MFSA MALTA FINANCIAL SERVICES AUTHORITY

SUPERVISION

RISKS IDENTIFIED, WEAKNESSES AND EXPECTED CONTROLS

A CROSS-SECTORAL ANALYSIS

Contents

CONTENTS 1
FOREWORD 1
TABLE OF ABBREVIATIONS 2
BACKGROUND 3
CHAPTER 1 4
CROSS-SECTORAL RISKS, WEAKNESSES AND EXPECTED CONTROLS 4

SECTION I - ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM 5

A. Risks 5
B. Reoccurring Weaknesses 5
C. Controls which the MFSA expects authorised entities to have in place 7

SECTION II - GENERAL RISKS, WEAKNESSES AND EXPECTED CONTROLS 9

A. Risks 9
B. Reoccurring Weaknesses 12
C. Controls which the MFSA expects authorised entities to have in place 14

CHAPTER 2 19
SECTOR-SPECIFIC RISKS, WEAKNESSES AND EXPECTED CONTROLS 19

SECTION I INSURANCE AND PENSIONS 20

A. Risks 20
B. Reoccurring Weaknesses 21
C. Controls which the MFSA expects authorised entities to have in place 22
D. Expected Controls (applicable for Insurance Intermediaries) 23

SECTION II CREDIT AND FINANCIAL INSTITUTIONS 24

A. Risks 24
B. Reoccurring Weaknesses 24
C. Controls which the MFSA expects authorised entities to have in place 26

SECTION III SECURITIES AND MARKETS 29

A. Risks 29
B. Reoccurring Weaknesses 30
B.II Reoccurring Weaknesses [EMIR] 32
C. Controls which the MFSA expects authorised entities to have in place 32

SECTION IV TRUSTEES AND CORPORATE SERVICE PROVIDERS 35

A. Risks 35
B. Reoccurring Weaknesses 35
C. Controls which the MFSA expects authorised entities to have in place 35

CONCLUDING REMARKS 37

Foreword



Joseph Cuschieri
Chief Executive Officer

The Malta Financial Services Authority, as the single regulator for financial services in Malta, is responsible for prudential and conduct supervision of the entities it authorises. In liaison with the Financial Intelligence and Analysis Unit, it also seeks to ensure compliance of such firms with anti-money laundering and counter financing of terrorism standards.

The financial services industry is undergoing considerable transformation and as the environment in which regulated firms operate changes, so do the risks they face. Emerging technologies, global interconnectedness and new business models bring opportunities but also pose new threats. In this context, the MFSA considers that it is of utmost importance that regulated firms place strong governance, accountability and investment in compliance and controls at the heart of their operations.

In line with the Authority's vision to strengthen Malta's position as a financial services centre, as well as its statutory objectives to safeguard investors and to ensure market integrity and financial soundness, work on authorised entities' culture, and their adherence with regulatory standards, continues to be one of the main priorities.

Going forward, the Authority is planning to intensify off-site work and the on-site inspections of firms, both in terms of coverage and standard. As indicated in the AML and CFT Strategy, published earlier this year, the MFSA has fused the three pillars of its supervisory strategy - prudential, conduct and AML supervision – to ensure a holistic supervisory approach, which will, in turn, improve overall efficacy.

The publication of this document, which is directed at regulated entities operating in the insurance, banking, securities, trusts and corporate service providers' sectors, is part of the Authority's commitment of increasing the supervisory engagement with authorised entities, in promoting and ensuring sound governance structures, compliance standards and conduct.

Table of Abbreviations

AIFM	Alternative Investment Fund Managers
AML	Anti-Money Laundering
BCP	Business Continuity Plan
CDD	Customer Due Diligence
CFT	Counter Financing of Terrorism
CIS	Collective Investment Scheme
CSP	Corporate Service Provider
DRP	Disaster Recovery Plan
ECB	European Central Bank
EMD	Electronic Money Directive
EMIR	European Market Infrastructure Regulation
FIAU	Financial Intelligence Analysis Unit
GDP	Gross Domestic Product
IDD	Insurance Distribution Directive
ICT	Information and Communications Technology
KPI	Key Performance Indicator
KRI	Key Risk Indicator
NPL	Non-Performing Loan
MFSA	Malta Financial Services Authority
MiFID	Markets in Financial Instruments Directive
MLRO	Money Laundering Reporting Officer
PABF	Payment Account with Basic Features
PAR	Payment Account Regulation
POG	Product Oversight and Governance
PSD	Payment Services Directive
RMICAAP	Risk Management and Internal Capital Adequacy Assessment Process
TII	Tied Insurance Intermediary
UCITS	Undertakings Collective Investments in Transferable Securities

Background

In promoting the safety and soundness of the financial services sector, the MFSA focuses on the risks that operators in the industry face or could face in the future. Over the past years, the MFSA has carried out extensive supervisory work to evaluate and reduce risks on consumers and market integrity, that may arise from the operations of the entities it authorises.

The MFSA is issuing this document in order to outline its views on the key risks that authorised firms[1] operating in the financial services sector might pose to their clients and the market in general. This document also sets out the Authority's expectations of the applicable controls for the various operators within the industry. Additionally, it highlights the common weaknesses and deficiencies, which have been encountered as part of the Authority's ongoing supervisory work and its engagement with operators and the expected standards which authorised entities are expected to meet.

This document comprises two Chapters. Chapter 1 includes a dedicated AML and CFT section and provides a list of cross-sectoral risks, weaknesses and expected controls. Such risks, common weaknesses and expected controls apply to industry practitioners operating in the various sectors. Chapter 2 then includes four dedicated sections. It identifies sector-specific risks, weaknesses and expected controls, each relating to the Insurance and Pensions, Credit and Financial Institutions, Securities and Markets, and Trusts and Corporate Service Providers sectors. Concluding remarks are included in the final part of this publication.

The list of various risks, common weaknesses and expected controls, as set out in this document per sector, should not be interpreted as being exhaustive in nature and these do not necessarily apply to all legal forms of incorporation.

The MFSA expects regulated entities to discuss the contents of this document with their Board of Directors (or equivalent administrative body) and assess how the highlighted points may apply to their business. Firms are expected to address any misalignments between their internal frameworks and practices and the expectations as set out in this document and to establish the necessary processes in order to ensure that the firm will continue to meet such expectations on an ongoing basis.

[1] References in this document made to "regulated entities", "authorised firms" and "firms" refer to any person, including any entity corporate or unincorporated, which may hold a licence or other authorisation issued by the Authority or which falls within the supervisory or regulatory authority of the Authority

Chapter 1

Cross-Sectoral Risks, Weaknesses and Expected Controls

Section I - Anti-Money Laundering and Counter Financing of Terrorism

A. Risks

In light of the Results of the National Money Laundering and Terrorist Financing Risk Assessment[2], the Authority considers the following as being some of the key financial crime risks in the financial services sector in Malta:

1. Complex corporate structures and business models;

2. Exposure to flows of funds from higher-risk jurisdictions and customers – Malta's economic policy and geographic location mean that it is exposed to flows of funds from higher-risk jurisdictions and customers. Whilst links with higher-risk jurisdictions or clients do not imply the presence of money laundering or terrorist financing, we expect firms to have in place greater controls, to mitigate the risks associated with them;

3. Exposure to the gaming sector;

4. Prevalence of cash and transferable cheques[3], in particular, in the real estate and luxury goods sectors;

5. Payment and e-money services.

B. Reoccurring Weaknesses

Through its supervisory work, performed in conjunction with the FIAU, the Authority has identified a number of reoccurring weaknesses in the AML/CFT arrangements adopted by regulated firms. In particular:

1. Weak Customer Risk Assessments

Key AML/CFT arrangements, such as due diligence and transaction monitoring, are to be applied in a manner that is proportionate to the degree of risk implicit in a customer relationship. As such, an inadequate customer risk assessment weakens a firm's entire framework of AML/CFT arrangements.

2. Inadequate Due Diligence

Firms often fail to demonstrate that they have, through due diligence, understood their clients, and the risks associated with their business. Decision-making rationales are also often lacking from client files, making it very challenging, if not impossible, to establish how a firm has come to determine whether a client is within its risk appetite.

[2] Results of the ML/TF National Risk Assessment - https://mfin.gov.mt/en/Library/Documents/Result_of_the_NRA_2018.pdf

[3] The use of which obscures the link between the payment and payer and the provenance of funds.

3. Timing of Due Diligence Assessments

Firms not infrequently onboard customers even prior to the due diligence process being satisfactorily completed. This is indicative of ultimate beneficial owners or other indirect controllers exercising undue pressure over firms' compliance structures. This is considered as a serious governance breach.

4. Inadequate Transaction Monitoring

Automated and comprehensive monitoring of transactions is key to the detection of financial crime activities. In particular, the MFSA is concerned by the widespread failure, by regulated entities, to have in place transaction monitoring systems that are capable of comprehensively scrutinising their transactional data for patterns indicative of money laundering and terrorist financing and of doing so in a timely manner. The Authority considers the prevalent approach to the documenting of the discounting rationale for 'alerts' and 'red flags' to be inadequate.

5. Inadequate Payment and Name Screening (against sanction lists)

As for transaction monitoring, the Authority is concerned by the widespread failure, by regulated firms, to put in place systems capable of robustly screening (a) names - at onboarding and on a regular basis - of clients and connected parties; and (b) payments - prior to their execution - for possible association with sanctions. Even in this case, weaknesses have been noted in relation to the approach to documenting the discounting rationale for 'alerts' and 'red flags'.

6. Poor Control over Data and Infrastructure

The MFSA is concerned by firms' poor control over data, in particular that relating to customers and their transactions. Regulated firms are frequently not able to produce complete datasets, because of their wilful or accidental destruction. In the absence of robust controls over data, it is impossible to conclude that firms are capable of assessing and monitoring the degree of money laundering risk they are carrying. Another area of concern relates to the extensive outsourcing of infrastructure without its adequate control and oversight.

7. Inadequate Management Information (e.g. KRIs, KPIs and other quantitative and qualitative metrics and indicators as to the degree of risk and how well it is mitigated by the firm's controls)

The Authority has often found firms to have no or inadequate levels of management information in relation to the levels of money laundering and terrorist financing risks that they face. This is, in turn, indicative of extremely weak governance structures.

8. Lack of accountability and competence and uncontrolled outsourcing of control functions

Firms have often failed to demonstrate that staff at all levels understand the money laundering and terrorist financing risks to which they are exposed and the controls in place to mitigate them. Compliance and control functions are often found to be under-resourced or controlled by senior management or indirect controllers. The Authority is generally dissatisfied with the controls established by firms when outsourcing compliance and other control functions.

C. Controls which the MFSA expects authorised entities to have in place

Firms are expected to:

1. have in place organisational structures and resources, both human and technical, capable of ensuring AML/CFT compliance at all times;

2. promote a culture of AML/CFT compliance and have in place a comprehensive framework of systems and controls to enable it;

3. be aware of, and manage, the potential conflicts of interest which may arise from the firm's commercial objectives and its employees' outside business interests/relationships versus its obligation to counter the risk of the firm being used to further ML/TF;

4. establish and document clearly-defined roles and responsibilities in relation to AML/CFT;

5. ensure that all employees demonstrably understand their role in relation to AML/CFT;

6. ensure that firms' implementation of AML/CFT measures is overseen by the Board of Directors (or equivalent function);

7. ensure that AML/CFT considerations are demonstrably incorporated within the firm's strategy;

8. ensure that the MLRO function is independent, receives unimpeded access to the Board of Directors (or equivalent function) and is provided with all the necessary resources and access to all the necessary information to perform the role in an effective manner; and

9. establish a clear escalation procedure for the reporting unusual customer activities or transactions.

Firms must also:

1. perform a firm-wide ML/TF Risk Assessment;

2. adopt formal policies setting out their stance on the ML/TF risk they face;

3. understand the ML/TF risk inherent to each prospective and actual customer relationship;

4. perform due diligence on prospective customers to understand their (prospective customers') circumstances, the networks around them and the nature and purpose of their relationship with them;

5. monitor, on an ongoing basis, their relationship with their customers; and

6. communicate AML/CFT standards, policies and procedures to all staff and provide training as to their application in a manner that is proportionate and specific to each member of staff's roles and responsibilities.

Firms are expected to give prominence to ongoing scrutiny of transactions. Scrutiny of transactions entails the use of the subject person's knowledge of the customer (including the information gathered on the purpose and intended nature of the business relationship and the customer's business and risk profile) as well as statistical and pattern-analysis that is independent of the aforementioned, to identify transactions which are, by their very nature, unusual.

These include, but are not limited to, suspicious, illogical, unnecessarily complex, or unreasonable transactions, as well as those which are inconsistent with the customer's risk profile or are significantly different to what is usually carried out or requested by the customer. The Authority's reviews of firms have identified a number of shortfalls in this area and further assessments will be conducted in relation thereto.

Section II - General Risks, Weaknesses and Expected Controls

A. Risks

1. Weak Corporate Governance

A number of authorised entities tend to operate with a lean internal governance structure, which may lead to ineffective Board oversight of the firm's operations and internal controls. Generally speaking, for certain firms, this would be due to their relatively small size and also the related proportionality and cost considerations. This risk is further exacerbated in instances where entities are owned by a sole individual and where such ultimate beneficial owner is a dominant figure within the entity.

This risk may lead to lack of independent directors forming part of Board setups and there is, at times, an insufficient level of engagement and questioning by independent directors. This risk is higher in instances where an authorised entity experiences a significant degree of shareholder intervention, thereby undermining the independence of the management body and/or senior management.

A related risk is when certain Board members, having several appointments in various firms, do not dedicate sufficient time to the proposed role, or, once appointed, they do not always continue undertaking ongoing professional training and development.

2. Ineffective Third Line of Defence

Given the relatively small size of certain authorised firms, proportionality and cost considerations, not all firms have a permanent, independent internal audit function. In such cases, at times, firms would not have in place effective mitigating arrangements, or in case where this is outsourced, such function would not be effectively monitored on a continuous basis and periodic updates are not always provided to the Board.

3. Key Person Dependency Risk

Given the relatively small size of certain firms and proportionality considerations, a number of authorised entities are also exposed to key person risk, particularly with respect to the management of core operations. This may expose firms to business continuity-related issues.

4. Lack of Effective Risk Framework and Risk Assessment

A number of authorised entities fail to undertake, implement and maintain a comprehensive risk assessment of their business. Deficient risk frameworks and poor risk assessment may result in firms not having sufficiently robust internal control functions and proper processes in place, potentially leading to lack of readiness by firms, in the event of unusual market events impacting their business.

5. Compliance and Regulatory Risk

Given the ever-increasing legislative and regulatory obligations that authorised entities are expected to comply with, exposure to regulatory and compliance risks should not be under-estimated. Risk is further heightened, when firms lack sufficient expertise, appropriate internal operational resources, suitable processes, or fail to embrace new technologies.

Compliance risk, which can also be considered as a subset of regulatory risk, may result in real financial and business losses due to potential penalties/other regulatory actions imposed on the firm – this aside from any resultant reputational impact.

6. Outsourcing – Resilience and Oversight Risk

A number of authorised firms outsource core critical functions. Firms lacking good contingency plans may find themselves unprepared in case of the failure of a critical service provider and this exposes them to resilience risk.

Furthermore, firms could also be exposed to oversight risk when they outsource certain core functions, if they are found as not having properly supervised companies they outsourced business to.

7. Poor Conflicts of Interest Management Risk

A number of authorised firms repeatedly fail to appropriately identify, monitor, manage and control the conflicts of interest inherent to their business model. This may result in poor governance practices and could possibly lead to harming the consumer.

8. Complex Business Models

The evolving and increasingly complex business models, including complex intra-group ownership structures, at times also involving the outsourcing of functions to intra-group entities, exposes firms to greater risk. Business models targeting high-risk customers or non-traditional business lines need long-term planning and adequate risk evaluation. A related risk is when firms have an insufficiently articulated, or uncomprehensive, risk appetite on acceptance of new business.

9. Business/ Strategic Risk

Technology is changing the landscape of various regulated entities operating in the financial services sector. Failure to adapt to such a changing environment gives rise to risks impacting the long-term business strategy of a firm. Failures in this regard may include the inability to rethink outdated frameworks of core systems or the lack of implementation of more efficient systems to meet consumer demands. Such shortcomings could easily lead to loss of business and market share.

10. Operational Resilience (including Cybersecurity and Technology Risk)

This mainly refers to the ability of authorised firms and the sector as a whole to prevent, respond to, recover and learn from operational disruptions. Operational failures pose a risk to authorised entities in terms of business continuity as well as to possible damage to the integrity of proprietary data. Our

supervisory work has shown that certain entities are exposed to operational incidents, which may heavily disrupt their business.

From the supervisory work undertaken in this area, the Authority has also found that certain entities are increasingly prone to operational shortcomings. As the business of a number of firms becomes more highly automated, any IT failure can have a substantial impact on the services that they provide. Entities may also be exposed to the risk of data leakage – this may lead to data protection issues, as well as significant operational and reputational risk.

Technological developments and the digital transformation may make firms increasingly susceptible to cyber-attacks. This could affect business continuity, undermine confidence in the sector and threaten financial stability.

11. Capital Resources Requirements

This relates to the risk that authorised entities (subject to capital resources requirements) may fall short of their initial capital requirements and their ongoing Own Funds requirements.

Specifically with respect to the banking sector, all banks currently "report some level of voluntary buffers, with the Tier 1 capital ratio adequately above the 9.875% minimum regulatory requirement under the Basel III phase-in arrangements and the additional capital add-ons highlighted under the Capital Requirements Directive (CRD) IV"[4]; however, future pressures on capital may arise due to higher risk exposures registered by the core banks and possible future activation of macro-prudential capital buffers by Authorities.

12. Prolonged Low Interest Rate environment

The prolonged low interest rate environment is a risk that the securities, insurance and banking sectors are exposed to. Major central banks, such as the ECB and the Federal Reserve, have reverted to an expansionary monetary policy. The ECB, for example, has officially announced that it will restart its asset purchase programme[5] and already has a deposit rate of below (-0.5%)[6].

Specifically, with respect to the securities sector, this may lure firms to the risky 'search for yield behaviour', which could artificially inflate asset prices.

On the insurance side, a sustained low level of interest rates poses a significant challenge to the sector as it would struggle to generate adequate returns to meet long-term obligations but also poses an on-going re-investment rate risk. This could lead money managers at insurance companies to seek higher returns through riskier, and possibly lower quality, investments.

A prolonged low interest rate environment also exerts pressure on bank profitability, especially for retail banks, by reducing their interest rate margin. This is leading banks to rebalance their activities, changing business models and focusing more on other income-generating business activities. This accommodative monetary policy stance is a response to subdued GDP growth in the euro area, which

[4] Central Bank of Malta, Financial Stability Report 2018, p 31 - https://www.centralbankmalta.org/file.aspx?f=82555,
[5] European Central Bank, Press Release: Monetary Policy Decisions, 12 September 2019
https://www.ecb.europa.eu/press/pr/date/2019/html/ecb.mp190912~08de50b4d2.en.html
[6] European Central Bank, Key ECB Interest rates:
https://www.ecb.europa.eu/stats/policy_and_exchange_rates/key_ecb_interest_rates/html/index.en.html

has been lagging behind that of other major economies in recent years. Such a macroeconomic environment may also erode profitability for banks.

B. Reoccurring Weaknesses

1. Lack of comprehensive risk assessment

- no comprehensive mapping exercise which would enable firms to properly identify and assess the relevant risks to which it is exposed to;
- typically, few firms are able to provide evidence that a risk assessment, which includes risk measurement and establishment of thresholds (where applicable), has been carried out.

2. Weak Internal Governance

- failure to ensure that all key functions are adequately staffed at all times;
- failure to ensure that key function holders possess the right skill set and experience;
- weak Board setups – inadequate number of directors, directors lacking the appropriate skill set, individuals taking up multiple directorships thereby limiting the time allocated to a particular institution;
- lack of independent directors on Boards and, when present, there is, at times, a lack of involvement and engagement by such directors;
- unstructured, incomplete and, at times, untimely Board Packs being presented to the Board;
- Board meetings do not reflect discussions but are limited to reporting parts of information packs;
- limited interaction from the Board members regarding challenging Board-approved policies, their actual content, as well as how such Board policies will be influencing the day-to-day processes and decisions across the entity;
- multiple appointments and/or lack of time dedicated to the proposed roles put strain on conflict of interest and time allocation to carry responsibilities and duties in an effective manner;
- Boards not taking a pro- active role with regards to cybersecurity.

3. Weak Compliance Function (including lack of independence and authority of the compliance function)

- not properly mapping the risk of non-compliance, which should enable firms to then set targets and allocate the required resources and work programme of the compliance function;

- inadequate compliance culture – including: not having sufficient authority recognised by the entity, not dedicating sufficient human and technical resources (in particular when this function is outsourced), the appointed compliance officer not possessing the right expertise to fully understand the risks of the firm, compliance officer not being given full access to all the information needed to be able to adequately perform function, failure to identify and harness regulatory requirements;

- repetitive and/or unjustified late submission of regulatory reporting, which may also imply that an authorised entity may lack sufficient internal resources and proper compliance monitoring;

- in instances where compliance is outsourced, at times, the function is not being carried out effectively and not always being properly monitored by the authorised entity;

- firms not ensuring that, besides the compliance function being effective, independent, undertaking monitoring checks and reporting, the compliance officer should also be advising the Board accordingly and is involved, for example, in projects which are likely to generate risk of non-compliance;

- ineffective and incomplete compliance monitoring programmes not covering all aspects of the authorised business's activities and failure to keep records, evidencing the ongoing checks being carried out in this respect;

- the compliance function does not always adequately report to the Board on compliance matters, such as providing a detailed assessment of how the various parts of the authorised firm is performing against compliance standards and goals (including methodology adopted with regards to such assessments);

- insufficient due diligence and oversight of outsourced critical functions - the individuals appointed to carry out oversight of outsourced functions are not provided with the necessary training to be capable of ensuring that oversight is carried out in an effective manner;

- incomplete policies and procedures which are not regularly updated and/or not being followed by the firm and staff not being given adequate training in relation to such policies and procedures;

- compliance officer involved in the execution of services that they are responsible for monitoring;

- compliance registers not always being accurately kept updated;

- certain firms implement changes to their business models without submitting the required notification (or request for approval, as applicable) to the Authority, as required in the applicable MFSA Rules.

4. Weak business continuity and disaster recovery plans (BCP/DRP) and lack of testing

- failure to have in place a documented BCP/DRP procedure enabling the entity to respond, recover, resume and restore to a pre-defined level of operations following a disrupting event;

- failure to distinguish properly between business continuity and disaster recovery concepts and to reflect such differences in the BCP/ DRP policies and procedures. Given that the BCP and the DRP account for different matters, they should be treated independently notwithstanding any perceived similarities;

- reliance on the BCP/DRP of intra-group entities which do not adequately cover the local firm's operations;

- lack of, or limited, testing of business contingency plans. This creates issues to identify any particular weaknesses of the business contingency plan as well as limits confidence with regard to the level of resilience of the BCP.

C. Controls which the MFSA expects authorised entities to have in place

1. Corporate Governance – Internal Controls

An authorised entity is expected to take reasonable care to establish and maintain internal controls as are appropriate to its business to ensure that it is managed and controlled in a sound and prudent manner. It is expected that the nature and extent of the internal controls which an entity needs to maintain take into account a variety of factors, including:

- the nature, scale and complexity of its business;

- the diversity of its operations, including geographical diversity;

- the volume and size of its transactions;

- the degree of risk associated with each area of its operation.

The MFSA expects the Board of Directors to establish and maintain effective internal controls, to be aware of the major risks facing the company and provide guidance and oversight to senior management. A good practice noted by the Authority and one that the Board of Directors tend to benefit from is when appointing an individual who can contribute further to the regulatory framework area; particularly, to strengthen the oversight of the Compliance Function.

The Board of Directors is expected to:

- conduct periodic discussions with senior management regarding the effectiveness of the internal controls;

- ensure regular and timely reviews of the effectiveness of internal control functions;

- ensure that all issues raised, including those by external auditors and the Authority, are followed up by management;

- ensure the effective implementation and oversight of the risk management system that includes setting and monitoring internal controls so that all major risks are identified, measured, monitored and controlled on an ongoing basis.

2. Corporate Governance – Board Proceedings

Good governance and ethical standards are considered by the MFSA as crucial. The right tone is expected to be set at the top and should cascade down the organisation, thus reducing possible consumer detriment. In this respect, authorised entities are expected to:

- hold regular Board meetings to discuss ongoing developments relating to the business;

- keep detailed minutes of discussions held at Board meetings, as well as any other ad hoc meetings wherein significant decisions are taken, and to document discussions, challenges and decisions taken at Board level, particularly those in relation to business strategy and plans (taking into consideration any Board-approved policies);

- ensure that at least two directors are involved in the day-to-day business of the licensed entity, in line with the four-eyes principle as set out in the relevant regulatory regimes;

- ensure that all directors are kept abreast with developments relating to the entity's clients and the business; and

- ensure that Boards dedicate more time for discussion on cyber risk during Board meetings.

3. Compliance Function

Firms are expected to:

- implement an effective compliance function which has unfettered access to all documentation and a direct reporting line to the Board of Directors of the authorised entity, whenever required. The function must be adequately resourced to ensure that all significant activities are reviewed in a timely manner;

- have an effective mechanism in place which enables:

    - the identification, assessment and evaluation, on an ongoing basis, of the significant risks to which the company is exposed to;

    - prudent management and control of material risks including the development and implementation of appropriate internal controls relating to risk mitigation and risk transfer arrangements and the establishment of contingency plans;

- development of risk appetite, risk tolerance limits and resilience strategies (that is, strategies to help manage the impact of risk on the entity) which are regularly reviewed;

- prepare a compliance procedures manual which covers all the licensable activities being provided by the licensed entity, which should be reviewed periodically. Staff should also receive training with regard to the contents of the compliance procedures manual and procedures;

- prepare a compliance monitoring programme, at least on a yearly basis, which should follow a thorough risk assessment of the authorised entity's business and which should monitor the overall operation and procedures of the licensed entity to ensure that all aspects of the business are adequately monitored;

- maintain documented records which demonstrate that monitoring and testing are taking place – findings and recommendations should be formally reported to the Board;

- set effective controls and monitor, on an ongoing basis, all outsourced functions, as if these functions were performed internally and subject to the normal standards of internal controls;

4. Lack of proper Risk Assessment

Certain authorised entities often fail to have in place an adequate risk appetite, risk assessment systems and procedures and consequently they also often fail to establish the necessary mitigating measures. This leads to the risk of trustees and CSPs not being sufficiently aware of their own business model and thus not being able to determine whether a certain activity or certain clients fit such business model.

Consequently, authorised entities may run the risk of taking unnecessary and unmitigated risks, which may lead to systemic and reputational risk. Firms are expected to:

- map out and identify all risks which may impact the licensed entity's business

- clearly establish a business model and a risk appetite

- put in place mitigating measures

5. Internal Audit Function

Where appropriate and proportionate, authorised firms are expected to implement an effective internal audit function, which shall be objective and independent from the operational functions.

Where an independent internal audit function is established, firms are expected to inter alia ensure that their internal audit function:

- has unfettered access to all the firm's business lines and support departments;

- has a direct reporting line to the Board of Directors;

- has sufficient status within the authorised entity to ensure that senior management reacts to and acts upon its recommendations;

- has sufficient resources and staff who are suitably trained and have relevant experience to understand and evaluate the business they are auditing;

- employs a methodology that identifies the key risks run by the company and allocates its resources accordingly.

Depending on the nature, scale and complexity of its business, it may be appropriate for an entity to form an audit committee ideally confined to non-executive directors of the company. It is recommended that at least one member of the audit committee shall be independent and shall have competence in accounting and/or auditing.

Where a firm opts to outsource such function, it is expected that proper monitoring and reporting arrangements to the Board are put in place.

6. Key Person Dependency

Firms which are exposed to key person dependency risk, are expected to, as much as possible, ensure that they have in place adequate business continuity arrangements. It is also considered good practice that, where such risk is present, this is adequately disclosed in an appropriate manner to clients.

7. Operational Resilience

Weak operational resilience may impact the long-term ongoing operations of a firm. Authorised firms are expected to have the ability to prevent, respond to and recover from operational disruptions. The Authority expects firms to be able to withstand such disruptive operational incidents and, as part of their business continuity arrangements and operational risk management, ensure that preventive measures, proper planning and impact assessments are undertaken, in order to ensure that their business can tolerate a certain level of disruption and ensure continuity of service (in terms of systems, people and processes).

8. Compliance and Regulatory Risk

Firms are expected to take a progressive approach to compliance. The Compliance and Risk functions should become part of the overall culture of the firm. Dedicating adequate resources to the area of compliance, or in the case of outsourcing, ensuring that the service meets the required standards (together with the required oversight by the firm), increases the firm's readiness and ability to be able to:

- be proactive in mitigating risk;

- understand the potential impact of a regulatory change;

- be in line with the respective legislative regulatory requirements. Authorised entities are required to keep up-to-date with regulatory changes that might impact their business and products/ services offered, their clients and the way they are operating.

9. Conflicts of Interest

The MFSA expects authorised firms to undertake comprehensive assessments in order to identify, manage, monitor and control conflicts of interest. Having a good understanding of what can give rise to potential conflicts is the responsibility of both the Board and its employees. Furthermore, conflict of interest policies, procedures and registers should be in place and kept updated.

10. Capital Requirements

Authorised firms are to ensure that they maintain and constantly monitor their regulatory capital. It is important that firms have in place early warning signs to prevent breaches from occurring. Firms should also have in place recovery plans to cater for instances where the firm falls in breach of its requirements.

11. Outsourcing

Whilst adding more layers to the overall process, outsourcing may increase the risk of lack of oversight over the activities being undertaken by outsourced parties. When outsourcing, besides ensuring robust internal controls, authorised entities are expected to remain fully in control and accountable for any outsourced activities and are expected to implement contingency plans addressing possible failures by critical service providers.

In addition, authorised entities are expected to ensure that proper oversight is being undertaken on the respective third party in order to ensure both a good level of service and continuity by the respective critical service providers. In addition to the required periodic compliance monitoring, it is considered good practice to have dedicated senior officials within the authorised entity responsible for the ongoing monitoring of outsourced activities.

Chapter 2

Sector-specific Risks, Weaknesses and Expected Controls

Section I Insurance and Pensions

A. Risks

1. Ageing population

The ageing population is also understood to have an effect on the profitability of life insurance portfolios and may potentially lead to portfolio shifts in different asset classes or markets where growth potential is stronger and potentially riskier.

2. Interconnectivity of risks

With respect to the local context, the failure of any one of the local significant banks would have a major impact on the insurance undertaking interconnected with it, and a very significant impact on the stability of the life insurance industry in Malta.

One of the larger life insurance undertakings is totally dependent on one of the main banks operating in Malta, whilst a significant proportion of the business of another large life insurance undertaking derives from the largest bank in Malta. Other than the use of the bank branches for the selling of insurance, there is interconnectedness through placing of bank deposits by the insurance undertakings and investments with the respective banks.

3. Climate Change

Climate-related risks are still considered top global risks. Weather-related disasters are not only becoming more severe but are also occurring more frequently. The emerging climate risks pose threats in particular for the insurance industry where they could be confronted with unexpected losses due to more extreme weather events. Actions beyond innovations on risk management techniques, new analytical tools and development of loss prevention solutions are needed for a fundamental shift towards sustainable insurance in the face of climate-related risks.

4. Lack of diversification of the Insurance Business Portfolio

The business model of a number of undertakings relies on either selling one insurance product or targeting one particular sector or market. There are also a number of undertakings which have one class of business that contributes materially to a good proportion of the undertaking's total portfolio.

Apart from government bond exposure, domestic insurance undertakings are highly exposed to equity and collective undertakings. Conversely, exposure to property is limited on aggregate, although a number of domestic insurances rely more extensively on this form of investment and thus risks from this sector should be considered in stress tests.

B. Reoccurring Weaknesses

1. Governance and Risk Management not aligned with set strategy

The entire system of governance and risk management system of certain firms are not aligned to the set strategy.

2. Lack of structured Training Programmes

A number of regulated firms do not always implement a structured training programme for the Board, senior management, key function holders and persons who effectively take decisions, addressing any weaknesses identified possibly following the Board effectiveness assessment and ongoing fitness and properness assessments that are expected to be conducted by the firm.

3. Ongoing Fitness and Properness Assessment

Generally, the ongoing fitness and properness assessment process does not produce effective outcomes, such as identifying any gaps in knowledge or competencies which can be the basis for the identification of structured training. Furthermore, outcomes and conclusions of the fitness and properness assessments are not being documented. Furthermore, such assessments may not specify the criteria supporting the selection of Board members, key function holders and persons who effectively take decisions that meet inter alia the following criteria:

- adequate professional and personal skills and experience, individually and collectively, that evidence proper knowledge of the structure and business of the company and proper understanding of its risks;
- checks that continuous professional development requirements are met; and
- the ability to avoid or remove conflict of interests.

4. Training to Distributors and effective monitoring of distribution network

Training provided to distributors especially TII's, tends to focus only on the products of the undertaking and company's procedures in effecting sales. Training with respect to the regulatory requirements applicable in the context of distribution seems to be rather lacking.

5. Remuneration to Distributors

The remuneration of distributors is, at times, based solely on sales, which should not be the case.

6. The Product Approval Process

The Product Approval process, as required in terms of the IDD, which an undertaking should follow when manufacturing new products or when carrying out significant adaptations to existing ones, is not always being drafted in a comprehensive manner which clearly indicates the responsibilities of persons within the organisation for specific aspects of this process.

C. Controls which the MFSA expects authorised entities to have in place

1. Governance and Risk not aligned with set strategy

The Authority expects that firms carry out a review of the entire system of governance and risk management on a regular basis and whenever there is a material change to the risk profile of the business.

2. Management Information Systems

Develop, maintain and utilise an effective comprehensive management information system so that sufficient, timely and relevant information may be produced to enable the business of the company to be prudently managed and controlled. It is expected that management information systems are reviewed regularly to assess the current relevance of information generated and the adequacy and quality of the system's performance over time.

3. Business Plan

Regulated entities are expected to have an appropriately documented business plan, which enables it to identify, measure, manage and control risks of regulatory concern. Business plans or strategy plans are expected to be documented and regularly updated to take into account any changes in the business environment.

4. Internal Controls

Licensed insurers are to have appropriate internal controls in place to fulfil their regulatory and statutory obligations with respect to adequacy, excess, periods of retention and security of records.

Authorised entities are expected to:

- establish and maintain appropriate internal controls over the accounting and other record-keeping process, including sufficient accounting procedures, reconciliation of accounts and control lists, with respect to both on and off balance sheet assets and liabilities. This will reasonably ensure the completeness of accounting information, the accuracy of all amounts reported, timeliness in the reporting of transactions/business activity, the validity of transactions and the proper maintenance of records. Internal controls should also address checks and balances; for example, cross-checking, dual control of assets, double signatures;

- have in place effective internal controls with respect to the segregation of duties in order to ensure that there exists a clear and distinct separation of duties. The segregation of duties, both between individuals and between departments, reduces the risk of intentional or unintentional manipulation or error by increasing the element of independent verification;

- ensure that no single person should be able to control sufficient stages of processing a transaction to the extent that errors, misappropriations or misuse could occur without a reasonable chance of detection. Ideally, workflows should be designed so that the work of one person is either independent of, or serves as a check on, the work of other persons.

5. Training to Distributors and effective monitoring of the distribution network

In terms of the IDD, insurance distributors are required to ensure that their staff and themselves obtain the necessary knowledge and ability through documented training and annual continuous professional development.

Some undertakings, especially those with a large TII network, need to closely monitor the activities of their TIIs even from a conduct of business perspective, given that as principals they are responsible for the activities of their TIIs.

6. Remuneration of Distributors

Factors such as the extent of compliance with the applicable regulatory requirements and the lack of complaints should also be taken into account when determining the amount of commission an undertaking pays its distributors.

7. The Product Approval Process

The responsibility of the approval of the product should remain with the Board of Directors of the manufacturer, which should, in turn, be in a position to engage with the persons responsible for the design of the product. This is to ensure that the product is sufficiently sound and suitable for its target market.

D. Expected Controls (applicable for Insurance Intermediaries)

1. Fair analysis

Insurance Brokers are required to act independently on behalf of the client. Accordingly, they should assess a fair number of similar products before identifying the one most suitable for a particular client.

2. Level of Disclosure

The level of disclosure and explanation of the product's features to clients' needs to be up to standard and in line with all the applicable regulatory requirements.

3. Product Distribution Arrangements

As distributors, insurance intermediaries are required to have in place product distribution arrangements (as part of their Product Oversight and Governance requirements). These should be drawn up in sufficient detail to clearly identify who within the entity is responsible for its implementation.

Section II Credit and Financial Institutions

A. Risks

1. Non-Financial Corporate loans

With respect to credit institutions, non-financial corporate legacy loans remain high, although improvements have been registered since the implementation of the Non-Performing Loans Reduction Plan requirement outlined by BR09/2019.

2. Technology Risk

In providing financial services, a number of credit and financial institutions are increasing their dependence on technology. This includes the use of biometric authentication, robo-advice, use of big data and machine learning processes (for example, for credit scoring), as well as cloud computing. Whilst providing credit and financial institutions with a number of opportunities, the use of such technologies may also be associated with potential prudential risks including legal risk, conduct risk, cyber security risk and third-party risk (particularly if external service providers are engaged). Specifically, in relation to Financial Institutions, in view of their business models and delivery channels, if not adequately managed, such risk could lead to a significant financial loss and security threats to data, the institution itself and customers.

3. Lifecycle and Business lines

A number of credit institutions rely on a limited number of business lines. Other banks are also at the initial stages of their life cycle. The business model of such banks is typically associated with a high degree of business model risk. The current market environment that is characterised by low and flat yield curves, tight credit spreads and a highly competitive market, puts pressure on the profitability of banks.

Similarly, a significant number of Financial Institutions are still at the growth phase of their business life cycle and may therefore be faced with difficulties in sourcing enough business to generate revenue that covers expenditure (high cost-to-income ratios). This search for business often exposes Financial Institutions to a higher risk.

B. Reoccurring Weaknesses

1. Credit Quality

In past years, regulatory authorities have continuously given attention to the issue of non-performing loans. This was one of the drivers which has led to a declining non-performing loans ratio in Malta. That being stated, pockets of vulnerabilities still persist.

2. Exposure towards residential real estate

A number of credit institutions have significant exposure towards residential real estate in Malta. Although currently there seems to be no indication of any material over-valuation in residential real estate prices, the regulatory Authorities have introduced borrower-based measures to strengthen the resilience of lenders and borrowers against the potential build-up of vulnerabilities which could result in financial losses both to lenders and borrowers stemming from potential unfavourable economic developments. The borrower-based measures came into force in July 2019.

3. Safeguarding of Funds (Financial Institutions)

In terms of PSD II and EMD II, as transposed in the Financial Institutions Act, Financial Institutions are required to safeguard funds received from customers and to ensure that these are not commingled with the institutions' own funds. In this respect, a number of Financial Institutions fail to provide the necessary assurances vis-à-vis the utilisation of adequate systems to ensure that such funds are safeguarded at all times and to carry out timely reconciliations.

4. Lack of adequacy of information provided (both written and verbal) to the customer and disclosures made by the bank branch representatives

A number of branch representatives of credit institutions are not always forthcoming in providing customers with information on the features and characteristics of the bank accounts that are being offered by the respective bank. At times, this information is only provided upon the customer's request, and in cases where this is provided, it is sometimes limited and therefore not sufficient to allow the customer to make an informed decision. Furthermore, certain credit institutions lack certain consistency in the information provided by their branches.

5. Knowledge of the bank branch representatives and training

Certain branch representatives, responsible for the distribution of the credit institution's products, do not always possess sufficient knowledge to enable them to reply to customers' requests and/or queries. Branch representatives, at times, have difficulties explaining matters, such as:

- the list of due diligence documents required to be submitted for the credit institution to be in a position to open a bank account. The list provided is, at times, inconsistent across the same credit institution;

- the difference between basic banking products, such as the difference between a 'Current Account', a 'Savings Account' and a 'PABF'.

6. Provision of information on the PABF

The PABF is not always being immediately offered to customers in all the branches of banks and, at times, it is only offered upon enquiry and request. In addition, when offered, a number of branch representatives are not always sufficiently knowledgeable to provide complete and correct information thereon.

7. Tariff of charges

In certain bank branches, no written information on the fees and charges applied by the credit institutions on their products is made available. The credit institution's "Tariff of Charges" is, at times, only being provided to the customer on request.

8. **Disclosures on credit institutions' websites**

Certain institutions' websites are not fully compliant with some requirements arising from the PAR, in relation to:

- the Glossary - a list containing at least the terms defined in the most representative services linked to a payment account as required under Regulation 9 of the PAR;

- switching Services - information about the switching service, including the role of each institution, time-frames for completion of each step, any fees that might be charged for the service, any information that will be requested from the client and the alternative dispute resolution procedures, as required under Schedule 3, paragraph 7 of the PAR;

- opening of a PABF – the website needs to provide detailed information about the process for the opening of a PABF and in addition to the list of documents which need to be submitted with the application, an application form should be included.

C. Controls which the MFSA expects authorised entities to have in place

1. Technology Risk

Given their dependence on technology, Financial Institutions should regularly assess their Technology Risk. In this respect they should inter alia ensure that IT frameworks adopted are in line with any applicable standards and best practices. Furthermore, institutions should closely monitor services offered by its service providers (outsourcing) to ensure that the level of service is up to the required standard. Financial Institutions should also regularly assess the integrity of their IT systems to minimise the risk of fraud or external attacks.

2. Credit Risk

Credit institutions should ensure continuous treatment of NPLs so as to ensure that the NPL ratio is in line with that of their European counterparts. Banks should also ensure that the credit standards are conducive to good credit quality to avoid the build-up of vulnerabilities resulting in adverse outcomes stemming from potential heightened levels of financial market instability or potential unfavourable economic developments.

3. Provision of Information to Customers

Credit institutions are required to ensure that:

- any customer-facing branch representatives are in a position to instantly provide to any customer approaching them, requesting information on the opening of a bank account,

detailed information, both written and verbal, on the features and characteristics of the different bank accounts available and being offered by the credit institution.

- IT systems in branches are duly updated to provide all the necessary information and documentation to branch staff. This can always be used as a support to help the branch staff in providing proper and correct information to customers.

- the credit institution's internal procedures should include a description of the information to be provided to customers, to ensure consistency in the information being provided to customers across the branch network.

- the information which is to be provided to customers should include, at least, information on the application process for the opening of a bank account, the Terms and Conditions, the Fee Information Document and information regarding the Depositor Compensation Scheme.

4. Adequate Training

Credit institutions are expected to:

- provide adequate and comprehensive training to all customer-facing branch representatives (including receptionists and cashiers). Such training must be provided on an ongoing basis and every time that there are any new developments, for instance, when new legislation coming into force or a new product being launched. It is strongly recommended that any training provided should be subject to an objective evaluation in order to ensure that the staff members completing the training fully understood the content of the training;

- keep record of the staff members completing the training.

5. Presentation of PABF

Credit institutions are expected to ensure that:

- credit institutions with a branch network in Malta of five or more branches, are required to present the PABF to all customers (even those of Maltese nationality) requesting information regarding the opening of a bank account;

- MFSA posters and leaflets providing information on the PABF (both in Maltese and English) are displayed in the credit institutions entire branch network prominently and in an area within the branches that is accessible by any customer entering the branch;

- the requirements and features of the account are explained in a correct way by the branch representatives. In this respect, credit institutions which are required to offer a PABF are to ensure to follow the requirements emanating from the PAR.

6. Tariff of Charges

The Tariff of Charges is a very important tool for the customer to take an informed decision. Credit Institutions are expected to ensure that:

- the Tariff of Charges should be made readily available by credit institutions in all the branches and made available to the customer, if so requested, on a durable medium, free of charge;

- the Tariff of Charges should also be made available on the credit institution's website. This is to be updated on an ongoing basis and every time that there are any amendments to the same;

- a copy of such document is always available in all the branches and this information is to be kept updated at all times;

- the customer is duly informed of all the costs which may be incurred when buying a banking product;

- institutions falling under the scope of the PAR are required to ensure that the above information is available on the respective websites, allowing the client to have a better understanding of the products available at, and being offered by, the institution. Moreover, institutions are required to ensure that any of the information required under the PAR is always kept updated.

Section III Securities and Markets

A. Risks

Within this section, risks are categorised in accordance with the type of authorised firm/sub-sector.

Investment (MiFID) Firms

1. Financial and Operational Risks

Depending on the MiFID service being offered, Investment Firms may be exposed to either financial risks, which may include: liquidity, market and counterparty risk, as well as operational-related risks, which may result from having inadequate internal processes and failures in relation to people or systems of the firm or from external events impacting the firm. Inadequate management of the relevant risks may result in risk of financial loss, risks of adversely impacting investors' interests and exposing the firm to reputational risk.

2. Market Event Risk: Market & Counterparty Risk – Forex firms

In view of the rapid and voluminous trades typically undertaken by MiFID firms that are specialised in providing online forex services, such firms would typically be more prone to market and counterparty risk, which could lead to unmatched trades and possibly negative equity, should there be a market event.

3. Online IT Systems

Investment Firms utilising online IT systems (e.g. platforms) have an additional inherent risk due to dependence on technology as well as their liquidity providers. Furthermore, the financial instruments which would usually be distributed using such platforms would be subject to more volatility. Weak business continuity processes exacerbate this risk even further, as disruptions can have an impact on businesses.

Recognised Fund Administrators

1. Transfer Agency - AML/ CFT Risk

Fund Administrators are typically engaged by CISs to carry out a number of transfer agency related tasks. These include, notably, the CDD of investors, handling transactions/monies in and out of the CIS and the maintenance of the shareholder register.

Fund Administrators play a critical role, acting as the point of contact between the investor and the CIS and provide the AML/CFT capability to the CIS in discharging its obligations. In view of this, the AML/CFT risk associated with fund administrators is considered to be higher than other service providers servicing CISs.

A lack of transparency of ownership and control associated with certain CIS structures can increase the risk for fund administrators in adequately determining the source and destination of funds. Furthermore, investors in funds may be wide-ranging, including PEPs, high net worth individuals and cash-based businesses. Furthermore, nominee investments can make it more difficult for one to be able to determine the ultimate beneficial ownership of invested funds.

2. Complex performance fees and commission structures

Complex performance fee and commission structures are on the rise, posing potential challenges to fund administrators when performing fund accounting activity and risking inaccurate calculations.

Investment Managers and Collective Investment Schemes (externally managed)

1. Financial and Operational Risks

Investment Managers may be exposed to either financial risks, which may include: liquidity, market and counterparty risk, and operational risks, which may result from having inadequate internal processes and failures in relation to people or systems of the firm or from external events impacting the firm. As stated, the mismanagement of risks could result in financial losses which adversely impact investors and the firm's reputation.

2. Valuation Risk

This risk relates to the possible incorrect valuation of underlying investments leading to an incorrect Net Asset Value and dealings, in turn resulting in incorrect allotment of redemption proceeds and share allocation in the case of subscriptions. This risk is even higher for hard-to-value/level 3 assets.

3. Risk Appetite of the CIS not being aligned with its Investment Risk Profile

This relates to the risk that the CIS's risk appetite, when it undertakes investments in certain asset classes/sectors, would not be aligned with the business model and underlying strategy of the scheme, as communicated to investors.

B. Reoccurring Weaknesses

1. Lack of conformity with the applicable legislative requirements (including in terms of documentation utilised by authorised entities), especially with MiFID II, AIFM and UCITS Directives and other relevant legislation.

2. Certain MiFID firms fail to make a clear distinction between the provision of advisory and non-advisory services. Such firms, when providing non-advisory services, are documenting such a service as execution only. Other firms are not fully satisfying the requirements when providing advisory services.

3. Proper identification/classification of complex instruments is not consistently being carried out by MiFID firms. Distribution and dissemination of complex financial instruments may therefore not be fully accurate.

4. Weak client onboarding and mis-selling practices - Investment advice and discretionary portfolio management services to retail clients may be prone to mis-selling risks. This risk is further exacerbated when firms have certain remuneration structures/packages which are not necessarily tied with the quality of service offered to consumers. Poor client onboarding practices and failure to implement adequate related processes and procedures (including in terms of systems), may expose firms to a wrong classification of clients and thereby increasing the risk of offering inadequate protection and products to clients. When assessing the client onboarding practices of certain Investment Firms during onsite inspections, it was noted that the Authority's observations highlighted during previous Client Fact Find thematic reviews, were, at times, not taken on board.

5. Weak Risk Management Function

   - when such function is not independent, there are, at times, insufficient and/or inadequate mitigating arrangements in place for the authorised entity to ensure that the function is nonetheless being undertaken effectively;

   - when such function is undertaken internally by the authorised firm, the appointed person does not always have the necessary authority and resources to perform his/her duties and to be able to challenge and question the Board accordingly;

   - when the function is undertaken via a secondment arrangement, or otherwise outsourced, there is, at times, either lack of monitoring of such outsourced function by the authorised firm, or the risk official is not granted with sufficient visibility in relation to the firm;

   - when the function is outsourced, at times, the risk management function would merely constitute the generation of risk measurement and risk reports, with insufficient engagement in advising the Board on risk-related matters;

   - operational risk not being given the necessary coverage in the risk management reports presented to the Board;

   - insufficient questioning by the Board on the technical data presented in the risk management reports;

   - no proper independent annual review to oversee the effectiveness and well-functioning of the risk management function and validating the firm's risk management practices;

   - the risk management and the internal capital adequacy assessment process (RMICAAP) of MiFID firms, is not always prepared in accordance with Title 2 Risk Management - Section 3 of Part B1 of the Investment Services Rules for Investment Services Providers;

   - a number of MiFID firms do not compile the risk calculation report correctly. Certain risks identified in the RMICAAP are being omitted from the risk calculation report;

- the RMICAAP of MiFID firms is not always signed by two directors, as stipulated in the Rules;

- several MiFID firms have capital requirements close to the regulatory thresholds, without having in place early warning mechanisms and/ or any contingency plan/s in case a shortfall occurs.

B.II Reoccurring Weaknesses [EMIR]

The below are reoccurring weaknesses which arise specifically from the outcome of supervisory work related to EMIR.

1. Procedures

A number of undertakings do not have a set of written procedures, which establish the processes carried out by the respective undertaking in order to be compliant with EMIR.

2. Delegation

Failure to keep in place the necessary documentation when delegating certain duties (such as an EMIR reporting delegation agreement) and related failure to conduct reasonable checks and requesting periodic confirmations to ensure that the delegated third-party is carrying out such duties in an accurate and timely manner, in accordance with the delegation agreement.

3. Risk Mitigation

Failure to implement risk-mitigating arrangements when entering into Over the Counter derivative contracts which are not cleared by a Central Counterparty Clearing Provider.

C. Controls which the MFSA expects authorised entities to have in place

Investment Firms

1. Identification of Conduct Risks and Controls

The MFSA expects Investment Firms to have a good planning strategy as well as adequate procedures and controls in place in order to ensure compliance with MiFID II requirements. Investment Firms must identify conduct risks and identify a sales strategy, which takes into account conduct issues in order to prevent and mitigate such risks. The Authority also expects that there is a robust due diligence process in place in order to adequately assess clients.

2. **Safeguarding of Clients' Assets**

In terms of MIFID II, when investment firms hold financial instruments belonging to clients, firms need to have adequate arrangements in place to safeguard the ownership rights of clients. Firms are expected in this regard to ensure that proper [i] segregation; [i] compliance oversight; [iii] reconciliation exercises; and [iv] choice of custodians, are maintained which will help in mitigating such risk.

3. Financial and Operational Risks

Investment Firms are expected to undertake a risk mapping exercise and assess the level of exposure to such risks on a periodic basis. It is critical that such an exercise captures all processes of the firm, which are linked to MiFID activities, and determines whether such risk is critical or otherwise for the firm by measuring probability that the relevant risk might occur.

MiFID firms are required to ensure that they have in place an effective risk management setup, policies and procedures to manage the risks that the firm is exposed to.

4. Market event risk: Market & Counterparty Risk – Forex firms

Given the large volume of transactions undertaken by these firms, and in view of the related risk of loss of either own or clients' monies, it is important that besides having in place appropriate risk management tools, a dealing desk is also maintained. This is in order to be able to continuously monitor such exposures.

Investment Managers (including externally managed Collective Investment Schemes)

1. Financial and Operational Risks

Investment Managers are expected to undertake a risk mapping exercise and assess the level of exposure to such risks on a periodic basis. It is critical that such exercise captures all processes of the firm which are linked to portfolio management related activities, and determine whether such risk is critical, or otherwise, for the firm, by measuring probability that the relevant risk might occur.

Full AIFMs and UCITS Management Companies are required to ensure that they have in place an effective risk management setup, policies and procedures to manage the risks that the investment manager may be exposed to.

2. Breach of Investment Restrictions

Investment Managers should ensure the implementation of a sound investment restrictions check process, including relevant processes and procedures and adequate systems covering such process.

3. Risk Appetite of a CIS not being aligned with the investment risk profile of the CIS

The Authority expects both the investment manager and a CIS's Board to fully understand and actively monitor the CIS's risk strategy and appetite and ensure that any investments and new business undertaken by the CIS are aligned accordingly.

4. Valuation Risk

Investment Managers (and CISs) are expected to:

i. before the launch of the CIS, ensure that the proposed valuation methodology is fully disclosed to investors;

ii. the Board of Directors also needs to be aware and have a good understanding of the proposed methodology in order to be able to know what to question in relation to liquidity as part of their fiduciary obligations on an ongoing basis;

iii. ensure that the valuation process is effective (including use of reliable pricing sources), and conflicts of interest are avoided or mitigated accordingly;

With regard to point [ii], Board members should exercise judgement with respect to what documentation of the valuation process they would like to have access to and to ensure that such documentation is providing adequate coverage for them to understand the methodology being used to value the assets.

In carrying out their valuation responsibilities, Board members need to be aware of the risks arising (such as valuation being obtained from a single source or counterparty, the reliability of data being provided for assets that are not exchange traded, use of models developed internally by the firm to undertake valuation, etc.) and assess what questions to raise during Board meetings in this respect.

Recognised Fund Administrators

1. Transfer Agency - AML/ CFT Risk

Recognised Fund Administrators need to ensure the adoption of comprehensive processes and procedures, and, to the extent possible, implement dual control on checks, invest in the training of staff undertaking such checks and make use of effective and reliable software tools to enable them to undertake CDD.

2. Complex performance fees and commission structures

Complex performance fee and commission fee structures in relation to CISs are on the rise, posing potential challenges to fund administrators when performing fund accounting activity.

Besides ensuring that appropriate systems that encapsulate such complex structures are in place, fund administrators need to ensure that staff are also adequately trained to understand such structures.

Section IV Trustees and Corporate Service Providers

A. Risks

1. AML/CFT risks

Trustees and CSPs are deemed to pose a high level of AML/CFT risk in view of certain ML/FT threats faced by the trusts and corporate entities set up or serviced by trustees and CSPs. That is, tax evasion, local criminal groups, drug trafficking, fraud and misappropriation, corruption and bribery, unlicensed financial services and terrorist financing. Often Trustees and CSPs lack sufficient awareness of these risks and threats leading to the unwitting possible use of trusts and corporate vehicles for ML/FT purposes.

B. Reoccurring Weaknesses

1. Lack of proper record keeping systems in place

Records relating to clients are not always retained in a centralised location, whether in paper or in soft copy format, and client-servicing directors/ staff members do not always have access to all records, which often also hinders the supervisory work of the MFSA.

2. Lack of proper systems in place to ensure segregation of assets

This is particularly important in the context of trustee service providers as one of the fundamental principles of trusts is segregation of the trust assets from the assets of the trustee and the assets pertaining to other trusts. It could also however be an issue for CSPs offering directorship services and therefore having control over the assets of the client company.

This issue arises, in particular, in relation to liquid funds, when there are instances where clients' monies are not appropriately segregated into separate bank accounts in respect of clients, or else pooled in a common clients' monies account, but are commingled with funds pertaining to the trust or company service provider.

C. Controls which the MFSA expects authorised entities to have in place

In this respect, Trustees and CSPs are expected to:

1. AML/CFT

- take a pro-active approach to increase their understanding of the threats and vulnerabilities posed by the structure which they are servicing and, based on that, develop proportionate and effective controls for the risks they face;

- use the National AML/CFT Risk Assessment and Strategy as well as any other sectoral risk assessment to drive risk appetite and internal business plans;

- develop a risk assessment methodology to ensure (potential) clients and their activities can be appropriately risk profiled, and consequently use the outputs to act as good gatekeepers to the financial system;

- maintain an up-to-date beneficial ownership database, and invest in technologies that ensure accurate collection of this information;

- collaborate with competent authorities to ensure practices are up-to-date with supervisory expectations on AML/CFT, including attending outreach workshops as relevant.

2. Record keeping

- ensure that all correspondence relating to client contact/introduction, onboarding of clients, client acceptance and all ongoing exchanges throughout the relationship are retained centrally;

- ensure that such records are readily available for inspection by the Authority as required.

3. Segregation of assets

- ensure that it has appropriate systems in place in relation to segregation of funds and assets;

- ensure that no clients' assets or clients' monies are commingled;

- ensure that, when any pooled clients' monies accounts are utilised by the service provider, proper reconciliations are kept.

Concluding Remarks

The reoccurring weaknesses that the Authority has identified, and continues to encounter, as part of its ongoing supervisory work, are a matter of high concern.

The MFSA's ability to protect the integrity of the Maltese financial services sector and consumers of financial services, rests on firms' ability and commitment to comply with their fundamental obligations. The Authority is therefore communicating, to regulated firms, its views on the expected standards with respect to core aspects of authorised business' operations.

As indicated at the outset, the Authority is aiming to increase the scrutiny of regulated operators in the industry. In the light of the various reoccurring shortcomings mentioned and the indicative guidance of expected controls, firms are strongly advised to review their internal control systems and procedures, to undertake a thorough and meaningful assessment thereof, and to proceed to take any corrective action to address possible identified deficiencies.

As part of such a process, regulated firms are expected to fully undertake an assessment and self-identify any action that is required to comply with the letter and spirit and the Authority's expectations as these emanate from this document. The MFSA will expect to see this on-going exercise as part of the onsite supervisory work that will be undertaken.

The Authority is committed to continue undertaking follow-up supervisory work in the future and expects to see that these initiatives have led to a factual increase in the robustness of setups and internal controls of authorised firms.

MALTA FINANCIAL SERVICES AUTHORITY

TRIQ L-IMDINA, ZONE 1, CENTRAL BUSINESS DISTRICT, BIRKIRKARA, CBD 1010

COMMUNICATIONS@MFSA.MT
+356 2144 1155

WWW.MFSA.MT