the Industrial Bank of Korea Act, respectively. The requirements in these acts have been assessed equivalent to a license, as required by Basel Core Principles 4, for banks.

Recommendation 27 – Powers of supervisors

In its 3rd MER, Korea was rated partially compliant with these requirements on the basis of technical deficiencies relating to an insufficient range of sanctions being available and the supervisory authorities having inadequate resources.

Criterion 27.1 – KoFIU is the designated supervisor for FIs and has powers to supervise and ensure compliance with AML/CFT requirements (*FTRA*, art.3(1)). KoFIU has entrusted 11 authorities (entrusted agencies) to supervise different financial sectors (see c.26.1) and ensure compliance with AML/CFT requirements (*FTRA*, art.11(6); *Enforcement Decree of the FTRA*, art.15(2)-(7)).

Criterion 27.2 – KoFIU and the entrusted agencies have the authority to conduct inspections of FIs (*FTRA*, arts.11(1) and (6)).

Criterion 27.3 – KoFIU and the entrusted agencies have the ability to request any information from supervised entities relevant to monitoring AML/CFT compliance (*FTRA*, art.11(7)).

Criterion 27.4 – KoFIU and the entrusted agencies have a range of sanctions available (*FTRA*, art.11(1)-(4)) including: issuance of a corrective order, warning or caution to a FI; and partially or fully suspending a license. Additionally, administrative sanctions can be applied to senior management (recommendation of dismissal, suspension of duties, warning and caution) and employees (removal, suspension, salary reduction and reprimand). For violations related to STR or CTR reporting, for verification and retention of CDD information and for failure to comply with orders, KoFIU can also impose administrative monetary sanctions (*FTRA*, art.17(2)). The sanctions available to supervisors are assessed proportionate and dissuasive.

Weighting and Conclusion

All criteria are met.

Recommendation 27 is compliant.

Recommendation 28 – Regulation and supervision of DNFBPs

In its 3rd MER, Korea was rated non-compliant with these requirements because there was no AML/CFT supervision of the DNFBP sectors, except for casinos.

Casinos

Criterion 28.1 –

(a) Casinos are required to obtain a license (*Tourism Promotion Act,* art.5).

(b) Korea has taken regulatory measures to prevent criminals or their associates from holding (or being the beneficial owner of) a significant or controlling interest, or being a casino operator (*Tourism Promotion Act,* art.22). However, this fit and proper test only applies to the person seeking to obtain a license or registration to operate a casino. It does not extend to beneficial owners, significant shareholders or senior management.

(c) Casinos are subject to supervision for AML/CFT compliance by KoFIU (*FTRA*, art.11, cf. art.2(1)(m)). KoFIU has delegated the authority to supervise casinos on Jeju Island to the SGP supervisor.

DNFBPs other than casinos

Criterion 28.2 – There is no designated authority or SRB responsible for monitoring and ensuring compliance of other DNFBPs with AML/CFT requirements.

Criterion 28.3 – Other DNFBPs are not subject to systems for monitoring compliance with AML/CFT requirements.

Criterion 28.4 – There is no designated authority or SRB responsible for monitoring and ensuring compliance of other DNFBPs with AML/CFT requirements. However, there are measures in place to prevent criminals from being professionally accredited (*Attorney at Law Act,* arts.4, 5; *Notary Public Act*, art.13, *Certified Public Accountant Act*, arts.8, 9; *Licensed Real Estate Agents*. art 10).

All DNFBPs

Criterion 28.5 – The frequency and intensity of on-site and off-site AML/CFT supervision of mainland casinos is decided by KoFIU, and the SGP supervisor for casinos on Jeju. Inspections are required to be conducted on a risk sensitive basis (*Regulation on Examination of FIs AML/CFT Activities*, art.4). Other DNFBPs are not subject to AML/CFT supervision.

Weighting and Conclusion

Casinos are required to obtain a license, however, only the person seeking a license is subject to fit and proper test, which does not prevent criminals and their associates from holding (or being the beneficial owner of) a significant or controlling interest, or being senior management. This deficiency is heavily weighted given the identified risks in Korea's gambling sector. Other DNFBPs are not subject to AML/CFT regulation or supervision, including fit and proper tests which is also weighted heavily. This deficiency is mitigated to a minor extent by the measures in various pieces of legislation preventing criminals from being professionally accredited.

Recommendation 28 is partially compliant.

Recommendation 29 - Financial intelligence units

Korea was rated largely compliant with these requirements in its 2009 MER. In addition to effectiveness concerns, the main technical deficiency was a lack of timely access to other agencies' financial, administrative and law enforcement information.

Criterion 29.1 – Korea has established a FIU, KoFIU, which acts as a national centre with responsibility for receiving and analysing STRs, CTRs, and information on foreign exchange transactions, and disseminating that analysis (*FTRA*, art.3).

Criterion 29.2 –

(a) KoFIU is the central agency for receiving STRs from reporting entities (*FTRA*, art.4).

(b) KoFIU is also responsible for receiving CTRs for cash transactions over KRW 10 million (EUR 7 800); reports on wire transfers over KRW 1 million (EUR 768) or USD 1 000 (EUR 904); data on export/import reports, and foreign exchange transaction reports (*FTRA*, arts.4-2, 5-3, 6; *Enforcement Decree to the FTRA*, art.8-2(1)).

Criterion 29.3 –

(a) KoFIU is able to request data from FIs where necessary to confirm the STR or CTR meets the legislative requirements, to obtain foreign exchange data, or to undertake its analysis of financial transaction information (*FTRA*, arts.4(5), 10(3)). In all other instances, this information can only be obtained with a court warrant in the context of an ongoing investigation.

(b) KoFIU has access to a wide range of financial, administrative and law enforcement information. This includes: information on foreign exchange transactions from the Bank of Korea (*FTRA*, art.6); cross-border declaration reports from the KCS (see R.32); criminal records, family relationship information, and resident records from the MOJ; credit information; business information; data on foreign investments; and land registry information (*FTRA*, art.10(1); *Enforcement Decree of the FTRA*, art.14(2)). KoFIU can also request information from the NPA, the SPO and other prosecutors' offices, or the NTA.

Criterion 29.4 –

(a) KoFIU conducts operational analysis to identify targets, follow transactions, and determine links between targets and potential criminal proceeds. Analysis occurs at both a computerised and human level using available STRs, CTRs, transaction records, foreign exchange transactions, and administrative and other information.

(b) Three teams within KoFIU conduct strategic analysis using available information to identify ML/TF patterns. Strategic analysis is conducted on certain themes, selected by KoFIU.

Criterion 29.5 – KoFIU disseminates the results of its operational and strategic analysis to LEAs depending on the offending identified. Dissemination can occur both spontaneously and upon request (*FTRA*, arts.10(1), 10(3)). Information is disseminated in an encrypted form through the KoFICS network which is a secure, government network that only approved KoFIU staff and end-users can access.

Criterion 29.6 –

(a) There are rules and guidelines in place governing the security and confidentiality of KoFIU information.[71] Strict rules are in place for KoFIU staff, end-users and reporting entities governing access to the information systems. Any mishandling of KoFIU information is criminalised (*FTRA*, arts.9(1), 13).

(b) KoFIU staff members' access to information depends on their rank, with the most sensitive information accessible to only three staff members (the Commissioner, the Head of Information Analysis, and the Information Analysis Supervisor). All KoFIU staff are subject to confidentiality commitments, including non-disclosure agreements, and undergo training on their responsibilities and the handling of confidential and sensitive data.

(c) Access to the KoFIU premises and information is limited. KoFIU staff, end-users and reporting entities all require access rights specific to their roles and functions which govern what information they are able to access/input in the system. The KoFIU premises are restricted and only authorised personnel may enter. Visitors are

71. KoFIU Guidelines on the Operation and Management of FIU Information System; KoFIU Guidelines on FIU Information Processing Work.

permitted only with prior approval and where accompanied. On-site computers require finger scanning and ID/password verification to access and activity is logged.

Criterion 29.7 –

(a) KoFIU is a subsidiary of the FSC and is made up of staff seconded from other Korean government agencies. Its Commissioner is appointed by the President on the recommendation of the FSC Chairman. Nonetheless, it performs its duties independently and under its own authority, including decisions to analyse, request, or disseminate information (*FTRA*, art.3(2); *Enforcement Decree of the FTRA*, art.5). KoFIU is required to report to the FSC only on matters of legislative amendments or when it is reporting to Cabinet. Intelligence analysis and dissemination priorities are set independently by the KoFIU Commissioner.

(b) KoFIU makes arrangements and independently engages with domestic and foreign authorities on its own behalf (*FTRA*, art.3(2)).

(c) Although KoFIU is located within the FSC, it has distinct, statutorily mandated core functions (*FTRA*, art.3).

(d) KoFIU's budget is part of a specific allocation and cannot be reallocated or redirected by the FSC. The KoFIU Commissioner has the authority to independently make decisions on redeploying or reorganising staff. However, due to a strict cap on the number of public officials in the Korean government, hiring new staff to KoFIU requires a Presidential Decree, which is required to be made with consideration to KoFIU's independence and political neutrality (*FTRA*, art.3).

Criterion 29.8 – KoFIU has been an unconditional member of the Egmont Group since 2002.

Weighting and Conclusion

All criteria are met.

Recommendation 29 is compliant.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

In its 2009 MER, Korea was rated largely compliant with requirements on the responsibilities of LEAs due to effectiveness concerns.

Criterion 30.1 – Korea has designated LEAs with responsibility for investigating ML, TF and predicate offences. The SPO and other prosecutors' offices, the NPA, and the KCG have responsibility for undertaking criminal investigations into ML, TF and predicate offences (*Criminal Procedure Act*, arts.195, 196). Investigations may also be undertaken by specific agencies (for example, the NTS for tax offences, the KCS for customs offences, the National Election Commission for electoral offences, and the FSC for capital markets offences).

Criterion 30.2 – The SPO and other prosecutors' offices are authorised to pursue the parallel investigation of ML/TF offences arising during the investigation of predicate offences (*Criminal Procedures Act*, art.195). Prosecutors may also delegate the investigation to the NPA, the KCG or other LEA depending on the nature of the offending.

Criterion 30.3 – All prosecutors are empowered to exercise search, seizure and various inspection powers (see R.31) with a view to identifying, tracing and freezing suspected criminal proceeds (*Criminal Procedure Act*, art.215; *Act on the Persons Performing the Duties of Judicial Police Officers and the Scope of their Duties*, art.6; *Procedure for the Punishment of Tax Evaders Act*, arts.9, 10; also see R.4). These powers can be exercised expeditiously with warrants usually taking 1-2 days to obtain, or less where necessary. The SPO and each prosecutors' office has specialised investigators and units for this purpose.

Criterion 30.4 – Recommendation 30 applies to all relevant authorities responsible for investigating predicate offences. Officials at authorities that are not solely LEAs (e.g. the KCA, the NTS, the FSC) may be designated "special judicial police" for the purpose of undertaking enquiries into relevant offences prior to submitting the case to the relevant prosecutors' office for criminal investigation (*Act on the Persons Performing the Duties of Judicial Police Officers and the Scope of their Duties*, art.6; *Procedure for the Punishment of Tax Evaders Act*, arts.1, 9, 10).

Criterion 30.5 – Anti-corruption authorities in Korea are not designated to investigate ML/TF offences arising from or related to corruption. The Anti-Corruption and Civil Rights Commission is a policy body and has no law enforcement or investigative role. Corruption cases and any related ML are investigated by prosecutors and/or the NPA.

Weighting and Conclusion

All criteria are met.

Recommendation 30 is compliant.

Recommendation 31 - Powers of law enforcement and investigative authorities

In its 3rd MER, Korea was rated largely compliant with the requirements related to law enforcement powers due to effectiveness concerns. The new technical requirements are much more detailed. The relevant competent authorities are the SPO and other prosecutors' offices, the NPA, and the KCG. Other authorities (e.g. the NTS, the KCS or the FSC) may also be able to exercise certain law enforcement powers either through designation as a "special judicial police officer" or via specific empowering provisions.

Criterion 31.1 – Competent authorities investigating ML, TF and predicate offending are able to obtain access to the necessary documents and information.

(a) All competent authorities, as well as the NTS and the FSC, can obtain records from FIs, DNFBPs, and other natural and legal persons through search, seizure, and inspection orders, demands for documents or information, and orders for financial, transaction, or taxation information, all of which are available with a warrant (*Criminal Procedure Act*, arts.215-217; *POCA*, art.10(3); *Procedure for the Punishment of Tax Evaders Acts*, art.8-10; *Financial Investment Services and Capital Market Act*, art.427).

(b) All competent authorities, as well as the NTS and the FSC, can search persons and premises with a warrant or without a warrant either upon arrest or in urgent circumstances (*Criminal Procedure Act*, arts.215-217, *Procedure for the Punishment of*

Tax Evaders Acts, art.8-10; *Financial Investment Services and Capital Market Act*, art.427).

(c) All competent authorities, as well as the KCS and the FSC, can request a witness to submit to a recorded interview. If the witness refuses, a judicial order can be obtained for a witness interrogation (*Criminal Procedure Act*, art.221, 221-2; *Financial Investment Services and Capital Market Act*, art.427). The NTS is also able to interview suspects, testifiers, or witnesses to tax offences (*Procedure for the Punishment of Tax Evaders Act*, art.8).

(d) All competent authorities, as well as the NTS and the FSC, can seize evidence with a warrant or without a warrant either upon arrest or in urgent circumstances (*Criminal Procedure Act*, arts.215-217; *Procedure for the Punishment of Tax Evaders Acts*, art.8-10; *Financial Investment Services and Capital Market Act*, art.427).

Criterion 31.2 – Competent investigative authorities are able to use some other investigative techniques for ML, TF and predicate investigations.

(a) All competent authorities, as well as the KCS, can use "pitfall operations" which are comparable to undercover operations. Pitfall operations cannot be used where they would create criminal intent (i.e. entrapment), which is a reasonable limitation (Supreme Court #82DO2433).

(b) All competent authorities, as well as the KCS, can intercept communications with a court warrant (*Protection of Communications Secrets Act*, arts.2, 5, 6).

(c) All competent authorities, as well as the KCS, can access computer systems with a court warrant using search and seizure powers (*Criminal Procedure Act*, art.215; Supreme Court #2011MO1839).

(d) All competent authorities, as well as the KCS, can perform controlled delivery for drug-related offending in accordance with specific guidelines and with a licence obtained from the head of a customs office (*ASPIT*, art.4). Controlled delivery is not available for other offences.

Criterion 31.3 –

(a) Korea has mechanisms available to identify whether natural or legal persons hold or control accounts. All competent authorities, as well as the KCS, can obtain this information through account tracing warrants which are typically issued in a timely manner (*Criminal Procedure Act*, art.215). These agencies and the NTS can also obtain this information from KoFIU within one week, if it is available, provided the information is requested in the context of investigations into ML, TF, and certain tax and customs offences (*FTRA*, art.7). The KCS, the NTS, and the FSC can also obtain this information directly from FIs in a timely manner where the request relates to matters within their mandate (e.g. customs breaches, tax inquiries, etc.) (*Real Name Financial Transaction Act*, art.4(1)).

(b) Account tracing warrants can be obtained on an *ex parte* basis (*Act on Real Name Financial Transactions and Confidentiality*, art.4(1)). Where information is obtained through KoFIU, the account holder does not receive prior notification.

Criterion 31.4 – All competent authorities, as well as the KCS and the NTS, can request information from KoFIU on STRs, CTRs, foreign exchange transactions, immigration, criminal records, family relationships and credit reports. However, information can only be requested in relation to investigations into ML, TF and certain tax and customs offences (*FTRA*, art.7).

Weighting and Conclusion

There are some minor shortcomings in the powers available to Korean LEAs. Controlled delivery is available only for drug-offending, and not for other smuggling or trafficking crimes, although this is weighted less heavily given Korea's risk areas. The information held by KoFIU can only be requested by LEAs in the context of investigations into ML, TF and certain tax and customs offences. This deficiency is minor, but is weighted most heavily as it omits certain high-risk predicate offences.

Recommendation 31 is largely compliant.

Recommendation 32 – Cash couriers

In its 2009 MER, Korea was rated largely compliant with these requirements. The main technical deficiency was that sanctions for persons who do not make declarations or who make false declarations were too limited (only fines) and too low to be dissuasive.

Criterion 32.1 –Korea implements a written declaration system for travellers arriving or departing Korea carrying more than USD 10 000 (EUR 8 800) of currency and/or BNIs (*FETA*, art.17; *FETA Reg.*, art.6-2(2)(1)). Declarations are made to the relevant KCS office. For incoming or outgoing mail and cargo, transports of more than USD 10 000 (EUR 8 800) must be declared to the relevant KCS office with documents proving the necessity and cause of the transportation (*FETA Reg.*, art.6-3).

Criterion 32.2 – All persons entering or leaving Korea with currency or BNIs totalling more than USD 10 000 (EUR 8 800) must declare this to the KCS office at their port of arrival or departure. Where such a declaration is made, KCS officers verify the identity of the traveller, the amount of funds and the source of wealth (*FETA Reg.*, arts.6-2, 6-3). Additional requirements apply to: (a) foreigners who must also obtain verification from the chair of the relevant foreign exchange bank before transporting over USD 10 000 (EUR 8 800) (*FETA Reg.*, art.6-2(2)(3)); and (b) non-residents who must also prove the necessity and cause of the transportation (*FETA Reg.*, art.6-3).

Criterion 32.3 – This criteria is not applicable because Korea has a declaration system.

Criterion 32.4 – For all declarations, including on discovery of a false declaration, KCS (or the KCG if the declaration occurred at sea) has the authority to request and verify information on the rationale for transportation, the amount and the intended use (*FETA*, arts.20, 23; *Enforcement Decree of the FETA*, art.37; *FETA Reg.*, art.6-4). Where there is a failure to declare, officers have the authority to ask questions regarding the funds (*Act on Persons Performing the Duties of Judicial Police Officers and the Scope of Their Duties*, arts.5(17), 6(14)(1)).

Criterion 32.5 – (Persons who make a false declaration or who fail to declare are subject to a fine proportionate to the incorrectly declared or undeclared amount. A discrepancy of more than USD 30 000 (EUR 26 400) is punishable by criminal sanctions of 1 year of imprisonment or a fine amounting to the higher of KRW 100 million (EUR 78 400) or three times the amount undeclared or incorrectly declared (*FETA*, art.29(1)(4); *Enforcement Decree of the FETA*, arts.40(2)). A discrepancy of less than USD 30 000 (EUR 26 400) is punishable by an administrative

fine of up to KRW 50 million (EUR 38 200) or 5% of the amount.[72] A fine of 5% of the undeclared or falsely declared amount may not be sufficiently proportionate (*FETA*, art.32(2)(3); *Enforcement Decree of the FETA*, art.41).

Criterion 32.6 – Information obtained by the KCS through the declaration process is available to KoFIU through a monthly electronic report in which the KCS provides all cross-border declarations from the previous month (*FTRA*, art.6(1); *Enforcement Decree of the FTRA*, art.11).

Criterion 32.7 – Korea has systems in place to ensure information-sharing and co-operation procedures between the KCS, the immigration service, and air and sea-port authorities, including to detect and prevent cross-border cash and BNI movements. These authorities also co-ordinate through informal mechanisms and *ad hoc* joint investigations.

Criterion 32.8 – A general provision allows the KCS to stop or restrain currency or BNIs for an unspecified period of time where there is a failure to declare (*FETA Reg.*, art.6-4; *FETA*, art.15). On its face, the provision is limited and does not appear to allow restraint on the basis of a false declaration, or a ML or TF suspicion. However, Korea has demonstrated that in practice, the provision is applied in such circumstances. In addition, where ML or TF is suspected, the KCS has the power to arrest or detain suspects and may seize or restrain the suspect's property without a warrant under urgent circumstances (*Criminal Procedure Act*, art.216).

Criterion 32.9 – Korea's declaration system allows for international co-operation and assistance (see R.36-40). To facilitate such co-operation, the KCS retains all declarations, including false declarations for a period of five years (*Customs Act*, art.327(1); *Public Notice on the Use and Operation of the Comprehensive Customs Duties Information Network of Korea*, art.327(1)). The KCS also retains all investigation information for ten years, including details of instances where there was a suspicion of ML or TF.

Criterion 32.10 – Korea ensures that safeguards exist to ensure proper use of information collected through its declaration system. This information is stored in a secure database with restrictions on use (*FETA*, art.22; *Customs Act*, art.327-4). The declaration system does not unreasonably restrict legitimate travel and trade. These safeguards do not restrict trade payments or the freedom of capital movements.

Criterion 32.11 – Persons who transport currency or BNIs related to ML or TF may be subject to penalties for false declarations or failing to declare (if applicable) (see c.32.5) or to ML/TF offences. However, the penalties for ML and TF are not sufficiently proportionate or dissuasive (see R.3 and R.5). Currency or BNI related to suspected ML or TF would be subject to seizure and confiscation (see R.4).

Weighting and Conclusion

The administrative sanctions available for lower-level false declarations or for carrying currency or BNIs related to ML/TF or predicate offences are not sufficiently proportionate or dissuasive. This is a minor deficiency as criminal sanctions for more serious offending are not sufficient.

Recommendation 32 is largely compliant.

72. If it is the second such offence within two years, the fine may be increased to 7% of the amount (Enforcement Decree of the FETA, arts.40(2).

Recommendation 33 – Statistics

In its 2009 MER, Korea was rated partially compliant with these requirements. The main technical deficiencies were a lack of centralised statistics on the number of AML/CFT inspections and their results, and the unavailability of statistics on the outcomes of court matters.

Criterion 33.1 – Korea keeps statistics on matters relevant to the effectiveness and efficiency of their AML/CFT system.

(a) Korea maintains statistics on STRs and CTRs received, cases disseminated, and the outcomes of those cases. This data can be broken down by sector providing the report, as well as by predicate offence.

(b) Korea keeps data on the number of ML and TF investigations, prosecutions, and convictions. Investigation and prosecution data can be broken down by predicate offence.

(c) Korea keeps data on the number of orders and the value of property frozen, seized and confiscated. This data can be broken down by offence.

(d) Korea keeps statistics on MLA and extradition requests, including on the requesting/requested state and the type of request.

Weighting and Conclusion

All criteria are met.

Recommendation 33 is compliant.

Recommendation 34 – Guidance and feedback

In its 2009 MER, Korea was rated largely compliant with these requirements on the basis that the only available guidance was generic for all obliged entities and there were no guidelines on AML/CFT requirements for different sectors.

Criterion 34.1 –

Supervisory guidance and outreach to FIs and DNFBPs

KoFIU is the responsible authority for supervising FIs' and casinos' compliance with AML/CFT compliance. KoFIU is required to research ML and TF trends and to provide training and education to FIs to combat ML/TF (*Enforcement Decree of the FTRA*, art.5). KoFIU has established guidelines and feedback procedures to assist FIs and casinos in complying with AML/CFT measures, particularly in detecting and reporting suspicious transactions (see section below on STR Guidance).

KoFIU has a common practice of publishing guidelines where urgent measures are required to address major AML/CFT risks and vulnerabilities. On that basis, KoFIU published guidance in January 2018 covering virtual assets (*Guidelines on Virtual Assets*) to guide FIs in effectively implementing their AML/CFT requirements when dealing with virtual assets which the NRA has assessed as a high-risk area. KoFIU is empowered to assess the implementation of relevant AML/CFT measures and in this context, if necessary, help FIs and casinos to improve their existing policies (*AML/CFT Reg.*, Section 6 of Part I (for FIs) and Section 5 of Part II (for casinos)).

Semi-annual meetings of the Private Sector Consultation Committee chaired by KoFIU are held with participation from the financial sector and casino associations (*Regulations on the Establishment and Operation of the AML/CFT Co-ordination Committee etc.*, art.30). This is the co-ordinating body for obtaining feedback from supervised entities on compliance with AML/CFT requirements and, if needed, proposing amendments to current legislation (*Regulations on the Establishment and Operation of the AML/CFT Co-ordination Committee etc.*, art.10). The committee is comprised of several private and public sector participants, including KoFIU.

No guidance has been provided on how to implement TFS obligations.

Guidance and feedback on STRs and CTRs

KoFIU provides LEAs with an annual report on STR reporting in the *Money Laundering Trends Review*. This provides examples of well-prepared and poorly-prepared STRs, but is not distributed to FIs or casinos.

For reporting entities, KoFIU distributes a report on *Case Studies: Suspicious Transactions* which provides guidance on the types and patterns of suspicious behaviour, including the types of suspicious transaction common to each sector, to help them identify suspicious transactions. This guidance is distributed by KoFIU and through industry associations. The report is updated every two to three years to take into account the latest trends. KoFIU has also published other guidelines and directions aimed at improving the quality of STRs: *Request for Stronger STR on Block Deal; Notify CTR Directions; Stronger CDD and STR on Virtual Currency; Notify Directions for High-Risk Companies and Representatives;* and *TF Risk Index by FATF and Type of Major TF Suspicion and its Analysis.*

The Private Sector Consultation Committee is also used to discuss STR quality. Regular meetings are held with AML/CFT relevant agencies to improve the quality of STRs. These meetings are used to generate annual feedback and feed into the reports and guidance mentioned above. KoFIU also provides individual feedback to reporting entities upon receipt of a STR. Finally, KoFIU issues an annual report which includes major analyses and STR types.

Weighting and Conclusion

Korea has provided outreach and guidance to the FIs and casinos. This includes emerging and new risks and feedback on STR and CTR reporting. However, no guidance has been provided to obliged entities on how to implement their TFS obligations.

Recommendation 34 is largely compliant.

Recommendation 35 – Sanctions

In its 3rd MER, Korea was rated partially compliant with these requirements, on the basis of the following technical deficiencies: sanctions for non-compliance with AML/CFT obligations were not proportionate and were limited to lack of STR/CTR reporting and lack of conducting financial transactions for designated persons.

Criterion 35.1 – Korea has the ability to apply criminal and administrative sanctions to natural and legal persons failing to comply with the AML/CFT requirements of R. 6, and R.8 to 23.

(a) Targeted financial sanctions (R.6): Criminal sanctions are applicable to any person who provides, raises, transports or keep funds for a designated person of imprisonment with labour not more than 10 years or a fine not exceeding KRW 100 million (EUR 78 000) (*PFOPIA*, art.6). Criminal sanctions are applicable to designated persons if the person in question fraudulently obtains permission to access funds. The penalty is imprisonment with labour for not more than three years or by a fine not exceeding KRW 30 million (EUR 22 622) (*PFOPIA*, art.6(2)1). The sanctions available are assessed to be proportionate and dissuasive.

Criminal sanctions can be applied to FIs, but only in situations where an employee has made a financial transaction or received a payment involving a designated person (*PFOPIA*, art.7, cf. art.5(1)). DNFBPs who have any type of transactions with designated persons or entities are subject to imprisonment for not more than three years or a fine of KRW 30 million (*PFOPIA*, art.6(2)). FIs and casinos are subject to sanctions for not freezing terrorist-related assets pursuant to the freezing mechanism. Other DNFBPs are not required to freeze such assets and therefore no sanctions apply to them (see R.6).

(b) NPOs (R.8): Korea can apply effective, and dissuasive sanctions for violations of the requirements applicable to NPOs. However, the applicable sanctions are not proportionate in all cases. See analysis c.8.4(b).

(c) Preventive measures and reporting (R.9-23): FIs and casinos failing to comply with AML/CFT requirements are subject to administrative measures. The administrative measures available to the KoFIU and the FSS include issuance of a corrective order, warning, caution to an FI, and partially or fully suspending a license (*FTRA*, art.11(1)-(4); *Banking Act*, art.53; *Financial Investment Services and Capital Markets Act*, art.335(2); *Mutual Savings Bank Act,* art.24; *Insurance Business Act*, art.134; *Specialised Credit Financial Business Act*, art.53).

KoFIU has the ability to impose administrative fines on FIs and casinos for failure to comply with most preventive measures (except for R.16). Violation of R.16 obligations are subject to a range of other sanctions, and subject to administrative fines in situations where FIs or casinos do not comply with a rectifying order. Administrative fines cannot exceed KRW 100 million (EUR 75 230) (*FTRA*, art.17(1)) for failings to report as per art.4 (STRs) and art.4-2 (CTRs), and failure to take necessary CDD measures as prescribed by art.5-2 of the *FTRA* (including measures covered by the *AML/CFT Regulation* in this regard). This administrative fine is also applicable in cases of failure or refusal to comply with the administrative obligations which can be imposed on FIs by the KoFIU as part of its supervisory activities (*FTRA*, art.11). For failings related to the record keeping requirements, the administrative fines cannot exceed KRW 30 million (EUR 22 706) (*FTRA*, art.17(2)). The sanctions applicable can be imposed concurrently for each identified violation. The level of applicable administrative fines is proportionate and dissuasive under all circumstances.

There are no sanctions available for non-compliance or violations by DNFBPs, other than casinos, as these DNFBPs are not yet subject to AML/CFT requirements.

Criterion 35.2 – KoFIU and its entrusted agencies have a range of administrative sanctions applicable to directors and senior management of FIs and casinos including recommendation of dismissal, suspension of duties, warning and caution (*FTRA*, art.11(1)-(4)). Additionally, employees are subject to administrative sanctions (removal, suspension, salary reduction and reprimand) (*FTRA*, art.11(1)-(4)).

Criminal sanctions can also be imposed on persons for violating confidentiality requirements (*FTRA*, arts.13, 14). The penalty ranges from imprisonment for not more than five year with labour and/or a fine not exceeding KRW 50 million (EUR 39 020). The sanction for violating *FTRA*, arts.13 and 14 can be applied concurrently where a person is sentenced to imprisonment with labour and a fine (*FTRA*, art.15).

Other than casinos, no sanctions for non-compliance or violations apply to directors and senior management of other DNFBPs as these entities are not yet subject to AML/CFT requirements.

Weighting and Conclusion

Korea can apply effective and dissuasive sanctions for violations of the requirements applicable to NPOs, but sanctions are not proportionate in all cases. DNFBPs, other than casinos, are not subject to TFS requirements including freezing, and thereby not subject to sanctions for violation. Sanctions for non-compliance with preventive measures are assessed to be proportionate and dissuasive. No sanctions apply to directors and senior management of DNFBPs, other than casinos, for AML/CFT violations. The deficiencies related to uncovered DNFBPs have been given less weight, as these are of lower importance in the Korean context (see Chapter 1, para.78).

Recommendation 35 is largely compliant.

Recommendation 36 – International instruments

Korea was rated partially compliant with these requirements in its last evaluation. The main technical deficiencies were issues in implementing the Vienna and TF Conventions, and no ratification or implementation of the Palermo Convention. Since its 2009 evaluation, Korea has ratified the Palermo Convention and amended its ML and TF offences.

Criterion 36.1 – Korea is a party to the Vienna Convention (ratified in December 1998), the Palermo Convention (ratified in May 2015), the Merida Convention (ratified in March 2008), and the TF Convention (ratified in February 2004).

Criterion 36.2 – By amending its ML and TF offences and confiscation regime (see R.3-5), Korea has addressed most of the deficiencies relating to its implementation of the Vienna, Palermo and TF Conventions. However, some limitations remain in Korea's implementation of the TF Convention (see R.5) and, as in its 3rd round MER, Korea has not yet chosen to implement the option to consider concluding agreements on disseminating recovered proceeds to intergovernmental bodies (Vienna Convention, art.5(5)(b)). The UNCAC Implementation Review Group identified some issues with Korea's implementation of the Merida Convention, including: the scope of bribery and corruption offences included as predicate offences is limited; there are no general provisions providing for the liability of legal persons for corruption offences (with the exception of foreign bribery); and the preparation of certain corruption offences is not criminalised.[73]

73 UNCAC Implementation Review Group, Review of Republic of Korea (2013).

Weighting and Conclusion

Korea has largely implemented the Vienna, Palermo, Merida, and TF Conventions. Minor deficiencies remain in its implementation of the TF Convention (see R.5) and the Vienna Convention (Korea has not considered concluding agreements on disseminating recovered proceeds to intergovernmental bodies.) Some minor issues were also identified by the UNCAC Implementation Review Group in its implementation of the Merida Convention.

Recommendation 36 is largely compliant.

Recommendation 37 - Mutual legal assistance

In its 2009 MER, Korea was largely compliant with these requirements. The main technical deficiency was a lack of mechanisms for determining the best venue for prosecution of defendants.

Criterion 37.1 – Korea has a legal basis for rapidly providing a wide range of MLA to any country in respect of ML, TF and predicate offence proceedings. This includes: locating persons or evidence; providing documents or records; searching or seizing evidence; conducting hearings; and asset recovery. MLA can be provided for all offences, without the need for dual criminality, meaning the limitations identified in R.3 and R.5 do not impact Korea's ability to provide MLA (*Act on International Judicial Mutual Assistance in Criminal Matters* (*MLA Act*), arts.1, 2, 5; *ASPIT*, arts.64-78; *POCA*, art.12; *Act on Special Cases Concerning the Confiscation and Return of Property Acquired Through Corrupt Practices* (*Corrupt Property Confiscation Act*), art.8; 30 bilateral and multilateral treaties).

Criterion 37.2 – The MOJ acts as the central authority for MLA requests, although such requests must be received through diplomatic channels. There are clear statutory processes for the execution of requests (set out in the *MLA Act*). Requests are typically handled in the order they are received, but can be executed more rapidly if requested and diplomatic channels can be bypassed in urgent cases (*MLA Act*, art.11). To monitor progress on requests, the MOJ maintains a case management system which tracks the requesting/requested country, the date received/sent, details of assistance requested, the executing agency, and the progress made.

Criterion 37.3 – MLA is not prohibited or made subject to unreasonable or unduly restrictive conditions. Discretionary grounds for refusal are consistent with international norms (e.g., where the offence is political in nature, there is a lack of dual criminality, the proceedings amount to persecution, etc.) (*MLA Act*, art.6; MLA treaties).

Criterion 37.4 – Korea cannot refuse MLA requests solely on the basis that the offence involves fiscal matters, or on the grounds of financial secrecy (*MLA Act*, art.6; bilateral and multilateral MLA treaties).

Criterion 37.5 – Korea's MLA treaties require Korea to maintain the confidentiality of MLA requests received and the information therein. Divulging information on "official secrets" obtained in the course of a public official's duties is a criminal offence, and this has been interpreted broadly to capture matters relating to criminal investigations (*Criminal Act*, art.127; Supreme Court #2014DO11441).

Criterion 37.6 – Dual criminality is not a condition for Korea to provide assistance involving either coercive or non-coercive actions. This is also the case for most MLA

treaties. However, a lack of dual criminality is a discretionary ground upon which Korea can refuse MLA requests (*MLA Act*, art.6). In practice, such refusals are relatively rare.

Criterion 37.7 – Dual criminality is not required for MLA. When considering its discretionary grounds for refusal, dual criminality is interpreted based on the underlying conduct rather than the words or categorisation of the offence. For treaty-based requests, most treaties provide that dual criminality is not necessary or will be deemed met for conduct covered by the treaties.

Criterion 37.8 – Powers and investigative techniques that are required under R.31 and available to domestic authorities are also available in response to MLA requests. These include production, search and seizure, and taking witness statements. Korea is also able to exercise a broad range of other powers, including communication interception or access to computer information, as any power available to Korean authorities can be exercised in response to a MLA request (*MLA Act*, arts.5, 17; 30 bilateral and multilateral treaties).

Weighting and Conclusion

Korea's legal framework for MLA is broadly consistent with the FATF Standards. While a lack of dual criminality is a discretionary ground for refusing coercive and non-coercive MLA, this has not been weighted heavily as it is rarely seen in practice.

Recommendation 37 is largely compliant.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

Korea was largely compliant with these requirements in its 3rd round evaluation due to insufficient formal arrangements for co-ordinating seizure and confiscation actions.

Criterion 38.1 – Korea is able to identify, freeze, seize and confiscate assets on behalf of requesting country (*MLA Act*, art.5; *POCA*, arts.11, 12; *ASPIT*, art.64). These powers apply to laundered property, proceeds, and instrumentalities used or intended for use in ML, TF and predicate offending, as well as property of corresponding value (*ASPIT*, arts.64-78; *POCA*, art.12; *Criminal Procedures Act*, art.215; *Criminal Act*, art.48; *Corrupt Property Confiscation Act*). Also see R.4.

Criterion 38.2 – Korea has the statutory authority to provide assistance in response to requests relating to non-conviction based confiscation and provisional measures. Such requests can be executed provided there is a final freezing or confiscation order (*POCA*, art.11; *ASPIT*, art.64).

Criterion 38.3 – Some of Korea's bilateral MLA treaties include provisions for co-ordinating seizure and confiscation actions with other countries. In other cases, co-ordination may occur on an *ad hoc* basis through available networks (see R.40). The mechanisms for managing and disposing of confiscated property are the same as for domestic confiscation (see R.4)

Criterion 38.4 – Korea is able to share confiscated property with other countries on an *ad hoc* basis. Formal rules are in place for sharing the proceeds of corruption (*Corrupt Property Confiscation Act*). For all other offences, Korea is able to share confiscated property on an *ad hoc* basis.

Weighting and Conclusion

All criteria are met.

Recommendation 38 is compliant.

Recommendation 39 – Extradition

In its 2009 MER, Korea was largely compliant with these requirements. The sole technical deficiency was that it was not required to prosecute nationals in lieu of extraditing them.

Criterion 39.1 – Korea is able to execute extradition requests in relation to ML and TF without delay (*Extradition Act*, arts.13-14).

(a) ML and TF are extraditable offences (*Extradition Act*, art.6; extradition treaties). However, the limitations identified in Korea's ML and TF offences (see R.3 and R.5) may mean there are instances where Korea is unable to provide extradition.

(b) The MOJ has an electronic case management system for extradition requests which tracks timelines, individuals involved and charges. There is a statutory process for extradition (set out in the *Extradition Act*) which includes timeframes to ensure the timely execution of requests. The MOJ prioritises requests based on the seriousness of the offence, although other factors may also be considered.

(c) Korea does not place unreasonable or unduly restrictive conditions on the execution of requests. Mandatory and discretionary grounds for refusal are in line with international norms. For example, mandatory grounds for refusal include: where the statute of limitations has expired; where the person sought has already been convicted or acquitted; or where there is no probable cause for the extradition offence; etc. (*Extradition Act*, arts.7, 8). Discretionary grounds for refusal include: where the person sought is a Korean national; where Korea has jurisdiction; where proceedings are already ongoing in Korea or a third state; or where extradition would be inhumane (*Extradition Act*, art.9).

Criterion 39.2 – Korea has the discretion to refuse to extradite its own nationals (*Extradition Act*, art.9). This discretion has never been exercised in practice. Korea's extradition treaties generally state that such cases would be submitted to domestic authorities upon request for the purpose of prosecution. For requests made outside the treaty framework, there is no explicit statutory provision requiring submission of the case for the purpose of prosecution to domestic authorities upon request, although the relevant prosecutors' office has a general duty of investigation where there is a suspicion of an offence.

Criterion 39.3 – Dual criminality is required for extradition (*Extradition Act*, art.6). Dual criminality is interpreted based on the underlying conduct rather than the words or categorisation of the offence. This is specified in most of Korea's extradition treaties.

Criterion 39.4 – Korea has simplified extradition mechanisms in place where the sought person consents to extradition (*Extradition Act*, art.15-2). Korea also permits provisional requests for arrest in advance of a formal extradition request.

Weighting and Conclusion

Korea's extradition framework is broadly consistent with the FATF Standards, with only minor shortcomings. The deficiencies in Korea's ML and TF offences (see R.3 and R.5) may impair Korea's ability to provide extradition in such cases. There is no explicit requirement to prosecute on request where an extradition request is denied for nationality, although this has been weighted less heavily as there is a general duty of investigation and Korea has never exercised its discretion to refuse to extradite its own national.

Recommendation 39 is largely compliant.

Recommendation 40 – Other forms of international cooperation

Korea was largely compliant with these requirements in its last MER. The technical deficiencies were that information exchange was only possible under an MOU and issues in the scope of the ML/TF offences. Korea has since revised its ML/TF offences (see R.3 and R.5).

Criterion 40.1 – Competent authorities (KoFIU, the SPO, the NPA, the KCG, the KCS, the NTS, the FSC and the FSS) can exchange a wide range of information and co-operate informally in relation to ML, TF and predicate offending. In general, co-operation can be provided rapidly, both spontaneously and on request (KoFIU: *FTRA*, art.8(1); the SPO: *Regulation on Establishment and Management of International Co-operative Task Force by Supreme Prosecutors Office*, art.3, MOUs with 23 countries; the NPA: *Regulation on National Police Agency and its Agencies*, art.15-2; the KCS: *Customs Act*, art.240-6(2), (3) and customs mutual assistance agreements; the NTS: *Regulation on National Tax Service and its Agencies*, art.8-3, the KCG: *Regulation on Korea Coast Guard and its Agencies*, arts.8(1), 3; the FSC and FSS: *Act on the Establishment of FSC*, arts.17(8)).

Criterion 40.2 –

(a) Competent authorities have a lawful basis for providing co-operation (KoFIU: *FTRA*, art.8(1); the SPO: *Regulation on Establishment and Management of International Co-operative Task Force by Supreme Prosecutors Office*, art.3, MOUs with 23 countries; the NPA: *Regulation on National Police Agency and its Agencies*, art.15-2; the KCS: *Customs Act*, art.240-6(2), (3) and customs mutual assistance agreements; the NTS: *Regulation on National Tax Service and its Agencies*, art.8-3, the KCG: *Regulation on KCG and its Agencies*, arts.8(1), 3; the FSC and FSS: *Act on the Establishment of FSC*, arts.17(8)).

(b) Nothing prevents the Korean competent authorities from using the most efficient means to co-operate.

(c) Competent authorities in Korea have clear and secure gateways for co-operation. Many authorities have established specific mechanisms to facilitate co-operation. KoFIU shares information through the Egmont Secure Web. The SPO has established an International Co-Operative Task Force that provides a channel for co-operation using secure emails, and legal attachés abroad may also be used. The NPA co-operates through Interpol and its secure mechanisms. The KCS has established a Customs Border Management Centre and an International Co-operative Agency that provide mechanisms to exchange information through approved contact points or secure encrypted emails, foreign liaison officers are also employed. The NTS has in place an Offshore Compliance Office that manages requests for co-operation and exchanges

information through a secure system and also has access to posted officers. The FSC and FSS utilise an Information Exchange Platform for secure co-operation and information exchange. The KCG shares information with counterparts through Interpol, as well as through the North Pacific Coast Guard Forum and liaison officers abroad.

(d) Certain competent authorities have clear processes for the prioritisation and timely execution of requests, but not all. The KCS has *Guidelines on Information Provision* which set out a process for prioritising and rapidly responding to requests. The FSS is required to execute requests in a timely manner (*Regulation on Task of Information Exchange with Foreign Supervisory Authorities and Others*, art.4). The NPA will follow the Interpol rules on urgency and prioritisation. The NTS will prioritise requests marked urgent, though there is no formal requirement for this. KoFIU, the KCG, and the FSC all have formal processes for providing information to foreign authorities, but these do not cover prioritisation or timeframes. The SPO exchanges information on an *ad hoc* basis, without a formal process for prioritisation or timely execution.

(e) Competent authorities have in place clear processes for safeguarding information received. KoFIU, the SPO, the NPA, the KCS, the NTS, the FSC, and the FSS treat any information received in the same manner as domestic information (KoFIU: *FTRA*, arts.9(1), 13; the SPO: *Criminal Act*, art.126; the NPA: *Rules on Criminal Investigations* (a NPA Directive); the KCS: customs mutual assistance agreements; the NTS: *Convention on Mutual Administrative Assistance in Tax Matters*, art.22; the FSC and the FSS: *Regulation on Task of Information Exchange with Foreign Supervisory Authorities and Others*, arts.3(3), 5; the KCG: *Detailed Rules on Security* and *KCG Rules on Criminal Investigations* (KCG Directives)).

Criterion 40.3 – When bilateral or multilateral agreements are required, these are negotiated in a timely way. This is aided by guidance from the MFA on negotiating, drafting, and signing such agreements. All competent authorities have access to multilateral agreements for information exchange.[74] In addition, most authorities also have bilateral agreements with a wide range of counterparts: KoFIU (69 countries), the SPO (23 countries), the NPA (28 countries), the KCS (34 countries), the NTS (multilateral treaties and seven MOUs), the KCG (seven countries), the FSC and the FSS (77 institutions/agencies in 50 countries).

Criterion 40.4 – Competent authorities are able to provide timely feedback to foreign authorities upon request and most authorities have done so.

Criterion 40.5 – Korea does not prohibit, or place unreasonable or unduly restrictive conditions on the provision of assistance or information.

Criterion 40.6 – Information exchanged by KoFIU cannot be used for another purpose or by another agency without authorisation (*FTRA*, arts.8, 9). The bilateral and multilateral agreements under which the NPA, the KCS, and the NTS exchange information require written approval before the Korean agency or its counterpart can use information for another purpose (*WTO Trade Facilitation Agreement*, art.5(1); *Multilateral Convention on Mutual Administrative Assistance in Tax Matters*, art.22(4); *Tax Information Exchange Agreement*, art.11(2)). The FSC and the FSS have statutory

74. KoFIU (Egmont Group), the Prosecutor's Office (Asset Recovery Inter-agency Network), NPA (Interpol), KCS (WTO), NTS (Convention on Mutual Administrative Assistance in Tax Matters), the Coast Guard (NPCGAS), the FCS and the FSS (IOSCO).

prohibitions on using exchanged information for another purpose (*Regulation on Task of Information Exchange with Foreign Supervisory Authorities*, arts.5, 6). It is a criminal offence for the SPO to use information provided to it for another purpose, and when providing information, the SPO will request that it be not used for another purpose or by another agency (*Criminal Act*, art.126).

Criterion 40.7 – Competent authorities have requirements to maintain the confidentiality of information exchanged in the same manner as they would protect domestic information (KoFIU: *FTRA*, arts.9(1), 13; the SPO: *Criminal Act*, art.126; the NPA: *Rules on Criminal Investigations* (a NPA Directive); the KCS: customs mutual assistance agreements; the NTS: *Convention on Mutual Administrative Assistance in Tax Matters*, art.22; the FSC and the FSS: *Regulation on Task of Information Exchange with Foreign Supervisory Authorities and Others*, arts.3(3), 5; the KCG: *Detailed Rules on Security* and *KCG Rules on Criminal Investigations* (KCG Directives)). Most of KoFIU's MOUs provide that it can refuse to provide information if the requesting information cannot protect it effectively. The SPO is also able to reject requests for this reason on the basis of its MOUs and other co-operation channels. No information was provided on whether other authorities (the NPA, the KCS, the NTS, the KCG, the FSC and the FSS) can refuse requests on this ground.

Criterion 40.8 – Competent authorities can conduct inquiries on behalf of foreign counterparts and exchange resulting information. The NPA, the KCS, the NTS, and the KCG can do so in accordance with multilateral and bilateral conventions and arrangements (e.g. Interpol), while the SPO can do so on the basis of reciprocity. The FSC and the FSS can also conduct inquiries on behalf of a foreign counterpart (see c.40.15).

Exchange of Information between FIUs

Criterion 40.9 – KoFIU has a legal basis for providing co-operation on ML, TF and the associated predicate offences (*FTRA*, art.8(1) in MOUs with 69 countries and through the Egmont Group).

Criterion 40.10 – KoFIU provides feedback to foreign counterparts upon request on the use of the information provided and the outcome of any analysis or investigation.

Criterion 40.11 – KoFIU is able to exchange:

(a) all information domestically available, including information in its STR, CTR, and foreign exchange databases and additional information it is able to request from FIs or DNFBPs (see R.29); and

(b) other information it is able to obtain domestically, such as credit information, criminal records, company registration information, business reports, financial statements, company information, etc. (*FTRA*, art.10(1)).

Exchange of information between financial supervisors

Criterion 40.12 – The FSC has a legal basis to provide international co-operation to foreign supervisory counterparts (*Act on Establishment, etc. of Financial Services Commission*, art.17(8); *FTRA,* art.11-2(1)) The FSC has entered into 77 MoUs with foreign counterparts on information exchange, including for AML/CFT purposes.

Criterion 40.13 – The FSC and FSS can exchange with its foreign counterparts all information domestically available to them, including information held by FIs, in a manner proportionate to their respective needs (Regulation on Task of Information Exchange with Foreign Supervisory Authorities, art.6).

Criterion 40.14 – The FSC and FSS can exchange the following type of information, when relevant for AML/CFT purposes, with foreign counterparts, provided that such information is solely used for the originally requested purpose and the receiving party complies with confidentiality requirements (Regulation on Task of Information Exchange with Foreign Supervisory Authorities, arts.6, 7):

(a) Regulatory information, including information on the domestic regulatory system, and general information on the financial sectors;

(b) Prudential information, such as information on the FIs' business activities, major shareholders, management, and fit and properness. However, this does not extend to FIs' BO (see R.26.3); and

(c) AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, CDD information, customer files, samples of accounts and transaction information.

Criterion 40.15 – The FSS and FSC can conduct inquiries on behalf of foreign counterparts. The FSS has the ability upon request on a case by case basis to facilitate foreign counterparts conducting supervisory inquiries in Korea or facilitating group-wide supervision.

Criterion 40.16 – Requesting financial supervisors are required to obtain prior authorisation from the FSC or FSS for any dissemination of information exchanged, or use of that information for supervisory or non-supervisory purposes, unless the requesting financial supervisor is under a legal obligation to disclose or report the information, in which case the requesting supervisor shall inform the FSC or FSS of this obligation (*Regulation on Task of Information Exchange with Foreign Supervisory Authorities*, art.3). However, there is no requirement that the FSC or FSS should be informed promptly.

Exchange of information between law enforcement authorities

Criterion 40.17 – LEAs (the NPA, the SPO, the KCS, the NTS, and the KCG) are able to exchange domestically available information on ML, TF or associated predicate offences with foreign counterparts (the NPA: *Regulation on National Police Agency and its Agencies*, art.15-2; the SPO: *Regulation on Establishment and Management of International Co-operative Task Force by Supreme Prosecutors Office*, art.3, MOUs with 23 countries; the KCS: *Customs Act*, arts.240-6, 301(1), *Regulation on Korea Customs Service and its Agencies*, art.8-2, and customs mutual assistance agreements; the NTS: *Regulation on National Tax Service and its Agencies*, art.8-3, the KCG: *Regulation on Korea Coast Guard and its Agencies*, arts.8(1)).

Criterion 40.18 – LEAs are able to use their powers, including non-coercive investigative techniques, to conduct inquiries on behalf of foreign counterparts (the NPA: *Regulation on National Police Agency and its Agencies*, art.15-2; the SPO: *Regulation on Establishment and Management of International Co-operative Task Force by Supreme Prosecutors Office*, art.3, MOUs with 23 countries; the KCS: *Customs Act*, art.240-6, customs mutual assistance agreements; the NTS: *Regulation on National Tax Service and its Agencies*, art.8-3; the KCG: *Regulation on Korea Coast Guard and its Agencies*, arts.8(1), 3). For all agencies, coercive measures require the use of formal MLA (see R.37).

Criterion 40.19 – The KCS and the NTS are able to form joint investigative teams under their bilateral and multilateral MOUs (*Multilateral Convention on Mutual Administrative Assistance in Tax Matters,* arts.8, 9); NTS MOUs on simultaneous

examination (with the U.S.) and on tax examination abroad (with Japan and U.S.); KCS MOUs (e.g. between Korea and Poland)). The SPO, the NPA, and the KCG can conduct joint investigations, although they are rare.

Exchange of information between non-counterparts

Criterion 40.20 – KoFIU can exchange information with non-counterparts, and Korea's other competent authorities can use this power to exchange information indirectly through KoFIU (*FTRA*, arts.7, 8). The KCS is able to exchange information indirectly under its bilateral MOUs. The FSC and the FSS can share information indirectly with consent from the relevant institution provided it is used for the specified purpose (*Regulation on Task of Information Exchange with Foreign Supervisory Authorities and Others*, art.6).

Weighting and Conclusion

Korea's framework for informal international co-operation and information exchange broadly complies with the FATF Standards. However, there are minor deficiencies. Certain competent authorities (KoFIU, the SPO, the KCG, and the FSC) do not have clear processes for the prioritisation or timely execution of requests (40.2(d)). This is weighted more heavily as it risks creating delays. No information was provided on whether some competent authorities (the NPA, the KCS, the NTS, the KCG, the FSC and FSS) can refuse requests where the requesting authority cannot protect the information (c.40.7). FSC and the FSS cannot exchange FIs' BO information (c.40.14(b)); and there is no requirement that they be informed promptly if the requesting supervisor is under a legal obligation to disseminate information exchanged (c.40.16).

Recommendation 40 is 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	• The approach to allocating resources and implementing AML/CFT measures does not specifically respond to risk, and actions are particularly limited for TF risks. • AML/CFT measures do not apply to DNFBPs, except for casinos. • FIs and casinos are not required to have their AML/CFT policies, controls and procedures approved by senior management.
2. National cooperation and coordination	LC	• Korea's AML/CFT strategies are not always clearly informed by identified risks. • There is no standing mechanism to ensure general domestic co-operation and co-ordination on PF at the policymaking or operational levels
3. Money laundering offences	LC	• The range of tax offences included as predicate offences is too narrow. • The sanctions for ML for natural are too low to be sufficiently dissuasive. • The sanctions for ML for legal persons are too low to be proportionate or dissuasive.
4. Confiscation and provisional measures	C	• All criteria met.
5. Terrorist financing offence	LC	• The TF offence incorporates an additional mental element which goes beyond the TF Convention. • The indirect collection of funds is not clearly covered by the offence. • The financing of FTFs is not clearly covered. • Sanctions for TF for legal persons are too low to be proportionate and dissuasive.
6. Targeted financial sanctions related to terrorism & TF	PC	• DNFBPs (other than casinos) are not subject to TFS. • The freezing obligation does not extend to (ii) funds and other assets which are indirectly owned or controlled by listed natural and legal persons, including joint ownership, or (iii) funds or other assets derived or generated therefrom, as well as (iv) funds and other assets of other persons and entities acting on behalf, or at the direction, of designated persons. • Criminalisation of all natural and legal persons providing funds and other assets are conditional upon a level of knowledge. • There is no mechanism in place to communicate designations, de-listings and un-freezings to DNFBPs other than casinos. • No guidance has been issued to FIs and DNFBPs on how to meet their TFS obligations or specifically on respecting delisting or unfreezing actions.
7. Targeted financial sanctions related to proliferation	PC	• DNFBPs (other than casinos) are not subject to TFS obligations, nor subject to monitoring. • The freezing obligation does not extend to (ii) funds and other assets which are indirectly owned or controlled by listed natural and legal persons, including joint ownership, or (iii) funds or other assets derived or generated therefrom, as well as (iv) funds and other assets of other persons and entities acting on behalf, or at the direction, of designated persons. • There is no mechanism in place to communicate designations, de-listings and un-freezings to DNFBPs other than casinos. • No guidance has been issued to FIs and casinos on how to meet their TFS obligations or specifically on respecting delisting or unfreezing actions. • It is not explicit that authorising access to funds must be based on a determination that the exemption conditions set out in UNSCRs 1718 and 2231 are met. • No specific guidance has been provided to FIs or casinos on their obligations to respect de-listing or unfreezing actions. • No legal basis to prohibit/permit addition to frozen accounts pursuant to UNSCRs 1718 or 2231 and no legal basis to allow designated persons or entities to make payments due under contracts.
8. Non-profit organisations	PC	• Korea has not clearly identified which of its 14 033 registered NPOs fall within the FATF definition of NPO.

Recommendations	Rating	Factor(s) underlying the rating
		• There are not comprehensive policies aimed at promoting accountability, integrity and public confidence for all NPOs. • Outreach efforts have not included certain high-risk NPOs or donor communities. • NPOs themselves have not been involved in the development of relevant guidance. • The largest group of identified at-risk NPOs are not subject to relevant reporting or disclosure requirements. • Monitoring of certain at-risk NPOs, monitoring is focused on criminal activity rather than ensuring compliance with R.8 requirements. • The range of sanctions for breaching R.8 requirements is relatively limited, which may reduce Korea's ability to impose proportionate sanctions. • No sanctions are available for the NPO's officers. • Information sharing on NPOs is limited as co-ordination committees do not include all NPO registrars.
9. Financial institution secrecy laws	LC	• The ability for FIs to share information does not extend to CDD information, in cases where this information is unrelated to a transaction.
10. Customer due diligence	LC	• For transactions in domestic currency FIs are required to apply CDD when carrying out a transaction of EUR 11 691. • FIs are required to identify any person acting on behalf of another person, but only when a person is carrying out transactions or opening an account, not in other cases. • There is no requirement to identify any natural person who otherwise exercise effective control over the trust. • FIs are not required to terminate a business relationship with an existing customer where CDD cannot be performed.
11. Record keeping	C	• All criteria met.
12. Politically exposed persons	PC	• There is no requirement to undertake enhanced ongoing monitoring of the relationship with a foreign PEP except for transactions monitoring. • There are no requirements for domestic PEPs or PEPs of international organisations • There are no requirements to determine whether a BO of a beneficiary of a life insurance policy is a PEP.
13. Correspondent banking	C	• All criteria met.
14. Money or value transfer services	C	• All criteria met.
15. New technologies	C	• All criteria met.
16. Wire transfers	LC	• There is no requirement to obtain and verify customer information for wire transfers below the threshold. • Ordering FIs are not prohibited from executing a wire transfer if it does not comply with the requirements specified above at criteria 16.1-16.7. • There is no explicit requirement covering appropriate follow-up actions related to executing, suspending or reject wire transfers. • MVTS providers controlling both the ordering and the beneficiary side of a wire transfer, are not required to consider information from both sides of the transfer nor file an STR in any country affected by the suspicious wire transfer.
17. Reliance on third parties	C	• All criteria met.
18. Internal controls and foreign branches and subsidiaries	LC	• FIs are not required to take appropriate additional measures when the host country does not permit proper implementation of the AML/CFT measures. • There is no explicit requirement for financial groups to implement the measures set out in c.18.1 and c.18.2(a)-(c) at the group-wide level
19. Higher-risk countries	LC	• It is not explicit that counter measures should be applied proportionate to the risks.
20. Reporting of suspicious transaction	C	• All criteria met.
21. Tipping-off and confidentiality	C	• All criteria met.
22. DNFBPs: Customer due diligence	PC	• Casinos are subject to the same technical deficiencies as FIs with regards to CDD and record keeping requirements under R.10 and R.12 and are not required to comply with the requirements under R.15 and R.17. • Real estate agents are not required to comply with all CDD measures and record keeping requirements. • For DNFBPs, only limited record keeping requirements and none of the requirements of R.10, R.12, R.15 and R.17 apply.

Recommendations	Rating	Factor(s) underlying the rating
23. DNFBPs: Other measures	PC	• There is no requirement for casinos to appoint a compliance officer. • Casinos are required to comply with the same higher-risk countries requirements as FIs under R.19 and are subject to the same technical deficiency. • DNFBPs (other than casinos) are not subject to any of these requirements.
24. Transparency and beneficial ownership of legal persons	PC	• Information is not publicly available on the processes for obtaining and recording beneficial ownership information. • It is not clear if associations and foundations are required to maintain registry information. • Legal persons are not clearly required to keep shareholder and membership information held by NTS up-to-date and registry information is not systematically verified for accuracy. • BO information is not always available in a timely manner to competent authorities. • Available beneficial ownership information is somewhat accurate and up-to-date. • Associations and foundations are not required to have a representative that is obliged to co-operate with competent authorities and company representatives do not have to be resident in Korea. • The requirement for registers to maintain basic information following dissolution of a company is not explicitly clear. • Competent authorities do not always have the power to obtain BO information at the intelligence gathering phase, and access is not always timely particularly if international co-operation is needed. • Sanctions for failing to ensure accurate and up-to-date basic information are not available for a legal person and it is not clear there are satisfactory sanctions for: failure to maintain an accurate and up-to-date register of shareholders or members; failing to maintain records; or failure to co-operate with competent authorities in determining the beneficial owner. • There is no formal system to monitor the quality of international assistance in obtaining basic and beneficial ownership information beyond Korea's generic case monitoring frameworks.
25. Transparency and beneficial ownership of legal arrangements	LC	• Trustees of civil and foreign trusts are not required to identify the settlor, trustee, or beneficial owner of the trust. • Trustees of civil and foreign trusts are not required to hold basic information on regulated agents or service providers to the trust. • Civil and foreign trustees have no specific obligation to keep information accurate and up-to-date beyond a general prohibition on negligent bookkeeping. • Civil and foreign trustees are not subject to a specific timeframe for providing information to competent authorities. • Sanctions available for trustees of a civil or foreign trust are not dissuasive or proportionate.
26. Regulation and supervision of financial institutions	LC	• The fit and proper requirement does not explicitly extend to beneficial owners.
27. Powers of supervisors	C	• All criteria met.
28. Regulation and supervision of DNFBPs	PC	• The fit and proper requirement does not extend to beneficial owners, significant shareholders or senior management. • DNFBPs (other than casinos) are not subject to AML/CFT regulation or supervision, including to some extent fit and proper tests.
29. Financial intelligence units	C	• All criteria met.
30. Responsibilities of law enforcement and investigative authorities	C	• All criteria met.
31. Powers of law enforcement and investigative authorities	LC	• Controlled delivery is not available for other offences than drug-related. • Information can only be requested in relation to investigations into ML, TF and certain tax and customs offences.
32. Cash couriers	LC	• A fine of 5% of the undeclared or falsely declared amount may not be sufficiently proportionate. • Penalties for ML and TF are not sufficiently proportionate or dissuasive.
33. Statistics	C	• All criteria met.
34. Guidance and feedback	LC	• No guidance has been provided on how to implement TFS obligations.
35. Sanctions	LC	• DNFBPs (other than casinos) and its directors and senior management are not subject to sanctions for failure to apply preventive measures or TFS. • The applicable sanctions to NPOs are not proportionate in all cases.
36. International instruments	LC	• Some limitations remain in Korea's implementation of the TF Convention (see R.5). • There are some issues with Korea's implementation of the Merida Convention, including: the scope of bribery and corruption offences included as predicate offences is limited where

Recommendations	Rating	Factor(s) underlying the rating
		the value is over KRW 300 million (EUR 229 000); there are no general provisions providing for the liability of legal persons for corruption offences (with the exception of foreign bribery); and the preparation of certain corruption offences is not criminalised.
37. Mutual legal assistance	LC	• Lack of dual criminality is a discretionary ground upon which Korea can refuse MLA requests.
38. Mutual legal assistance: freezing and confiscation	C	• All criteria met.
39. Extradition	LC	• The limitations identified in Korea's ML and TF offences (see R.3 and R.5) may mean there are instances where Korea is unable to provide extradition. • There is no explicit requirement to prosecute on request where an extradition request is denied for nationality. • Korea has the discretion to refuse to extradite its own nationals.
40. Other forms of international co-operation	LC	• Certain competent authorities do not have clear processes for the prioritisation and timely execution of requests. • No information was provided on whether other authorities (the NPA, KCS, the NTS, the Coast Guard, the FSC and FSS) can refuse requests to provide information if the requesting information cannot protect it effectively. • BO information is not available in all cases and can therefore not be exchanged. • There is no requirement that the FSC or FSS should be informed promptly when a requesting financial supervisor is under a legal obligation to disclose or report the exchanged information.

Glossary of Acronyms[75]

Abbreviation	
ARIN-AP	Asset Recovery Interagency Network – Asia Pacific
ASPIT	Act on Special Cases Concerning the Prevention of Illegal Trafficking in Narcotics
BO	Beneficial ownership
CARD	Criminal Asset Recovery Division (of the SPO)
CARIN	Camden Asset Recovery Network
CDW	Customer Database Warehouse (of the Korea Customs Service)
CEO	Chief executive officer
CPIT	Criminal Proceeds Investigation Team (of the NPA)
CRETOP	Korea Enterprise Data
CTRs	Cash transaction reports
DART	Data Analysis, Retrieval and Transfer System (by the FSS)
DPMS	Dealers in precious metals and stones
DPO	District Prosecutors' Office
DPRK	Democratic People's Republic of Korea
EDD	Enhanced customer due diligence
EU	European Union
EUR	Euros
FIs	Financial institutions
FOCAS	FIU Financial and Other information Consolidated Analysis System (of the National Tax Service)
FSC	Financial Services Commission
FSS	Financial Supervisory Service
FTF	Foreign terrorist fighters
FTRA	Financial Transaction Reports Act
GDP	Gross domestic product
GIS	Geospatial Information System (of the NTS)
ICAS	International Consolidated Analysis System (of the NTA)
ICC	International Co-operation Centre (of the SPO)
KCG	Korea Coast Guard
KCOC	Korea's Council for Overseas Development Co-operation
KCS	Korea Customs Service
KICS	Korea Information System of Criminal Justice Services
KoFIU	Korea FIU
KoFICS	Korea Financial Information Connect System (of KoFIU)
KOICA	Korea International Co-operation Agency (within the MFA)
KRW	Korean won
LEAs	Law enforcement agencies
LERA	Legal entity risk assessment
MFA	Ministry of Foreign Affairs
MLA	Mutual legal assistance
NIS	National Intelligence Service
NPA	National Police Agency
NRAs	National risk assessments
NTIS	Neo Tax Integrated System (of the NTS)

75. Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

Abbreviation	
NTS	National Tax Service
ODA	Overseas development aid
PF	Proliferation financing
PFOPIA	Act on Prohibition against the Financing of Terrorism and Proliferation of Weapons of Mass Destruction
SDD	Simplified customer due diligence
SGP	Jeju Special Self-Governing Province
SPO	Supreme Prosecutors' Office
TIIC	Terrorism Information Integration Centre (within the NIS)
TFS	Targeted financial sanctions
U.K.	United Kingdom
UNSC	United Nations Security Council
U.S.	United States
USD	U.S. dollars
WMD	Weapons of mass destruction

www.fatf-gafi.org | www.apgml.org

April 2020

Anti-money laundering and counter-terrorist financing measures - Republic of Korea

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 Republic of Korea (Korea) as at the time of the on-site visit from 30 June to 18 July 2019.

The report analyses the level of effectiveness of Korea'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.