FATF

RISK-BASED SUPERVISION

MARCH 2021

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 (CFT) standard.

For more information about the FATF, please visit **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.

Citing reference:

FATF (2021), *Guidance on Risk-Based Supervision,* FATF, Paris,
www.fatf-gafi.org/publications/documents/Guidance-RBA-Supervision.html

Acknowledgements

Supervisors oversee the measures put in place by the private sector to implement anti-money laundering checks and report suspicions. Effective, risk-based supervision is an essential part of a strong anti-money laundering system. This document guides supervisors on how to assess risks in the sectors they oversee and adapt their resources accordingly and includes strategies to address common challenges. The guidance is based on the work of the following project team members and the extensive input by the FATF Global Network of FATF Members and FATF-Style Regional Bodies (FSRBs), together making up more than 200 jurisdictions. The guidance also benefited from informal consultation with a range of private sector representative bodies and financial inclusion stakeholders.

The work for this guidance was led by Jun Yuan Tay (Monetary Authority of Singapore), Philippe Bertho, (L'Autorité de contrôle prudentiel et de resolution of France), Hamish Armstrong (Jersey Financial Services Commission), with Shana Krishnan, Jay Song and Ben Aldersey from the FATF Secretariat. The project team received significant contributions from Joo Seng Quek (Monetary Authority of Singapore), Julien Escolan and Fadma Bouharchich (ACPR France), Damian Brennan (Central Bank of Ireland), Ke Chen and Grace Jackson (International Monetary Fund), Kuntay Celik (World Bank), Carolin Gardner, (European Banking Authority), Claire Wilson (UK Gambling Commission), Melanie Knight and Lee Adams (UK Office for Professional Body AML Supervision (OPBAS)), Lesya Yevchenko (The Office of the Superintendent of Financial Institutions (OFSI) Canada), Marlene Manuel-Fevrier, (Department of Finance Canada), Mike Hertzberg (US Treasury with the input of various US supervisors), Juliana Petribu and Izabela Correa (Central Bank of Brazil), Tomohito Tatsumi and Arisa Matsuzawa (Financial Services Agency Japan) and Alexandr Kuryanov (Rosfinmonitoring Russia).

Table of contents

Acronyms 4
Executive Summary 5

PART ONE: HIGH-LEVEL GUIDANCE ON RISK-BASED SUPERVISION 7

1. Introduction 7
1.1. Objectives and scope 7
1.2. Overview of relevant FATF recommendations and assessment methodology 8
1.3. Common supervisory frameworks 10
1.4. Characteristics of an effective risk-based supervisory framework 11
1.5. Overview of the risk-based supervision process 12
2. Supervisors' risk understanding 14
2.1. What is the scope and purpose of supervisory risk assessments? 14
2.2. What does the supervisory risk assessment process involve? 17
2.3. What information does a supervisor need to identify and understand the risks? 22
2.4. How do supervisors keep their risk understanding updated? 24
3. Risk-based approach to supervision 25
3.1. What is a supervisory strategy? 25
3.2. How can supervisory strategies address the risks identified? 26
3.3. How can supervisors adjust their approach to vary the nature, frequency, intensity and focus of supervision? 27
3.4. How can supervisors use a combination of off-site and on-site tools to strengthen their risk-based approach? 29
3.5. How should supervisors treat lower risk sectors and entities? 31
3.6. How can supervisors develop a more robust risk-based approach over time? 33
3.7. How should remedial actions and available sanctions be applied in risk-based supervision? 35
3.8. How should supervisors measure the effectiveness of their risk-based approach? 36
3.9. Domestic co-operation, including between AML/CFT supervision and prudential supervision 39
3.10. International co-operation to achieve a risk-based approach to supervision 39
4. Cross-cutting issues 42
4.1. Use of technology by supervisors ("SupTech") 42
4.2. Engagement with the private-sector 43
4.3. Use of third-parties 44
Annex A. Overview of supervisory tools 46

PART TWO: STRATEGIES TO ADDRESS COMMON CHALLENGES IN RISK-BASED SUPERVISION & JURISDICTIONAL EXAMPLES 48

Objectives and scope 48
Overview of challenges identified in Mutual Evaluations 48
5. Strategies to address challenges in assessing ML/TF risks 49
5.1. Disconnect from, or misalignments with, the NRA 49
5.2. New areas of supervisory responsibility – identifying the regulatory population 50
5.3. New areas of supervisory responsibility – identifying and understanding the risks 51
5.4. Difficulties in assessing risks at the entity-level 51
5.5. Building risk understanding over time 53
5.6. Engagement with other authorities to supplement the risk assessment 54
5.7. Data collection issues 55
5.8. Special considerations for DNFBP supervisors 56
5.9. Other guidance 57
6. Applying risk-based supervision 58

6.1. Sequencing to establish risk-based supervision 58
6.2. Insufficient resources or inexperienced staff 59
6.3. Supervising sectors with a large number of entities and limited risk information 60
6.4. Poor independent audits of entities 60
6.5. Special considerations for DNFBP supervisors 61
6.6. Role of self-regulatory bodies for DNFPBs 62
6.7. Lack of clarity in the division of supervisory roles and responsibilities 63
6.8. Zero-tolerance or zero-failure approach 63
6.9. Integrated vs. Standalone AML/CFT Supervision 64
6.10. Risk-based supervision strategies should be up-to-date and dynamic 65
6.11. Logistical challenges in performing on-site inspections 66
6.12. Useful resources for further reading 66

PART THREE: COUNTRY EXAMPLES 68

Objectives and scope 68
7. Supervision of financial institutions 68
7.1. Assessing risks and risk-based supervision 68
7.2. Use of technology by supervisors ("SupTech") 75
7.3. Engagement with the private sector 77
7.4. Offsite supervision tools 79
7.5. Domestic Co-operation 80
7.6. Special considerations for the MVTS sector 83
8. Supervision of DNFBPs 86
8.1. Risk assessment 86
8.2. Introducing a risk-based approach to supervision of DNFBPs 87
8.3. Co-ordination and information sharing 90
9. Supervision of VASPs 92
9.1. Identifying the VASP population 92
9.2. Identification of risk in the VASP sector 92
9.3. VASP sector outreach and guidance 94
9.4. Use of technology in VASP supervision 94
9.5. Recruitment and training of VASP supervisors 95
9.6. Multi-jurisdictional operations and supervisory co-operation on VASPs 95
10. Supervision in the COVID-19 context 97
10.1. Risk-based flexibility for reporting entities and clear communication of expectations and provision of Guidance 97
Glossary 98

Acronyms

AML/CFT	Anti-money Laundering/Countering the Financing of Terrorism
DNFBF	Designated Non-financial Businesses and Professions
FATF	Financial Action Taskforce
FI	Financial Institution
FIU	Financial Intelligence Unit
MI	Management Information
ML	Money Laundering
MVTS	Money Value Transfer Service
RPA	Robotic Process Automation
SRA	Supervisory Risk Assessments
SRB	Self-Regulatory Body
TF	Terrorist Financing
TCSP	Trust and Company Providers
VASP	Virtual Asset Service Providers

Executive Summary

1. Preventing money laundering or terrorist financing (ML/TF) is more effective in protecting communities from harm than pursuing prosecution of the activity after it happens. AML/CFT supervisors[1] play an essential role in protecting the financial system and other sectors from misuse by criminals and terrorists by: (1) increasing regulated entities[2] awareness and understanding of the ML/TF risks and setting regulatory obligations and facilitating and encouraging good practices, (2) enforcing and monitoring compliance with AML/CFT obligations, and (3) taking appropriate measures where deficiencies are identified. In order to perform this function effectively and efficiently, supervisors must implement a risk-based approach.

2. A risk-based approach involves tailoring the supervisory response to fit the assessed risks. This approach allows supervisors to allocate finite resources to effectively mitigate the ML/TF risks they have identified and that are aligned with national priorities. Tailoring supervision to address the relevant ML/TF risks will reduce the opportunities for criminals to launder their illicit proceeds and terrorists to finance their operations and improve the quality of information available to law enforcement authorities. It will also ensure that supervisory activities do not place an unwarranted burden on lower risk sectors, entities, and activities. This is critical for maintaining or increasing financial inclusion which could reduce overall ML/TF risks by increasing transparency. A robust risk-based approach includes appropriate strategies to address the full spectrum of risks, from higher to lower risk sectors and entities. Implemented properly, a risk-based approach is more responsive, less burdensome, and delegates more decisions to the people best-placed to make them.

3. Mutual evaluations reveal that making the transition to risk-based supervision is a challenging task. Supervisors need a good understanding of risks, a strong legal basis (mandate and powers) as well as political and organisational support and adequate capacity and resources to succeed in implementing a robust risk-based supervisory approach. The transition from a rule-based to a risk-based approach takes time. It requires a change in the supervisory culture, and investment in capacity building and training of staff, in addition to the development and implementation of a comprehensive supervisory toolkit. To assist in this exercise, the FATF sets out high-level guidance in **Part One** of this document, practical advice to address common implementation challenges in **Part Two** and country examples in **Part Three,** including strategies and examples of supervision of Designated Non-Financial Business and Professions (DNFBPs) and Virtual Asset Service Providers (VASPs). This Guidance should be read alongside forthcoming guidance on proliferation financing (PF) that explains new requirements introduced in October 2020 for countries and regulated entities to assess proliferation financing (PF) risks and implement risk-based measures.

---

1 For the purposes of this Guidance, the term 'supervisors' refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by regulated entities of AML/CFT requirements and includes Self-Regulating Bodies (SRBs) designated to perform this function.

2 Under the FATF Standards this includes: financial institutions (FIs); Virtual Asset Service Providers (VASPs); and Designated Non-Financial Businesses and Professions (DNFBPs) which are casinos; real estate agents; dealers in precious metals and stones; lawyers, notaries and other legal professionals and accountants; and, trust and company service providers. It can also include any other businesses and professions a country decides to include in this category based on risk.

PART ONE:
HIGH-LEVEL GUIDANCE ON RISK-BASED SUPERVISION

1. Introduction

1.1. Objectives and scope

4. The objective of this non-binding Guidance is to clarify and explain how supervisors should apply a risk-based approach to their activities in line with the FATF Standards. In addition to explaining common expectations, the Guidance is also forward looking and identifies innovative practices that can help improve the effectiveness of AML/CFT supervision and thus the overall AML/CFT system.

5. This Guidance focuses on the general process by which a supervisor, according to its understanding of risks, should allocate its resources and adopt risk-appropriate tools to achieve effective AML/CFT supervision. While the Guidance identifies some of the specificities in supervising the financial sector vis-à-vis other sectors, it does not seek to identify or address sectoral risks. This guidance complements the sector-specific guidance in the FATF's sector specific risk-based approach guidance documents.[3]

6. This Guidance does not advocate any specific institutional framework for supervision. The institutional measures and other means that jurisdictions use to apply risk-based supervision and enforcement should be tailored to each jurisdiction's context. This can include the existing institutional and regulatory framework (such as the prudential regulation of relevant sectors), the size and complexity of the regulated sectors and the degree of ML/TF risks (including threats and vulnerabilities) to which they are exposed. In this Guidance, any reference to practices applied in a particular jurisdiction are provided by way of example only and is not to be considered FATF-approval or endorsement of the effectiveness of that system.

[3] Guidance on the following sectors is available on the FATF website: Legal professionals (2019), Accountants (2019), Trust and Company Service Providers (2019), Securities (2018), Life Insurance (2018), Money or Value Transfer Services (2016), Virtual Currencies (2015), Banking Sector (2014), Prepaid cards, Mobile Payments and Internet-Based Payment Services (2013), Casinos (2008), Dealers in Precious Metals and Stones (2008), Real Estate Agents (2008). See Section 6.12 for a list of resources.

1.2. Overview of relevant FATF recommendations and assessment methodology

7. The requirements in relation to risk-based supervision are set out in the FATF Recommendations and FATF assesses the effectiveness of AML/CFT supervision under Immediate Outcome 3 of the FATF Methodology.

8. Recommendation 1 (R.1) and its interpretative note (INR.1) explain the risk-based approach (RBA) and Recommendation 2 (R.2) highlights the importance of national co-ordination, including with and among AML/CFT supervisors. R.1 and INR.1 require jurisdictions to identify, assess and understand the ML/TF risks and to apply a RBA to mitigate the risks accordingly – this applies to supervisory activities. INR.1 requires supervisors to review and consider risk profiles and assessments developed by financial institutions and DNFBPs in applying the RBA. The RBA set out in R.1 is a foundation for allocating resources and implementing measures to combat ML/TF. The RBA applies in relation to:

   - which entities should be subject to a jurisdiction's AML/CFT regime and to what extent they are subject to its obligations
   - how those entities should comply with the AML/CFT requirements, and
   - how those entities should be supervised (including the scope, frequency and intensity of the supervisory activities).

9. In October 2020, the FATF amended R.1 and INR.1 to include a requirement for countries, financial institutions and DNFBPs to assess proliferation financing (PF) risks as defined under the Standards. This means that supervisors are now required to consider how the entities they supervise or monitor are exposed to PF risks and ensuring the effective implementation of targeted financial sanctions (TFS). FATF is developing a Guidance on PF risk assessment and mitigation and supervisors should take that into account while developing their supervisory/ monitoring approach on those issues noting that supervisors and entities are able to use existing AML/CFT and TFS frameworks to address the new PF requirements instead of creating new risk assessment or compliance frameworks.

10. Recommendation 26 (R.26) requires risk-based supervision of financial institutions, Recommendation 28 (R.28) requires the risk-based supervision or monitoring of DNFBPs and Recommendation 15 (R.15) requires the risk-based supervision of or monitoring of VASPs.[4] INR 15, 26 and 28 recommend that supervisors should allocate their supervisory resources based on risk. This requires supervisors understand the ML/TF risk in their jurisdiction, sector, and entities and have onsite and off-site access to all information relevant to those risks.

11. Additionally, R.15, 27 and 28 require supervisors to have powers to impose a range of effective, proportionate and dissuasive sanctions (in line with Recommendation 35 (R.35)) to address failures to comply with AML/CFT requirements.

12. The FATF Standards refer to both the 'supervision' and 'systems for monitoring' of regulated entities (see R.14, R.15, R.26 and R.28):[5]

---

4 Recommendation 28 allows for DNFBPs other than casinos to be regulated by a supervisor or an appropriate self-regulating body (SRB), if such a body can ensure that its members comply with their obligations to combat ML/TF.

5 Some entities may provide services across several of these designated activities. While these entities are not required to be captured under two separate supervisory regimes, it is important that the covered activities are subject to the relevant

- Financial institutions subject to the Core Principles should be subject to licencing and supervision in line with the applicable Core Principles and R.26. All other financial institutions (including MVTS or money or currency changing providers) and VASPS must be licenced or registered and must be supervised or monitored depending on the ML/TF risks present in line with R.14, R.15 and R.26.
- Casinos should be licenced, regulated and supervised in line with R.28. DNFBPS other than casinos should be subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements on a risk sensitive basis in line with R.28.

13. The concepts of 'supervision' and 'systems for monitoring' involve a spectrum of activities and tools available to supervisors that should be applied in a risk-based manner. For the purposes of this Guidance, having in place a 'system for monitoring' implies a difference in the approach and focus of supervisors rather a fundamental difference in tools available and activities undertaken:

    - Under a 'system for monitoring' the ongoing observation of the activities of regulated entities is **generally less intrusive** than traditional supervision regime. For example, entities may not usually be subject to regular inspection cycles. Nonetheless, under a system for monitoring, supervisors should be able to use a range of interventions, including intrusive measures, where risks are identified and should not be limited to off-site activities.
    - Under a 'system for monitoring' interventions are **more reactive to specific (or materialised) risks** than in a traditional supervision regime. That said, effective monitoring requires a range of *proactive measures* to detect and respond to significant changes in risks (e.g., periodic data returns, periodic updates of risk assessments to identify changing risk profiles, and ongoing monitoring of relevant data or events such as suspicious transaction filings or significant risk events and active interventions with entities as necessary). For example, the system of monitoring helps to detect entities that are consistently failing to undertake CDD or report STRs or having potentially facilitated illicit financial flows which is the basis for triggering more intrusive supervisory intervention.

14. In deciding whether systems for monitoring are appropriate, supervisors need to take into account the ML/TF risks in the sector. For example, while the Standards allow most DNFBPs to be subject to 'systems for monitoring', in many countries higher-risk DNFBP sectors are subject to a level of oversight which the FATF would categorise as 'supervision'. Under a system for monitoring, supervisors are also required to provide adequate guidance and feedback and ensure that entities are complying with the AML/CFT requirements and be able to apply effective, proportionate, and dissuasive sanctions in line with R.35.

15. The term 'monitoring' is used broadly by supervisors to cover a range of activities, including activities or processes to observe changes in risk profiles or detect atypical behaviour. It is difficult to draw a clear line between 'supervision' and 'monitoring' as both concepts involve activities that are on a spectrum of tools available to supervisors. The discussion of 'monitoring' or 'systems for monitoring'

requirements in the Standards. For example, when a casino exchanges funds in virtual assets (partially or exclusively), these activities should be subject to any additional requirements in R.15 and INR.15.

set out in this Guidance refers to their use in the aforementioned FATF Recommendations rather than the common-use of the term. Also this guidance does not apply in the context of monitoring of relevant non-profit organisations (NPOs) under R.8.

16. The two core issues most relevant for this Guidance under the effectiveness methodology in Immediate Outcome 3 (IO.3) of the FATF Methodology are:

- Core Issue 3.2: How well do the supervisors identify and maintain an understanding of the ML/TF risks in the financial and other sectors as a whole, between different sectors and types of institution, and of individual institutions?
- Core Issue 3.3: With a view to mitigating the risks, how well do supervisors, on a risk-sensitive basis, supervise or monitor the extent to which financial institutions, DNFBPs and VASPs are complying with their AML/CFT requirements?

17. Other aspects of the FATF Standards and Methodology are also critical for the risk-based approach but are not the focus of this guidance. For example:

- R.34 and Core Issue 3.6 highlight the importance of guidance and feedback and the need for supervisors to promote a clear understanding of AML/CFT obligations and ML/TF risks. Supervisory inspections will only ever reach a percentage of the regulated entity population. Clear guidance, education and innovative outreach strategies to regulated entities regarding their ML/TF risks and AML/CFT obligations are also an important part of an overall supervisory programme. These initiatives, while not necessarily utilising regulatory powers, enable supervisors to promote the application of risk-based AML/CFT obligations as broadly as possible to a large number of regulated entities.
- R.15, 26 and 28 and Core issue 3.1 highlight market-entry requirements which should also apply in risk-based manner such that supervisors adjust their measures based on the potential risks (for example, different types of ownership of entities).
- Core Issue 3.4 on applying dissuasive, proportionate and effective sanctions is addressed briefly in section 3.7 of this guidance. Further guidance on this is provided in the FATF's Guidance on Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement.
- Core Issue 3.5 on demonstrating supervisors' effect on compliance by entities is briefly addressed in section 3.8.

1.3. Common supervisory frameworks

18. A variety of supervisory frameworks are available and utilised to take into account jurisdictional context and risks. The FATF focuses on outcomes rather than process – i.e., it does not prescribe a particular supervisory framework as long as the supervisory outcomes effectively addresses ML/TF risks. Effective communication and co-ordination between AML/CFT supervisors and, as relevant, other relevant supervisors, including prudential supervisors, self-regulatory bodies (SRBs), central banks, finance ministries and other relevant authorities such as Financial

Intelligence Units (FIUs) and Law Enforcement Agencies (LEAs) is critical to ensuring that the jurisdiction is applying an effective risk-based approach overall.

19. Examples of common AML/CFT supervisory frameworks include arrangements where there is:

- A single AML/CFT supervisor responsible for AML/CFT supervision of all regulated entities (this task is usually exercised by the same authority which fulfils the task of the FIU or the prudential supervisor).
- Integration of some aspects of supervision, for example, integrated AML/CFT and prudential supervision of the financial sector and/or the FIU or tax or other authority is responsible for AML/CFT supervision of all or some non-financial sectors.
- A decentralised model for AML/CFT supervision with multiple agencies and/or SRBs responsible for AML/CFT supervision across and within different sectors. The FIU or another authority may also play a role in overseeing or coordinating supervision of all or some DNFBP sectors.

20. It is important to keep in mind the relevant supervisory framework in a jurisdiction when developing models for risk assessments and risk-based supervision. There are benefits and challenges associated with each model relative to resources, expertise and cost efficiencies, the availability of information for assessing risks and compliance, co-ordination of supervisory approaches at a national and international level and other factors. Different models can have intended or unintended consequences on the overall effectiveness and allocation of resources. For example, the level of attention given to DNFBP sectors may vary significantly between a jurisdiction with a single AML/CFT supervisor (which also covers a range of financial sectors) and a jurisdiction that has separate supervisor for DNFBPs and therefore has a different scale and perspective on how to assess risks. A comprehensive National Risk Assessment (NRA),[6] and meaningful national co-operation, are critical to ensure that supervisors coordinate and adjust their assessments of risks and supervisory approaches as appropriate. Where relevant functions are performed by different authorities in accordance with their respective mandates (e.g. FIU + prudential + AML/CFT supervisor), countries need to be able to bring all the relevant information together to reach an overall view of the risks. It is important that the country ensures that there is a correlation between sectoral risk and resources available to the supervisor responsible for that sector. See sections 2.1.2 and 3.9 for more detail.

1.4. Characteristics of an effective risk-based supervisory framework

21. Under an effective risk-based supervisory framework, the supervisor identifies, assesses and understands ML/TF risks within the sector(s) and entities under its purview and mitigates them effectively on an ongoing basis. This involves implementation of a sound risk assessment system that enables the identification, measurement, control and monitoring of ML/TF risks, as well as a risk-based supervisory approach that enables timely supervisory intervention to address any significant changes or elevation in risks. More specifically, the supervisor:

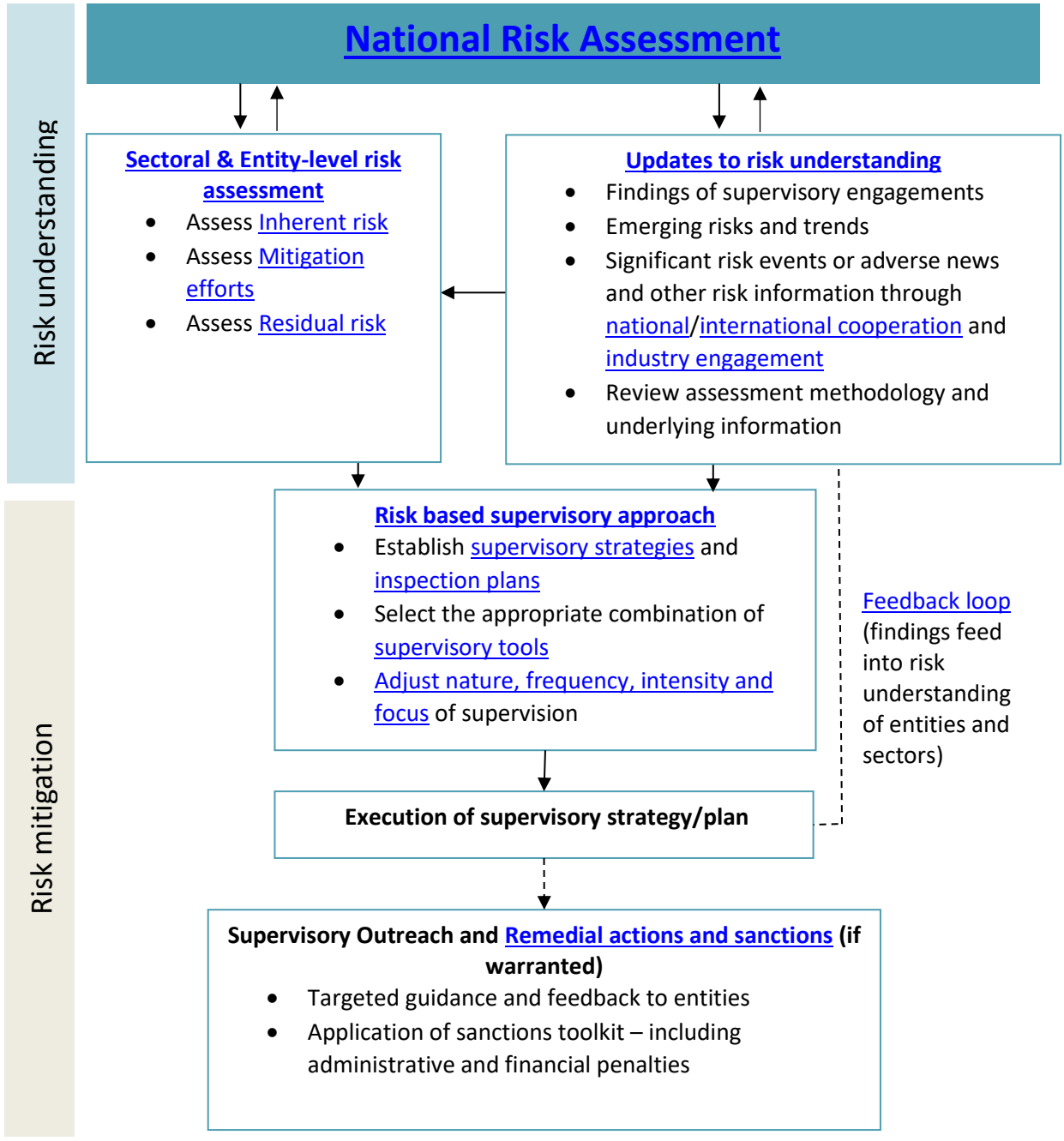
6 Or other forms of nationally coordinated ML/TF risk assessments.

- Develops and maintains a good understanding of ML/TF risks at the sectorial as well as entity level based on sound risk assessment of inherent risks and quality of mitigation measures and informed by national ML/TF risk assessment (see section 2. and note the new requirements to assess PF risk and refer to FATF's forthcoming PF Guidance);
- Develops and implements a supervisory strategy that effectively directs supervisory focus to higher or emerging ML/TF risks while ensuring that there are appropriate, risk-based strategies in place to address lower risks effectively and efficiently without impacting unnecessarily on access to and usage of financial services (see section 3.);
- Positively influences entities' behaviour by ensuring they have effective AML/CFT policies in place and where issues are identified, providing targeted guidance and feedback, directing and/or overseeing remedial actions and exercising enforcement powers in a dissuasive and proportionate manner taking risk, context and materiality into account;
- Monitors the evolving risk environment and stays agile to identify emerging risks and respond promptly (for example, see section 2.4);
- Is equipped with the expertise, powers, discretion, and tools needed and adequately resourced to perform its functions; and
- Coordinates with other competent authorities when relevant, including the FIU, law enforcement agencies and other supervisory agencies, as well as its foreign counterparts by sharing information, prioritising risks and carrying out joint supervisory activities as appropriate (see sections 3.9 and 3.10).

1.5. Overview of the risk-based supervision process

22. The risk-based supervision process consists of two main components illustrated below and further explained in this Guidance: (1) identifying and understanding risks, and (2) mitigating those risks.

Figure 1.1. Overview of a risk-based supervision process



2. Supervisors' risk understanding

2.1. What is the scope and purpose of supervisory risk assessments?

23. To apply risk-based supervision, supervisors first need to understand the ML/TF risk exposure of the sectors and entities they regulate. Supervisors should develop, document and update their ML/TF risk understanding by undertaking a supervisory risk assessment (SRA). The purpose of undertaking a SRA is to help supervisors plan their activities in a risk-sensitive manner by determining how much attention to give relevant sectors and entities within those sectors, and to identify which risks should be prioritised. The scope of the SRA should cover: threat, vulnerability and consequence, which are explained in detail in previous FATF Guidance.[7]

24. As set out in paragraph 9, in October 2020 the FATF introduced a requirement for countries and regulated entities to assess proliferation financing (PF) risks in addition to ML/TF risks. This means that supervisors are now required to assess how the entities they supervise or monitor are exposed to PF risks and take this into account in applying risk-based measures. This Guidance should be read alongside forthcoming guidance by the FATF on PF risk assessment and mitigation.

2.1.1. Sectoral and entity-level risk assessment

25. Understanding inherent risks and common weaknesses in AML/CFT controls at the sectoral level is the starting point for understanding risks at a more granular, i.e., entity-level. In order to achieve a comprehensive risk understanding, supervisors should establish and maintain ongoing risk assessments of sectors[8] and individual entities and/or groups.

26. The different risk assessment approaches adopted by AML/CFT supervisors may depend on the jurisdiction's supervisory framework (see section 1.3), the number of sectors under their supervision and the number of individual entities within each sector. For example, AML/CFT supervisors of banks may choose to risk assess each entity under their supervision or group together banks with similar characteristics, including size, structure and ML/TF risk exposure. As a result, the intensity of supervisory activities would be different for these subgroups.

27. Where appropriate considering their risk and materiality, DNFBP supervisors may determine risks at the entity level bases on risk assessments at the sector level where classes of entities can be clearly identified and defined based on specific characteristics (e.g. class of activities, business model or structure, profile of customers and geographic risks). Where supervisors rely on sectoral risk assessments to understand risks of particular entities, the risk assessment should be sufficiently nuanced to consider each class of entities identified, and their ML/TF risks. For example, in the trust company service providers (TCSPs) sector, TCSPs that are in the business of acting as a formation agent of legal persons may be identified to be of greater risks when compared to other TCSPs.

---

7 FATF Guidance (2013), National Money Laundering and Terrorist Financing Risk Assessment and FATF Guidance (2019), Terrorist Financing Risk Assessment.

8 In some cases, sectoral risk assessment may be part of the national risk assessment process.

28. **Identifying risks particular to different sectors is essential for prioritising supervisory activities within the sector**. In order to determine the risk of a sector as a whole, it is necessary to take into account the nature of the business models within the sector, as well as the business and risk profiles (e.g. volume of business, customer profiles) of the entities in the sector. It may also be useful to categorise entities in sub-sectors as a way to group together different types of risks (for example, within the banking sector, sub-sectoral risks may be identified for those providing mainly retail services, private banking or investment banking because of similar types of customers, distribution channels, types of products and services etc. provided). In this context, when deciding whether to carry out a sub-sectoral risk assessment, supervisors should also take into account the number of entities in a sector, the nature of and variation of business activities carried out by entities in a sector, their specific business volume and the extent of compliance by each type of entity. They should also consider the size or other characteristics of the sector vis-à-vis other sectors. In developing a risk assessment methodology, supervisors should consider the jurisdiction's AML/CFT supervisory framework for financial, VASP and DNFBP sectors as this may affect risk mitigation (e.g., certain sectors may not be supervised adequately and may therefore introduce additional risks to other related sectors).

29. Sectoral level ML/TF risk understanding is also important to prioritise supervisory activities among the different sectors, particularly where there are multiple supervisors. An effective risk-based supervisory framework requires a supervisor to understand the risk of the sector(s) that they supervise, relative to others. Otherwise, they may spend a disproportionate amount of time and effort dealing with a risk that it important to them, but not to the jurisdiction overall.

30. Entity-level risk assessments help to identify entities' standalone ML/TF risk levels to guide the level and focus of supervisory engagement required. The inherent risks facing a specific entity may vary, for example, based on the type of business it conducts, its size, the profile of its customers and its exposure resulting from doing business with high-risk jurisdictions. What constitutes adequate mitigation measures will also vary from entity to entity.

    - At the entity-level, risk assessments may involve obtaining information on transaction data and other information pertaining to the entity's activities relative to products, services, customers, delivery channels and geographic locations, and assessing how this information affects the entity's ML/TF risk exposure. This could involve comparing volumes and types of activities against peer entities to determine which entities are higher risk compared to the "average" in their sector. It could also involve analysing broader data on entities, including studying the entity's operating models, policies and procedures, suspicious transaction reports filed by the entity etc. to arrive at an understanding of the entity's risks and controls. In some cases, a preliminary entity-level risk assessment can be determined based on a combination of criteria.

    - Supervisors often rate the quality of an institution´s mitigation measures, using ratings weighted and tailored to the sectoral risks and entity-level inherent risks, i.e., not every deficiency is equal.

31. A common approach to rating the residual risk presented by each sector or entity is to develop an ongoing and iterative risk matrix with ratings for the inherent ML/TF risks on one axis and the vulnerabilities or quality of AML/CFT-mitigation, on

another. The probability of ML/TF taking place should also be considered.[9] The risk indicators used to assess inherent risks should be tailored to each sector. Some indicators are applicable to most sectors, while others are specific to some sectors or sub-sectors.

32. Aggregating ML/TF risk assessments of individual entities is not the same as a sectoral risk assessment but can help supervisors identify common ML/TF risks. At a sectoral level, entity-level risk assessments provide competent authorities with important information on deficiencies in sector and national regimes, allowing authorities to develop appropriate responses that may include publishing new regulations or amending existing ones, applying enhanced measures, and issuing supervisory guidance.

2.1.2. Supervisory risk assessments and the National Risk Assessment

33. **The interplay between supervisory risk assessment and the NRA process is two-way.** On the one hand, supervisors' understanding of their sectors and entities under their purview should feed into the NRA. On the other hand, the understanding of risks by supervisors should be informed by, and be consistent with, the NRA that includes input from a range of AML/CFT stakeholders. This will provide the information and insights on risks from other authorities and entities (such as other supervisors, law enforcement, judicial, customs, FIU, or intelligence authorities). In addition, the exchange of the relevant risk information could also be provided by working groups that include different national authorities with responsibilities in AML/CFT as well as through meetings with the private sector. It is crucial that supervisors develop their own understanding of risks that feeds into the NRA. If supervisors base their sectoral risk understanding on the NRA, supervisors should assess whether the NRA analysis meets their information needs (including whether it is sufficiently up-to-date and granular) and complement it as necessary.

34. Some of the specific examples of the interplay between supervisory risk assessments and the NRA include:

- Higher or lower risk activities identified by the competent authorities through the NRA process should align with the approach taken by supervisors in overseeing the risk-based approach to compliance with AML/CFT requirements implemented by entities.
- Revision of inherent risk modelling or controls assessment based on identified risks in the NRA.
- Continuing supervision of entities that contribute to and/or challenge or confirm identification of risk in the NRA.
- Understanding financial inclusion products and services, including risks associated with financial exclusion and the risk assessment needed to justify exemptions or an appropriate level of due diligence measures.

9 See for example : www.fca.org.uk/publication/opbas/opbas-sourcebook.pdf, section 4.9

2.2. What does the supervisory risk assessment process involve?

2.2.1. Assessing inherent risks

35. ***Inherent risks*** are ML/TF risks intrinsic to a sector or an entity's business activities before any AML/CFT controls are applied. Inherent risks are associated with features of a business (including their nature, scale and complexity) or characteristics of their business activities with respect to customers, products and services, geographic regions and delivery channels. Certain features or characteristics pose higher or lower risks than others. INR.10 provides some examples of possible higher- and lower-risk factors (see paragraphs 15–17) and the FATF's range of sectoral RBA Guidance[10] and typologies reports can help guide supervisors' assessment of inherent risks of a certain sector or entity.

36. Supervisors should allocate adequate resources to ensure a good understanding of the inherent risks of the regulated entities, leveraging their own knowledge of the business activities of the sector or through engagement with experts in those fields.

37. As set out in R.1, regulated entities must assess the ML/TF risks facing their businesses. **Regulated entities' risk assessments may help to inform supervisors' view of risk** and enable them to obtain information on specific risk categories (e.g., products, services, customers, delivery channels and geographic locations) relevant to the entity. They also help to inform supervisors' understanding of risks within a sector and at the entity level. Supervisors should provide guidance and clarify the supervisory expectations for entity risk assessments. This will help supervisors receive more organised and informative entity-level risk assessments to support their understanding of the entity-level risks.

38. In addition to risk categories referenced in R.1, AML/CFT supervisors in developing their risk assessment should also take into account other supervisory information available to them (see Box 2.1 below), including entity type risks such as the systemic importance of the entity to the sector in which it operates from the AML/CFT angle and its key financial indicators. When considering these factors, supervisors should take into account characteristics of the sector(s) as well as contextual factors and use judgement to determine their implications for ML/TF risks. For example:

    - An institution that aggressively expands its market share or changes its business model may be more willing to take risks, compared to an institution with an established, lower risk client base and operating model.
    - For entities which are part of a larger group of entities, supervisors may also need to consider the risks posed by the other aspects of the group's business, including the complexity of the business operations, geographic risks associated with the different countries in which the group operates and the AML/CFT standards applied therein, etc.[11]
    - Supervisors may become aware of beneficial owners or directors of entities whose fitness and propriety are questionable and raise concerns about the

10 See Section 6.12 for a list of additional resources.

11 See Basel Committee on Banking Supervision Guidelines on Sound Management of risks related to money laundering and terrorist financing (revised in July 2020) paras 63 – 83 for discussion of AML/CFT risks to entities in a group-wide and cross-border context and paras 89 and 90 for discussion of supervisory considerations related to such risks.

ability and/or willingness of the entity or group to establish and implement a sound AML/CFT framework and "tone at the top".

- AML/CFT and prudential problems often form a mutually reinforcing spiral in seriously troubled institutions. In some cases, banks have weakened or abandoned their AML/CFT controls in an attempt to attract illicit funds to solve problems of liquidity or solvency. Equally, the loss of business as a result of supervisors' findings of AML/CFT violations can seriously affect the nature and volume of business, causing liquidity or solvency problems – particularly for a small or specialised bank.
- The entity or sector largely services financially excluded individuals or organisations and has adequate mitigation measures to limit the risks associated with their products and services. Without these services, the risks might be transferred to the unregulated economy where risks are left unmitigated.

Box 2.1. Categories for assessing inherent risks presented by regulated entities

Supervisors may consider:

- Entity type risk: the industry in which it operates, the entity's materiality in the sector it operates and/or its market share, complexity of its operations and its business structure or model and strategy (including planned expansions into new business segments or regions, merges and acquisitions), its shareholding/beneficial ownership information which may elevate ML/TF risks, key financial indicators (e.g., asset and deposit growth, liquidity and cross-border flows).
- Customer risk: additional factors such as demographics and specialized product/service offering for select client groups, including on the basis of whether the customers are natural or legal persons or persons representing legal arrangements, types of businesses serviced, whether customers are domestic or foreign and whether there are specific categories of customers involved (e.g., Politically Exposed Persons).
- Geographic risk: geographic footprint of the entity's operations both domestic and international (including where funds are received from/sent to and where clients are based and residency of beneficial owners), markets served, etc.; robustness of the foreign AML/CFT legal framework under which it operates, contextual factors (e.g., levels of corruption, crime or terrorism) and how that might influence the entity's approach particularly in relation to online service providers or financial or other groups.
- Products and services risk: types and features of the products and services (e.g. anonymity, volume and speed of transactions, duration of the contracts, etc.). The revenues generated from

these also play an important role in understanding the entity's risk profile.

- Delivery channel risk: the features of delivery channels used which may include: the ability to reliably identify/verify customers through remote or digital onboarding,[12] products or services delivered exclusively by post, telephone, internet etc., or the use of introducers or intermediaries (and the nature of their relationship with the entity)..
- Transactional risk: types of transactions, financial flows, information and analysis received from the FIU of the transactional reporting from the entity may provide additional insights and independently verified information.

Note: This is not a comprehensive list – for more information see the FATF's range of sectoral risk-based approach guidance and the list of useful resources at the end of this Guidance. Also see the FATF's forthcoming PF Guidance for further detail on how these categories may be relevant for PF risk.

2.2.2. Assessing mitigation efforts

39. ***AML/CFT systems or controls*** are the measures in place within an entity/s to mitigate ML/TF risks. There are different approaches to assessing the adequacy of controls[13] but supervisors should look beyond the specific controls and processes (e.g., CDD, record keeping, transaction monitoring, etc.) to also assess the overall effectiveness and soundness of the AML/CFT framework, including whether the broader corporate governance environment and compliance culture enables sound and effective AML/CFT internal controls.

40. Supervisors should use a range of tools to enable the proactive monitoring of entities in order to assess the adequacy of their AML/CFT systems or controls. Such mechanisms could include the periodic collection of information on the key AML/CFT controls across the sector to proactively identify entities with major deficiencies in controls and/or common or thematic control weaknesses among entities. Another mechanism could be the use of data analytics to analyse suspicious transaction reports filed by supervised entities to identify potential control weaknesses in specific entities. Taken together, such pro-active approaches can augment supervisors' ability to identify at-risk entities for targeted supervisory scrutiny or point to a need to provide more broad-based supervisory guidance to improve certain control practices across the sector.

41. **Supervisors should develop a holistic assessment of the AML/CFT systems or controls within an entity** (for examples Box 2.2 below). In determining if the entity has the necessary conditions to apply AML/CFT mitigation measures effectively, it is important to pay attention to the level of oversight exercised by the boards and managements of entities (who are ultimately responsible for the entity's AML/CFT controls). Many of the large-scale AML/CFT compliance failures in recent years occurred either with the will or knowledge of top management, board and

12 See FATF's Digital ID Guidance

13 Some jurisdictions may have a framework to objectively assess an entity's AML/CFT risk management processes and controls through a scoring methodology while others may do so more subjectively, or using a combination of both.

sometimes owners of these institutions, or due to a lack of adequate oversight. It is therefore critical that AML/CFT supervisors understand the risk appetite of the owners, board, and management of the regulated entity. Supervisors may be able to obtain this information in the board minutes, policy documents and exchanges with other supervisors (including prudential and conduct supervisors where applicable) but supervisors will need to have a more holistic understanding of the actual control dynamics and the risk appetite of an institution (and its beneficial owners). It is important to meet with and assess the competency of senior management, board, owners and non-executive directors as relevant. Monitoring of open source information and risk-appetite data indicators (such as aggressive expansion) may also assist in assessing the entity risk appetite. Developing risk indicators (refer examples provided in Box 2.1) may assist supervisors in identifying wilful or reckless defiance of AML/CFT obligations. Group-level supervision has an important role to play in understanding the group-level dynamics and risk tolerance.

Box 2.2. Assessing entities' AML/CFT systems and controls

To assess entities' AML systems and controls in a holistic manner, supervisors should consider the adequacy of the:

- oversight by board and senior management
- number of qualified/experienced staff with appropriate authority and resources
- AML/CFT policies and procedures and conflicts with other policies and procedures, e.g., remuneration based on turnover
- risk management function
- compliance function
- internal controls (e.g., CDD, record keeping, transaction monitoring, etc.)
- management of information systems
- independent testing (internal and external audit), and
- training provided to staff on AML/CFT.

The above list is both non-exhaustive (there may be other factors to consider) and not always applicable considering the size and characteristics of the entity. For example, the factors will need to be adapted to small businesses who may not have a board or separate compliance function.

42. When identifying and assessing the mitigation of inherent risk factors, supervisors should consider risks specific to their jurisdiction and sectors they oversee as well as the size and characteristics of supervised entities. For example, Singapore's NRA identified trade-based money laundering, abuse of legal persons and corruption to be key risk faced by financial institutions. Singapore's financial sector supervisor, the Monetary Authority of Singapore, has considered these risks in developing a list of inherent risk indicators that it uses to collect the relevant information from FIs and to assess FIs' controls in mitigating these key identified threats and risks. In

Germany, supervisors assess the appropriateness of an institution´s transaction monitoring system depending on criteria such as the entity´s business model and transaction volume.

43. A supervisor's assessment of an entity's mitigation efforts should be based on its interactions and knowledge of the entity, but it can be supplemented by the results of work completed by third parties where available. Supervisors should only place reliance on such third-party work to the extent that it is comfortable with the robustness of the work performed, and it does not contradict its own understanding of the entity's AML/CFT systems and controls. See section 4.3 on the use of third-parties for more information. Examples of third-party work could be:

- Reports produced by the entity's external auditors, the FIU, foreign supervisors for entities with foreign operations, and home supervisors of foreign entities operating in the jurisdiction. If permitted by law, a supervisor might hire a third party to conduct targeted AML/CFT reviews or audits on their behalf.
- AML/CFT supervisors for the financial sector with access to the prudential or conduct supervisory work may take into account broader risk management factors that have an impact on the overall state of the entity's AML/CFT program. For example, these additional elements include the quality of governance and oversight across the 'three lines of defence',[14] state of the operational controls and data quality and availability across the organisation. Information from prudential or conduct supervision work is particularly useful when it reveals inconsistent views of the prudential/conduct and AML/CFT supervisors on an entity's general governance and suggests the need to revisit the issue.

2.2.3. Assessing residual risks

44. ***Residual risks*** are ML/TF risks that remain after ***AML/CFT systems and controls*** are applied to address inherent risks. For example, an entity with weak AML/CFT controls may not be high-risk if the inherent risks arising from its businesses are low (although over time, the weaker controls may be exploited by criminals causing a change to the entity's inherent risk exposure). An entity with high inherent risks may not necessarily be high-risk if strong AML/CFT controls are applied so that the residual risks are lowered. The residual risk assessment should not be a purely quantitative approach based solely on numerical risk scores. Where supervisors have significant concerns about the potential ML/TF risk impact to the system posed by an entity, supervisors should have the ability to reflect such concerns in the residual risk assessment.

45. Supervisors should acknowledge that no matter how robust AML/CFT controls are, inherent risks cannot be entirely mitigated. Therefore, residual risks will always remain that require management by the regulated entities in line with the risk appetite of the institution.

46. Supervisory risk models usually consider both inherent and residual risks. For example, a high inherent risk rating would generally indicate the need for closer supervisory attention, so that supervisors can assess and intervene where

14 See the Glossary and the *Basel Committee on Banking Supervision's Guidelines for the Sound Management of Risks relating to Money Laundering and Financing of Terrorism* at page 5.

necessary to strengthen the entity's risk mitigation. The residual risk may influence the intensity/scope, and where necessary be used to prioritise between entities (see example 7.1.4).

47. When determining the level of tolerable residual risk, supervisors can consider a range of factors including the potential impact on the jurisdiction and its supervisory population if a residual risk is high, the possible unintended consequences of over-applying mitigation measures (e.g., increased overall ML/TF risks due to financial exclusion) and the entities' ability to manage their own residual risk i.e. appropriate governance, staff training and competence.

48. See Part Three for further examples of supervisory risk models.

2.3. What information does a supervisor need to identify and understand the risks?

49. Supervisors' understanding of ML/TF risks should be formed based on the analysis of all relevant qualitative and quantitative information. This may include prudential and conduct information already held by the supervisors including regulatory and supervisory records, information gathered through surveys or periodic off-site reporting records of past supervisory activities, AML/CFT supervisory returns, information shared by other domestic or foreign competent authorities including the FIU and LEAs on the usefulness of the entity's AML/CFT outputs, and open source information. See Box 2.3 for a list of possible information sources.

50. In their efforts to assess and understand ML/TF risks, supervisors may take into account risk assessments conducted by the supervised/monitored entities themselves but **supervisors should always maintain an independent view instead of unduly relying on the entity's own risk assessments**.

51. Supervisors should take into account the jurisdiction's privacy laws[15] and inter-agency information exchange abilities. Supervisors should protect privacy interests, but privacy should not serve as an undue impediment to sharing to combat ML, TF, and other illicit financial activities. The ability to obtain various AML/CFT-related data will have a direct influence on the granularity of the assessment under each of the inherent risk categories/factors considered in the risk assessment methodology and the supervisor's ability to maintain an up-to-date risk assessment. As set out under R.2 of the FATF Standards, AML/CFT authorities (including supervisors) and authorities responsible for data protection and privacy should co-operate and coordinate to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy rules and other similar provisions.

15 Note also that FATF Recommendation 2 requires cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy rules.

Box 2.3. Sources of information for risk identification and understanding

- **National risk assessment**, including inputs from other stakeholders
- Findings of past **supervisory activity** (either entity-level or horizontal/thematic reviews)
- Input from **other supervisors** (domestic and international) for example, prudential supervisors' findings on the broader corporate governance environment in an entity. Information from the **regulated entities on**
  - Entity's risk assessment and risk appetite
  - Data returns / responses to questionnaires, e.g., annual compliance reports[16] that consist of questions relating to the implementation of AML/CFT systems and controls the entities implemented to meet legislative obligations. See section 7.1.1 for further examples.
  - Financial and operational data that is being shared with the supervisory agencies as a part of routine off-site reporting (including prudential data).
  - Risk input from public/private partnerships or other consultation mechanisms
  - Results of independent testing/audit that is provided to supervisory agencies.
- Feedback from the **FIU** on suspicious transaction reports filed by entities, for instance, on their timeliness and quality of filing, under or over-reporting compared to peers and their responsiveness to the FIU's request for information. Those elements should be analysed in regard to the overall number of operations recorded in the entity's sector and taking into account the concentration level of this sector. The FIU may also be able to identify situations where a suspicious transaction report (STR) should have been filed but was not, which may be an indicator of the effectiveness of the entity's internal control system. Recurring typologies identified in STRs may suggest specific risk exposures or deficiencies of the mitigation measures in place at an entity. Regular exchanges between the supervisor and the FIU on their assessment on the governance, functioning and overall risk culture of the entity's AML-CFT teams. Additionally, information may be shared by the FIU before inspections or as result of other events such as reports by whistle-blowers.
- Input from other **competent authorities** (police, prosecutors, intelligence agencies, tax, customs, anticorruption authorities and agencies dealing with targeted financial sanctions, for example). This includes ML/TF typologies and their observations and risk perceptions about the sector and, where available, the

effectiveness/usefulness of the outputs of a financial institution's AML program. See section 5.6 for examples.

- Findings from **public sources** (media, adverse reporting, etc.). At the French financial sector supervisor (ACPR), there is a dedicated division in charge of press reviews that feed the offsite supervision teams with regular press reviews, upon request. Regular press reviews can be dedicated to specific issues (for instance on tax havens) or specific FIs (providing inputs on a FI's litigations in other jurisdictions, negative information on FI's shareholders, etc.). Apart from news outlets, common third-party reports include Transparency International and the Organized Crime and Corruption Reporting Project (OCCRP).
- Findings from matters reported by **whistle-blowers** and complaints.
- Data on financially excluded populations.
- Input from international counterparts, groups and organisations (FATF and FSRB Reports; ESAs Risk Factor Guidelines etc.)

2.4. How do supervisors keep their risk understanding updated?

52. Effective supervision depends on supervisors' ability to identify and prioritise on a timely basis, areas and institutions for greater supervisory attention. Supervisors typically review and update their risk assessments according to a fixed cycle and in response to trigger events (especially in relation to entity-level risk assessments, and this is further explained below). In addition to such updates, there are opportunities to leverage available information and data to move towards more dynamic and timely assessment of risks (see section 4.1).

53. Supervisors should ensure that their ML/TF risk assessments remain up to date and relevant, by doing the following:

- **Set out the frequency and triggers for updates to sectoral and entity risk assessments** under the supervisory risk assessment methodology.
- **Identifying and assessing emerging risks and trends**[17] within their supervised population, then revising the risk assessment on an ongoing basis. It should be reviewed and updated on an ongoing so that they can perform their risk assessment against a backdrop of observations by law enforcement agencies on emerging ML/TF threats and typologies, and consider how these factors would affect the risks of the sector or entity that is being supervised. See examples 7.1.4 and 7.5.4.
- **Regular dialogue and information sharing with the public and private sector** to understand latest trends and risks (see sections 3.9 and 4.2 for further information).

16 In some jurisdictions, e.g., Australia, this is a legal requirement. See www.austrac.gov.au/compliance-report-2019.

17 Emerging risks and trends can be identified from different sources including through analysis of information from FIUs, LEAs, inspection teams, interactions with prudential or other AML/CFT supervisors, or typology papers by the FATF, or FSRBs etc.

3. Risk-based approach to supervision

54. The risk-based approach to supervision enables supervisory authorities to allocate their resources and attention based on identified risks. Supervisory authorities should develop and implement supervisory strategies that are risk-based and graduated using the information obtained as part of the risk assessment process. The strategy should provide a clear nexus between the ML/TF risks (the risks specific to the jurisdiction or sector) and indicate how the proposed strategy and the use of supervisory tools (covered in Annex A of this Guidance) addresses these risks. A risk-based supervisory strategy ensures the risks determine the *nature, frequency, intensity,* and *focus* of supervision, setting expectations for engagement with entities across the risk spectrum including higher risk and lower risk entities.

3.1. What is a supervisory strategy?

55. A supervisory strategy sets clear objectives for AML/CFT supervision, explains how supervisors will address the ML/TF risks they have identified across their sector(s) and how they will respond to emerging risks.[18] The strategy should not only focus on the highest risk entities or sectors, but should also set out adequate supervisory coverage (including monitoring where relevant) of all entities or sectors, including those associated with lower ML/TF risks. The supervisory strategy sets out the approach the supervisor will take in applying its tools to address the risks identified. The strategy and the output of the risk assessment are used to plan supervisory activity (commonly including 12 or 24 month supervision or inspection plans). In some cases, supervisors may include inspection plans in their strategy, however a supervision strategy should set out how the supervisor will address each category of risk, including how other non-inspection supervisory tools will be employed to address risks. Importantly, the strategy should also address the information, support and guidance the supervisor plans to provide regulated entities to address identified risks. The supervisory strategy is developed in line with the supervisory risk assessment and should be revised as needed.

56. Where relevant, supervisors should refer to the relevant supervisory principles when choosing appropriate types of supervisory interventions, including the Basel Committee on Banking Supervision's Core Principles for Effective Supervision. In developing an AML/CFT supervisory strategy, supervisory authorities should ensure that there is an understanding of broader supervisory considerations. For example, authorities should share information and communicate with prudential or other relevant supervisors regularly to ensure that any areas of concern are raised and incorporated into the supervisory plan (as required) and that there is a shared awareness of the respective supervisory programs (planned inspections, desk-based reviews, etc.).

[18] In developing such strategies, supervisory authorities should ensure that there is an understanding of broader supervisory considerations. For example, authorities should share information and communicate with prudential or other relevant supervisors regularly to ensure that any areas of concern are raised and incorporated into the supervisory plan (as required) and that there is a shared awareness of the respective supervisory programs (planned inspections, desk-based reviews, etc.).

3.2. How can supervisory strategies address the risks identified?

57. Supervisory strategies should include an approach for the application of the supervisory tools on a graduated basis across the spectrum of supervised entities/sectors, with the nature, frequency, intensity and focus being determined in accordance with the level of ML/TF risk (see Sections 3.3, 3.4 and Annex A. Overview of supervisory tools).

58. The supervisory strategy should articulate the rationale for the approaches to the application of each of the specific supervisory tools in accordance with the ML/TF risk ratings assigned to the sector or specific entity (i.e., details of the purpose of the tools in terms of the outcome to be achieved and also the reasons for the regularity of their application). As the FATF standards focus on outcomes rather than process, it is important for supervisors to consider whether their activities contribute to supervisory outcomes (i.e. AML/CFT risk identification / risk mitigation) rather just the form or quantity of those interventions.

59. The application of these tools should be determined by the supervisors' understanding of the level and nature of ML/TF risk at both the sectoral and entity-levels. Supervisors should consider developing additional tailored/bespoke strategies for engaging with entities presenting the highest ML/TF risk within the supervisory population, which may be above the level of activity defined for other entities in the cohort. Strategies should be tailored to target risks specific to the jurisdiction or sector that includes not only identifying and targeting entities more exposed to these risks but also the potential for carrying out thematic supervisory reviews across a selection of entities in response to any risk-trigger events, or identified priority ML/TF risk areas (see Box 3.1).

60. Supervisors should actively consider how to improve or augment the fixed cycle-based approaches with more timely interventions to address significant changes or escalation of risks levels of regulated entities. Given the fast-evolving nature of ML/TF risks, supervisors should recognise the limitations of relying solely on cycle-based supervisory inspections where the length of the cycle is determined periodically (e.g. annually) using a point-in-time assessment of entity risk levels (see section 2.4 on keeping an up-to-date understanding of risks).

Box 3.1. The use of thematic assessments to address risks across a range of entities

Supervisors are increasingly focused on addressing priority ML/TF risks using thematic inspections and supervisory engagements. This could be conducted on-site, off-site, or a combination of both, and serves to facilitate a holistic assessment of the industry's awareness and mitigation of risks identified from the national (and sectoral) risk assessments. In this regard, a thematic inspection or supervisory engagement typically prioritises entities that supervisors assessed to have heightened exposure to the planned thematic risk focus area based on their entity-level risk assessments and ongoing monitoring, and could include entities that might otherwise have a lower overall ML/TF risk profile. Through these thematic-focused supervisory efforts, supervisors are able to raise awareness among supervised entities of

ML/TF risks that are most pertinent to the financial system, so that they can focus minds on effectively mitigating these risks.

For instance, based on the Monetary Authority of Singapore's (MAS) supervisory observations and information obtained through its national risk assessment and co-ordination mechanisms, MAS has in recent years identified and conducted targeted thematic inspections on FIs' effectiveness in areas such as combating proliferation financing, transaction monitoring, and detecting the abuse of legal persons.

These inspections have offered good opportunities for deeper dialogue with financial institutions on the priority risk areas to generate deeper risk understanding and identify consequential enhancements to strengthen risk mitigation efforts. To ensure that the broader industry is also kept apprised of these risks, MAS has published guidance papers on its findings and good practices observed from these thematic inspections.

Source: Singapore

3.3. How can supervisors adjust their approach to vary the nature, frequency, intensity and focus of supervision?

61. Supervisors should keep in mind the following four principles in deciding the tools to adopt for supervision. The first three principles should guide supervisors in the selection of tools to use based on their risk assessment of the regulated entity, as well as how the various tools interact with each other. The fourth principle is important given the fast-changing risk environment and need for supervisors to identify key risk areas and to adapt their supervisory approach/plan to target those risks.

    1. **Outcome-focused:** Supervisors should be clear about the intended objective of supervision for the sector and for individual entities. These objectives help inform the supervisor's approach in selection of tools to adopt.
    2. **Risk appropriateness:** The type and intensity of tools applied to an entity should be aligned with the supervisor's understanding of the nature and level of risks of the entity as well as the supervisory strategy in place.
    3. **Efficiency:** In selecting the most suitable tool, supervisors should consider the type of resources that are available. Supervisors should ensure that the tool chosen is the most efficient means of achieving the supervisor's objective.[19]
    4. **Dynamism and responsiveness:** Supervisors should be prepared to respond to identified emerging risks in a timely and agile manner, amending their supervisory strategy and plans to address such risks.

62. Examples of ways in which supervisors can adjust their approach based on identified risks include:

19 For example, shorter, more targeted inspections/meetings could be appropriate. In addition, resources should be used as efficiently as possible, for example: the reduction in administrative elements (where possible); using smaller teams to carry out inspections to gain greater coverage; outsourcing certain activities etc.

- Adjusting the supervisory **approach**, for example, by adjusting the ratio between off-site and on-site supervision.
- Adjusting the **focus** of supervision, for example by focusing on the management of higher risks associated with particular products or services, or on specific aspects of the AML/CFT processes such as customer identification, risk assessment, ongoing monitoring and reporting activities. It could include adjusting the range of interviews, and premises to be visited (i.e. headquarters vs branches).
- Adjusting the **frequency and duration** of supervisory engagement.
- Adjusting the **intensity and level of supervisory scrutiny**, for example by determining, according to risk, the scope, coverage and depth of transaction testing.
- Adjusting the **resources** to ensure the needed experience and skillsets are allocated to assess the identified risk.

63. Supervisors are using increasingly diverse supervisory tools. As each supervisory tool has a different and specific objective, supervisors could consider adopting one or more or combinations of these tools, and to calibrate their supervisory approaches to their objective and risks of the entities. For example, thematic inspections could be carried out to better address material risk concerns that are assessed to be of a systemic nature. For entity-specific risk concerns, supervisors may initiate a targeted inspection on that entity or employ appropriate monitoring tools, depending on the assessed risk impact. The maturity of the AML/CFT regulatory and supervisory framework should also be factored in when considering the most appropriate model to implement. For example, supervisors may need to balance resources dedicated to training/awareness raising, inspections and setting expectations when implementing a newly established regulatory framework. Consideration of such a balance is also necessary when a supervisor is newly designated as the AML/CFT supervisor of a sector and decisions are required regarding dedicating resources to cover a larger percentage of entities in shorter/targeted inspections rather than carrying out full scope AML/CFT inspections. See example 13 in the FATF Guidance on Effective Supervision and Enforcement which describes Canada's compliance continuum and the application of a range of "low intensity, high coverage" activities to "high intensity, low coverage" activities.

64. The most intensive supervisory tools are those that comprehensively test the AML/CFT controls that the supervised entity has in place. Entities associated with higher ML/TF risks should be subject to more frequent and more intense scrutiny than entities associated with lower levels of ML/TF risk. For example, in the US, many of the largest financial institutions have resident inspection staff that conduct continuous AML inspections (referred to as examinations in the US) of the various components of the large financial institution. The box below sets out how supervisors should take into account ML/TF risk when developing inspection plans. See examples 7.1.6 and 7.1.2 for how inspections are planned on a risk-sensitive basis.

Box 3.2. Planning inspections and associated resources in line with the supervisory strategy

An important part of implementing supervisory strategy when it comes to inspections is developing an **inspection plan**.

Inspection plans should list:

- the entities that will be subject to planned AML/CFT inspections or reviews during a specified period (i.e., inspections to be conducted over one year or a number of years and may also include follow-up on previous inspections)
- the type and scope of those inspections or reviews, taking into account the level of risk associated with each entity
- where relevant, the focus of each inspection or review, taking into account specific risks that have been identified or specific objectives that have been agreed (e.g. fact-finding to inform an ongoing risk assessment), and
- the supervisory resources required for each inspection or review, as well as a timeline for each inspection or review.

Inspection plans should:

- include the approach to be taken on entities with different levels of risk exposure, in line with the supervisory strategy
- leave sufficient flexibility to accommodate or address unplanned inspections triggered by risk events or new information that could not have been foreseen when the plan was agreed
- be adequately documented and amended where the risk exposure of an entity included in the plan has changed or if a new risk is identified in the course of on-site or off-site supervision, and
- be governed by an internal policy that sets out at what level the plan should be agreed/approved within the supervisory unit, how progress against the plan can be reviewed, the approval process for changes to the plan, and the extent to which an overview of the plan can be published (e.g. number of inspections per risk rating).

Source: Adapted from guidance from the European Banking Authority & IMF

3.4. How can supervisors use a combination of off-site and on-site tools to strengthen their risk-based approach?

65. As set out above, there is a range of supervisory tools that supervisors can use individually or in combination to achieve the intended supervisory outcomes. These tools when used in combination could have mutually reinforcing effects in strengthening supervisory effectiveness.

66. Off-site monitoring helps keep supervisors up-to-date on the ML/TF risk landscape, inherent risk profiles of regulated entities, and potential control weaknesses in these entities. The insights gained from performing off-site monitoring would thus guide the approach and focus of supervisors' on-site reviews. For example, the results of preliminary evaluations[20] can be used to tailor the nature, frequency, intensity and focus of supervision, as well as guide the supervisory authority to how to pivot attention to higher-risk areas. Effective off-site monitoring entails collecting and analysing data and information to enable ongoing monitoring of an entire sector, instead of a snapshot of one or several entities. As an example, risk surveillance (a supervisor's monitoring of relevant data and information including STR/CTR information where available) could help detect emerging risk areas in the sector being supervised, as well as indications of significant AML/CFT control issues in regulated entities.

67. Where off-site monitoring activities point to material risk concerns in a regulated entity, it might warrant supervisors adjusting existing on-site inspection plans in order to trigger an immediate for-cause inspection on the entity. Consistent with a risk-based approach, such for-cause inspections should take precedence over any routine inspections, given that a material risk trigger event has materialised.

68. In general, on-site inspections offer supervisors an opportunity to conduct a more thorough review of the entities' controls through the performance of sampling tests and complement off-site work. Similarly, it also helps validate the risk profile of the entity so that it can be adjusted as needed. Relatedly, there can also be an off-site process (pre-engagement) where the regulated entities' risk assessment is revalidated prior to an on-site inspection. The interactions with entities' board, management and staff during the inspection process would help inform supervisors' assessments of the entities' risk culture.

69. Some or all elements of supervisory inspections, including sample testing may also be very effectively carried out off-site, by obtaining the information from the entity and the application of SupTech tools. Where live testing is not possible off-site, the prior standard sample testing can augment additional, more targeted live testing during the on-site – e.g. when carrying out a walkthrough of a CDD system, select customers (random selection/based on level of risk etc.) and in a "live" assessment, request the member of the entity to produce the customer risk assessment, CDD documentation etc.

70. As their access to and use of technology improves, supervisors may be able to perform a significant amount of their activity off-site (see section 4.1). As regulated entities transform their business and AML/CFT compliance functions with technology, the boundaries between off-site and on-site interventions are increasingly blurred as their data is kept electronically and supervisory technology is a necessary to perform effective supervision. As off-site monitoring capabilities mature, there may be supplementary or alternative approaches that enable supervisors to more effectively identity, monitor and target risks. Where appropriate, supervisors should assess and consider adapting their supervisory frameworks, taking into account the pros and cons of the various approaches.

---

20 The relied-upon risk assessments and independent audits should properly consider and test all risk areas, including products, services, customers, delivery channels and the geographic locations in which the financial institution or DNFBP operates and conducts business, used in determining review procedures and any testing that should be performed.

3.5. How should supervisors treat lower risk sectors and entities?

71. While most supervisory resources should be dedicated to the **higher ML/TF risk areas**, supervisory' strategies should also set out the supervisory approach for areas of **lower ML/TF risk**. Within a risk-based supervision framework, it is expected that there will be areas and segments of regulated entities that are assessed to be of lower ML/TF risk. As set out above in this Guidance, the sound assessment of risks at a sectoral or sub-sectoral level does not necessarily require an assessment of each entity in the sector (see section 2.1.1). Risk analysis can be undertaken with varying degrees of detail, depending on the type of risk and the purpose of the risk assessment, as well as based on the information, data and resources available[21] (for example, keeping in mind the nature, scale and complexity of the relevant entities/sectors).

72. It should be clear that lower risk entities are still subject to supervisory attention commensurate with the level and nature of risk they present. The latter may entail the application of the supervisory tools by a combination of less frequent supervisory cycles, sample testing and/or reactive interventions. Supervisory authorities are not expected to cover all lower ML/TF risk entities under a fixed inspection cycle over time, particularly where there are large populations of lower ML/TF risk entities. [22]

73. Monitoring of lower-risk entities may allow for limited application of on-site tools. For example, one possible supervisory approach for lower risk entities is to centre it on the detection of any material risk events or escalations in risk profiles among the lower risk entities, so that supervisors can intervene effectively to mitigate risks. In such scenarios, the nature of the materialised risks and desired supervisory outcomes should guide the application of an appropriate set of tools (either onsite, offsite or a combination). See section 3.4 for further information.

74. Supervisory authorities should regularly test their understanding and assumptions of the level of ML/TF risk and the adequacy of controls in the entity/sector (see section 2.4). Supervisors should also have the capacity to carry out supervisory activities on a responsive or reactive basis, where intelligence has been received that would merit supervisory intervention (e.g., intelligence from returns or questionnaires, from other supervisors, from media reports or whistle-blowers, or from law enforcement or the FIU/STRs).

75. Supervisors should also ensure that education and outreach extends to lower risk sectors to enable them to implement risk-based, proportionate measures and to help identify and report any ML/TF risks that may arise. With reference to national financial inclusion objectives, supervisors can also play a role in: a) reducing requirements on lower risk entities that do not mitigate risk sufficiently to justify the effort they consume; b) reassuring other regulated entities that provide

---

21 See FATF Financial Inclusion Guidance that sets out further detail on risk assessment for the application of simplified due diligence and justified exemptions.

22 Supervisors should, however, not put in place blanket exemptions that exempt all low-risk entities or a complete low risk sectors from possibly being subject to on-site inspections. From a preventive point of view, to foster compliance, even if normally only a small portion of regulated entities could receive an on-site inspection during any time period, any entity/sector could possibly be subject to an on-site inspection at some point. This could be achieved through a minimum number of (annual) random on-site inspections, and / or there should be a policy that dictates in what high risk circumstances (e.g., when certain risk indicators are present) an on-site inspection of an entity or sector would be warranted despite the otherwise low risk.

financial services to lower risk entities those lower risk entities are adequately supervised. See examples 7.6.1 and 7.6.3.

Box 3.3. Supervising lower risk sectors and entities and supporting financial inclusion

An important consideration in risk based supervision is the risk-proportionate distribution of resources across the different risk areas and sectors. In particular, there may be lower-risk sectors at the national level, lower-risk segments in a certain sector, or lower-risk institutions in a sector. Furthermore, within a reporting institution, there may be lower-risk products, services, delivery channels, clients or geographic areas. However, lower risk does not mean no risk and supervisors should ensure that they can effectively detect any new significant risk concerns within the lower risk sectors and entities. While supervisors may devote less resources to lower risk areas, they should still devote sufficient resources to verifying and monitoring risk understanding of those areas while also allowing greater supervisory resource allocation to higher risk sectors.

The regulatory requirements should also be commensurate with the level and nature of risk present in sectors and entities. Recommendation 1 and INR 1 allow jurisdictions to exempt particular types of regulated entities from compliance with some of the FATF Recommendations if there is a proven low risk and the exemption occurs in strictly limited and justified circumstances. Further, in a risk-based AML/CFT regime, the CDD, internal controls, compliance function, ongoing monitoring, STR and other reporting requirements should also correspond to the risk-level of the sector and the institutions.

Risk- based supervision of lower risk sectors is also important from a financial inclusion perspective. Disproportionate legal or regulatory obligations, supervisory expectations and lack of guidance from supervisors may result in the application of unnecessarily prohibitive CDD and other AML/CFT controls in lower risk sectors, increasing the cost of products and services, and eventually undermining financial inclusion objectives. From a holistic perspective, excessive AML/CFT obligations may increase overall ML/TF risks by:

- driving potential users to the unregulated sector as a result of their failure to gain access to available financial services , or
- Increasing the costs of compliance such that it becomes unprofitable to provide products and services to people or entities that do not generate substantial income (such as Non-Profit Organisations (NPOs) (see section 10.1)) and shifting these transactions to less transparent channels.

In the US, banking supervisors have reiterated the risk-based approach with respect to NPOs in which banking supervisors reminded banks that offer financial services to this sector should not view the charitable sector as a whole as presenting a uniform or unacceptably high risk for

ML/TF risks.[23] Banking supervisors provided non-binding guidance of factors to consider in identifying the AML/CFT risk profile of NPOs.

Box 3.4. The role of supervisors in identifying de-risking or in encouraging financial inclusive practices

While a risk-based approach requires supervisors to focus their attention on higher risk areas, lower risk areas still require attention particularly if financial exclusion is a concern. Financial exclusion of customers holds serious ML/FT risks as customers may seek the unregulated cash economy or access services by providers who may not have robust risk control measures. Where supervisors identify that an institution is involved in large-scale and indiscriminate account closure or denial of services or does not implement simplified due diligence measures where risks are generally assessed as lower, supervisors should engage the institution to understand the reasons for its decisions.

As set out in the FATF Guidance on Money Value Transfer Services (2016) while the decision to introduce simplified due diligence measures or to accept or maintain a business relationship is ultimately a commercial one for the entity, supervisors need to scrutinise these decisions to understand whether these decisions may indicate a need for supervisory clarifications or reforms, or whether they indicate an area of changing risks, or some other dynamic such as profit concerns. Where decisions to restrict or terminate relationship with customers is due to a lack of understanding of the flexibility of the risk-based approach, supervisors will be able to provide appropriate guidance as to what the RBA entails.[24]

Entities may be engaging in indiscriminate denials of service to entire classes of customer, without taking into account, seriously and comprehensively, their level of risk and risk mitigation measures for individual customers within a particular sector. This is contrary to the advice given by FATF.[25]

3.6. How can supervisors develop a more robust risk-based approach over time?

76. **Supervisors should ensure that their supervisory strategies are kept under regular review**. In implementing the strategy, supervisors will develop a better understanding of the quality of the supervised entities' AML/CFT controls and the ML/TF risk profiles of the business models, as well as the effectiveness of various supervisory tools. This knowledge should be utilised to enhance the overall ML/TF risk understanding at both the sectoral and the individual entity levels along with

23 https://home.treasury.gov/news/press-releases/sm1183

24 www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf

25 www.fatf-gafi.org/documents/documents/rba-and-de-risking.html

consideration of any new/emerging ML/TF risks. Building and maintaining the institutional memory is key to achieve this.

77. Further, supervisory authorities should use the experience garnered from carrying out supervisory tasks to enhance the effectiveness of their supervisory strategies and to **continuously refine and enhance these methods**. In addition, on an ongoing basis, the risk assessment (along with supervisory planning process) should not be conducted in isolation, but in close co-ordination with prudential supervision and other relevant departments (or other supervisors). Any changes to the ML/TF risk understanding and/or proposals for refinement or enhancement of the mix of supervisory tools to be applied should be considered in the context of the review of the overall strategy with the aim of continuing to improve and strengthen the supervisory approach to ensure it remains effective.

78. Supervisors should implement mechanisms to ensure sound and consistent supervisory assessments and independence regarding decision-making in AML/CFT risk-based supervision. For example, when determining a risk rating for a sector and for individual entities the decision should be supported by a documented outline of the assessment (including findings from onsite and offsite activities etc.) and the rationale to explain the proposed risk rating.

79. Supervisors, particularly supervisors with larger, more complex supervisory populations, may apply additional measures to ensure consistency. For example, assigned risk ratings could be subject to peer review/challenge by other staff members within the AML/CFT supervisory unit who were not involved in the assessment.[26] Other examples of methods to further enhance the integrity of the assessment (at both the sectoral and entity level), could include a supervisory panel to provide independent judgement and to promote consistency. Such panels could comprise management members/representatives/specialised staff from the supervisory body who are not involved in the direct supervision of entity/sector. Supervisors responsible for direct supervision of entities could present their findings and recommendations to the supervisory panel for a "horizontal" review to ensure consistency of supervisory judgement. The supervisory panel would over time develop a sense of how AML/CFT supervisory issues are dealt with in a range of contexts and will be able to usefully transmit this to supervisors/ teams whose perspective is inevitably narrower based on the entities they directly supervise.

80. **Adequate training is required to support an effective AML/CFT risk-based supervisory framework**. Training is required at all levels, from front-line supervisors to managers and board members. The training should cover issues such as how to interact with entities and risk-based decision making. The visible and active engagement of senior staff in training sends a strong signal about their commitment to the process.

81. In some circumstances, **the transition from a rules-based to a risk-based approach takes time.** It can require a change in the supervisory culture and the management of supervisory bodies need to articulate their risk tolerance. There also needs to be recognition that AML/CFT related weaknesses in areas of lower ML/TF risk may go undetected by supervisors in the application of risk-based

[26] It is preferable that this step is always carried out when there is a change to a sectoral risk rating. It is not intended for this step to be carried out for all entities, it could be based on a prescribed number of entities, on an annual basis, that are selected on a sample basis and should include entities across all risk ratings.

supervision and responses to these will be governed largely by whether they are within or outside the range of acceptable outcomes implied by the risk tolerance.

82. Supervisors of different sectors and supervisors in different jurisdictions should encourage collegiality and share best practices, for example, through facilitating "best practice" visits, especially for those authorities that have less mature frameworks to learn from more established/effective AML/CFT supervisors, In addition, more established supervisors should share good practices and facilitate "best practice" inspections. For examples of co-operation between supervisors, see Section 7.5.

3.7. How should remedial actions and available sanctions be applied in risk-based supervision?

83. R.35 requires jurisdictions to have a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons that fail to comply with AML/CFT requirements. The FATF Guidance on Effective Supervision and Enforcement is a comprehensive guide on remedial actions and sanctions. This section focuses on links between taking a risk-based approach to supervision and applying remedial actions and sanctions.

84. Supervisory authorities should have access to a range of remedial actions and sanctions that can be applied based on the level and nature of identified deficiencies or gaps in the regulated entity's AML/CFT controls and risk management system. This range could include warnings, action letters, orders, agreements, administrative sanctions, penalties and fines and other restrictions and conditions on an entity's activities that may be progressive in severity, requiring entities to remedy AML/CFT deficiencies and any breach of AML/CFT obligations or failure to mitigate risks in a timely manner.

85. In assessing the appropriate remedial actions or sanctions to apply in a risk-based supervision approach, supervisors should consider the following:

- the nature of findings – deficiencies in relation to higher risk areas, including those identified in a national, sectoral or supervisory risk assessment, could be prioritised for remedial action or sanctions as appropriate
- the impact or harm that the identified deficiency or gap in terms of ML/TF risk exposure of the entity, sector and the public (e.g., whether it is a systemic breakdown, isolated incident or other egregious activity, such as failing to report large volumes of suspicious activity or other required reports and the length of time the identified deficiency or gap in the regulated entity's risk management system remained outstanding or uncorrected. Supervisors may consider the scope of the deficiency in terms of the probability of the risks materialising given the entity's size, nature, geographic reach, volume of business conduct)
- using the power to withdraw, restrict or suspend the entity's license (or equivalent for those registered), where applicable, for example, in situations where the entity has been determined by legal process to have engaged in criminal activity related to ML or TF, a severe and systematic violation of AML/CFT measures, or similarly applicable sanctions or prohibition of directors and senior managers.

- publishing the results of the supervisory actions and providing information on the relevant entities' deficiencies to help address risks across the sector as other entities take note of the consequences of similar failings.

86. Based on these considerations, effective remedial actions and sanctions application should seek not only to discourage past inappropriate actions and correct weaknesses in processes, procedures and systems or controls within regulated entities but also to **promote changes in behaviour to foster a corporate culture of compliance that covers the board, senior management, compliance teams and all other relevant staff of the relevant entity**. To this end, supervisors should be able to apply remedial actions and sanctions proportionately to greater or lesser breaches of supervisory requirements against board of directors and management, controlling owners and other employees of regulated entities, depending on their level of responsibility in committing the breach, especially in the case of intentional or serious breaches. Supervisors should also ensure that the compliance departments of regulated entities have sufficient stature, independence, staffing and resources commensurate with the risk profile of the entity. The confidence that a supervisor has in the demonstrated intent, commitment and capability of an institution to satisfactorily remedy identified deficiencies may influence the supervisor's selection of formal or informal remediation tools or techniques. For example, if supervisors identify a large control deficiency, yet believe the institutions has a satisfactory culture of compliance and a high capability of remediating the issue, the supervisors may opt to take a lighter approach in remediation techniques.

87. **Supervisors should also consider transparency, consistency and proportionality in applying remedial actions or sanctions** while taking into account the specifics of the particular entity, the nature and significance of the risk mitigation failures and the identified deficiency or gap. Consideration should be given to establishing policies/guidelines for determining which remedial action and/or sanctions are most appropriate to be applied in particular circumstances, and methodologies for calculating/determining amount of fines, severity of orders and administrative sanctions that are dissuasive and proportionate to the size of the regulated entity as well as the seriousness of the failure. Such transparent and consistent application could improve effective implementation of AML/CFT measures among regulated entities.

88. On the other hand, supervisors should avoid taking a "zero tolerance" or "zero failure" approach, or applying mandatory sanctions on entities where the risk impact is not material, or where the deficiencies are less relevant from a risk-mitigation perspective as this could give regulated entities the wrong message and create an incentive for entities to return to a rules-based approach. While sanctions may in some cases be appropriate for non-compliance in areas of lower risk (for example, to address repeated, knowing or wilful non-compliance with AML/CFT requirements), supervisors should consider the totality of the entity's mitigation efforts and use the flexibility of the risk-based approach to supervision to avoid sanctioning entities for focusing their efforts on areas of higher risk.

3.8. How should supervisors measure the effectiveness of their risk-based approach?

89. **Supervisors should also properly record, monitor, and analyse their own supervision activities and outputs**. Supervisors, when developing their

supervision models, should ensure that they have a repository for recording supervisory engagements (ideally in digital form) with each entity including details of the issues identified, relevant action plans and the risk assessment for each entity. The supervisor should be able to extract data and management information (MI) in order to measure performance against key risk indicators and on issues identified and risk profiles of each individual entity and sector, and feed these in aggregate form back into the NRA process.

90. **Supervisors are encouraged to use data to determine and demonstrate the impact of their supervision.** For example, using a system to record supervisory engagements that enables the extraction of data to illustrate how supervision has impacted risk management and compliance, both at the firm and sectoral level. Data can help to identify changing patterns in terms of numbers, degree of seriousness of issues identified overtime and fluctuations in ratings of the effectiveness of the controls. This includes the analysis of the changes in the quality or risk management and risk profile of the individual institutions as well as overall trends in the sector, including de-risking and financial exclusion concerns.

91. This information should also be used to better target the application of supervisory resources and supervisory tools and to inform the approach on outreach initiatives. For example, analysis of the supervision data may indicate increasing problems resulting from potential deficiencies in the transaction monitoring capabilities of the regulated entities, leading the supervisor to issue new guidance or requirements to address this developing trend. Other the other hand, data can also indicate whether supervisory efforts are succeeding in terms of their impact on the improvement of AML/CFT measures in an entity or across a sector whereby findings identified during inspections move from the space of significant gaps being identified to overtime findings identified being of a less serious nature and being more in the space of refinements or enhancements. Improvements in the quality of risk assessments undertaken by entities may be another measure of effectiveness.

92. Another measure which can assist supervisors in determining the impact of their supervision on entities' risk management effectiveness is to **consider the key outputs from AML/CFT frameworks, e.g., the quality of suspicious transaction reports**. Supervisors should seek feedback from FIUs as to the number, quality and timeliness of reports they have received from sectors and entities, as improvements in this area can also be an indicator of the successful results of supervisory activities. Some of the relevant factors supervisors could consider include:

- The number of ML/TF offences committed using the sector's infrastructure and any relevant changes in trends
- Changes in the number and quality of STRs submitted by entities in the sector and the timeliness of this reporting
- The number of breaches or deficiencies, including repeated failings, committed by entities and the severity of these deficiencies,
- Complaints received from stakeholders, and
- Evidence of entities going beyond a tick-box approach and demonstrating a commitment to risk-based AML/CFT objectives, including proportionate responses across the spectrum of risk (including higher and lower risk areas).

93. The measurement of the results of supervisory measures and feedback on the key outputs of AML/CFT frameworks can help safeguard against confirmation bias.

When this feedback does not align with supervisors' understanding of risks, this should prompt supervisors to reconsider assumptions. Supervisors should apply measures to revisit their risk models or risk assessments based on engagement with law enforcement agencies, the FIU and international partners and ad hoc or sample testing or using whistle-blowers reports or adverse media reporting.

94. **There should be mechanisms in place to promote accountability and transparency**, of the effectiveness of the supervisor's risk-based approach. This should include at least one of the following: (i) oversight by the supervisor's management board; (ii) oversight by the supervisor of SRBs (in a decentralised model); (iii) review by a State Audit Office or similar governmental body; and (iv) as appropriate, publication of information relating to the supervisory strategy and inspection plans and results of supervisory engagements. For example, without impinging on the operational independence of the supervisor:

- the supervisor's board, State Audit Office or national co-ordination authority could set key performance indicators against which they periodically assess effectiveness of the supervisor
- industry surveys could be used to periodically assess performance of the supervisor, and/or
- supervisors and the FIU could periodically report on the number and quality of reports by sector, since this is often considered to be a good measure of the level of effective implementation of preventive measures by supervised entities.

Box 3.5. UK's Office for Professional Body Anti-Money Laundering Supervision (OPBAS) measures to test the effectiveness of DNFBP supervisors' risk-based approach

OPBAS supervises Self-Regulating Bodies (SRBs) that are designated DNFBP supervisors under the UK's money laundering regulations. As part of their supervisory activity, a DNFBP supervisor which supervises a sector described as high risk in the UK NRA, identified their 103 highest risk entities. At the request of OPBAS, they conducted an on-site deep dive assessment of those entities and identified a high level of non-compliance and poor systems and controls. Their findings, and follow up discussions with OPBAS, influenced them to allocate appropriate resources to an on-going programme of more intensive supervision for these entities. They will also dip sample visit some entities identified as high, medium and low risk to assess if their wider supervisory strategy is fit for purpose or needs further evaluation and refinement.

Where DNFBP supervisors, particularly SRBs, have multiple functions (for example, as an advocate for their members who they also supervised for AML/CFT compliance) care must be taken to ensure potential conflicts of interest are managed appropriately. In the UK, this was a particular focus for OPBAS when assessing supervisors who maintained both an AML and advocacy role. Robust governance in place within the supervisor helps mitigate this risk.

Source: United Kingdom

3.9. Domestic co-operation, including between AML/CFT supervision and prudential supervision

95. Co-operation and information exchange between AML/CFT supervisors, other supervisors, FIUs, and other competent authorities, including tax authorities and law enforcement, is important to ensure that all stakeholders have a good understanding of, and can act to mitigate, ML/TF risks. Co-ordination with LEAs and the FIU can help to assess the effectiveness/usefulness of the outputs of entities' AML/CFT programs and provide coordinated messages on risk prioritisation.

96. Prudential and AML/CFT supervisors should establish an effective co-operation mechanism regardless of the institutional setting to ensure that ML/TF risks (informed by NRA processes) are adequately supervised in the domestic and cross-jurisdictional context for the benefit of the two functions. Even when a prudential supervisor is not part of an integrated supervisory authority with the AML/CFT supervisor, and that authority therefore does not have direct responsibility for supervising or monitoring compliance with AML/CFT requirements, it will often be responsible, among others, for licensing, and will monitor implementation of systems and controls from a prudential perspective that may be relevant for AML/CFT purposes. For further details see the *Basel Committee on Banking Supervision's Guidelines for the Sound Management of Risks relating to Money Laundering and Financing of Terrorism* at Annex 5 "Interaction and Co-operation between Prudential and AML/CFT Supervisors".[27] Jurisdictional examples are provided in the FI Compendium at Section 7.5.

97. In addition to risk understanding, domestic co-ordination mechanisms (especially the NRA process) should also allow the allocation of resources to AML/CFT supervision based on ML/TF risks (see section 2.1.2). As a practical matter, supervisory attention of different sectors may be affected by available resources. For example, a well-resourced supervisor of a lower risk sector may apply a disproportionate amount of resources to monitoring compliance with AML/CFT requirements, because it has strong funding arrangements. Conversely, a poorly resourced supervisor of a higher risk sector may fail to apply adequate proportion of its resources to AML/CFT supervision since the resources available to it are insufficient. National Risk Assessment processes and co-ordination between supervisors should aim to help to allocate resourcing in a risk-sensitive manner.

3.10. International co-operation to achieve a risk-based approach to supervision

98. Many regulated entities routinely operate across national borders and may therefore be subject to AML/CFT supervision by several supervisory authorities in multiple jurisdictions. The ML/TF risks in question are frequently cross-border in nature, and systems and control failings in one part of the group can be replicated elsewhere. Taking a risk-based approach to supervision requires international co-operation, particularly in relation to groups operating across multiple jurisdictions. Co-operation between supervisors is important to mitigate those risks and is covered under Recommendation 40.[28]

---

[27] https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2020/935606/Opinion%20on%20how%20to%20take%20into%20account%20MLTF%20risks%20in%20SREP.pdf

[28] Interpretative Note to Recommendation 40, paragraphs 10-13.

99. International co-operation increases the effectiveness of the risk-based approach by:

- Enhancing risk understanding – including understanding the group's attitudes and understanding of risks. Broader information on risks could also be shared to increase awareness among supervisors of emerging risks or to develop a common understanding of risks associated with particular types of initiatives, sectors or activities (for example, sharing risks associated with MVTS corridors for financial inclusion purposes). Sharing risk and controls assessments among supervisors would strengthen their collective understanding of the group's risk profile, and its impact on their respective regulated entities.
- Harnessing synergies in supervisory efforts – to coordinate on supervisory interventions and follow-up, and to identify and drive synergies by sharing supervisory priorities, strategies and programs. Supervisors may conduct inquiries on behalf of foreign counterparts and authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to achieve effective group supervision.
- Ensuring effective risk mitigation – to assess implementation of preventative measures and the strength of control and audit functions at a group-level.

100. There are challenges to international co-operation between AML/CFT supervisors that in turn may limit the effectiveness of supervision such as a lack of common understanding about the AML/CFT information that should be shared or where there could be legal obstacles to information sharing with counterparts and non-counterparts across borders. Data protection and privacy provisions often inhibit sharing of relevant personal information for fit and proper tests. In some cases, information on ongoing cases being pursued by supervisors is not shared with foreign counterparts due to fear of tipping off or causing undue alarm. Cross-border contact between AML/CFT supervisors may be ad hoc, rather than ongoing, even when it concerns an ongoing cross-border risk.

101. Supervisors of higher risk entities operating in groups should actively communicate with other relevant supervisors and there should be official channels in place for co-operation amongst supervisors of groups of higher risk entities, including spontaneous sharing of information that may be relevant to other supervisors. The *Basel Committee on Banking Supervision's Guidelines for the Sound Management of Risks relating to Money Laundering and Financing of Terrorism* includes guidance on the roles of home and host supervisors and sets out guidelines for supervision of group-wide AML/CFT measures for financial institutions. In the EU, supervisory co-operation can occur in AML/CFT colleges in relation to entities active in multiple EU member states (see box below). Even though co-operation between supervisors of DNFBP sectors is less well developed, there are efforts to increase international co-operation on DNFBP supervision. For example, DNFBP supervisors are involved in the "International Supervisors Forum" which includes supervisors from Australia, Canada, New Zealand, the United Kingdom and the United States.

Box 3.6. AML/CFT supervisory colleges in the European Union

AML/CFT and prudential legislation in the European Union (EU) establishes an obligation for competent authorities to co-operate and exchange information, but it does not set out in detail how this should be achieved. In the absence of a common framework, co-operation and information exchange between prudential and AML/CFT supervisors for the purposes of AML/CFT supervision can sometimes be difficult.

To address this, the European Supervisory Authorities (ESAs) issued Guidelines on supervisory co-operation and information exchange in December 2019. These Guidelines lay down the rules on the establishment and operation of AML/CFT colleges.

As is the case with prudential colleges, AML/CFT colleges serve as a forum for collaboration and exchange of information. They support the development of a common understanding, by all supervisors, of the ML/FT risks associated with a bank or financial institution and inform the AML/CFT supervision of that bank or financial institution. For example, the Guidelines set out how AML/CFT supervisors can use AML/CFT colleges to adopt a common approach and agree on coordinated actions.

The Guidelines provide that AML/CFT colleges be set up for all banks and financial institutions that operate in at least three EU member states. All EU AML/CFT supervisors involved in the supervision of the bank or financial institution for which a college is set up are permanent members of that college.

EU prudential supervisors and the AML/CFT supervisors of non-EU countries where the institution operates are invited to participate in the AML/CFT college as observers. Prudential supervisors from non-EU countries and the FIU of the EU member state where the lead supervisor is located may be invited to participate as observers as appropriate.

All observers have to be subject to confidentiality rules equivalent to those in force in the EU. They are expected actively to participate, including by exchanging information within the AML/CFT college. Observers that are prudential supervisors are further expected to take action to ensure that information from AML/CFT college meetings is shared with colleges of prudential supervisors and acted upon as appropriate.

FIUs from other jurisdictions, as well as other relevant persons, may be invited to participate in the AML/CFT college on an ad hoc basis as necessary.

4. Cross-cutting issues

4.1. Use of technology by supervisors ("SupTech")

102. This section is intended to share experiences of how supervisors have leveraged technology for their supervisory work and how they have benefited from the use of such tools in the conduct of risk-based supervision. It does not advocate any specific technological tools which must be adopted for supervision.

103. New sources of data and advanced analytical tools can help supervisors be more efficient and effective at detecting and mitigating ML/TF risks. There are also new technologies available for supervision, in particular collecting, storing, analysing and transforming supervisory data to sharpen risk assessment, as well as to improve the supervisory process.

104. By harnessing the benefits of new technologies where appropriate, supervisors can more effectively and efficiently achieve their supervisory objectives.

- Technologies can automate routine processes and free up valuable supervisory resources allowing supervisors to focus on tasks that require human judgement expertise and experience.
- Advances in data processing capabilities, network-linked analysis techniques, robotic process automation, machine learning and artificial intelligence in general provide opportunities for supervisors to glean additional useful supervisory insights and identify risk trends across sectors and groups of regulated entities. Some supervisors have access to a far greater pool of information than any individual entity and, while it should not perform the role of an FIU, technology that enables analysis of system wide risk should be shared with other agencies and, as appropriate, the private sector, so as to collectively manage risk and preserve the integrity of the financial system.
- The opportunities for harnessing the use of new technologies for greater supervisory effectiveness are present in almost all areas of supervisory work. Some examples include:
    - Risk assessment of regulated entities: Technology could enhance supervisors' risk assessments of regulated entities, and across the sector.
    - System-wide risk surveillance: Technology could strengthen overall risk surveillance capabilities, supporting activity-focused supervision to augment entity-focused supervision so as to target evolving risks more effectively.
    - Supervisory reviews: Technology could enhance the effectiveness of on-site/off-site supervisory reviews by augmenting supervisors' manual reviews with machine-assisted analyses of large datasets.
- Technology could also enable deeper collaboration, including by strengthening linkages with regulated entities. Technology could open more effective channels for information sharing between regulators, law enforcement agencies and regulated entities, and strengthen collective defences against financial crime. Where regulated entities are using technologies to assist with AML/CFT functions or are providing technology-

based services, effective supervision also necessitates good understanding of the use of technology by these entities and the resulting impact.

- Supervisors must also consider the potential risks of adopting new technologies including the possible amplification of cyber-related risks (by making the impact of cyberattacks or operational failures much more serious than when using traditional procedures), over- reliance on tech-models and reputational risks (if incorrect algorithms are input into technological applications that result in wrong supervisory assessments and actions). Some practical limitations may also persist, including cost/benefit considerations and the availability of underlying data. There is also a need to periodically review the effectiveness of the technological solutions and enhance the solutions where necessary, to ensure it remains relevant and accurate. In decentralised systems, supervisors may not be of sufficient size and scale to harness SupTech. Efforts to mitigate potential risks, such as running new technology in parallel form to the existing process for a reasonable period of time, should also be evaluated to ensure the resulting level of residual risk can be effectively managed.
- FATF is exploring the risks and opportunities of new technologies under its current project on digital transformation. For practical examples of the use of technology to risk-rate entities, conduct ongoing monitoring and better target supervisory resources see section 7.2.

4.2. Engagement with the private-sector

105. To develop a good understanding of the risks facing supervised entities, supervisors should maintain ongoing engagement with the private sector. ML/TF typologies evolve rapidly and the private sector may be able to detect these changes and inform supervisors. The private sector is likely to identify these changes before supervisors since they have direct contact with customers. On-going co-ordination between supervisors and other government authorities in their engagement with the private sector ensures clear messages are sent on expectations for risk management. In more recently regulated sectors, industry engagement should include education and awareness raising. Some of the features of a well-coordinated inter-agency and private sector dialogue system could include:

    - Ongoing and regular dialogue between a range of government agencies (supervisors, law enforcement agencies and the FIU, for example) and a range of participants from regulated sectors. In some jurisdictions, this takes the form of standing consultation forums, conferences or committees. This provides an opportunity to discuss risks, and also supervisory guidelines or other developments. While the primary purpose of these events is not to provide specific feedback on an entity's compliance, they can help to raise awareness of common challenges and responses.
    - Regular information sharing, education and outreach with and across the private sector to improve understanding of risks, including through public-private partnerships. This can help supervisors and other authorities achieve a more sophisticated and up to date understanding of risks faced by the private sector. It can also help entities develop their understanding of risks (see the example at 7.4.2).

- Seeking private sector feedback on particular issues. For example, seeking public feedback on the main outcomes from an inspection cycle or thematic review, or identifying the issues in which the regulatory guidance is needed most or clarification on simplified requirements in proved low risk customers/products.
- Broadening dialogue and outreach beyond regulated entities to a wider range of relevant audiences. For example, in Japan industry outreach includes engagement with trade associations and ship-owner associations to share risk information with regulated entities and the public sector to level awareness on inherent AML risks the sector faces, and necessities of transaction due diligence and investigations that the regulated entities take against customers.

4.3. Use of third-parties

106. Supervisors may use third parties (such as external consultants or auditors) to support their AML/CFT functions. While these activities can provide useful expertise and conserve key resources for the most important functions, ultimately the responsibility remains with supervisors to ensure compliance with their supervisory obligations. This section highlights some of the opportunities and risks that supervisors should be aware of in this context.

107. It is essential to strike the right balance between internal capacity building and use of third parties. The priority should be building the internal capacity of the supervisory authorities to fulfil their functions effectively and independently. This includes adequate number of in-house staff who are equipped with a range of skills and qualifications. Using third parties in AML/CFT tasks may have some efficiencies. However, overreliance or dependence on third parties can undermine the building of internal expertise and capacity.

108. Use of third parties has become more relevant especially as the financial sector's level of sophistication has increased with respect to innovations in financial products and services (e.g., 'FinTech'), business models, and IT capabilities. Therefore, the ability to tap into the expertise of financial engineers, IT experts, data scientists, and other professionals in supervisory activities becomes essential for effective supervision.

- Some financial products involve financial engineering that can go into the design of even a single transaction or contract (so-called 'exotic financial products'). While supervisors need to develop their own understanding of these products and associated risks, in some cases access to specialist expertise and skills may assist in developing this understanding.
- The rapid changes in the information processing, analysis, and storage technologies, and innovations such as distributed ledger technology or artificial intelligence increase the importance of supervision and oversight of technology employed to undertake AML/CFT functions.
- AML/CFT supervision of the banking sector and other large financial institutions cannot be undertaken without a thorough examination and understanding of their IT systems (so-called MIS) including their monitoring systems, parameters and third-party AML/CFT compliance solutions.

109. The use of third-parties to assist in monitoring lower risk sectors or entities can also help supervisors focus on higher risk entities. The FATF Guidance on a risk-based approach to the MVTS sector highlights that engaging third parties to assist in performing periodic reviews of lower-risk MVTS providers can help supervisors focus on the higher risk MVTS providers and avoid being overwhelmed by the broader population.

110. The use of third-parties can aid supervisors to monitor entities' remediation efforts. For example, in the UK, the Financial Conduct Authority can require an entity to engage the services of a 'Skilled Person' to carry out a review and provide a report to the FCA.[29] The Skilled Person can test a firm's systems and controls, identify weaknesses, and in some cases, remediate the weaknesses identified.

111. Supervisory authorities' employment practices should allow enough flexibility to ensure that supervisors can access technical expertise necessary to meet their regulatory requirements. External assignments and secondments can also help these staff to diversify and deepen their experience. When engaging a third party, the supervisor should:

- Have processes to evaluate and recruit third party candidates (e.g., competencies, credentials, experience in the risk area, potential conflicts of interest, etc.)
- Have and relevant data protection laws.
- Put in place controls to ensure that the third parties carry out their tasks efficiently, effectively and independently, and in line with the tasks or instructions provided by the supervisor
- Ensure adequate protocols for communication of issues identified
- Have processes in place to oversee and monitor the quality of work being delivered, and
- Have third-parties request permission for controlled access to supervisors' confidential information and require compliance with clear terms of reference and manual and electronic processes to protect sensitive information, including with respect to relevant data protection laws.

112. The steps set out above are important for supervisors to satisfy themselves that the expertise being provided is of high quality and delivering the expected outcome and that the supervisor is aware of systems and controls problems identified within entities.

113. Another increasing trend is the use of the third parties by the reporting entities to carry out some of the AML/CFT functions (such as record keeping, some components of customer due diligence, monitoring of terrorist individuals and entities identified as-per the relevant UN Security Council Resolutions, and monitoring of PEPs). In such cases, the legal responsibility to comply with AML/CFT obligations remains with the reporting entity. However, at least through the reporting entity, the supervisors should have the power to examine the capabilities and effectiveness of these third-parties in fulfilling the contracted AML/CFT tasks.

29 www.fca.org.uk/about/supervision/skilled-persons-reviews

Annex A. Overview of supervisory tools

Understanding and profiling risks	
AML/CFT returns	Regular or ad hoc requests to entities for quantitative and qualitative data and information relating to key ML/TF risk indicators (e.g. business lines, product segments, types of customers) and general information about the entity and the nature and scope of their activities. The collection of regular AML/CFT returns could be automated and aims to help supervisors gain a better understanding of the ML/TF risks to which their sector is exposed, to aid in the risk profiling of the supervised entities.
Engagements with Board and Senior Management	Regular engagements with the Board and Senior Management of supervised entities, particularly those that are systemically important, could enable supervisors gather timely information on potential changes in business strategy or focus which could impact the inherent ML/TF risks of the entity.
Ongoing surveillance of emerging risks and trends	Supervisors look to identify key risk trends and systemic risks through mechanisms such as engagements with other regulators, mining of system-wide risk-relevant data, conversations with regulated entities, and ongoing news monitoring. This would help in more dynamic and up-to-date ML/TF risk assessments of the regulated entities. Results from surveillance would also directly impact the calibration of supervisory response (e.g. thematic inspections to address systemic weaknesses, or specific areas of focus for individual entities).
Assessing AML/CFT systems and controls	
Questionnaires on AML/CFT risk management controls	These questionnaires, which are typically updated on a regular basis, enable supervisors to form an early view of the adequacies of an entity's controls in mitigating ML/TF risks, and to formulate a purposeful supervisory engagement plan. The questionnaires could encompass various aspects of entities' AML/CFT risk management controls including the governance framework in place, updates on relevant policies and procedures, robustness of controls execution, etc. Observations from entities (e.g. common weaknesses noted) at a sectoral level could also serve as feedback to supervisors on whether thematic reviews should be conducted, to improve industry's risk understanding.
Review adequacy of board and management reporting and oversight	Supervisors could assess robustness of the entities' governance structure and framework, and adequacy of AML/CFT reporting to board and management, as an indication of the risk culture of the entity. The reviews could be done on site or off site.
Review adequacy of policies and procedures	This enables supervisors to assess the sufficiency and effectiveness of an entities' policies and procedures in mitigating ML/TF risks. It could also provide supervisors with opportunity to corroborate the findings and results of the ML/TF risks assessment conducted by the entity. The reviews could be done on site or off site.
Review of internal and external audit reports	These reports could help supervisors identify any potential areas of weaknesses in regulated entities for further supervisory engagements. The reviews could be done on site or off site.

Interviews with staff of various functions and seniority including Boards and senior management	These interactions enable supervisors to assess the level of understanding and ability of employees of the regulated entity to effectively identify and mitigate ML/TF risks through the execution of controls. Discussions with the Board and senior management of the entity allow supervisors to assess their competency, risk awareness and risk appetite towards ML/TF risks, and get a sense of the tone from the top. In turn, interviews with staff executing the controls, typically performed during inspections, allow supervisors to assess the 'echo from the bottom' to ensure alignment of the working level risk culture with the tone set by the Board and management.
Entity-specific inspections/ reviews	Entity specific inspections or reviews could be performed onsite or offsite, depending on the supervisory intensity required under the risk-based supervisory approach. In sectors with large numbers of small lower risk supervised entities, off-site inspections and virtual meeting can be effective. Scheduled onsite or offsite inspections or reviews are arranged in line with the risk-based approach and generally encompass a review of the existing frameworks and policies mentioned above. The intensity and scope of the reviews could vary depending on the purpose of the inspection or review. For onsite inspections, sample testing are often performed to validate the effectiveness of controls execution. This is usually not performed for offsite reviews. Triggered onsite or offsite inspections or reviews are more targeted and triggered by a specific event, such as whistleblowing, public allegations of wrongdoing (such as the Panama papers), a new ML/TF typology or findings from another supervisory action such as an assessment of wider internal controls, or findings from an AML/CFT questionnaire.
Thematic inspections/ reviews	Similar to entity-specific inspections or reviews, thematic inspections or reviews could be conducted onsite or offsite. Thematic reviews are performed on a number of entities, often from the same sector, focusing on one or a few specific aspects of the entities' AML/CFT systems and controls, such as transaction monitoring treatment of PEPs, or specific risks such as TF, proliferation financing and trade-based money laundering. Thematic reviews often serve to help supervisors gain a better understanding of the way specific ML/TF risks are managed by a sector, or particular types of entities.
Tracking of rectification of lapses identified in past inspections	This allows supervisors to monitor if past observed weaknesses have been satisfactorily remediated in a timely manner, and if additional supervisory actions may be warranted.
Outreach to industry	Supervisors may also conduct outreach activities to convey supervisory expectations to entities, and to educate entities on emerging ML/TF issues that are applicable sector-wide. This may include workshop, training, seminar or periodic engagement with industry associations.

PART TWO:
STRATEGIES TO ADDRESS COMMON CHALLENGES IN RISK-BASED SUPERVISION & JURISDICTIONAL EXAMPLES

Objectives and scope

114. This section identifies common challenges in applying risk-based supervision and presents potential strategies to address these challenges, but does not oblige authorities to take any of the specific measures outlined. It should be read alongside the FATF Standards and the Guidance in Part One of this paper.

115. The examples covered in this section and in Part 3 should be considered in light of the supervisory frameworks in place in those jurisdictions – the strategies may not be appropriate in all contexts. The inclusion of examples in this report is for illustrative purposes only and does not constitute the FATF's endorsement of the effectiveness of the country's supervisory framework for the purposes the FATF mutual evaluations or otherwise. Readers are advised to bear this in mind when drawing reference to these examples.

Overview of challenges identified in Mutual Evaluations

116. While mutual evaluations demonstrate some successes in applying the risk-based approach to supervision, in three out of four evaluations, major and fundamental improvements are required. The majority of the 102 countries evaluated against the 2013 FATF Methodology are rated "moderate" for IO.3. A Core Issue by Core Issue review shows that the largest gaps to achieving "substantial" ratings are in the implementation of the risk-based approach to supervision (Core Issue 3.2) and the application of sanctions for non-compliance (Core Issue 3.4). Analysis of a sample of 59 evaluations suggests that only 24% of FI supervisors and 7% of DNFBP supervisors have conducted an updated risk assessment. Analysis of Core Issue 3.2 of these reports reveals that the ability to apply supervision on a risk-sensitive basis is not necessarily connected to sector supervised, but rather to the overall quality of supervision (i.e. means and tools available to supervisors). Supervisors with more resources and tools were able to mitigate, although not eliminate, this gap and adequately supervise both FI and DNFBP sectors.

117. Countries are performing generally very well in terms of technical compliance with requirements related to supervision, with largely compliant to compliant ratings obtained in most Recommendations. However some weaknesses remain with 44% countries rated NC on R.28, related to the supervision of DNFBPs.

118. The evaluations highlight different degrees of supervisory focus and resources put on financial and DNFBP sectors. Implementation of risk-based supervision is generally more advanced for FIs than it is for DNFBPs. The DNFBP sectors are often newer to regulation and there are challenges for the supervisors and the industry. Entities in DNFBP sectors often have insufficient understanding of their obligations and sectoral and –entity level- risk assessments, when available, are less developed. Often there are also limitations within the agencies responsible for supervising or monitoring DNFBPs (i.e. lack of capacity/expertise and resources to supervise the large sectors, agencies new to supervision, overlapping responsibilities, etc.). In addition, these sectors often include a large number of entities that vary widely in size, nature and sophistication while also involved in a diverse range of activities, creating challenges in risk assessment and risk-based supervision. The challenges in relation to VASP supervision can be similar to those faced in other sectors but are also unique due to a number of factors, including the novel nature of the sector, its global reach and the speed at which transactions can take place.

5. Strategies to address challenges in assessing ML/TF risks

5.1. Disconnect from, or misalignments with, the NRA

119. National Risk Assessments (NRAs) are intended to inform the national AML/CFT policy and strategies and implementation of a risk-based approach to both AML/CFT regulation and supervision. They provide a point in time view of the risks of ML/TF that the country is exposed to. NRAs should be regularly reviewed and kept up to date. If the ML/TF risks at national or sectoral level are not assessed comprehensively, or there is a disconnect or misalignment between the NRA findings and the AML/CFT supervision framework, AML/CFT supervision cannot be effectively risk-based. For example, while working on the design and development of risk-based AML/CFT supervisory frameworks, some jurisdictions have noticed gaps and deficiencies in their NRAs, as the NRAs did not comprehensively identify all the ML/TF risks or provide the necessary insights and information on the risks. This has led these jurisdictions to revisit their NRAs and supplement them with additional analysis, particularly on sectoral risks. Another example of possible issues in NRAs is the lack of information on medium-risk and low-risk areas/sectors, and ML/TF risks in the DNFBP sectors, which are also essential for effective risk-based approach to AML/CFT supervision. The NRA and the SRA do not have align perfectly in terms of risk scoring etc., but there should be a general coherence between the findings of both assessments.

120. Strategies to address this challenge:

- Supervisory authorities should participate in the NRA process and share and discuss their understanding of sectoral risks with other stakeholders. The NRA report and findings should be accessible to supervisory authorities and should be taken into account in the development of supervision strategies. If the NRA is not complete or comprehensive enough to inform the risk-based supervision framework, it should be reviewed and improved.
- Authorities should ensure ongoing communication among supervisors on the NRA to ensure identified risks remain current and to understand emerging risks that need to be reflected in NRA updates.

5.2. New areas of supervisory responsibility – identifying the regulatory population

121. If a supervisor's authority is extended to include a sector not previously supervised for AML/CFT purposes, a first step is to identify the regulatory population and begin to understand the risk environment. This is particularly important, as it underpins a number of decisions, including what resources, skills and experience are needed to effectively supervise the sector. This task is often more straightforward if the authority is being extended to cover activities carried out by entities that are already regulated for other purposes (the challenge may be to track down and share this information among authorities). Identifying the population is more challenging when it involves entities that are not already supervised for another purpose (e.g. VASPs in most jurisdictions). For example, it can be difficult to accurately predict the size of the population before the registration/licensing process begins. In one jurisdiction that was early to introduce AML/CTF regulations for VASPs, the supervisor estimated that approximately 50 VASPs would register as obliged entities. However, when the regime came into force, the actual number of registrations received was around 350. The challenge can be more acute where there are no trade associations or industry bodies and there are numerous smaller operators. Additional challenges occur when entities are physically based outside the jurisdiction but are able to operate within them (e.g. online casinos or VASPs).

122. Even when it is not a new area of responsibility, there may be fluctuations and changes in the regulatory population or failures to fully identify the regulatory population. For example, in the UK, the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) found at the end of its first year in operation, 18% of relevant DNFBP supervisors had not fully identified their supervised population. Following a series of workshops in June 2019, by the end of that year, this had been rectified.

123. Strategies to address this challenge:

- A number of other domestic and international authorities or organisations may hold relevant information. For example, revenue and tax agencies, corporate registries and trade or professional associations. Already supervised entities may also provide a source of information (e.g., banks will hold information on activities of customers).
- Open source information (e.g., web searches or industry contact directories) may also be of assistance in this regard. Outreach actions and workshops may also assist the supervisor not only in understanding the risk environment but also in identifying the regulatory population (e.g., outreach actions towards representative bodies of DNFBP or VASP sectors).
- Supervisors should continue to identify and verify their regulated population on a periodic basis to capture fluctuations and reassess supervision strategies and resources required to deliver them. Where point-of-consumption regulation applies, supervisors should establish communication channels with jurisdictions that have a concentration of entities located, but not operating within them (e.g., jurisdictions that host a large number of online casinos that ae mainly used by customers in other jurisdictions).
- See VASP sector examples at section 9.1.

5.3. New areas of supervisory responsibility – identifying and understanding the risks

124. Where supervisors' mandates have been expanded to include new activities not previously subject to AML/CFT supervision, supervisors may not have a good understanding of the risks in the sector or the strength of mitigation measures and need to consider how best to integrate entities engaging in such activities into their risk models.

125. Strategies to address this challenge:

- As a starting point, supervisors should focus on the potential level of ML/TF risk in the sector (i.e., inherent risks). Supervisory authorities should seek to build an initial understanding of the inherent risk that these new activities could present and seek to supplement this knowledge through engagement with law enforcement authorities, other supervisory authorities which are already supervising and licencing/registering such entities and through engagement with the entities themselves (for example, through issuing a ML/TF questionnaire, engaging in meetings with the sector or with specific entities as part of registration or licensing processes).[30] To ensure that this process does not result in diverting resources from existing higher risk sectors, additional resources may be required or sought. These resource considerations should be part of planning and rolling out regulation to new sectors. Supervisors can also learn from other jurisdictions that are already supervising the activities (i.e. where regulation has been introduced by their international counterparts).
- Putting in place a dynamic risk assessment process which is kept under review and duly updated as the understanding of the sector develops (including appropriate re-rating of sectors and entities), can help ensure resources are targeted at the highest risk areas. See guidance on updating risk assessments at section 2.4, including incorporate findings from supervision work and feeding in other sources of information.
- In some cases, existing information from regulated entities can help supervisors obtain information on newly regulated entities.
- Where a significant number of entities are entering a market or seeking licencing or registration at the same time (e.g., VASPs), it may be useful for supervisors to ensure that sufficient flexibility is built into their approach, to allow for prioritisation of incoming requests. This could involve identifying and prioritising entities carrying out the highest risk activities for early registration, monitoring key risk indicators, or increased emphasis on ad-hoc onsite and off-site reviews, and engaging regularly with industry bodies.

5.4. Difficulties in assessing risks at the entity-level

126. In certain situations, an entity may not have developed a risk assessment, or the risk assessment that was developed may be overly broad and does not provide sufficient granularity or analysis.

30 Cooperating licensing and registering authorities can help develop an understanding the ML/TF risks at an entity level. Any exchange of information would be need to have a legal basis and/or memoranda of understanding to facilitate this exchange.

127. Some sectors have a large number of (mostly smaller) active institutions and it is difficult to develop comprehensive risk profiles for each individual entity. In the case of newly established institutions or recently regulated sectors, there may not be in depth knowledge about the risks presented by those individual entities' business models and activities, and the results from the supervisory authority's own audits or other supervisory activities are not yet available.

128. Strategies to address this challenge:

- Undertake sectoral risk assessments as a first step. The sectoral risk analysis primarily provides a good overview of the risks to which an institution is exposed as a result of its business activities in this sector, and therefore important insights can be gained for the risk profile of the individual institution. It also makes it possible to provisionally apply the sectoral risk rating as a default rating to newly established or recently regulated institutions.
- Depending on the specificities of the regulatory population, develop clusters of entities that share common characteristics, where the risks of ML/TF affecting the entities in the cluster are very similar.
- Encourage the supervised entities to leverage the sectoral risk assessment created by supervisors as a starting point or model to develop their own risk assessment over time. Supervisors could also consider making application to register conditional upon preparation of a risk assessment (reviewed at time of application).
- The larger, more comprehensive and higher risk the business activities of an entity are, the greater degree of granularity in the assessment of risks should be carried out when developing a risk profile. On the other hand, this means that, for small entities with very limited business activities, risk profiles can be developed based on the sector analysis combined with the entity's key financial figures (e.g. turnover, transaction volume, cross-border transaction of the business volume).
- To improve entities' risk assessments, identify themes and common shortcomings that may be addressed through guidance and feedback. Ensure a number of channels are used to disseminate the outcomes of the NRA or supervisory risk assessments. E.g. Jersey recently produced a video explaining the key ML/TF risks entities in the jurisdiction are subject to. Other jurisdictions have produced summarised information to provide a snapshot of risks, etc.
- Provide clear guidance to entities for their institutional risk assessments. Consider developing ready to use templates that will guide them in their institutional risk assessments. If the entities do not have the analytical capacity, these templates may target to collect low risk information (i.e. the volume of certain products or services, number of non-resident clients) which can be the basis for the risk assessment by the supervisory authority.

5.5. Building risk understanding over time

129. Developing a supervisory risk assessment methodology for the first time, or updating the methodology, to provide more nuanced risk assessment, can be a daunting task.

130. Strategies to address this challenge:

- Supervisory authorities should seek to build an initial understanding of the inherent risk in the sectors they supervise and the national context from the NRA, sector experts and engagement with other relevant authorities. This will ensure that the risk factors assessed are adapted for ML/TF purposes.
- Supervisors should seek to identify and use quantitative and qualitative data when starting or updating a risk assessment. Ideally, risk assessments should be performed with a set of up-to-date, accurate, relevant and consistent data. This data can be obtained through a questionnaire or data return from entities which can include information such as data on ML/TF alerts, STR activity, staff training (among other quantitative data), as well as information on the financial and economic activity of the entity.
- Supervisory authorities' risk understanding will develop overtime through the experience and knowledge gained from carrying out supervisory work, engagement with law enforcement and other supervisory authorities, and from regular participation at domestic and international AML/CFT operational and policy fora. This enhanced understanding should be incorporated into supervisory authorities' risk assessments and supervisory authorities should have processes in place to ensure that risk assessments are subject to regular review and update. Supervisory authorities' processes should seek to undertake risk assessments at the individual entity level when applying supervisory tools and these individual risk assessments should feed into the sectoral risk assessments.
- Supervisory authorities should seek to enhance and strengthen their models for risk understanding by supplementing the qualitative approach to risk understanding with quantitative information. Supervisory authorities that are applying supervisory tools as part of their supervision models through which they are routinely collecting data from supervised entities or that have access to data from other sources, should ensure that relevant data is integrated into the risk assessment process. Supervisors should also consider adapting the data requested via questionnaires or data returns to address the latest risks. See case study 7.1.2.
- While developing a risk assessments methodology, supervisors should opt for the models that provide results at various levels (e.g., at individual risk category for one or across multiple entities, provide consolidated views, trends year-over-year, etc.). The methodology should allow supervisors to form a view on the levels of risks across the entities of similar size and operations, or within the same sector. Supervisors should be able to obtain from entities or generate reports on changes in the risks and quality of controls from one risk assessment period to another.
- As the risk model becomes more sophisticated it may be adapted to provide greater distinction of the relative risks of entities within and across sectors

(e.g. more specific risk rating categories may be added). Supervisors should review periodically their risk rating approach to assess whether it remains adequate and proportionate to the regulatory population.

- The methodology and results of the supervisors' risk assessment should be well supported with a clear rationale and understanding of how risks are identified and weighted. These should regularly be revisited in accordance with the changes in the risk environment.

5.6. Engagement with other authorities to supplement the risk assessment

131. Other authorities hold important information that should inform supervisory risk assessments. For example, regulated entities report suspicious activities to FIUs that are further investigated by other authorities and supervisors need to obtain feedback on this reporting and on typologies to better understand the risks facing the entities they supervise. In the same vein, prudential authorities or other foreign authorities can be aware of new activities in a regulated entity that supervisors are not aware of, which can give rise to new AML/CFT risks.

132. Strategies to address this challenge:

- Supervisors should diversify the sources of inputs of their risk assessments by engaging with other stakeholders, especially other AML/CFT or prudential supervisors, the FIU, law enforcement agencies, and relevant foreign authorities. Some ways to facilitate this are secondments and liaison officers for pertinent relationships and joint meetings or guidance for regulated entities. In some jurisdictions, the FIU provides regular reports on the quality and quantity of STR filings by regulated entities and/or specific warnings that highlight deficiencies or weaknesses identified in some regulated entities' internal control systems. See section 3.9 and case studies at 7.5.
- Building strong co-operation with the prudential authorities or other authorities regulating the sectors being supervised. Where the same authority is responsible for supervising both ML/TF and prudential risk of FIs, there can be significant synergies for the ML/TF supervision but information sharing and co-operation continue to be critical as in cases where these functions are performed by different agencies. Synergies can be found in terms of understanding FIs' business models, internal governance arrangements and internal control system weaknesses.
- Building strong co-operation with foreign authorities: this can be achieved through informal and proactive exchanges of information, establishing international supervisory colleges and official channels for communication, participating in supervisors' forums and having regular meetings with other authorities. See section 3.10 for further detail.
- Co-operating across public/private partnerships: For example, the UK has published its Economic Crime Plan, which sets out the actions being taken by the public and private sectors to ensure that the UK cannot be abused for economic crime. Inputs and outputs on the plan are being considered at ministerial as well as working level, to ensure the right risks are identified, shared and mitigated across the financial service and DNFBP sectors.

5.7. Data collection issues

133. Data collection is an important way for supervisors to identify and monitor risks, but it can be time consuming and burdensome for entities and supervisors when it is done inefficiently. Entities may have difficulties collecting data required by supervisors or providing data where their systems are not compatible with that of the supervisor. Supervisors may also face challenges in handling and processing data, particularly large-scale data sets. Some of the common data collection challenges include:

    - a lack of relevant historical quantitative data or the data requested is not retained by the entity in the form requested by the supervisor
    - lack of information in digital format or held in multiple databases
    - high volume of information
    - inconsistent definitions may affect the quality of the data collected and there may be compatibility issues among the data from different institutions
    - information requires data cleaning before using, and
    - cost of collection, validation, storage, processing and dissemination.

134. When developing or revising data collection from regulated entities there are several challenges that can arise. For example, entities may not understand the requirements or interpret them differently creating consistency and comparability issues and ultimately leading to inaccurate outcomes because of the data quality issues. Although supervisors are increasingly using technology and need to feed their automatic tools with data, they should also consider that any request of a new set of data may require the supervised entities to adapt their information system to be able to report adequate and reliable data, so advance notice is needed.

135. Strategies to address this challenge:

    - Effective co-ordination and information sharing within the supervisory agency to ensure information already collected by a department is not requested by another. For example, in the UK the FCA has an Information Governance Board to ensure that uniform requests for data are justified by meeting certain criteria, including that the data has not already been collected. It is also prudent to consult with other relevant authorities, such as the FIU that may also seek or hold relevant data from regulated entities.
    - Regulated entities should be consulted early in the development of data collection tools. In France, there is a consultation phase with FIs before issuing the yearly ML/TF questionnaire. Presenting the new questions and the rationale for any changes of the questionnaire (i.e. quantitative and qualitative data) is an opportunity to present the priorities if the changes result from an increasing attention to a specific risk. It helps supervised entities understand the purpose of any new or amended question and to answer it accurately and specifically. It also gives an opportunity for regulated entities to raise any difficulties they may face in answering the questionnaire (difficulty in implementing new regulations, availability of data requested that may need IT developments, etc.). This prior consultation facilitates the collection of better data.

- Increase the type of information requested gradually, starting with information already collected and moving towards information not collected, thereby giving entities the time to start collecting data. Automated data collection should also be considered. Carefully assess which data is required at a minimum to make an informed assessment of ML/TF risk, bearing in mind that more information does not necessarily translate into a better risk assessment. Give sufficient prior notice to the regulatory population to adapt its information system and to ensure the quality and reliability of the reported data and provide adequate time for entities to adapt to the new or revised requirements.
- For significant providers of data, supervisors may liaise with the entities' technology providers so they can build in back-end/output supervisory requirements to front end/input data collection portals.
- For sectors involving fast-paced changes in technology and or changes in the market environment (e.g., the VASP sector), authorities could engage with industry bodies or self-regulating bodies to understand the technology and adapt its data collection accordingly.

5.8. Special considerations for DNFBP supervisors

136. Some sectors, in particular DNFBPs, have a very large number of entities such that understanding ML/TF risks of each entity is difficult as supervisors may have no or little data on individual entity activities. In addition, the range of sizes of entities (from sole traders up to groups operating internationally) and the diversity of activities undertaken by DNFBPs often makes understanding and assessing ML/TF risks across all sub-sectors challenging, in the absence of highly specialised resources (supervisors) who are knowledgeable and experienced in the specific activities carried out by all types of DNFBPs.

137. On a more practical level, data collection from DNFBP sub-sectors may be difficult due to:

- the sub-sectors having little or no capacity to generate or produce the type of comprehensive and reliable data required by supervisors to asses risk, due to a lack of understanding by the entities
- a lack of legal authority to collect data (particularly in the case of self-regulating bodies (SRBs))
- challenges in identifying reporting entities or determining whether a person/company is a reporting entity, especially in those sectors that are not directly regulated or licensed by any licensing authorities or self-regulating bodies (SRBs), and
- the absence of compliance data on individual entities (e.g. in lower risk sectors, or newly regulated subsectors with no history of supervision or regulatory relationship); meaning that assessing the effectiveness of control frameworks and hence residual risk in some DNFBPs is a particular challenge.

138. Strategies to address these challenges:

- Supervisors of these sectors may seek to identify sub-sectors or market segments or clusters within the sector and understand their respective

features or characteristics so that risk profiles can be established at the sub-sectorial or segment level.

- Supervisors may develop simplified risk assessment templates for less complex entities with lower risk profiles for ML/TF and other illicit financial activity. Such templates may collect the information from institutions on their business and transactions, products and services, client profiles etc. Supervisors can form a broad judgement about the risks based on this data.
- In addition, supervisors may coordinate and liaise with licensing bodies and sectoral associations to obtain information on the entities in the sector, subject to a legal basis to share information between the supervisor and these bodies. Licensing bodies and sectoral associations could help to identify entities for supervisory focus based on criteria developed by the supervisor.
- Supervisors may introduce and strictly enforce obligations to submit risk and activity information (e.g., an annual report or similar). These obligations need to be augmented by provisions in law together with sanctions for non-submission.
- For sectors with little data available, supervisors may initially implement a relatively simple risk-based supervisory strategy (e.g., driven by broad indicators of inherent risk). More complexity may be incorporated into the approach as better data becomes available and supervisory engagement increases, allowing an effective consideration of control frameworks and residual risk. Also see sections 5.4 and 6.3.
- Supervisors may undertake on-sites of a random sample of sectors where there are data gaps (e.g. lower risk subsectors that are not subject to regular inspection cycles). These may be used not only to assess control frameworks but also to confirm a supervisor's risk understanding of that sector and/or confirm the validity of risk information provided.

5.9. Other guidance

- Supervisors should have skilled and trusted personnel who can assess and understand risks, including recruitment through fit and proper tests or integrity testing as appropriate. This also requires these authorities maintain high professional standards to ensure that individuals have the necessary skills and expertise to carry out this work, which should be commensurate with the complexity of the entity's operations and risk profile and comply with integrity standards.
- Consider a balance between having staff specialised in particular sectors or entities for a number of years to build up knowledge/experience and building in rotation or other safeguards to ensure objectivity and sharing of expertise within supervisory teams. Secondments from industry are also a good way of complementing knowledge and experience.

6. Applying risk-based supervision

6.1. Sequencing to establish risk-based supervision

139. Where there are new supervisory responsibilities or AML/CFT supervision is applied to new sectors, it may be difficult to achieve a fully effective risk-based supervision over the short term.

140. Strategies to address this challenge:

- Consider building into the supervisory strategy a step-by-step approach to risk-based supervision. For example, below is the process followed by the Anti-Money Laundering Compliance Unit in the Irish Department of Justice which supervisors several DNFBP sectors.

Box 6.1. Step-by-step approach to establishing risk-based supervision

- Develop legal framework and define scope of the regime (e.g. what activities or types of entities will be regulated). Think about powers needed for the specific sector based on the risks it presents. For example: specific powers to enter premises, remove files etc.
- Establish a preliminary understanding of the sector, including identifying an estimate of the entities in scope, the size of their operations, etc.
- Establish supervisory authority and staff (think about needs, e.g., knowledge and skills gaps, additional technology, etc.)
- Programme of staff training (Who should deliver it? Who should you involve? What training is available?)
- Develop inspection procedures around obligations in legislation, international best practice (e.g. FATF/EU)
- Think about frequency (e.g. more often for high risk) and focus (e.g. particular cohort challenges) of inspections
- Learn about your cohorts – identify inherent risks by understanding the specific threats and vulnerabilities in each sector. Review any existing information (e.g., national risk assessments or assessments by other authorities) or international documentation on sector and risks it faces e.g. FATF, EU etc. (see section on risk assessment) and identify missing information.
- Think about the balance between off-site reviews and. onsite inspections. Sometimes it is difficult to establish residual risks in certain cohorts without an on-site visit.
- Identify residual risks after applying AML/CFT measures.
- Undertake outreach with sector before commencing inspections e.g. information booklets, templates etc.
- Think about undertaking capacity-building inspections for both the entity and the supervisor.

- Share information within the AML supervisor. For example, internal team meetings every fortnight to share findings, discuss issues arising, FATF/EU guidance, trends, media, strategies for improvements etc.

Source: Department of Justice, Ireland
Note: In reality, many of these steps may happen in a different order or in tandem.

6.2. Insufficient resources or inexperienced staff

141. There may be a lack of, or inadequately trained staff, to conduct a proper risk-based supervision. Teams conducting AML/CFT supervision may be new or covering new sectors or AML/CFT responsibilities newly assigned to existing regulators. There may be a lack of supervisory tools and technologies.

142. Strategies to address this challenge:

- Allocate the limited supervisory resources based on sector's/entities' risks in an effective manner. In allocating resources, based on the outcome-focused approach (See Section 3.4), supervisors should focus not only on the headcount but also the capability and training of the AML/CFT staff.
- Ensure that there is requisite senior management support and buy in within the supervisory body. Use the results of the risk assessment to secure additional resources by demonstrating the risks that remain unmitigated. For those who are part of a larger agency, consider designating specific resources for AML/CFT to build expertise and support other supervisory staff. If staff lack AML/CFT expertise, or expertise in relation to a particular sector, develop strategies to build capacity and consider appropriate use of other experts. Consider seconding staff from more experienced AML/CFT supervisory authorities to transfer knowledge and expertise. Consider appropriate use of third parties or consultants as an interim measure (see section 4.3 for more detail).
- When designing the supervisory approach and determining the target operating model, conduct a detailed training needs analysis and allocate resources for training. Where a supervisor is taking on supervision responsibilities for a newly regulated sector, it is unlikely that they will have existing staff with both the technical knowledge of the sector and experience in carrying out risk based supervision. It is also unlikely that they will be able to easily recruit individuals to meet this need. Providing tailored training and forming teams with a mix of skilled supervisors and technical experts is an approach to addressing this issue.
- Provide AML/CFT training courses or learning opportunities to AML/CFT supervisors and adequate provision of budget and staff time for learning and development, along with exploring opportunities to gain insight into best practice from more established AML/CFT supervisors. This may include, for example: a resource centre that has job aids, templates, and other tools that can assist less experienced staff in a time of immediate need; access to financial crime training courses or online or pre-recorded training material that staff can access and participation in international or regional training or experience exchange with supervisors in other jurisdictions.

6.3. Supervising sectors with a large number of entities and limited risk information

143. Strategies to address this challenge:

- See the advice in the section above on strengthening the risk assessment. If adequate information is available, using risk rating scales that include more risk ratings (e.g., high, medium high, medium, medium low, and low) ratings may help provide greater distinction of the relative risks of entities within and across sectors with a large number of entities than a lower number of ratings in a scale, for example a three-risk rating scale. With greater distinction, supervisors can further tailor their supervisory approach.
- Identify key players in the sector, for example those that make up a large percentage of market share or those that belong to a sub-sector presenting higher risks. It may also be possible to engage with entities providing AML/CFT compliance services for a large number of entities in a sector e.g. outsourcing of transaction monitoring or CDD. It may be possible to use economies of scale by leveraging off an inspection to one entity by making some assumptions about other entities using the same service provider, subject to any particularities/refinements adopted by individual entities and any differences in the use of the product or service.
- Identified sub-sectors or clusters of entities can be grouped together by similar, factual inherent risk characteristics such as services offered in a specific location, for example, conveyancing in London. Supervisors can supervise these sub-sectors by picking entities using criteria under a risk-based sampling methodology for further attention via on-site or off-site supervision. Where the outcomes of these assessments are significantly varied, the sub-sector may not be specific enough and not appropriate to be clustered together for supervision purposes.[31] Where the outcomes are similar, trends can be identified and supervisory strategies can target the entire sub-sector. This allows supervisors to effectively target resource in the most appropriate way.
- Identifying and engaging with AML/CFT compliance officers in these entities to increase awareness of risks and regulatory requirements.
- Ensure communications and guidance are used to set expectations and provide feedback on good and poor practices. This can be achieved through a number of channels including, industry outreach, publishing the outcomes of thematic reviews and detailing specific failings in enforcement notices. This enables businesses that may receive less direct supervisory engagement to conduct gap analysis on their systems and controls to ensure they align with good practice.

6.4. Poor independent audits of entities

144. Many supervisors of financial institutions make use of FI's internal and external audits as an important source of information on FI's AML/CFT controls (many smaller DNFBPs do not have internal audit functions). Independent audits with an inadequate scope or of poor quality may present a challenge for the supervisor. In

31 The effectiveness of mitigations and controls may lead to greater diversity in end risk ratings despite the inherent risk being consistent and may help supervisors further distinguish between entities.

some systems, supervisors may rely heavily on audit information regarding the entity's specific risks, to understand how these risks are being managed and controlled, and the status of the compliance program. Therefore, if the entity's independent audit is inadequate, those independent audit findings cannot be leveraged to tailor the review areas covered by the supervisory authority and to allocate the resources necessary to assess the entity's compliance program. Moreover, poor independent audit report(s) and supporting paper work can hinder supervisors in understanding audit coverage and the quality and quantity of transaction testing that was performed as part of the independent audit. Without this knowledge, supervisors may be limited in their ability to risk-focus and identify areas for greater (or lesser) review.

145. Strategies to address this challenge:

- To prevent this issue, supervisory authorities should assess whether the entities have processes in place to ensure the audit scope and depth is appropriate and that audits are performed by competent, qualified and reputable independent auditors and take steps to satisfy themselves that the audits performed are of sufficient quality, for example by carrying out sample checks. Moreover, supervisors should confirm that the financial institution or DNFBP's independent audit plan assesses the effectiveness of AML/CFT controls across and within the entity or group's operations.
- Cross-compare findings from supervision activities and independent audit to help detect the deficiencies in independent audit and auditors.

6.5. Special considerations for DNFBP supervisors

146. Challenges in data collection and assessment of risk are detailed in section 1.9 above, while further challenges to risk-based supervision of DNFBPs include:

- Difficulties in ensuring an adequate level of DNFBP supervision (where risk models/Supervisory programmes usually focus on larger FIs like banks). This is discussed in the context of monitoring in Part A, but is particularly relevant to DNFBP supervision in a single supervisor.
- Notably, in order to achieve "statistical significance", a meaningful number of supervisory engagements (whether on-site or off-site) need to be carried out relative to the population size. In the case of DNFBP sectors with large populations, achieving statistical significance may not be attainable. In these cases a supervisor could instead focus on a sub-group or selection of entities within the population that presents the highest risk.
- Difficulties in ensuring supervisors are specialists and/or sufficiently trained, experienced and knowledgeable in relation to the widely diverse activities carried out by supervised entities.
- DNFBP supervisors, in particular self-regulatory bodies, may not have full legal authority to carry out supervision on all entities within the sector.

147. Strategies to address these challenges:

- Intensive outreach and engagement with and via sectoral associations (which may not be necessarily the self-regulatory bodies), including the provision of specific DNFBP sectoral typologies.

- Comprehensive training for supervisors on the business models and activities of the various DNFBP sub-sectors.
- Ensuring that random, reactive and event-driven supervisory activity provides sufficient coverage across DNFBP subsectors which are not subject to cyclical on-site programmes.
- Defining a strategy which is adapted to the sector and degree of risk presented by entities.
- As set out at section 5.8 above, supervisors may initially implement a relatively simple risk-based supervisory strategy (e.g., driven by broad indicators of inherent risk in a subsector). More complexity may be incorporated into the approach as better data becomes available and supervisory engagement increases, allowing an effective consideration of control frameworks and residual risk in individual entities.

6.6. Role of self-regulatory bodies for DNFPBs

148. According to the FATF Standards, a jurisdiction may decide to assign all or some of supervisory tasks and responsibilities to self-regulatory bodies (SRBs) of DNFBPs (except for casinos). However, this arrangement needs to consider the jurisdictional context and may not be optimal for all jurisdictions. In general, SRBs may lack the power and the tools of government supervisory agencies, particularly the sanctioning power. There may be conflict of interest and independence related issues for some SRBs (particularly where SRBs are dependent upon membership fee income). In addition, many SRBs have serious human resources and other capacity constraints, or are not adequately focused on, or adequately trained/experienced in relation to, AML/CFT issues.

149. Strategies to address this challenge:

- The designation of the appropriate AML/CFT supervisory authorities should carefully analyse these factors before deciding the possible role of the SRBs in supervision accordingly. Based on this analysis, a jurisdiction may decide that the role of the SRBs can be more complementary in nature, for example, contributing to implementing market entry controls, awareness raising, training, and guidance.
- If an SRB is chosen as a supervisor laws and regulations need to be drafted/amended to ensure that they have the necessary powers and tools. The laws and regulations should also ensure the conflict of interest situations are dealt with.
- There should be some level of oversight/supervision by a competent authority over the AML/CFT work of SRBs. In the UK, OPBAS was set up as a supervisor of SRBs designated as DNFBP supervisors under the Money Laundering Regulations to ensure there is a consistent approach to AML/CFT supervision across the relevant DNFBP sectors and to assess whether they are effectively meeting their obligations set out in legislation. While further improvements in the effectiveness of AML/CFT supervision remain, there has been significant progress made. OPBAS continues to deliver its second phase of supervisory work and expects to publish its third report in 2021.

6.7. Lack of clarity in the division of supervisory roles and responsibilities

150. In many jurisdictions, there is a lack of clarity in the division of the labour and responsibilities between AML/CFT supervisory authorities, particularly between the FIU and the other supervisors but also between prudential and AML/CFT supervisors or AML/CFT supervisors that are responsible for the AML/CFT supervision of different aspects of the same entity's activities. In those cases, it is not always clear which agency has the primary role and responsibility for AML/CFT supervision.

151. Strategies to address this challenge:

- Ideally, the law should clearly identify which agency has the primary responsibility of AML/CFT supervision of a sector. To this end, any ambiguities in the laws should be addressed, and the overlaps and conflicts between AML/CFT laws and sectoral supervision laws should be examined and eliminated, as necessary. In addition, as appropriate, memoranda of understandings can help define the respective roles the authorities and the principles for collaboration and information sharing among them. Such arrangements and clear division of AML/CFT supervision roles and responsibilities becomes particularly essential when a multinational authority and/or a federal authority have AML/CFT supervisory responsibilities over domestic or local entities.
- Set up mechanisms to ensure co-operation and a consistent approach between those agencies and ensure that information flows freely and in a timely manner.

6.8. Zero-tolerance or zero-failure approach

152. A zero-tolerance approach that does not tolerate imperfections, particularly in areas identified to pose lower risks, is counterproductive to an effective AML/CFT system and for risk-based supervision. This is valid both at the supervisory agency and in terms of an entity's approach to meeting its requirements. In certain cases, it may be difficult to develop institutional support for taking a risk-based approach due to fears of missing compliance failures in areas deemed as lower risk. It also requires deep knowledge of sectors and providers, critical thinking and subjective judgment by supervisors. As set out in section 3.7, there may be valid reasons for supervisors to take remedial or other action across the risk spectrum if, for example, the failure is due to repeated, knowing or wilful non-compliance with AML/CFT requirements. At the entity level, a zero tolerance approach could lead to indiscriminate cutting loose of entire classes of customer, without taking into account, seriously and comprehensively, their level of risk and risk mitigation measures for individual customers within a particular sector.

153. Strategies to address this challenge:

- Especially in the introductory stages of the implementation of a risk-based approach to AML/CFT, supervisors should explain the approach to their regulatory population and clearly explain and provide guidance on how it should be applied. In justifying their approach internally, supervisors should seek high-level support for their supervisory strategies by explaining its rationale and be able to demonstrate the benefits of this approach.

- The development and senior management sign-off of supervisory risk statements and frameworks would also be an appropriate strategy.
- Supervisors should introduce the RBA gradually, and give greater flexibility to the sector as their expertise and risk assessment capability increases.
- Supervisors should make clear that it is inappropriate to indiscriminately terminate or restrict business relationships of entire classes of customer, without taking into account, seriously and comprehensively, their level of risk and risk mitigation measures for individual customers within a particular sector.

6.9. Integrated vs. Standalone AML/CFT Supervision

154. While some supervision agencies have dedicated AML/CFT supervision programs and teams, some others conduct their AML/CFT supervision as an (integrated) part of general or prudential supervision program. Both approaches may have pros and cons. For example, in an integrated supervision framework, on-site inspection plans may depend heavily on prudential risks leaving prudentially sound entities with higher ML/TF risks out of the inspection plan, which is not in line with the RBA to supervision. On the other hand, when AML/CFT supervision is conducted on a standalone basis, co-ordination and collaboration with the prudential supervisors and other aspects of supervision is often challenging.

155. Strategies to address this challenge:

- When choosing one of these approaches or a combination of both, authorities should carefully consider these advantages and disadvantages. See the diagram below and please refer to Basel Committee's guidance on co-ordination between AML/CFT supervision and prudential supervision for further guidance on this topic.

Table 6.1. World Bank comparison of integrated and stand-alone inspections

	by GENERAL OR PRUDENTIAL SUPERVISOR	by SPECIALISED AML/CFT SUPERVISOR
INTEGRATED AML/CFT INSPECTION	**All supervisors are or can be involved in AML/CFT inspections as an extension of the prudential inspections.** **Pros:** All supervisors gain AML/CFT experience and are involved in AML/CFT agenda. Co-ordination between prudential and AML/CFT inspections will be smoother. **Cons:** Prudential risks will determine the inspection plan. AML/CFT risks may not be always parallel to the prudential risks. Supervisors may tend to see the AML/CFT as a secondary issue compared to prudential risks. Specialisation in and the depth of AML/CFT inspections may remain limited.	**A specialised AML/CFT supervisor joins the team during the prudential inspection and conducts the AML/CFT inspection.** **Pros:** A group of experts will excel in AML/CFT, leading to deeper, and higher quality AML/CFT inspection. Co-ordination between prudential and AML/CFT inspections will be smoother. **Cons:** Prudential risks will determine the inspection plan. AML/CFT risks may not be always parallel to prudential risks.
STAND-ALONE AML/CFT INSPECTION	**Standalone AML/CFT inspections conducted by general or prudential supervisors. (Possible but not common).** **Pros:** All supervisors gain AML/CFT experience and involved in AML/CFT agenda.	**AML/CFT inspections done by specialised supervisor, independently from prudential inspections.** **Pros:** A group of experts will excel in AML/CFT, leading to deeper, and higher quality AML/CFT inspections.

	There will be a separate AML/CFT inspection plan that is independent from prudential side, allowing better alignment of AML/CFT supervision to ML/TF risks. **Cons:** Specialisation in and the depth of AML/CFT inspections may remain limited. Co-ordination between prudential and AML/CFT inspections may require more effort.	There will be a separate AML/CFT inspection plan that is independent from prudential side, allowing better alignment of AML/CFT supervision to ML/TF risks. **Cons:** Co-ordination between prudential and AML/CFT inspections may require more effort.

Note: *Integrated with prudential supervision. AML/CFT inspection is conducted as a sub-component of prudential supervision plan and activities.
Source: World Bank

- Standalone AML/CFT supervision teams should seek input from other supervision areas in formulating a sector risk assessment and in terms of identifying specific risks and areas of focus for the assessment of particular entities. For example, AML/CFT supervision teams may want to understand if there are any concerns from a cyber-security or client assets perspective when considering AML/CFT risks, as these concerns may indicate a vulnerability for exploitation by financial criminals. The AML supervision teams should also ensure supervisory findings, either derived from offsite or onsite activities, are shared with the prudential supervisors as major AML/CFT issues may lead to or indicate critical prudential concerns.
- Although prudential and conduct risk may inform supervisors' understanding of ML/TF risks, AML/CFT supervision should be driven by ML/TF risks rather than prudential or conduct risks.
- For those jurisdictions with dedicated AML/CFT supervision teams, supervisory resources may be categorised as teams/supervisors/responsibilities for 1) high risk supervision 2) medium risk supervision 3) low risk supervision 4) responsive supervision 5) risk analysis, data collection, horizon scanning, or the split may be divided by the type of supervisory intervention (e.g., on-site and off-site). The appropriate sub-categorisations used by the supervisory authority will depend on the size, characteristics and risks presented by the supervisory population.

6.10. Risk-based supervision strategies should be up-to-date and dynamic

156. Through the advances in finance and technology today, the risks can change faster than before. Outdated assessments can undermine risk-based supervision. As set out in section 2.4, it is important to keep risk assessments under review and updated so that resources can be targeted to the highest risk areas.

157. Strategies to address this challenge:

- Supervisory authorities should also be fast and agile in understanding the risks and, if possible, take the advantage of SupTech in monitoring the risks in real time/on a continuous basis. They also need to have the flexibility to adapt their supervision approach and plans to promptly address the emerging ML/TF risks. See the section on 'use of technology'.

6.11. Logistical challenges in performing on-site inspections

158. In jurisdictions that allow businesses located outside the country to operate within their regulatory perimeter (for example, provision of services online), or certain functions of an entity are located in different locations (e.g. where an organisation operates as a group), on-site inspections are challenging and resource intensive. External factors (current global pandemic) can also make it difficult for on-site inspections to go ahead.

159. Strategies to address this challenge:

- Utilise tools such as video-conferencing to simulate the types of testing that would occur at an on-site inspection, ensuring adequate vigour and spontaneity. For example, the UK Gambling Commission supervisors online casinos that offer services in the UK and it has used various tools to undertake effective supervision including: Microsoft Teams assessments over a number of days with key individuals and the ability to view real time data and interrogation of their systems. Prior to the Microsoft Teams assessment, materials are requested and reviewed (including, the entity's risk assessment, policies, procedures and controls) and the initial findings assist to steer the assessment and it is only during the live assessment that we usually specifically advise operators which customer accounts will be assessed. Additionally, the Gambling Commission requires annual assurance statements from highest impact operators that cover around 90% of the market and asks entities to complete 'calls for information'.

6.12. Useful resources for further reading

On supervision

- FATF Guidance on Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement (October 2015)
- World Bank Practical Guide for Bank Supervisors on Preventing Money Laundering and Terrorist Financing (2009, new edition expected in 2021)
- Basel Committee on Banking Supervision *Guidelines on Sound Management of risks related to money laundering and terrorist financing* (revised in July 2020)
- Financial Stability Institute, *Closing the loop: AML/CFT supervision of correspondent banking* (September 2020)
- Joint Forum Principles for the Supervision of financial conglomerates Core Principles (BSBC, IOSCO and IAIS)
- European Supervisory Authorities Joint Guidelines on Risk-based supervision (November 2016), under revision
- United States Supervisory Authorities Joint Statement on Risk Focused AML/CFT Supervision (July 2019)[32]

[32] US Statement on risk-focused AML/CFT supervision published by U.S. Federal Banking Regulators and Financial Intelligence Unit www.federalreserve.gov/supervisionreg/srletters/sr1911.htm; www.fdic.gov/news/press-releases/2019/pr19065a.pdf; www.occ.gov/news-issuances/news-releases/2019/nr-ia-2019-81a.pdf; www.fincen.gov/news/news-releases/joint-statement-risk-focused-bank-secrecy-actanti-money-laundering-supervision

On risk-based measures

- FATF Risk-Based Approach Sectoral Guidance on:
  - Banks
  - Life Insurance
  - Securities
  - Money or value transfer services
  - Virtual Assets and Virtual Asset Service Providers (and VA Red flag indicators)
  - Legal Professionals
  - Accountants
  - Trust and company service providers
  - Prepaid cards, mobile payments and internet-based payment services
  - Casinos
  - Dealers in precious metals and stones
  - Real estate agents
- FATF Guidance on AML/CFT Measures and Financial Inclusion, with a supplement on customer due diligence
- European Supervisory Authorities Joint Guidelines on Risk Factors (January 2018 – also available in all EU languages)
- Basel Committee on Banking Supervision *Guidelines on Sound Management of risks related to money laundering and terrorist financing* (revised in July 2020)
- Bank of International Settlements Committee on Payments and Market Infrastructures *Correspondent banking – final report* (July 2016)
- Relevant publications and initiatives by the AML/CFT private sector bodies such as, but not limited to:
  - The Wolfsberg Group, Correspondent Banking Due Diligence Questionnaire (October 2020)
  - The Wolfsberg, International Chamber of Commerce and Bankers Association for Finance and Trade, Trade Finance Principles (2019 amendment)
  - GSMA Proportional risk-based AML/CFT regimes for mobile money and GSMA Mobile Money Certification

PART THREE: COUNTRY EXAMPLES

Objectives and scope

161. This section should be read alongside the FATF Standards and the Guidance in Part One of this paper. The country examples covered in this section should be considered in light of the supervisory frameworks in place in those jurisdictions – the approaches mentioned may not be appropriate in all contexts. The inclusion of examples in this report is for illustrative purposes only and does not constitute the FATF's endorsement of the effectiveness of the country's supervisory framework for the purposes the FATF mutual evaluations or otherwise. Readers are advised to bear this in mind when drawing reference to these examples.

7. Supervision of financial institutions

7.1. Assessing risks and risk-based supervision

7.1.1. Belgium

162. In Belgium, the National Bank of Belgium (NBB) is the AML/CFT supervisory authority for banks, life-insurance undertakings, investment firms, and payment and e-money institutions. The NBB makes use of three tools centred on information from an Annual AML/CFT questionnaire completed by the regulated entities.

163. The periodic AML/CFT prevention questionnaire

164. The NBB uses an AML/CFT questionnaire to obtain an understanding of the ML/TF risk environment of each entity (the inherent AML/CFT risk it faces, its vulnerability to these risks, including the completeness and effectiveness of the mitigating measures it applies). In order to tailor the AML/CFT questionnaire to each sub-sector of financial institutions supervised by the NBB (banking, securities, insurance and payment sectors), four different questionnaires have been developed for each subsector, with the concern nevertheless to maintain consistency and comparability between these four variations of the questionnaire. The four questionnaires can be found on the NBB's website.

165. Automated QLB Response Analysis Tool ("FRA")

166. The AML/CFT supervision group at the NBB developed an internal tool to automatically analyse and score the responses provided. This tool is known as the Automated QLB Response Analysis Tool ("FRA"), which assigns one of the following

risk profiles to each financial institution: High, Medium High, Medium Low or Low. The FRA also makes it possible to visualize and compare the responses to the questionnaire provided by all financial institutions or by a group of them. In future, it will also enable comparisons over time.

167. In addition to being designed as a tool for automated and systematic pre-analysis of the responses to the periodic questionnaire, the FRA is also a tool for the AML/CFT supervisory staff to carry out ad hoc analyses on an institution-by-institution basis. Through visualization techniques, the AML/CFT supervisory staff can quickly identify the main risks generated by the financial institution's activity as well as any shortcomings in its internal procedures as revealed in the second part of the questionnaire relating to weaknesses in the financial institution's AML/CFT control environment.

168. The tool for refining the individual risk analyses ("Scorecarding")

169. The risk profiles assigned automatically by FRA (see above) are based exclusively on each financial institution's responses to the AML/CFT questionnaire. These profiles are therefore influenced by the quality of these responses.

170. The tool is limited in design in that it does not incorporate the following information:

- other relevant information provided to the NBB by these same financial institutions, particularly in the context of their reporting on their overall risk assessment, the annual report of the AML/CFT Compliance Officer (AMLCO), or the internal audit reports that can be requested by the NBB
- the results of previous off-site supervisory actions and on-site inspections
- information that can be provided by other national or foreign AML/CFT supervisory authorities regarding the same financial institution or the group to which it belongs
- relevant prudential information received by the AML/CFT supervisory staff
- information provided by CTIF/CFI, particularly in relation to the intensity and quality of the reporting of the individual financial institutions
- information submitted by the legal authorities on investigations or criminal prosecutions in cases potentially involving the financial institution, and
- all publicly available relevant and reliable information.

171. Moreover, more subjective elements such as, for example, the assessment of the expertise, transparency or reliability of the AMLCO or the managers of the financial institution, and the assessment of the overall view of the situation ("supervisory judgement") are not taken into account in the risk profiles allocated by FRA.

172. In order to be able to integrate in an orderly manner all the information listed above into the individual assessment of the risks associated with each financial institution, and thus to refine or even correct the risk profile allocated in an automated manner by "FRA", the NBB has developed an additional tool called "Scorecarding", in which the results of the analyses carried out by FRA are transferred and in which the AML/CFT supervisory staff can make, when it appears necessary, the required modifications for a correct assessment of the risks.

173. This "Scorecarding" tool should be fully operational in 2020, following certain IT developments and after the risk profiles assigned automatically by FRA on the basis of the responses to the periodic questionnaire submitted to the NBB by 30 June 2019 are supplemented with external information and with the results of the analyses and knowledge of the NBB's staff.

7.1.2. France

174. In France, the financial sector supervisor, the *Autorité de Contrôle Prudentiel et de Résolution* (ACPR) requests its supervised entities complete a questionnaire that contributes to feed both assessment of the entity's inherent risks (questions related to the nature of activities, type and level of risk of customers, type of distributions channels, etc.) and the assessment of the mitigating factors (questions related to the systems of internal controls, transaction monitoring, asset freezing, etc.). This questionnaire evolved over the years; for instance, the ACPR added questions on the screening devices and TF risk assessment in light of increasing terrorist threats since 2015 and updated the information sought based on updated regulatory requirements in the EU. Quantitative data requests with the entity questionnaire have also been increased (e.g. data on training, STR activity, number of alerts from the transaction monitoring tools, time needed to process alerts, etc.).

7.1.3. Germany (BaFin) – entity-level risk ratings

175. BaFin introduced a system of risk classification for AML/CFT supervision according to which each supervised entity is assigned to different risk classes. The risk classification takes into account the individual abstract risk situation of the respective financial institution on the one hand and the quality of the financial institution´s AML/CFT measures and safeguards in place on the other hand.

176. For the assessment of the quality of an institution´s AML/CFT measures and safeguards, the fulfilment of duties from different categories are rated and scored. For the overall rating, the quality of several individual criteria tailored to the financial sector is checked.

177. The scoring system needs different multipliers for the categories of preventive measures giving substantial deficiencies much more weight for the rating than average or low deficiencies (Result: The more a deficiency derogates the efficiency of a safeguard-measure the lower is the rating for the preventive system of an institution).

178. Finally missing or unclear findings in the annual audit reports lead to uncertainties in the evaluation of the quality of the risk management. The rating procedure takes into account lacking and unclear findings in the annual audit reports.

179. For the purpose of a final risk classification the results of the ratings for the potential threat of ML/TF and the quality of AML/CFT-prevention have to be combined (matrix) and each entity has to be allocated to a risk class to deduct the intensity and scope of its supervision.

7.1.4. Ireland: AML/CFT risk model and AML/CFT Supervisory Strategy

180. The Central Bank of Ireland maintains a Financial Sector Money Laundering and Terrorist Financing Risk Assessment model (ML/TF Risk Assessment), which identifies and assesses ML/TF risks from a supervisory perspective in order to

ensure that the Central Bank applies a risk-sensitive approach to AML/CFT supervision.

181. The ML/TF Risk Assessment is managed and maintained by a specialist risk team in the Central Bank's Anti-Money Laundering Division (AMLD). The ML/TF Risk Assessment is an iterative process, given the evolving and changing nature of ML and TF risk in the financial sectors supervised by the Central Bank.

182. AMLD (in consultation with other supervisory divisions in the Central Bank) is responsible for analysing and determining the ML/TF risks of its supervisory population. There is a specialist risk team in AMLD that works with the AML/CFT supervisory teams and the policy team to analyse risk and the full division meets regularly to discuss risk and policy. The risk, supervisory and policy teams also meet with prudential and conduct supervisors on a regular basis (at least every quarter).

183. AMLD, through its supervisory engagements, its outreach programme and interaction with, amongst others, law enforcement, national and international policy makers and other regulators (national and international) keeps informed of developments that may impact ML/TF risk ratings and incorporates these developments into the ML/TF Risk Assessment. AMLD also communicates and shares information with prudential supervisors to ensure that the ML/TF risk profile of the financial sectors included in the ML/TF Risk assessment is kept up to date.

Risk assessment model and risk analysis

184. The Central Bank became competent authority for AML/CFT supervision of financial institutions in July 2010 and as it was developing its AML/CFT supervisory process it determined that its prudential risk assessment framework, the Probability Risk and Impact SysteM (PRISM), prudential risk ratings were not appropriate indicators for ML/TF risk purposes because the underlying metrics used for PRISM ratings are based on the impact of a financial institution's failure on financial stability. It became apparent that there was a distinction between the focus of prudential supervisors and AML/CFT supervisors as whilst a financial institution may be lower risk from a prudential (systemic) perspective, the same financial institution may be high risk from an ML/TF risk perspective. For example, while a money remittance firm may not be considered a high impact firm under prudential risk ratings, the jurisdictional reach and services provided by money remittance firms means that they may be high risk from an ML/TF perspective.

185. The Central Bank devised a separate risk assessment model that would assess financial institutions based on their ML/TF risk in order to inform the AML/CFT supervisory strategy. The ML/TF Risk Assessment sets out the Central Bank's understanding of the ML/TF inherent risks and the overall level of controls and mitigants in each sector. While the ML/TF Risk Assessment analyses the risks of each sector in accordance with established categories, this is not a mechanistic process. It is necessary to consider not only the vulnerability of sectors to ML/TF but also what the Central Bank understands from its engagement with other agencies, e.g. intelligence gathering from law enforcement and the Revenue Commissioners concerning relevant sectors and ML/TF threats and vulnerabilities. The final rating assigned represents the Central Bank's full ML/TF risk assessment, taking on board its findings and information and intelligence gathered in respect of ML/TF.

186. There are four categories of ML/TF risk (high, medium-high, medium-low and low) assigned to sectors. AMLD has created within the high category an ultra-high risk sub-category for the purposes of informing its inspections strategy. In determining these ratings, the supervisory risk model considers both inherent and residual risks. A high inherent risk rating generally indicates the need for closer supervisory attention, so that supervisors can assess and intervene where necessary to strengthen the entity's risk mitigation. The residual risk rating influences the intensity/scope of supervision, and where necessary can be used to prioritise between entities. Under the Central Banks ML/TF risk model, inherent risk carries 80% weight of the overall risk score and is the main driver of the risk rating.

Supervisory strategy and AML Supervisory Engagement Model

187. AMLD formulates its annual supervisory strategy and allocates its supervisory resources commensurate with risks identified with a view to ensuring that supervisory coverage is maximised as far as possible. AMLD's supervisory strategy is focused on bringing about compliance and ensuring awareness of AML/CFT obligations and ML/TF risk.

188. AMLD adopts a graduated approach to AML/CFT supervision where the primary tool used to monitor compliance is through the use of on-site measures that consist of inspections (and follow-up measures) and review meetings. AMLD uses off-site measures consisting of AML/CFT returns, pre-authorisation reviews and other desk top reviews. It also utilises an expansive outreach and awareness building programme that maximises supervisory coverage of a wide range of types of financial institutions to ensure that there is an awareness of and compliance with AML/CFT obligations and ML/TF risk.

189. The Central Bank's AML/CFT supervisory activities are risk-sensitive and it has developed an engagement model based on ML/TF risk assessment as set out in the table below:

	Ultra High	High	Medium High	Medium Low	Low
Inspection Cycle (Years)	1	3	5	Spot check & Responsive	Spot check & Responsive
AML/CFT review meetings (Years)	Annually	Annually	5	Spot check & Responsive	No
AML/CFT Returns (Years)[33]	Annually	Annually	2	3	Spot check & Responsive
Relationship Manager	Yes	No	No	No	No

190. While there are four categories of ML/TF risk (high, medium-high, medium-low and low) assigned to sectors, AMLD has created within the high category an ultra-high risk sub-category for the purposes of informing its inspections strategy. The financial institutions that are classified as ultra-high are at the apex of AMLD's engagement strategy. These financial institutions have a relationship manager assigned, who acts as a point of contact between the financial institution and AMLD,

33 As a result of being able to automate the data return, the Central Bank of Ireland is planning to move to annual completion of AML/CFT returns by all firms irrespective of risk profile.

to help ensure the timely flow of AML/CFT information between AMLD and the financial institution.

7.1.5. Russia: Assessing entity level risks

191. In 2013, the Bank of Russia's supervisory mandate and powers were extended to a range of non-credit financial institutions.[34] The Bank of Russia was required to accomplish within short time frames the organisation and implementation of AML/CFT supervision of these entities while facing scarce resources, lack of information and an insufficient regulatory framework to address deficiencies.

192. The Bank of Russia recognised that non-credit financial institutions are always customers of banks, which are legally required to implement AML/CFT obligations and that information on their transactions via these banking accounts is largely available through the Bank of Russia's payment system. This information was analysed to address the information gaps and understand the risks associated with non-credit financial institutions. This approach has served as a kind of a strategic 'bridge' for the launch and subsequent development of the AML/CFT supervisory framework for non-credit financial institutions.

193. The Bank of Russia is using the following criteria to assess risks at the entity-level:

- The extent to which the entity is involved in transactions of a complex or unusual nature that have no apparent economic or visible lawful purpose.
- the entity's level of technical compliance with the requirements of the AML/CFT legislation.
- the effectiveness and efficiency of the entity's AML/CFT system.

194. In addition to the above principal criteria, the Bank of Russia also uses the following additional assessment criteria:

- information provided to the Bank of Russia by FIU (Rosfinmonitoring), law enforcement and tax authorities;
- prudential information (breaches of relevant legislation, lack of transparency of the business model and /or specific transactions effected by the entity, its lack of financial resilience and heightened risks for its lenders and depositors);
- information or requests received from foreign banking supervisors or financial market regulators through AML/CFT co-operation.

7.1.6. Kingdom of Saudi Arabia

195. The AML/CFT Department in the Saudi Central Bank (SAMA) uses a Risk Matrix Tool to assist in implementing a risk-based approach to supervision. This tool identifies and assesses each financial institution for its ML/TF risks as Very High, High, Upper Medium, Lower Medium, or Low. This assessment is determined based on residual risk derived from the risk matrix after assessing the financial institution's internal controls that are weighted against the inherent risks as well as the impact of the financial institution on the Saudi financial sector.

196. The Risk Matrix Tool has four main elements:

[34] Professional securities market participants, asset management companies, insurance entities, non-state pension funds, microfinance organisations, consumer credit cooperatives, agricultural consumer credit cooperatives, pawnshops.

- The first element is the assessment of the inherent risks of the financial institution through quantitative analysis i.e. data collection. It analyses structural information e.g. the number of branches, number of employees, number of customers, and volume of transaction as well as the business risk factors i.e. high risk customers, products and services offered, geographical risks, and service delivery channels. Each criterion is weighted according to its importance to calculate the degree of inherent risk.
- The second element is assessment of internal controls applied by the financial institution to mitigate the ML/TF risks. Based on the assessment of these controls, a weight is given to each criterion to determine the effectiveness of the internal controls implemented.
- The third element after calculating the inherent risks and the effectiveness of internal controls, the residual risk is determined by deducting the internal control ratio from the inherent risk, and, based on that, an assessment of residual risk is given.
- The fourth element is the extent of the financial institution's impact on the financial sector and thus, on the overall ML/TF risk of the sector. This is measured by two factors; the size of the assets and the financial institution's reputation in the financial sector.

197. The risk profile of the financial institutions is updated based on the outcomes of the Risk Matrix Tool, inspections and compliance reports, media news, and any other trigger events such as change in the size of the company, merger or acquisition, changes in ownership, and offering of a new product or service. Accordingly, this will result in:

- Planning inspection visits on a risk sensitive basis.
- Determining inspection frequency, intensity, and scope.
- Conducting off-site supervision on a risk sensitive basis.
- Determining the inspection mechanism.

Planning on-site visits on a risk sensitive basis

198. In order to ensure an effective Risk-based approach to AML/CFT supervision and proper allocation of supervisory resources in Saudi Arabia, the Saudi Central Bank has developed the Supervisory Prioritizing Tool, which organizes the inspection and follow-up visits on a risk-sensitive basis pursuant to the outcomes of the risk assessment , taking into consideration the availability of resources and any trigger events i.e. new product/service provided by the financial institution, changes in ownership, mergers and acquisition.

199. This tool prioritizes the inspection and follow-up visits by calculating a score for each financial institution. This score is determined by the date of last visit, the result of the risk assessment of the financial institution specifically, and the risk of the sector in general. Therefore, the higher the score, the higher will be the priority and intensity of the visit.

200. For sectors with higher ML/TF risks, there is a dedicated AML/CFT on-site inspection plan that is independent from the prudential supervision. On-site inspection visits are carried out by the AML/CFT supervisors with the participation

of prudential supervisors to encourage co-operation and information sharing between supervisors, whilst focusing on ML/TF related risks. Conversely, for lower risk sectors, on-site inspection is carried out by prudential supervisors with the participation of AML/CFT supervisors. The scope of inspection covers both AML/CFT and prudential supervision but requires a fewer number of AML/CFT resources.

7.2. Use of technology by supervisors ("SupTech")

7.2.1. Singapore: Risk-rating, risk surveillance and preparing onsite inspections

Use of technology to risk-rate entities

201. The approach for the inherent risk assessment of banks typically involves the regular collection of some aggregate data from each bank to assess their respective level of ML/TF risks. It is often a labour intensive and time-consuming process, involving a desktop comparison of data across peer banks, and can involve a considerable amount of qualitative judgement.

202. Recognising the potential of data analytics in enhancing ability to collect and process large amounts of data, supervisors have worked with data professionals to compile a comprehensive list of relevant ML/TF risk indicators, designed a form to collect the required data in machine readable format, and developed a risk scoring methodology that is to be applied consistently. Today, the inherent ML/TF risk rating of each financial institution (FI), together with a report on their key risk drivers can be quickly generated once data is received. This has allowed supervisors to better identify and target higher risk FIs for greater supervisory scrutiny. Where unexpected material risk profile changes year-on-year are identified in specific FIs, more timely supervisory intervention can be initiated with the FIs concerned.

Use of technology in risk surveillance

203. Applying techniques such as network link analysis in ML/TF risk surveillance could enable better analysis of risk-relevant source data and yield useful supervisory insight.

204. One such data source is STR data. Using network analysis techniques, supervisors have developed an analytical tool to detect networks of entities and individuals who are connected across different STRs filed over various time periods by different regulated entities. The networks are enriched with transactional data of the entities mentioned in the STRs (e.g. size of transactions and counterparties), and companies' profile information (e.g. business activities and key appointment holders) from its corporate registry. By performing network analysis on this multi-dimensional dataset, supervisors can identify higher risk activities and financial institutions for targeted supervisory scrutiny.

Use of technology to inform on-site inspections

205. Technology could also transform the manner in which on-site inspections are conducted. For instance, supervisors use an analytical tool during inspections to enable them to target unusual accounts and transactions for deeper examination, including where the entity concerned had failed to file STRs. This automated analytical tool examines the inspected entity's entire pool of transactions over 2-3

years at the outset. It has removed the need for inspectors to manually sight and review transactional data of sampled accounts for the unusual behaviour.

206. More importantly, it has enabled supervisors to be much more risk-targeted during inspections, and facilitated deeper dialogues with senior management of the FI on their risk governance, culture and controls, with discussions framed around actual case examples.

7.2.2. United Kingdom (Financial Conduct Authority): Targeting supervisory resource

207. The FCA is leveraging technology by developing a series of supervisory tools that will enrich their picture of the supervisory landscape and increase the effectiveness of their risk-based AML Supervision. This includes the successful completion of a proof of concept stage of a data & analytics tool that will assist supervisors to identify firms that require supervisory attention – both offsite and onsite – based on indicators that are collected from regulated firms through various returns.

208. It is still in early stages of development and will require further work over the coming months to successfully embed it into their business as usual data led supervisory work. However, they anticipate that it will create a framework to leverage data and overlay with supervisory judgements and intelligence to allow the FCA to point focus on both large and small size firms which display features that create vulnerabilities that could be exploited by criminals. To support this, they are consulting on the extension of financial crime reporting requirements to more supervised firms.

7.2.3. Brazil: Off-site supervisory reviews

209. Supervisors are increasing exploring the possibilities of using technology to transform the way supervisory reviews are conducted, allowing for off-site reviews to become more intrusive.

210. For example, Brazil has applied SupTech tools to review of entities' policies, procedures and controls, analyse customised data, test samples, and interviews management and key personnel. New technologies are also used to cross-verify data provided by entities against other supervisory data and public information. See related case study 7.4.1.

7.2.4. Mexico: SupTech Inspection Tool

211. Since January 2019, the Supervisor of the Financial Institutions in Mexico began using a SupTech tool during inspection visits to receive various operational information from regulated entities (databases of clients and transactions, alerts, reports). The tool allowed supervisors to validate this information in a matter of hours instead of days through the use of application programming interfaces (APIs). As the tool utilised machine learning to identify risk patterns and unusual scenarios based on risk criteria established by supervisors, the tool was useful in generating supervisory recommendations to optimise the warning systems of the regulated entities; carry out an analysis of the operations of the regulated entities and make a comparison with the sector to which it belongs, as well as generate reports for the purposes of supervision and development of policies in matters of AML/CTF.

212. Additionally, the tool helped supervisors to analyse large volumes of information provided by the regulated entities during the inspection visits, such as databases and regulatory reports that, on some occasions, could exceed up to ten million records. The results of the analysis could be summarised in dashboards. The tool also helped supervisors in the selection and review of client files from regulated entities.

7.2.5. Tunisia: Use of Blockchain technology to assess cross-border cash transportation risks and target supervision of entities

213. In 2017, cross-border cash transportation and smuggling was identified as a high risk activity under the Tunisian National Risk Assessment. As a result, Tunisian authorities including the Tunisian FIU, the Central Bank, Customs and the Ministry of Interior in partnership with the private sector (banks and currency exchange offices) developed a national platform using the blockchain technology called "Hannibal" to gather, storage and analyse related data from all of the mentioned stakeholders.

214. The platform generates dynamic dashboards to enabling better analysis of the ML/TF risks related to cross-border cash transportation. It also helps FIU, LEAs, banks and currency exchange offices to identify and detect networks of cash couriers. The AML/CFT supervisor, the Central Bank, can also use the platform to identify higher risk banks and currency exchange offices to better target its supervisory missions.

7.3. Engagement with the private sector

7.3.1. Saudi Arabia: Ongoing engagement with private sector

215. The financial supervisors, the Saudi Central Bank (SAMA) and the Capital Market Authority (CMA) maintain an ongoing outreach and awareness program that includes workshops, dialogue, and committees that maximises supervisory coverage of all risk and ensure awareness of ML/TF risk in the financial sector, ensuring compliance with AML/CFT obligations.

216. Both supervisors maintain an ongoing engagement with the private sector on a monthly basis through a number of permanent committees.

217. The purpose of these committees is to assist both supervisors to understand the risks faced by the private sector and react accordingly and also assist the private sector to share the latest developments and best practices to combat money laundering and terrorist financing and discuss the common risks, issues and concerns that are prevalent in the industry, raising awareness of any emerging risks in the financial sectors and come up with consolidated recommendations and analysis of such issues.

7.3.2.Russia: Know Your Customer database

218. In October 2019, a roadmap for the SupTech and RegTech solutions of the Bank of Russia, listing the major projects and initiatives in the field of supervisory and regulatory technologies, was approved. The technologies will make it possible to reduce the regulatory burden on supervised entities and to improve internal processes, including internal monitoring.

219. One of the initiatives contained in the roadmap is the creating of Know Your Customer platform (KYC Service). While conducting real time analysis of large amounts of data, the KYC Service will generate relevant up-to-date assessments of the ML/TF risk level of each FIs' customer (except for natural persons) on a daily basis. The KYC Service will break down customers into three risk categories (rated them as high, medium or low risk) and provide this information to FIs. FIs will use this information for their compliance procedures. The KYC Service is planning to start in 2021.

7.3.3. United States: Public-private partnerships

220. U.S. regulators, law enforcement, and other entities have developed robust programming for exchanging illicit finance trend and risk information with the private sector. The Financial Crimes Enforcement Network (FinCEN), the U.S. FIU, shares risk and trend information through several channels. These include the Bank Secrecy Act Advisory Group and the issuance of public and confidential advisories on illicit finance trends and threats. In 2017, FinCEN built upon these existing initiatives by establishing FinCEN Exchange, a voluntary public-private information sharing partnership among law enforcement, FIs, and FinCEN aimed at effectively and efficiently combating ML, TF, organised crime, and other financial crimes; protecting the financial system from illicit use; and promoting national security. FinCEN has convened FinCEN Exchanges on several emerging issues, including the illicit use of virtual currency, ransomware, and business email compromise schemes. FinCEN Exchange was codified in January 2021 with the passage of the Anti-Money Laundering Act of 2020, which also permits the discretionary sharing of information with the appropriate Federal financial institution regulators

221. Other components of the U.S. Department of the Treasury, including the Office of Terrorist Financing and Financial Crimes (TFFC), regularly engage private sector practitioners and leaders, both domestic and international, across the full spectrum of ML and TF issues. For example, TFFC convenes multilateral and bilateral public-private sector dialogues with key jurisdictions and regions to discuss mutual AML/CFT issues of concern and publishes national risk assessments on ML, TF, and PF.

222. Several U.S. law enforcement agencies, including the Federal Bureau of Investigation and Homeland Security Investigations, regularly engage U.S. FIs and others on ML typologies, methods, and trends, as well as ongoing investigations (where appropriate). U.S. federal financial regulators – the federal banking agencies, Securities and Exchange Commission, and Commodity Futures Trading Commission - and self-regulatory organisations (SROs) also publish guidance on ML/TF risks for the FIs they supervise.

223. Sharing information through these public-private partnerships supports more, and higher-quality, suspicious activity reports and assists law enforcement in detecting, preventing, and prosecuting terrorism, organised crime, money laundering, and other financial crimes, as well as assisting FIs in prioritising their own internal efforts. Additionally, it assists supervisors in understanding current trends in illicit finance and risks to supervised institutions, and enhances the examination process by evaluating whether institutions are aware of these risks, have incorporated these risks into their risk assessments and, where necessary, have mitigated these risks through their AML/CFT compliance programs.

7.4. Offsite supervision tools

7.4.1. Brazil: IT systems for ongoing monitoring and engagement

224. The Central Bank of Brazil (BCB) applies a methodology called Conduct Continuous Monitoring (ACC) for the highest risk financial institutions which means that at least one supervisor is in charge of continuously assessing the corporate governance, risk management and compliance of each of these institutions. The ACC methodology provides the BCB with an updated risks profile for each of these financial institutions. For less risky banks and non-banking institutions, the BCB developed a methodology and an IT system for carrying out off-site inspections, called APS-Siscom (BCB SupTech). With this technology, remote compliance inspections (ICR) assess AML / CFT policies, procedures and internal controls. All interactions with the institutions, as well as requesting and analysing documents and information, are carried out through APS-Siscom. If any breach is detected during the ICR, the institution is notified and requested to present an action plan, which is approved and followed by the supervisor through APS-Siscom. Depending on the ICR outcomes, the supervisor may propose remedial actions or sanctions, including termination of the business.

7.4.2. Russia: RegTech solution to provide ongoing feedback to the private sector

225. The Russian FIU, Rosfinmonitoring, implements a RegTech solution it calls 'Personal Account' to provide feedback to entities on STRs filed but also the specific risks the entity is exposed to, based on a range of information including compliance with AML/CFT requirements – see the diagram below.

226. The Information Quality Index is communicated to the reporting entities as well as to supervisory authorities via the Supervisory Authority's Personal Account on the website of Rosfinmonitoring.

227. The supervisor uses the information provided by Rosfinmonitoring in its risk assessment models. Information about the inspections, preventive measures, their results, as well as about the elimination of violations of mandatory AML/CFT requirements by a specific reporting entity is entered by the supervisor through the Supervisory Authority's Personal Account. Through the Supervisory Authority's Personal Account, Rosfinmonitoring also provides the supervisory authorities with information on current ML/TF risks, typologies and trends in the supervised sector, as well as with visualized statistics, etc.

228. This enables the private sector to identify on a rolling basis what their deficiencies are and to address them and potentially relieve the burden on supervisors although verification has to take place. When entities report on adjustments to their AML/CFT measures, the risk-level automatically recalculates.

Figure 7.1. Rosfinmonitoring's 'Personal Account' Information Quality Index

Source: Russia

7.5. Domestic Co-operation

7.5.1. Argentina: Co-operation between the FIU and financial sector supervisors

229. Argentina's FIU oversees AML/CFT supervision of the financial and DNFBP sectors. The FIU collaborates closely with other financial sector supervisors such as the Central Bank of Argentina, the National Securities Commission, the National Insurance Authority and the National Supervisor for Co-operatives and Mutual Associations.

230. In Argentina, the financial sector supervisors assess the risks of entities under their supervision and prepare Annual Supervision Plans (ASPs) that establish the type, level and frequency of supervisory activities. The FIU approves the risk matrices used by the financial sector supervisors to assess entity-level risks, and in doing so informs the risk assessment from an AML/CFT perspective. The FIU also reviews the financial sector supervisors ASPs and supervision procedures and is empowered to suggest modifications. The FIU can participate in the oversight of the financial sector supervisors and carry out direct supervision of regulated entities in the sector. The analysis of the results of supervisory activities are managed in working groups between the financial sector supervisors and the FIU.

7.5.2. Australia: Legal, Organisational and Functional Framework to Enable and Facilitate Domestic Co-operation

231. In Australia, there are several domestic co-ordination mechanisms to minimize operational challenges and facilitate co-operation. Below are the key mechanisms:

- Memorandums of Understandings (MOUs) to act as a framework to share information between authorities involved in AML/CFT supervision.
- Regular meetings between supervisors. For example, Australia's FIU (AUSTRAC) has regular meetings with the Australian Prudential Regulation Authority to ensure strong domestic co-ordination between Australia's AML/CTF regulator and its prudential supervisor. The benefits of such co-ordination include making each party aware of investigations or enforcement actions given the overlap of regulated entities.
- Adoption of the dual-model of AML/CTF regulator and financial intelligence unit within one agency, to ensure that the AML/CTF regulator and the FIU are within the same agency such as AUSTRAC. The dual model approach enables AUSTRAC to use its knowledge of regulated entities, industry trends and ML/TF risks to direct our supervision towards vulnerabilities and high-risk entities, which increases resilience to criminal abuse within the financial sector. AUSTRAC's supervision and engagement with regulated entities improves the volume and value of financial intelligence provided and then subsequently disseminated to partner agencies.

7.5.3. China: Co-operation between AML/CFT and prudential supervisors – a phased approach

232. At the start of 2019, the AML Bureau within the People's Bank of China (PBC) entered an agreement with the Banking Inspection Bureau within the Chinese Banking and Insurance Regulatory Committee (CBIRC) to strengthen co-operation. Based on this agreement, they undertook their first joint on-site inspection of a large bank. Supervisors reported that the benefits of the joint inspection were:

    - Broadening of each supervisor's knowledge and expertise - the prudential supervisor brought its understanding of the entity's corporate governance, internal controls, products and business processes to the inspection, while the AML/CFT supervisor brought its specialise expertise to the table. The joint action complemented each supervisor's understand of risks with expertise from the other.
    - Better quality intervention which looked at mitigation measures holistically with reduced costs for the entity by reducing supervisory overlap.
    - Both supervisors became more aware of how to ensure regulated entities comprehensively and systematically embed the AML/CFT requirements into their products and business processes.

233. Based on the positive results of the exercise, the PBC and CBIRC signed an MOU at the ministerial level and established a formal mechanism to exchange regulatory information, conduct joint risk evaluations and carry out joint inspections.

7.5.4. Ireland: Central Banks's engagement with law enforcement and other agencies/supervisors

234. As part of its information gathering for the ML/TF Risk Assessment, the Central Bank meets with an Garda Síochána (the police agency which houses the FIU), the Revenue Commissioners (tax agency), the Director of Public Prosecutions and the Criminal Assets Bureau (CAB). In addition, the Central Bank researches publicly available information, including annual reports of the relevant agencies, crime

statistics and information regarding relevant predicate offences and seized assets. Such engagement and research is useful in gaining an understanding as to the nature of the most significant ML/TF threats and how the financial system is being used for ML and TF - for example threats associated with the use of certain sectors such as banking, money remitters and bureaux de change were identified and incorporated into the relevant sectoral ML/TF risk assessments. Additionally, in keeping with the iterative nature of the assessment, any information emerging from the National Risk Assessment (NRA) or Supranational Risk Assessment (SNRA) process is considered and incorporated into the ML/TF Risk Assessment, as necessary. This ensures the on-going alignment of the ML/TF Risk Assessment with both the NRA and the nascent SNRA in this regard.

235. In assessing the threats to particular sectors, the Central Bank also has regard to information available from an Garda Siochana and from Revenue in relation to Suspicious Transaction Reports (STRs).

236. The Central Bank participates at meetings of the national Anti-Money Laundering Steering Committee (AMLSC). The AMLSC meets on a regular basis and provides an information sharing and collaboration forum for the various Irish government departments, agencies, and competent authorities with AML/CFT responsibilities under the Irish legislative framework. The AMLSC provides the opportunity for the Central Bank to be updated on ML/TF threats/vulnerabilities, which may impact the financial institutions it supervises, other sectors outside its direct remit and any interplay between the various sectors as a whole. Such information is incorporated into the ML/TF Risk Assessment, where relevant.

7.5.5. Spain: Co-operation between prudential and AML/CFT supervisors

237. In the financial sector, SEPBLAC, as the FIU and devoted AML/CFT supervisor, coordinates its supervisory activities with the prudential supervisors: the Bank of Spain, Directorate-General for Insurance and Pension Funds (DGSFP), and National Securities Exchange Commission (CNMV), which also perform AML/CFT supervisions.

238. In particular, SEPBLAC and the Bank of Spain work closely and have regular exchange of views, experiences and information for its respective supervisory activities through a Standing Committee that meets 3 / 4 times per year. The legal framework and the MOU in place foresee such co-operation and information exchange.

7.5.6. United States of America: Consistent messaging by banking supervisors, including on lower risk sectors/entities

239. For example, in the United States, the banking supervisors issued multiple statements[35] describing their approach to risk-based supervision with respect to planning and performing AML/CFT inspections (referred to as examinations in the US), including at lower risk entities. Specifically, the joint statement established how

35 US Statement on risk-focused AML/CFT supervision published by U.S. Federal Banking Regulators and Financial Intelligence Unit www.federalreserve.gov/supervisionreg/srletters/sr1911.htm; www.fdic.gov/news/press-releases/2019/pr19065a.pdf; www.occ.gov/news-issuances/news-releases/2019/nr-ia-2019-81a.pdf; and www.fincen.gov/news/news-releases/joint-statement-risk-focused-bank-secrecy-actanti-money-laundering-supervision

banking supervisors tailor examination plans and procedures based on the risk profile of each bank.

240. Common practices for assessing the bank's risk profile include:

- monitoring changes to the institution's business model, complexity, and risk profile between using publicly available information
- tailoring requests for information to the institution's business model, complexity, and risk profile
- leveraging available information, including the bank's AML/CFT risk assessment, independent testing or audits, analyses and conclusions from previous examinations, and other information available through the off-site monitoring process or a request letter to the bank, to determine the financial institution's risk profile and the scope of the next
- contacting banks between examinations or prior to finalising the scope of an examination to help inform an examiner's assessment of an institution's risk profile
- considering the bank's ability to identify, measure, monitor and control risks when risk-focusing examinations, and
- Following-up between examinations on institutions' actions taken to address areas in need of improvement.

241. After assessing this information, banking supervisors generally allocate more resources to higher-risk areas, and fewer resources to lower-risk areas. This approach promotes financial inclusion by allowing supervisors to tailor supervisory attention based on the risk profile of their supervised entities, including lower risk entities.

7.6. Special considerations for the MVTS sector

242. The MVTS sector encompasses a wide variety of players. Some MVTS providers are specialised in money transfer in specific geographic areas with limited outlet locations and operate only in one or two jurisdictions while others have a global footprint and transfer funds internationally to a large number of geographic areas (or "corridors") using very dense networks of agents. These two broad categories of MVTS providers often use the same agents (such as grocery stores, internet cafés, bureaux de change, etc.) who offer the services of several MVTS.

243. MVTS are a powerful enabler of financial inclusion in many developing countries. In many jurisdictions, either the whole sector or a sub-sector of MVTS providers are considered to be exposed to significant ML/FT risks. These risks need to be frequently (re)assessed and carefully monitored. Such assessment and monitoring should be conducted both at the sectoral and entity levels, in order to develop a sharp and accurate understanding of the threats and vulnerabilities. Supervisory authorities need to ensure a risk-based approach to mitigate against financial exclusion or unauthorised MVTS activities that will increase the ML/TF risks in the jurisdiction. For further information, see FATF Guidance for a risk-based approach to MVTS.

244. The FATF Guidance for a risk-based approach to MVTS includes various examples of how strategic analysis and off-site supervision can assist in implementing risk-based supervision of the MVTS sector:

- In the Netherlands, De Nederlandsche Bank N.V. (DNB) analyses all money transfers made in the Netherlands each quarter and performs (network) analysis on these transfers. Based on this (network) analysis, DNB is able to detect potentially unusual transaction patterns and take direct action by arranging on-site inspections. DNB leverages this technique to supervise around a thousand locations in the Netherlands.
- In Spain, payment institutions are required to send monthly statistical information broken-down by country and agent. This requirement expanded the statistical information which the Bank of Spain had been collecting and which was accessible by SEPBLAC and it enabled SEPBLAC's Supervision Area to conduct strategic analysis on the money remittance sector. The findings of this strategic analysis were used to implement additional risk-based supervisory measures, selecting the targets according to the level of risk detected in the analysis and to adapt SEPBLAC's operational analysis to be more useful for competent authorities.

7.6.1. Australia: Developing an MVTS corridor risk assessment

245. In Australia, remittances to Pacific Island countries form a key source of income for recipients. One issue that has been facing MVTS providers for several years is 'derisking' or 'de-banking'— that is, the termination or restriction of business relationships with remittance providers by financial institutions and the withdrawal of correspondent banking relationships, based on the perception of high ML/TF risk. This subsequently affects the costs and availability of some remittance services.

246. Australia conducted a risk assessment in close consultation with industry to better understand, and provide public information on, the money laundering and terrorism financing (ML/TF) risk environment associated with remittance corridors from Australia to Pacific Island countries[36] through remittance providers. The study brought together extensive expertise from the remittance sector, and was a collaboration between Australia's financial intelligence and regulatory agency and AML/CFT supervisor, AUSTRAC, and the Department of Foreign Affairs and Trade (DFAT).

247. Four main intelligence inputs informed the risk assessment: analysis of transaction reports and other AUSTRAC intelligence holdings, intelligence holdings of law enforcement agencies, interviews with remittance providers, banks and industry experts, and a survey of the remittance providers that remit funds from Australia to the Pacific. Five key areas were examined: criminal threat profile, customer profile, transaction profile, the purpose of remittances, and detection/mitigation controls.

248. The risk assessment found that the ML/TF risks associated with non-bank remittances from Australia to the 14 South Pacific Island nations were low. The risk assessment provided valuable information for banks and remittance businesses on the risks of money laundering and terrorism financing in the region.

36 Cook Islands, Federated States of Micronesia, Fiji, Kiribati, Marshall Islands, Nauru, Niue, Palau, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu and Vanuatu

249. Identifying that these activities were low risk has encouraged several new initiatives aimed at reducing cost barriers and increasing access to remittance services from Australia to the Pacific. These include simplified customer due diligence procedures, developing further industry-specific guidance, and the commencement of development of a "know-your-customer utility" to enhance the capacity for Pacific-based remitters to confirm the identity of their customers, while not increasing costs.

7.6.2. France: measures to assess risks in the MVTS sector

250. In France, the Autorité de Contrôle Prudentiel et de Résolution (ACPR) the same risk assessment methodology for MVTS sector as it used for other FIs. However, specific data is collected on the MVTS sector to better assess risks. Since 2015, a dedicated team in the ACPR is assigned to MVTS off-site controls. This team collects dedicated MVTS data (economic data and compliance checks with regulation) to better understand characteristics of this sector, to define a tailored supervisory strategy and to launch on-site inspections. Since 2015, ACPR's supervisory practices have been adapted to take into consideration the risks associated to this sector (notably the use of agents). For example, ACPR uses a specific tool to supervise MVTS providers that are only present in France via agents and the interactions with the FIU have been strengthened in relation to co-operation on MVTS providers.

7.6.3. Malaysia: Outreach with the private sector to address potential de-risking

251. In order to address the risk of de-risking on the MVTS sector (i.e. money services business entities), there are ongoing engagements among the entities, government agencies and banks. The objective of these engagements is to ensure the relevant stakeholders understand and are aware of the regulatory framework and oversight provided by the regulator on MVTS entities as well as the overall risk assessment of the sector under the National Risk Assessment.

8. Supervision of DNFBPs

8.1. Risk assessment

8.1.1. Brazil

252. The Financial Intelligence Unit (FIU) of Brazil, named Council for Financial Activities Control (COAF, in its Portuguese acronym), supervises the AML/CFT obligations of those who perform the following activities: a) factoring, b) trade in jewelry, gems and precious metals, c) trade in luxury or high-value goods, and d) some kinds of business involving rights of transfer related to athletes and artists. As at August 2020, there were 20 334 entities under COAF's supervision.

253. COAF's risk model uses a matrix that plots variables of impact and probability and determines a risk and priority rating. This process is applied on entities registered with COAF as well as natural or legal persons that are not registered but are carrying our regulated activities. Based on the matrix' ratings, COAF applies the appropriate risk-sensitive supervisory tools.

254. While the focus is on higher risk entities, the use of technology to assess entity-level risk enables supervisory efforts to achieve a broader range of regulated entities, including those of lower risk. This approach allows COAF to balance enhanced and simplified measures depending on the risk level shown by the matrix.

255. The main tools applied in COAF works of inspection are: a) the Electronic Compliance Assessment (AVEC, in its Portuguese acronym); b) the Preliminary Objective Assessment (APO, in its Portuguese acronym), and the Comprehensive Preliminary Assessment (APA, in its Portuguese acronym).

256. The AVEC is an electronic inspection instrument that assesses the degree of compliance of groups or whole sectors of supervised persons with their AML/CFT obligations (i.e., it can reach many supervised entities simultaneously). The AVEC is a fully automated IT platform , through the standardised channel used for communication between COAF and its supervised persons that have already been registered, consuming less effort and time by COAF's workforce. The AVEC's results impact the risk and priorities matrix.

257. The APO, on the other hand, is designed to assess issues at an individual entity level and requires some involvement by the supervisor. The APO is also on an IT platform and is used to verify the compliance of certain natural or legal persons with some of their obligations, focused on lower-risk situations. In case of supervised persons that have already been registered, the APO also can be conducted, at least in part, using the above mentioned standardised channel of communication.

258. The APA, in turn, is the inspection procedure for higher complexity and risk situations. It involves requiring, besides information more easily verifiable by simple confrontation with the databases accessible by COAF, documents that, added to information of those data-bases, allow deep analysis in order to identify compliance gaps.

8.1.2. Malaysia: Shift from DNFBP Sectoral Analysis to Entity Analysis

259. In Malaysia, the Central Bank of Malaysia (Bank Negara Malaysia – BNM) is the main AML/CFT supervisory authority for DNFBP sectors. Due to the large size of DNFBP

sectors, risk-based supervision on the sector is crucial. The application of risk-based is cut across from selection of entities, supervisory activities and actions.

260. In terms of identification higher risk DNFPB entities, Malaysia shifted its risk analysis from a "sectoral basis" to an "entity basis". In the early implementation of risk-based supervision, BNM focused the inspection on higher risk sectors as identified under the National Risk Assessment (NRA) with specific entities were selected based on risk factors relevant to the sectors. For example, risk factors of dealers in precious metals and stones are mainly based on the degree of vulnerabilities in the supply chain such as luxury segments and large retail chains. Over the years, the risk identification process has been improved by adopting more granular data which allows for analysis on specific entities rather than sector-only as a whole, which contributes to a more accurate and robust selection process of entities.

261. DNFPB supervisory activities and actions became risk-based depending on the risk and context of entities, ranging from comprehensive review inspection, abridged review inspection or off-site supervisory tools including submission of annual Data and Compliance Report (DCR). The DCR is the method in which information about inherent risk is collected and analyzed. The type of information requested in the DCR include the following:

- Data on customers (profile of customers, i.e. natural persons, legal persons, legal arrangements, PEPs status, customers from high risk jurisdictions;
- Products (e.g. cash based, nominee product, easily transferable products)
- Delivery channel (e.g. face-to-face or non-face-to-face, agent relationship)
- Geographical location
- Business information (size, turnover, revenues, types of activities)
- Other risk factors that may be specific to the sector (e.g. exposure to nominee relationship for TCSPs)

262. During the inspection process, the risk-based assessment methodology is used in assessing the ML/TF risks and controls measure whereby all components assessed are rated accordingly and final ratings are assigned. For each component, the assessment is guided by baseline parameters and the ratings of inherent risk and control measures will determine the net risk (residual risk) of an entity inspected. The net risk rating will be a deciding factor on the actions to be undertaken on the entity which can be in the form of supervisory actions or enforcement actions, depending on the severity of the issues identified.

8.2. Introducing a risk-based approach to supervision of DNFBPs

8.2.1. United Kingdom: The supervisor of DNFBP supervisors (OPBAS) experience

263. Financial Institutions have historically been more tightly regulated for AML/CFT than the DNFBP sectors. This has driven significant investment in FI AML systems and controls; for example, technology to monitor transactions. Similar oversight by the DNFBP supervisors of their relevant firms has been lower in places, although, through OPBAS's work with SRBs, that has started to change.

264. SRB designated as DNFBP supervisors under the money laundering regulations are overseen by OPBAS and cover a wide range of sub-sectors including tax advisory, audit, insolvency, conveyancing and trust company formation, and cover roles including accountants, bookkeepers, solicitors, barristers and notaries across England and Wales, Scotland and Northern Ireland. The vulnerabilities can be specific to each activity the supervised entity undertakes. Risks in these sectors are continually developing, for example sham litigation, or planting Organised Crime Gang members into a firm due to weak staff screening processes.

265. At the start of its regulatory work in 2018, OPBAS identified a number of concerns. For example, it needed to obtain buy-in around the value of AML systems and controls; some supervisors, and some firms within their supervised population, didn't view AML as a core function.

266. A lack of focus on AML supervision by some DNFBP supervisors meant their systems and controls lacked sophistication, with some viewing AML as a tick box exercise.

267. Another challenge has been the need to ensure supervisors have separated advocacy from regulatory functions. This has happened with the legal sector supervisors; however, this is not always clear in the accountancy DNFBP supervisors. Without a clear demarcation of AML/CFT supervisory responsibilities, supported by robust governance, there can be a conflict of interest, with the need for robust regulatory action against member firms potentially weighing against the need to protect member interests and membership revenue.

268. While there is still progress to be made, DNFBP supervisors with focused support and challenge from OPBAS continue to take positive steps in developing their ability to deliver effective AML/CFT supervision in their sectors.

Remote review of files to enable off-site AML/CFT supervision of SRBs who supervise DNFPBs

269. OPBAS conducts its regulatory activities through a combination of on-site and off-site activities. In both sectors, OPBAS can request from a DNFBP supervisor a remote review of relevant files, which are delivered securely and electronically.

270. Accordingly, OPBAS can review these files to identify concerns with AML/CFT risks or indicators of non-compliance with UK AML/CFT legislation. Any negative outcomes can warrant further investigation and prompt additional evidence gathering by OPBAS, which can alter its risk rating of the DNFBP supervisor if any shortcomings are proven. OPBAS also analyses yearly data provided to the UK government. This can be cross-referenced with other reports and information accessible to conduct forward-looking risk analysis to determine an AML/CFT risk profile and then, if required, adjust any ratings assigned to the DNFBP supervisor.

8.2.2. Singapore: ACD's experience as a new DNFBP supervisor

Supervising a large number of entities and with limited risk information

271. The Anti-Money Laundering/Countering the Financing of Terrorism Division (ACD) under the Ministry of Law was established in 2019 to regulate and supervise the precious stone and precious metal dealer (PSMD) sector in Singapore. Approximately 1 900 PSMDs are currently registered with ACD.

272. As the AML/CFT regulatory regime for the PSMD sector was new, there were initially limited information on the type of risks that PSMDs faced which could be used for the entity risk assessment. To overcome this, a survey was conducted in February 2020 to all PSMDs to gather more information on their business and risk profile but only 73% of PSMDs responded to the survey. In December 2020, ACD imposed a semi-annual reporting requirement on the PSMDs to improve the quality and timeliness of the data collected for risk assessment and off-site monitoring purpose. ACD had also reached out to law enforcement agencies (LEA) to share suspicious transaction reports (STR) and intelligence reports involving PSMDs to better understand the ML/TF typologies and identify higher risk dealers in the PSMD sector. Together with the results from probity checks obtained during registration and our environmental scanning, this information was fed into the supervisory risk model for the PSMDs' entity risk assessment, which was completed in April 2020.

273. ACD adopted a risk-based approach to supervision, and subjected higher risk PSMDs to more intensive supervisory scrutiny, e.g. more frequent and intense inspections in addition to the regular off-site monitoring. Each PSMD was risk-rated based on the risk assessment methodology which considered data collected from the PSMDs, intelligence from LEAs and existing and emerging typologies in the PSMD sector. ACD would review and re-calibrate the risk rating of PSMDs on a periodic basis. The review would also take into account inspection outcomes, ongoing surveillance, offsite monitoring and financial intelligence received on the PSMDs.

274. To ensure that its officers were familiar with and well equipped to supervise the sector, given its more nascent supervisory regime, ACD participated in AML/CFT-related capacity building or training initiatives to learn regulatory best practices and understand regional ML/TF typologies

275. ACD also complemented its supervision model by engaging a third party professional firm to conduct compliance reviews on PSMDs who were rated as medium-high risk, but with no identified risk factors. A process has been set in place to monitor the quality of work delivered by the third party. This arrangement allowed ACD to channel its focus on higher risk PSMDs that require closer scrutiny.

Working with private sector

276. ACD has been working with Industry Associations (IAs) to continue to educate and raise the PSMD's sector ML/TF risk awareness. The IAs represent diverse sub sectors within the PSMD sector, such as the jewellery retailers, watch dealers, diamond dealers and bullion traders. ACD has partnered and consulted with IAs to elevate the sector's ML/TF risk awareness, AML/CFT standards and capabilities and co-developed educational materials for the sector. ACD also provided guidance on common AML/CFT issues raised by members of the IAs through regular broadcasts. Besides engagements with IAs, ACD has published a number of information and fact sheets and conducted various outreach programmes to educate and raise AML/CFT awareness for the PSMD sector to help better understand the different ML/TF risk typologies and concerns each sub sector face so that a more targeted risk-based supervision approach could be designed.

8.2.3. United Kingdom (Gambling Commission) – monitoring low-risk entities

277. The UK Gambling Commission uses a three-year full assessment cycle to monitor lower risk entities. To be considered lower risk, the business must have demonstrated compliance with required regulatory requirements. During the three-year cycle, lower risk entities are assessed during thematic and targeted compliance activity. Under this approach the supervisor is reassured that this part of its supervised population remains lower risk.

8.3. Co-ordination and information sharing

8.3.1. United Kingdom - Office for Professional Body Anti-Money Laundering Supervision (OPBAS)

278. In 2019, OPBAS established two new Intelligence Sharing Expert Working Groups (ISEWGs) with the National Economic Crime Centre (NECC). The ISEWGs are loosely based on the UK's existing Joint Money Laundering Intelligence Taskforce (JMLIT) model involving law enforcement and the financial services sector, and are globally pioneering in public private intelligence sharing forums for the legal and accountancy professions.

279. There is an ISEWG for each sector with members consisting of DNFBP AML supervisors, law enforcement (via the NECC), Her Majesty's Revenue and Customs, the Financial Conduct Authority and OPBAS. Both ISEWGs have agreed published Terms of Reference. The ISEWGs have two distinct functions: strategic and tactical. The strategic element involves discussion and consideration by all members on the high-level threats and emerging risks for their sector. Members give anonymised real-life case examples of where they have found a specific money laundering risk identified from their supervisory work, along with mitigating actions. The strategic sessions have also seen the development of a drafting group of volunteer supervisors who receive JMLIT alerts and redraft them to make them relevant to their sector.

280. The tactical element is a confidential disclosure meeting between members, under the relevant legal gateways, relating to a live investigation. To participate in an ISEWG tactical session, members have agreed to be security vetted and have secure email addresses for correspondence. As part of the terms of reference, members also commit to feeding back anonymously to the wider membership in the next strategic session on any overarching themes from tactical sessions. This enables a better understanding of inherent money laundering threats to their sector. Since inception, the ISEWGs have delivered a significant improvement in the collaborative working relationships, engagement and trust between AML supervisors and law enforcement. They have also enabled an improvement in the effectiveness of supervision across the member supervisors through sharing of best practice, themes and trends. Another benefit from the ISEWGs has been a more consistent flow of high-quality information and intelligence sharing in both sectors and increased SARs reporting. We expect the impact of the ISEWGs to continue to grow throughout 2021 as the work of the groups is adopted by and embedded in the member organisations.

8.3.2. Singapore: ACD's experience

281. To assist ACD in identifying and understanding the ML/TF risks posed by the PSMD sector, an inter-agency PSMD Workgroup comprising relevant AML/CFT supervisory authorities, LEAs and FIU was set up to improve the ML/TF risk understanding of the PSMD sector, strengthen the AML/CFT regulation and enhance the enforcement of the PSMD sector. This also helps to ensure a coordinated and risk-based supervisory effort on the sector.

282. To remain updated on current and developing ML/TF typologies involving the PSMD sector, ACD also launched a monthly Open Source Intelligence ("OSINT") Bulletin. The ACD OSINT bulletin collates typologies/ media articles from environmental scanning of ML/TF and crime trends involving the PSMD sector, and highlights red flag indicators observed in the articles. This bulletin is also circulated to agencies under the PSMD Workgroup for knowledge sharing purpose.

9. Supervision of VASPs

9.1. Identifying the VASP population

9.1.1. Canada

283. There are a number of factors that pose challenges during the identification of the VASP population in a jurisdiction. Despite the challenges, early outreach and engagement can help with estimates and complement analysis and research. Canada introduced regulation for VASPs in July 2020. In November 2019, FINTRAC invited VASPs to register early. This enabled the authorities to better anticipate the resources required for supervision and to develop its supervisory strategy. The approach also benefitted the VASPs, as they were able to better understand the requirements with early engagement with the regulator. Although VASP regulation is new in most jurisdictions, this does not mean that all entities within the population are new to regulation. There are a number of examples where FIs, in particular money service businesses involved in cross border exchanges, have integrated a VA exchange component into their business model and where casinos exchange fiat to crypto for their customers. This reiterates the importance of supervisor co-operation, particularly where there are multiple supervisors with entities that provide VASP services, where this may not be their primary activity.

9.2. Identification of risk in the VASP sector

9.2.1. Kingdom of Saudi Arabia

284. The Kingdom of Saudi Arabia has conducted a ML/TF risk assessment on VAs and VASPs to identify, assess, and understand the ML/TF risks associated with this sector.

285. At the data collection phase, which aims to identify the current level of exposure to VAs and VASPs, questionnaires were circulated to a number of public sector bodies and private sector entities. Those questionnaires captured statistics and information related to STRs, cases under analysis, investigations, prosecutions and convictions, international co-operation requests involving VAs/VASPs, the internet traffic on VA or VASP activities, the nature and type of services provided on the websites and host countries, the number of business relationships held by private sector entities with VASPs, and any transactions involving VA.

286. Additional information has also been captured to determine the overall level of risk, as follows:

- How many foreign legal persons/arrangements, which are VASPs operate within Saudi Arabia?
- How many ICOs were organized through a Saudi legal entity or a foreign entity registered in KSA?
- What type of activities/operations do these VASPs conduct: a. exchange between virtual assets and fiat currencies; b. exchange between one or more forms of virtual assets; c. transfer of virtual assets; d. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and e. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

- What type of products and services do these VASPs provide to KSA customers?
- Where are these VASPs operating from?
- Where are these VASPs registered?
- How many legal persons/arrangements registered in Saudi Arabia provide VASP services?
- What type of products and services do these VASPs provide?
- What type of customers do these VASPs serve?
- In what geographical regions are these VASPs providing their services?
- Where do their customers come from?
- Have VAs been frozen under TF/PF-related targeted financial sanctions?

287. Workshops were held for all relevant public sector bodies and representatives from private sector entities to discuss the data and information gathered through the questionnaires and provide expert judgement. The risk assessment is intended to shed light on the extent to which VASP operations are taking place in KSA, the level of use by the population of VAs and the extent to which VAs/VASPs have been misused for criminal purposes. The risk assessment also looks into vulnerabilities within the KSA framework, particularly the ability of the authorities to detect, deter and repress criminal activity involving VAs/VASPs. The outcomes of the risk assessment have been discussed with other relevant authorities in order to determine the policy responses to the risk identified.

9.2.2. Japan

288. In general, JFSA annually collects AML/CFT statistical and qualitative data from obliged entities for JFSA to assess their risk exposures, and assign risk rating on individual obliged entities based on the methodology JFSA developed, which will be then used to develop annual off-site monitoring plan. Those source data collected from obliged entities are approximately 60 Key Performance Indicator data, which are tailored to each sector. For the VASP sector, JFSA collects the following non-exclusive list of information which is subject to annual revision:

- Whether blockchain analysis tools are used for transaction monitoring and/or risk analysis purposes
- Type of virtual assets offered to customers
- Numbers of customers detected to have used mixers and/or tumblers
- Percentage of hardware or paper wallet usage allocation
- Whether or not a VASP accepts corporate clients as customers (number of accounts, transaction value)
- Whether or not a VASP offers business payment services
- Attributes of counterparty VASP (geographical distribution and transaction volume)
- Number and geographical location of VA-ATMs a provider manages

9.3. VASP sector outreach and guidance

9.3.1. Japan

289. Because most VASPs are new to AML/CFT regulation, common shortcomings can emerge based on a lack of awareness of requirements. For example, when it first started supervising VASPs in 2017, the Japanese FSA (JFSA) found consistent failings in quality of KYC/CDD and record keeping as well as a lack of regulatory understanding and expertise in key positions. Dialogue with the sector can be an important way to address these issues and present best practice. The JFSA has periodically reached out to VASPs through mainly the Japan Virtual and Crypto assets Exchange Association, SRO in Japan, to provide feedback on issues it is encountering and to stress the importance. Those explanatory sessions covers topics such as, but not limited to: scope of AML Risk Assessment, recent cases of suspicious transaction reporting in VASP sector, terrorist Financing, the revised National Risk Assessment, AML Internal Audit, Recent AML Law revision/e-KYC, Travel Rule – INR.15 (7b) revision and FATF 12 month review report. JFSA has found its initiatives so far have worked to enhance industry's awareness and its AML/CFT controls. In addition to the above, JFSA participated in several domestic and international seminars held by private sector stakeholders, industry associations or technology vendors, to cover VA involving AML topics for a wider audience.

9.3.2. United States

290. In the US, the FIU Financial Crimes Enforcement Network (FinCEN) and other functional regulators issue regulatory guidance to clarify regulatory expectations to the sector. For example, in May 2019 FinCEN issued guidance that consolidated all previous FinCEN statements on regulatory applicability of the Bank Secrecy Act (BSA) to VASP and VA activities, as well as outlining how BSA regulations apply to certain commonly observed business models in the VA market. This guidance assists the industry in understanding regulatory obligations, as well as assist other supervisors and law enforcement in effectively identifying when a person may be operating as an unregistered VASP. FinCEN has also maintained consistent engagement with the VA sector around AML/CFT regulatory expectations, compliance challenges, and illicit finance trends through public remarks at financial conferences and public-private private partnerships, such as the FinCEN Innovation Hours Program and the FinCEN Exchange Program.

9.4. Use of technology in VASP supervision

291. The nature of blockchain and other distributed ledger technology means that most VA transactions are recorded on a ledger, and some information may be publically available. Blockchain analytical tools can be used to understand certain aspects of these transactions. A number of jurisdictions are using, or exploring using, blockchain analytics services to assist with their supervision. The services can be used in a number of ways, including to pinpoint areas that supervisors may wish to focus on during assessments in individual firms and helping to categorise the highest risk firms based on their activity, as well as in assessing more strategic and global risks to support developing of risk-based regulations and development of national ML/TF risk assessments. While such tools can support risk monitoring and supervision, using such tools requires financial resources and requires recruitment

and training of a workforce able to use such tools[37]. Additionally, not all VAs are covered by all vendors. Blockchain analytics are also widely used by VASPs and some FIs to monitor their own exposure to risk (e.g. transactions that have passed through mixer or tumbling services or that have originated from known illicit websites), so supervisors should understand how they function in order to adequately assess a VASP's implementation of their risk-based framework and internal controls.

292. Supervisors that use blockchain analytics should consider how the use of the data derived from these solutions meets the data protection requirements in their jurisdictions.

9.4.1. Singapore

293. In Singapore, the Monetary Authority of Singapore (MAS) has been using its surveillance capabilities in its supervision for money-laundering and terrorism financing (ML/TF) risks in the VASP sector. For example, the MAS uses data analytics techniques to detect unlicensed VASP activities for enforcement action, using both public and other data sources (such as corporate registry information, intelligence and STRs). It also uses real-time block chain information to augment statutory information collected from licensed entities. This allows for timelier prioritisation of supervisory measures to target emerging risks and typologies. Key insights from these analyses are also shared with industry to raise risk awareness and vigilance.

9.5. Recruitment and training of VASP supervisors

9.5.1. United Kingdom (Financial Conduct Authority)

294. It is unlikely that many supervisors new to VASP supervision will have existing staff with both expertise in the technical nature of VAs and VASPs and supervisory knowledge and experience. Furthermore, individuals with this combination of skills and knowledge are also currently difficult to recruit.

295. To address this issue, the FCA established a specific multi-disciplinary team largely comprising of experienced supervisors with financial crime and AML skillset, supplemented by external and internal recruits with expertise in VASPs. In addition, the FCA procured training from an external provider on blockchain and virtual assets to ensure all members of the team had at least a certain level of sector and supervision understanding as a starting point.

296. This ensured that from the start of the regime, the team had the ability to understand complex business models, analyse VASP activity, identify risks and also employ the most appropriate supervision tools and interventions. FCA continues to enhance the technical knowledge and supervisory expertise of VASPs.

9.6. Multi-jurisdictional operations and supervisory co-operation on VASPs

9.6.1. Singapore

297. VASPs can operate across borders and establish relationships with customers in multiple jurisdiction fairly easily without the need for a physical presence in those

[37] FATF delegations may wish to refer to the 2019 Heads of FATF FIU Forum Virtual Assets Project Paper as a resource

countries. As a way to develop a better understanding of the global presence of VASPs applying for registration, several supervisors, such as Singapore have indicated that they specifically include a question requesting information on registrations or applications in other jurisdictions. This enables the supervisors to identify international counterparts that they may wish to reach out to better understand the risks involved.

10. Supervision in the COVID-19 context

10.1. Risk-based flexibility for reporting entities and clear communication of expectations and provision of Guidance

298. Disruption to supervisory authorities and regulated entities have highlighted the importance of the risk-based approach in the context of the COVID-19 pandemic. In some cases, FATF members have continued onsite inspections or hybrid or virtual on-sites, prioritising high-risk sectors or entities. Some supervisory authorities have indicated they have provided risk-based flexibility on the filing of annual reports and other data returns and have delayed issuing new licenses, particularly for some sectors that are not permitted to operate due to lockdowns.

299. Communication, guidance and outreach has played an important role in balancing access and controls. The FATF's report on COVID-19 Risks and Policy Response s includes a range of examples at Annex B. As a further example in the context of COVID-19, banking supervisors in the United States reminded banks that offer financial services to NPOs to avoid viewing the charitable sector as a whole as presenting uniform or unacceptably high ML/TF risks.[38] Consistent with a risk-based approach, banks should evaluate NPOs according to their particular characteristics to determine whether they can effectively mitigate the potential ML/TF risk. Banking supervisors provided non-binding guidance of factors that banks should consider in identifying the AML/CFT risk profile of NPOs.

10.1.1. Saudi Arabia: COVID-19 - Monthly Reporting and Monitoring of Financial Institution AML/CFT Control Environment

300. As a response the COVID-19 crisis, the Saudi Central Bank (SAMA), who is the country's AML/CFT supervisor, requested financial institutions to submit remote working plans of their AML/CFT departments in order to assess and monitor their ability to work remotely and effectively during periods of lockdown.

301. Moreover, for monitoring purposes, SAMA established a new monthly data collection form and questionnaire focusing on the provision of digital financial services. These returns provided information on measures applied by regulated entities to the change in consumer behaviour during the pandemic, including details on their financial activities such as the volume, frequency and destination of cross-border activities.

302. Finally, SAMA's AML/CFT department established a process of supervising FIs remotely on a risk-sensitive basis during lockdown by completing most of the inspection work off-site to reduce the number of employees required on premises and to reduce the duration of the inspection without compromising on effectiveness.

38 https://home.treasury.gov/news/press-releases/sm1183

Glossary

AML/CFT systems or controls are the measures in place within an entity to mitigate ML/TF risks, including the preventative measures set out in the FATF Recommendations (see section 2.2.2).

Core Principles refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

Designated non-financial businesses and professions (DNFBP) means:

a) Casinos (include ship and online casinos)

b) Real estate agents.

c) Dealers in precious metals.

d) Dealers in precious stones.

e) Lawyers, notaries, other independent legal professionals and accountants (when performing the activities outlined in the FATF Glossary definition of DNFBPs)

f) Trust and Company Service Providers (when performing the activities outlined in the FATF Glossary definition of DNFBPs).

Emerging risks is a broad term used to refer to recently identified but not fully explored ML/TF threats or vulnerabilities or other phenomena. Previously identified risks that become apparent in new or unfamiliar conditions can also be considered emerging risks.

Financial group means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.

Financial institutions means any natural or legal person who conducts as a business one or more of the activities or operations listed in the FATF Glossary definition of "financial institutions" for or on behalf of a customer.

Inherent risk refers to the ML/FT risks present in an entity or sector before mitigating measures are applied. Inherent risk is often assessed based on entities' customer base, products, delivery channels and services offered and the jurisdictions within which it or its customers do business.

Inspection/examination: These terms are used interchangeably to refer to intrusive/vigorous reviews of an entity's AML/CFT systems and controls in practice. In addition to a review of the entity's policies and procedures, an inspection or examination includes an assessment of the entity's implementation of those policies through inter alia interviews with key personnel, testing of systems used in the AML/CFT compliance and a review of risk assessment and customer files (see Annex B). Inspections are commonly an on-site intervention; however, the greater adoption of technology may allow inspections to happen off-site.

Internal controls: as defined in the FATF Standards under R. 18 and INR.18, refer to the implementation of programmes against ML and TF which should include:

- the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees;
- an ongoing employee training programme; and
- an independent audit function to test the system.

Management Information (MI): refers to systems and processes used to provide an entity's Boards, management and the dedicated officers with timely and appropriate information about the entity's risk management and internal control framework.

Monitoring in the broadest sense refers to processes aimed at controlling the effective application of legal and regulatory AML/CFT requirements and the effectiveness of mitigation measures applied, starting from the detailed examination of real life documents, identification files, transactions or activities, and aiming at identifying in a second stage the "root causes" of weaknesses or breaches identified in the first stage of the process with the view to (impose to) remedy them effectively. **Monitoring tools** enable supervisors to observe changes in risk profiles or detect atypical behaviour. See section 1.2.

Money or value transfer services (MVTS) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including hawala, hundi, and fei-chen.

On-site supervision refers to on-site supervisory work in which supervisors independently verify that adequate policies, procedures and controls exist at regulated entities, determine that information reported by regulated entities is reliable, obtain additional information on the regulated entity and its related companies needed for the assessment of the condition of the regulated entity, monitor the regulated entity's follow-up on supervisory concerns.

Off-site supervision (including monitoring and risk surveillance) refers to off-site, or desk-level, supervisory work to regularly review and analyse the financial condition of regulated entities', follow up on matters requiring further attention, identify and evaluate developing risks and help identify the priorities, scope of further off-site and on-site work.

Regulated entities refers to FIs, VASPs and DNFBPs.

Residual risks are ML/TF risks that remain after ***AML/CFT systems and controls*** are applied to address inherent risks. See section 2.2.3.

Risk tolerance: Taking a risk-based approach means recognising that residual risks will never be zero. 'Risk tolerance' refers to the accepted level of unmitigated or un-mitigatable risk. An entity's risk tolerance (a factor of its risk appetite) refers to the boundaries within which the entity is comfortable operating given residual ML/TF risks will exist after mitigation measures are applied. A supervisors' risk tolerance

refers to the level of unmitigated residual risks that supervisors are willing to accept, taking into consideration the potential impact. In this regard, supervisors' risk tolerance is generally lower for entities with higher ML/TF risks yet weaker controls, or where AML/CFT control failures could have a material impact on the rest of the financial system. On the other hand, risk tolerance may be higher in situations where entities have demonstrated ability to monitor and mitigate any escalation in residual risks.

Risk indicators: are risk metrics and/or statistics that provide insight into an entity's risk exposure and used to monitor the main drivers of exposure associated with key risks.[39] In AML/CFT, risk indicators are commonly used to assess and monitor the level of inherent risks, however risk indicators can also be established to monitor the quality of AML/CFT control measures.

Robotic Process Automation (RPA) is a form of business process automation technology based on metaphorical software robots (bots) or on artificial intelligence (AI)/digital workers.

Self-Regulatory Body (SRB). A SRB is a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.

Supervisor/s refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by regulated entities[40] with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.

Supervisory risk assessments (SRA) help supervisors develop, document and update their ML/TF risk understanding by undertaking a supervisory risk assessment. See sections 2.1 and 2.2.

Supervisory strategy: Taking into account the supervisory risk assessment, a supervisory strategy helps supervisors plan their activities in a risk-sensitive manner by determining how much attention to give relevant sectors and entities within those sectors. It sets clear objectives for AML/CFT supervision, explains how supervisors will address the ML/TF risks they have identified across their sector(s) and how they will respond to emerging risks. See Section 3.1.

Systems for monitoring: the ongoing observation of the activities of regulated entities to identify any weakness or breaches in compliance but in a manner that is generally less intrusive than traditional supervision regime. See R.14, 15, 26 and 28 and paragraph 13.

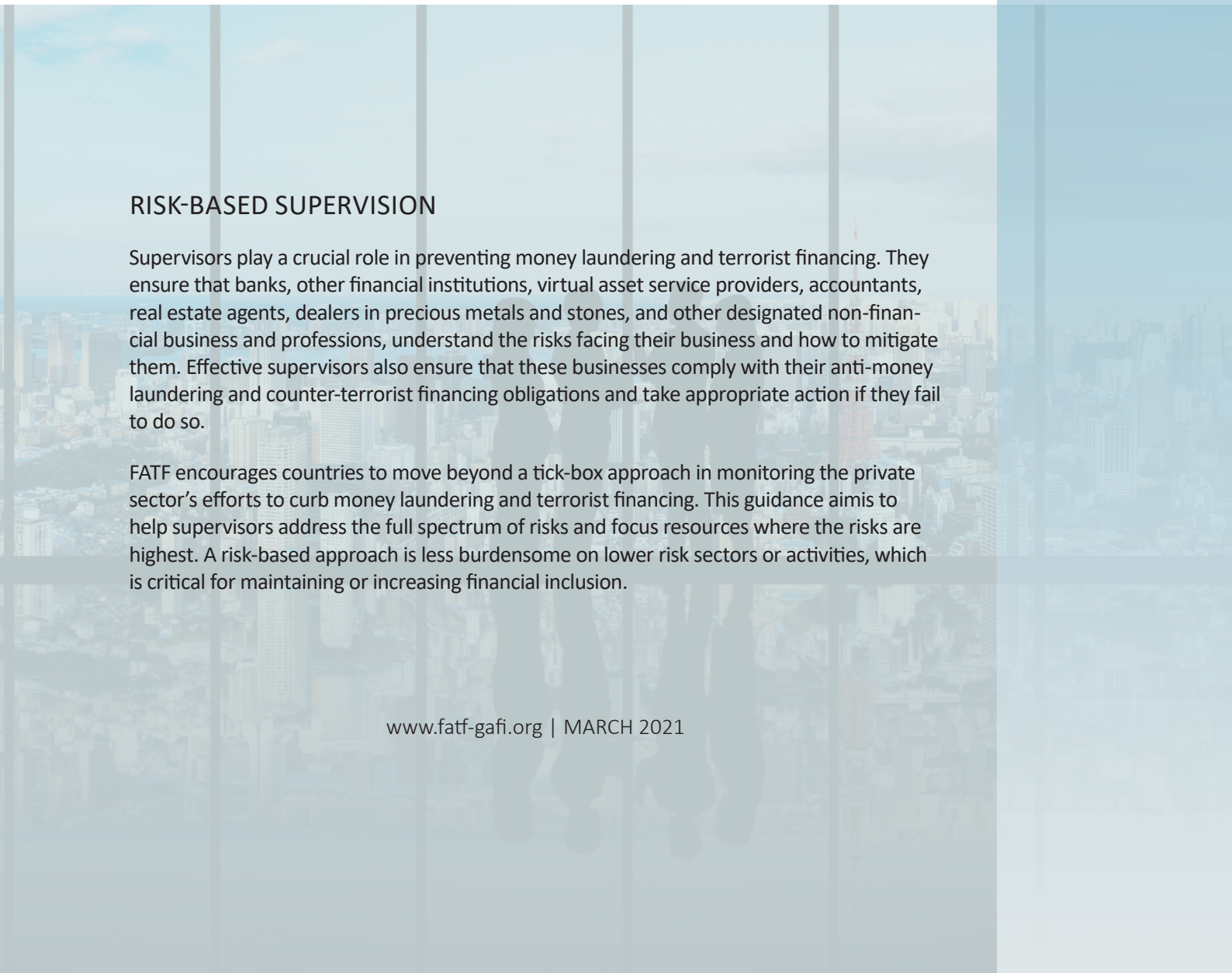
39 https://www.bis.org/publ/bcbs195.pdf

40 Including Core Principles supervisors who carry out supervisory functions that are related to the implementation of the FATF Recommendations.

Three-lines of defence: See the *Basel Committee on Banking Supervision's Guidelines for the Sound Management of Risks relating to Money Laundering and Financing of Terrorism* at page 5. As a general rule and in the context of AML/CFT, the business units (e.g. front office, customer-facing activity) are the first line of defence in charge of identifying, assessing and controlling the risks of their business. The second line of defence includes the chief officer in charge of AML/CFT, the compliance function but also human resources or technology. The third line of defence is ensured by the internal audit function.

Targeted financial sanctions: The term targeted financial sanctions means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities. See R.6 and R.7 of the FATF Recommendations.

Virtual Asset Service Providers (VASPs): In October 2018, FATF extended AML/CFT requirements to VASPs under Recommendation 15. A VASP means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations listed in the FATF Glossary definition of VASPs for or on behalf of another natural or legal person.



RISK-BASED SUPERVISION

Supervisors play a crucial role in preventing money laundering and terrorist financing. They ensure that banks, other financial institutions, virtual asset service providers, accountants, real estate agents, dealers in precious metals and stones, and other designated non-financial business and professions, understand the risks facing their business and how to mitigate them. Effective supervisors also ensure that these businesses comply with their anti-money laundering and counter-terrorist financing obligations and take appropriate action if they fail to do so.

FATF encourages countries to move beyond a tick-box approach in monitoring the private sector's efforts to curb money laundering and terrorist financing. This guidance aimis to help supervisors address the full spectrum of risks and focus resources where the risks are highest. A risk-based approach is less burdensome on lower risk sectors or activities, which is critical for maintaining or increasing financial inclusion.

www.fatf-gafi.org | MARCH 2021