21 November 2024

Investment Services Supervision
Tel: (+356) 21441155

Dear Chief Executive Officer,

Dear Compliance Officer,

General Main Findings – 2022 / 2024 Supervisory Engagements ('Engagements')

You are receiving this letter as the Chief Executive Officer and Compliance Officer and/or the designated person responsible for the Compliance Function (the "Compliance Officer") of an Investment Firm supervised by the Malta Financial Services Authority (referred to herein as the 'MFSA' or the 'Authority').

BACKGROUND AND METHODOLOGY

As part of its mission, the MFSA's priority is to ensure that the highest standards of governance, risk management, culture and conduct are applied across the financial services market, contributing towards enhanced accountability, market integrity and transparency. As per Article 4 of MiFID II, an Investment Firm refers to any legal person whose regular occupation or business is the provision of one or more investment services to third parties and / or the performance of one or more investment activities on a professional basis. As at the end of July 2024, the MFSA regulated and supervised a total of 73 licensed Investment Firms and a further 7 credit institutions which also held an Investment Services Licence.

The Authority is committed to guiding the industry to ensure that all Investment Firms comply with the applicable rules governing investment services licensed entities., Our ultimate objective is to protect investors and uphold the reputation of the financial services sector in Malta. To this end, the Authority's supervisory activities are aimed at attaining high compliance standards within the supervised licensed entities through the use of diversified supervisory tools encompassing on-site interactions, as well as off-site desk-based reviews and ad-hoc engagements.

In this regard, the Authority utilises a risk-based approach, as part of its supervisory process, ensuring that the necessary supervisory resources are applied proportionately. Several factors are taken into consideration in the MFSA's risk dashboard, namely business model, financial information, capital adequacy, operational set-up, and internal controls.

In the period 1 July 2022 to 31 July 2024 the Investment Services Supervision Function within the MFSA performed a total of 26 engagements which represents circa 36% of the total population of Investment Firms (excluding credit institutions which hold an Investment Services Licence). These engagements proved highly effective as they facilitated fruitful dialogues between the Investment Firms and the Authority, enabling the discussion of pertinent issues and resolution of any inquiries. The Licence Holders selected for such engagements included a mix of both Class 2 and Class 3 Investment Firms. In preparation for the engagements, the firms were required to submit to the Authority specific documentation which *inter alia* included: i) Board of Directors' minutes; ii) Committee minutes; iii) compliance reports, iv) risk reports; (v) internal audit reports (where applicable); and v) Investment Firms Regulation (IFR) specific capital requirement calculations.

As a follow-up to the aforementioned engagements, and further to a thorough assessment of the documentation provided, the Authority has prepared this letter, which provides insight on the observations identified and highlights the Authority's minimum expectations from its Investment Services Licence Holders.

KEY FINDINGS

1. Governance and the internal control framework

During the course of the Meetings and Engagements held with the Board Members and from a review of the Board of Directors' Minutes provided, the MFSA officials were able to obtain a good understanding of the overall competence and level of engagement of Board Members. As expected, the Executive Directors were more familiar with the Company's business and the day-to-day operations, in view of their major involvement and presence within the business. Further to the review of the Board Minutes and discussions with Board Members, it was however noted that Non-Executive Directors appeared to provide limited interaction in the Board Meetings, in view that the Minutes had very limited reference to what was said and asked by the Non-Executive Directors.

While some Non-Executive Directors had a good understanding of the Investment Firm and its respective business model, we observed that others were less familiar with the Company's activities. Additionally, some Directors restricted their involvement to attending Board Meetings and did not engage in regular meetings or discussions with senior management, either at the time of their appointment or periodically thereafter, to gain a more practical understanding of the business and any potential challenges.

From a review of the Board Minutes and from the discussions held during the engagements, we noted that little or no reference at all was made to Sustainable Finance and Environmental,

Social and Governance factors ('ESG'). The importance of discussing ESG and taking it into consideration in its daily culture is discussed in further detail below.

Where applicable, we also reviewed the Investment Committee Minutes and found them to lack detailed information. Specifically, discussions on strategies, performance, and potential new investments were minimal. Furthermore, there was limited documented evidence of committee members challenging decisions or providing recommendations.

The engagements also served as an opportunity to discuss and assess the adequacy of the internal controls in place, including *inter alia* compliance and risk management functions which are discussed in further detail in separate sections below. Furthermore, it was noted that some Investment Firms lacked certain controls when it came to reconciliations, whereby some firms were not always adopting the approach of having the reconciliations signed by both the preparer and the checker and then subsequently by the compliance officer when they fell within their sample. We also came across situations when transactions were processed not utilising dual authorisation procedures. Another identified weakness was the lack of regular training on key topics at both the Board level and among lower levels within the Investment Firms. This included training on specific areas, such as the IFR/D mentioned in section 6 below, as well as compliance-related training.

Regulatory Requirement & Guidance

I. Corporate Governance Code
II. Guidelines on Internal Governance under Directive (EU) 2019/2034
III. Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU
IV. Regulation (EU) 2019/2088 on sustainability – related disclosures in the financial services sector
V. The nature and art of financial supervision volume vii
VI. Commission Delegation Regulation (EU) 2021/ 1253
VII. MFSA Circular on the amendments to the Investment Services Rulebooks to Transpose and Implement EU Directives, Regulations and EBA Guidelines.

Investment Firms are expected to familiarise themselves and implement the Corporate Governance Code and the EBA Guidelines on Internal Governance, as these provide insight on the composition, nature and operations of the Board and the internal controls expected to be in place and applied in a proportionate manner to the scale of operations of the Licence Holder. It is of vital importance that the Investment Firms' Board of Directors are robust and composed of a good mix of Executive and Non-Executive members who know the business and actively engage in ensuring the best interests of its stakeholders.

The EBA Guidelines on Internal Governance emphasise the critical role of the Board of Directors in ensuring sound and effective governance within investment firms. These guidelines aim to strengthen governance frameworks and foster a culture of accountability within investment firms. Key considerations include:

- **Roles and Responsibilities**: The Board must set the firm's strategy, ensure effective oversight of management, and promote a sound risk culture.

- **Composition**: The Board should have a balanced mix of skills, experience, and diversity to fulfil its responsibilities effectively. As mentioned above, Non-Executive Directors play a vital role in providing independent oversight.

- **Independence and Objectivity**: Directors must act in the firm's best interests, free from conflicts of interest, with clear policies to identify and manage potential conflicts.

- **Oversight and Accountability**: The Board is responsible for monitoring the firm's risk management framework, internal controls, and compliance with regulatory obligations.

- **Training and Evaluation**: Regular training is required to keep Board members updated on relevant laws, regulations, and industry practices. The Board's performance should also be periodically assessed to ensure effectiveness.

Moreover, the Authority issued the Corporate Governance Code (Enhancing the Governance, Culture, and Conduct of MFSA Authorised Entities) providing guidance on what is expected by an efficient and effective Board. *"Corporate Governance ensures the Board of Directors and Management are discharging functions effectively"* and that adequate systems for control and oversight are in place.

Whilst the Authority acknowledges that a number of Investment Firms are generally small in size, certain basic corporate governance principles are not the subject of proportionality. For instance the frequency of Board of Directors meetings, at least on a quarterly basis, in order to discuss a number of areas, namely general directions and strategies to adopt, the financial performance of the firm, the compliance, risk and anti-money laundering (AML) controls in place, the compliance and risk related work to be performed during the year and any other areas the Board would like to formally address.

The Authority also expects Investment Firms to have comprehensively detailed Board Minutes and Investment Committee Minutes, which provide a clear detailed overview and transparent summary of the discussions and contributions made by all attendees. This applies to any committee formed by the entity. As per 2.1.7.2.8 of the Corporate Governance Code, "*Board*

Minutes should provide a true and accurate record of discussions held, decisions taken and resolutions made".

Dissenting views should be clearly identifiable, as well as any actions assigned to individuals or committees, and the Minutes should allow external parties, such as MFSA officials or the auditors, a clear understanding of the Board discussions and who said what. It is recommended that the minutes are accompanied by a list of action points, possibly with tentative deadlines, which is updated and revised from one Board meeting to the next.

We further re-iterate the importance of fostering a Board comprised of members who actively challenge, scrutinise and question the operations and strategies of the Investment Firm they represent, whilst taking into consideration the implementation of sound corporate governance principles.

In this regard, independent Non-Executive Directors have a critical role to play both during Board Meetings, as well as in the oversight of control functions of the Investment Firms they represent.

Licensed entities are to be led and managed by an effective Board, who collectively ensure responsibility and accountability of the business. As per 2.1.2.1.3 of the Corporate Governance Code, the Board of an entity, "*where practicable, be composed of a combination of Executive and Non-Executive Directors including at least one Independent Non-Executive Director*". The composition of such a mix is aimed at ensuring that no member or group of members can dominate decision making, influencing the entity disproportionately.

As a general understanding, Directors are to possess a diverse range of knowledge, judgment, and experience to effectively fulfil their responsibilities and ensure all members are in possession of the relevant information to enable them to actively participate in discussions and decision-making processes. Together, they are tasked with supervising and evaluating daily operations, prioritising risk management, and maintaining transparency regarding the business model and operations.

We also take this opportunity to remind Investment Firms that as per Title VII (19) of the EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU, *"institutions should access the composition of the management body in its management and supervisory functions separately. The assessment of collective suitability should provide a comparison between the actual composition of the management body and the management body's actual collective knowledge, skills and experience…."*.

In this regard, we remind Investment Firms that the duties of the Board of Directors should be clearly defined, distinguishing between the duties of the management, executive directors and the supervisory non-executive directors, in a written document. Duties assigned to specific board members shall be clearly explained and documented.

Investment Firms are expected to give internal controls the necessary importance in a bid to ensure that the firms operate efficiently and within the required regulatory parameters. Internal controls should be in place to ensure that processes flow smoothly and operations are carried out efficiently and effectively.

These *inter alia* include areas such as training, resources for any additional staff identified as required to strengthen a function, or areas which need to be outsourced in order to ensure that the Investment Firm is operating in accordance with all the applicable regulatory requirements. Investment Firms are also to ensure that the four eyes principle is adopted for the majority of its checks and duties.

On a separate note, Licence Holders are reminded of the importance of sustainable finance, which is a fast-growing area in this field. We now expect that the Board delves into this matter and considers Environmental, Social and Governance ('ESG') factors as a recurring item of discussion, particularly when taking into consideration any ESG risks that may arise. Regulation (EU) 2019/2088, (the "SFDR") and most of its provisions have started applying as of 10 March 2021. In this regard, we highly recommend that Investment Firms refer to the MFSA publication entitled "The Nature and the Art of Financial Supervision Volume VII", as linked above, which is an initial study on sustainability – related website disclosures in terms of the sustainable finance disclosure regulation which provides insights as to what is expected by inter alia Investment Firms in this area.

Investment Firms should also refer to the Commission Delegation Regulation (EU) 2021/ 1253 amending Delegated Regulation (EU) 2017/565 and our Circular dated 23 May 2022 in relation to the integration of sustainability factors, risks and preferences into certain organisational requirements and operating conditions for investment firms.

2. Policies and Procedures

As part of our supervisory work, we reviewed the relevant policies and procedure manuals. While Directives, Rules, and Regulations outline the general requirements, it is the responsibility of the Investment Firm to ensure these requirements are implemented in detail, tailored to the firm's specific business operating model through its policies and procedures.

The manuals provided included, among others, i) compliance manuals, ii) conflicts of interest policies, and iii) governance manuals. While it is commendable that these manuals appear to be relatively customised to reflect the specific circumstances of the respective entities, most lacked detailed, step-by-step, user-level instructions on the processes and procedures staff are

expected to follow, particularly in critical areas essential for the Company's continued operations. To mention a few examples, these include the process of using the Company software to carry out trades, or a specific manual addressing the reconciliation procedures explaining different responsibilities, in what order these must be carried out, systems or tools being used, the output that one needs to provide as well as the approval that needs to be obtained.

Moreover, some of the procedure manuals did not include detailed reporting lines clearly detailing the responsibilities of key members of staff within the Investment Firm, which would provide employees with a clear understanding of the role of each person and who to report to when necessary.

Regulatory Requirement & Guidance

1. Part BI of the Investment Services Rules for Investment Services Providers
2. Corporate Governance Code
3. Guidelines on Internal Governance under Directive (EU) 2019/2034

Investment Services Licence Holders are required to have policies and procedures in place which *inter alia* provide details in relation to decision making. The management body should ensure a suitable and transparent organisational structure and should have a written description of it, specifying reporting lines and allocating functions and responsibilities accordingly. Staff are to be made aware of the procedures which must be followed for the proper discharge of their responsibilities.

Policies and procedures need to address various aspects of the firm and not just be limited to the operations side of the firm, and can *inter alia* include compliance, administrative, complaints handling, disaster and business continuity and accounting procedures as per R1-1.5.4.1 of Part BI of the Investment Services Rules for Investment Services Providers.

Furthermore, as per R1-1.5.1.1 of Part BI of the Investment Services Rules for Investment Services Providers, Licence Holders "*shall also ensure that the management body define, approve and oversee: i) the organisation of the firm for the provision of investment services and activities and ancillary services, including the skills, knowledge and expertise required by personnel, the resources, the procedures and arrangements for the provision of services and activities…..*".

As per section 2.1.1.2.7 of the Corporate Governance Code, the Board should *inter alia "establish appropriate policies and ensure that management has implemented appropriate procedures for the entity to maintain the highest standards of corporate conduct, including compliance with applicable laws, regulations and business and ethical standards. The Board should ensure that such policies and procedures are kept under review to ensure effectiveness."*

Firms are expected to have in place comprehensive, robust and updated policies and procedures covering all requirements emanating from applicable legislative and regulatory requirements. The absence of, or inadequate policies and procedures, as well as weaknesses in the necessary controls to ensure adherence therewith, may reflect poor governance practices adopted by the Investment Firm, which in turn may lead to failures in other aspects of the business. It is considered a good practice to review policies and procedures at a pre-determined frequency and at least on an annual basis.

Investment Firms should give importance on having detailed policies and procedures in place on all areas as these will allow its staff the opportunity to easily refer to the documents and allow them to understand what they are required to do and what is expected from them at all times. Policies and procedures should be considered as a stand-alone document in the case of succession planning. They should enable the Licence Holder to continue to operate with minimum interruptions in the case of departures of key personnel or absences. It is further recommended that there is a formal sign-off procedure in place whereby staff members will confirm that they have read the Company's respective policies and procedures.

We take this opportunity to remind Investment Firms that it is the Board of Directors who is ultimately responsible for the establishment of policies and procedures and for their respective updates and approvals.

3. Risk Management

3.1 Risk Management and Reports to the Board

During the course of the engagements, discussions were carried out with the Investment Firms' Risk Manager or the designated person responsible for overseeing risk within the Firm, in the absence of a functionally and hierarchically independent risk management function. In this regard, it was noted that the Firms did have risk policies in place detailing the specific risks they face and the impact this may have on the entity, by carrying out a risk assessment.

It was however noted that not all firms were preparing risk reports which are to be presented to the Board of Directors, on at least an annual basis, as stipulated in R1-1.5.4.3 of Part BI of the Investment Services Rules for Investment Services Providers. Risk reports should provide the board with a comprehensive understanding of potential threats and guide the effective allocation of resources to address and mitigate identified risks. These risk reports ensure that the board is informed and accountable for the Company's risk management practices, to make informed decisions, and guide the Company towards sustained stability. These can also help the board assess whether the Company's risk exposure aligns with its risk appetite and make necessary adjustments.

From a review of those firms who were presenting risk reports to the Board, it was noted that these were not always drawn up in the best standards and lacked certain details. A major finding noted was that emerging risks were not being brought to the attention of the board, and these may affect the Company's long-term strategy and analysis of market trends. All firms are obliged to monitor and manage risks, delving into all those risks which may affect their Company such as the loss of client monies, liquidity and counter exposure. Firms must also maintain comprehensive risk reports that offer thorough insights into the risks faced by the firm and the corresponding mitigation strategies in place.

Subsequent to the Meetings, and a review of the respective documentation provided, it was also noted that Risk was not always an Agenda item in the Board Meetings. It is the Board's responsibility to ensure that there are adequate risk management frameworks and policies in place and that the area of risk is given the necessary importance and formally discussed at every Board Meeting.

Regulatory Requirement & Guidance

1. Part BI of the Investment Services Rules for Investment Services Providers
2. Guidelines on Internal Governance under Directive (EU) 2019/2034

Investment Firms should have a sound, diligent and consistent risk culture and should be a key element of their effective risk management. This culture should enable Investment Firms to make prudent and well-informed decisions.

Risk management is considered as a very important safeguard and is to always be given the necessary importance. Investment Firms are to ensure that they maintain adequate policies and procedures designed to detect any risk of failure, at all times, and mitigate the risk identified accordingly. In this regard, Investment Firms should implement a risk register to ensure that risks are monitored and updated on an on-going basis and is therefore considered as a live document. Firms should develop an integrated and wide risk culture, based on a full understanding and holistic view of the risks they face. Furthermore, Investment Firms should develop a culture through policies, communication and staff training regarding the firm's activities, strategy and risk profile.

When determining the risks of an Investment Firm, the risk management framework should encompass all risks, including actual risks and emerging risks that the Investment Firm may be exposed to. All relevant risks should be captured in the risk management framework with appropriate consideration given to both financial and non-financial risks.

We take this opportunity to remind Investment Firms that they are to confirm on an annual basis, in the Confirmations tab of the audited MiFID Firms Quarterly Reporting, whether a Risk

Management Function is in place or whether a derogation was granted as specified in R1-1.5.4.6 of Part BI of the Investment Services Rules for Investment Services Providers.

Irrespective of the Class of the Investment Firm, risk reports are to be prepared and presented to the Board on at least an annual basis as per R1-1.5.4.3 of Part BI of the Investment Services Rules for Investment Services Providers. That said, it is strongly recommended that risk reports are circulated to the Board on a quarterly basis.

In view of the importance of having a thorough risk assessment carried out and risk reports presented to the Board in a timely, accurate, understandable and meaningful manner by all Investment Firms, the Authority also expects to see the very important area of Risk as an agenda item in Board Meetings and duly discussed.

3.2 Internal Capital Adequacy and Risk Assessment "ICARA"

The ICARA replaced the previous RMICAAP (Risk Management and Internal Capital Adequacy Process) and is to be prepared by all Investment Firms, with the exception of those which do not meet the conditions for qualifying as non-interconnected firms as per Article 24 of the IFD. The Authority requested and carried out a review of the ICARA reports for a number of entities for which an engagement was held with.

In this regard, the following were our main findings:

- The ICARA reports lacked thoroughness and did not offer detailed insights into the identified risks. Certain reports did not include the business risk culture and respective assessment of the risks to be considered, such as the i) risk identification and description, ii) risk estimation, iii) risk mitigation, iv) risk tolerance and evaluation, and v) risk recording, reporting and monitoring. Others lacked detail on the risk governance in place and specifically the three lines of defence in place.

- The ICARA reports lacked specific workings, namely those in relation to their own funds' requirements. In this regard, some reports did not provide detailed workings in relation to their permanent minimum capital requirements, fixed overhead requirements and K-Factor requirements.

- The stress testing scenario analysis were very limited in a number of cases and were at times only limited to one scenario. It is important to document the choice of stress test scenarios.

Regulatory Requirement & Guidance

1. Investment Firms Directive ("IFD")
2. Investment Firms Regulations ("IFR")
3. Part BI of the Investment Services Rules for Investment Services Providers
4. MFSA Circular 2 February 2022
5. MFSA Circular 22 August 2023
6. The Investment Firms Regulation and Directive – 7th Briefing
7. Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP).
8. Regulatory Technical Standards on Pillar 2 add-ons for Investment Firms

Investment Firms which do not meet the conditions for small and inter-connected Investment Firms, as set out in Article 12(1) of Regulation (EU) 2019/2033, shall have an ICARA in place and are required to ensure that the ICARA is detailed and includes granular detail and calculations accordingly. In this regard,

we expect to see specific details relating to *inter alia* i) the business model and strategy of the firm, ii) the three lines of defence adopted iii) details on the risks identified and the respective risk mitigation measures in place, iv) details on the prudential capital and liquidity including calculations, v) stress testing and vii) Scenarios leading to a firm to wind down which should include detailed estimates of the costs involved in the winding down of the Investment Firm. In this regard and where applicable, it is highly recommended that the scenarios are also taken into consideration when drafting the Company's respective recovery plan.

Furthermore, as communicated in our Circular dated 22 August 2023, the Authority is reviewing the Rulebook for firms to start requesting the submission of the ICARA document as part of the annual auditing reporting requirements stipulated in R1-2.2.1 of Part BI of the Investment Services Rules for Investment Services Providers as applicable.

Firms should also consider including additional stress testing scenarios to offer a more comprehensive understanding of potential outcomes in adverse circumstances, thereby ensuring that they maintain, on an on-going basis, the amounts, types and distribution of internal capital and liquid assets that they consider adequate to cover the nature and level of risks in accordance with Article 24(1) and (2) of the IFD. It is also recommended to consider reverse stress testing, as applicable, for instance in the case of an Investment Firm providing discretionary portfolio management services, to test whether the portfolio has enough liquidity to meet redemptions.

Accordingly, Investment Firms are required to assess whether the risks that the Company faces or poses to others is/are not sufficiently covered by the own funds' requirements, set out in Part Three and Four of the IFR. Those risks which are not addressed by any own funds' requirements

should be added in the Pillar 2. In this regard, the Authority will access the risks disclosed by Investment Firms and determine whether the own funds held provide sufficient coverage of risks to capital stemming from regulated and non-regulated business to which the Investment Firm is, or might be exposed to, or poses to others. The Authority can determine the additional own funds Investment Firms may be required to hold to cover risks the Investment Firm is exposed to or poses to others, that are not covered or not sufficiently covered by Parts Three and Four of Regulation (EU) 2019, 2033. Any additional own funds requirement should be always met by Investment Firms.

4. Conflicts of Interest

The Board of Directors is responsible for identifying, recording and appropriately managing conflicts of interest. In this regard, the Board of Directors is to ensure that the influence of third parties does not negatively impact the independent judgement of Directors.

During the course of the engagements held, discussions revolved around whether the Investment Firms carried out an assessment on what possible conflicts of interest may arise and what safeguards were in

place in order to mitigate any conflicts of interest. In this regard, most Investment Firms confirmed that they have a conflicts of interest policy and register in place. Moreover, in terms of Board conflict, it was confirmed that at the start of every Board Meeting, each Board Member was to declare any possible conflict they may have. As expected, there were also a few Firms who did not have a conflicts of register in place.

From a review of the conflict of interest policies provided, it was noted that whilst most firms did stipulate a number of situations which will result in a conflict of interest, some firms provided very limited detail in relation to the mitigation and conflicts prevention and management which was being applied to each conflict identified.

It was also noted that some Investment Firms, which had no conflicts of interest to disclose, had an empty register with no statement stipulating that no conflicts were identified during a particular calendar year.

Regulatory Requirement & Guidance

1. Part BI of the Investment Services Rules for Investment Services Providers
2. Corporate Governance Code
3. Guidelines on Internal Governance under Directive (EU) 2019/2034

4. Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU

Disclosing and managing possible conflicts of interest is imperative in ensuring good governance and in ensuring transparency. In this regard, the Board of Directors should ensure that the entity has in place and maintains an effective policy to identify, access, manage and mitigate or prevent actual or potential conflicts of interest that may arise. It is the Board who is responsible for the entity's conflicts of interest policy approval and oversight.

As indicated in the Corporate Governance Code, entities should have in place and maintain adequate internal alert policies and procedures to report on potential or actual conflicts of interest or breaches of the conflicts of interest policy. Investment Firms should have policies in place which also aim to identify conflicts of interest of staff, including the interests of their closest family members, as applicable. This shall also apply to those persons holding roles in control functions such as financial crime compliance managers and MLRO's, particularly where such persons occupy other roles that may give risk to conflicting interests. Moreover, entities should implement appropriate organisational measures to ensure conflicts of interest do not harm its clients' interests and should clearly document the measures adopted to manage conflicts of interest.

Conflicts of interest may vary significantly and may *inter alia* include the Investment Firms managers, employees and tied agents, or any person directly or indirectly linked to the Investment Firm by control

or between one client and another that arise in the course of providing any investment advice and ancillary service, or combinations thereof, including those caused by the receipt of inducements from third parties or by the Investment Firm's own remuneration and other incentive structures. It is therefore imperative that Investment Firms carry out a proper assessment of every potential conflict of interest and identify the course of action to mitigate and address a potential conflict. In the case where a conflict is repetitive and may jeopardise the operations of a certain role, the respective involvement of the individual shall be considered all together.

In terms of Board member conflict, it is highly recommended that Investment Firms refer to the Joint ESMA EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU and specifically Guideline 89 which lists down a number of situations it is presumed that a member of the management body in its supervisory function is regarded as not being independent. As a practice, Board member conflicts of interests' declarations should be listed as standard agenda items during Board and Committee meetings.

A register of all Directors and staff interests giving rise to conflict, should be maintained and should indicate the views taken by the Board regarding the conflict. As per 2.1.8.2.4 of the Corporate Governance Code, "*a register of all Directors' interests giving rise to conflict should also be maintained*" and updated every year, even when there are no conflicts to report during a particular year.

We would like to remind Investment Firms that if no conflicts of interest arise during a calendar year, it is strongly recommended to indicate in the register that no conflicts were identified during that period, rather than leaving the register blank. Although in general the Board remains responsible to manage conflicting situations, the Licence Holder may consider assigning a specific individual within its control functions to monitor conflict of interest situations.

5. Compliance

During the course of the engagements, the MFSA officials held high level discussions with the respective Compliance Officers and also carried out a review of the compliance related documentation such as compliance manuals, compliance reports and compliance monitoring programmes ("CMP").

Whilst we note that the Compliance Officers appeared to be familiar with their roles and responsibilities and were aware of the subject matter in question, we noted that some Compliance Officers were not very familiar with the Investment Firms Regulation and Directive ("IFR/D") and respective guidelines.

It was also evident that in cases where the Compliance Officer has been outsourced, the Compliance Officer lacked familiarity on the operational aspects of the Firm, which would raise questions on the adequacy of the compliance reviews carried out, particularly in terms of the CMP. In this regard, during the course of our supervisory work, the benefits of having an in-house Compliance Officer were clear.

It was clear that an outsourced Compliance Officer lacked the same level of knowledge, visibility, and expertise regarding the Investment Firm they were responsible for, compared to an in-house Compliance Officer who was dedicated solely to one firm.

From a review of the documentation submitted it was further noted that whilst some CMPs were drafted accordingly by *inter alia* documenting the: i) area to be tested, ii) the applicable rule, iii) a description of the requirement, iv) the test to be carried out, v) the frequency of the test, vi) a description of the findings and vii) recommendations, some of the CMPs lacked details and information on the checks carried out. Some of the CMP's reviewed did not always incorporate all the applicable compliance risk areas and further noted that some areas identified and

included in the CMP were not detailed enough with the relative actions to be tested being very limited.

When drafting the CMP, the Compliance Officers need to first ensure they are fully aware of the business model of the Company and the nature of the investment activities. Once that is properly understood, in order to draft the CMP, the Compliance Officer would need to clearly define the objectives and then address the scope in order capture the different areas to be covered by the CMP. The CMP helps firms identify, monitor, and manage compliance risks effectively. Key components of the CMP include risk assessment and prioritisation, where firms identify, assess, and prioritise compliance risks to focus on high-risk areas. This again requires the Compliance Officer and the senior management to hold discussions and see which areas of the business are most risky. This then ties into the services being offered, whether or not monies are being held, the manner in which the service is being provided, face to face or online, and the type of clients.

Moreover, monitoring activities should be both proactive and reactive, with clear documentation and regular reviews. In most cases, the CMP would be prepared similarly on a yearly basis, with Firms utilising a 'Calendar' type of report. Although this 'Calendar' report helps in ensuring Firms are compliant with submissions required under the respective regulations, this does not suffice as a CMP. The reporting per se would be considered as one area within the CMP or an annex within the CMP.

The CMP should include robust record-keeping and documentation practices, regular reviews for continuous improvement, and a process for regulatory engagement. Utilising appropriate technology and tools can support monitoring activities and ensure effective data management. The latter was another finding noted. I.T infrastructure and system-based tools have become a requirement to carry out general day to day business and it is therefore important that the Compliance Officer familiarises him/herself with the Company's systems in place, in order to properly oversee respective business operations.

Moreover, during certain engagements, it was also noted that Compliance Officers are not always provided with access rights to certain systems and reliance for information is placed on staff. This is a critical finding and the Authority expects that the Compliance Officer is provided access to all systems. It is then up to the Company's discretion whether or not access rights are read only or otherwise.

The compliance reports reviewed were generally detailed, and *inter alia* provided an overview of i) any breaches in the reporting period, ii) submissions made in the reporting period, iii) details on any MFSA regulatory updates, iv) sections relating to AML and risk; and v) correspondence with the MFSA. However, the compliance reports did not consistently include details on the compliance checks performed, the results of those checks, or any recommendations made by the Compliance Officer to the Board of Directors on how to address any identified deficiencies.

Clear and effective reporting and escalation procedures are essential to ensure that compliance issues are promptly communicated to senior management and the board, with well-defined escalation paths for significant concerns. Whilst we note that some Compliance Officers had other working papers to support their checks, at times, reference to these checks, their results and the respective working papers were not disclosed in the Compliance Reports presented to the Board of Directors, thus providing inconclusive updates.

Regulatory Requirement & Guidance

1. Part BI of the Investment Services Rules for Investment Services Providers
2. ESMA Guidelines on certain aspects of the MiFID II compliance function requirements
3. Guidelines on Internal Governance under Directive (EU) 2019/2034

Investment Firms should establish a permanent and effective compliance function to manage compliance risk and should appoint a person to be responsible for this function across the entire Investment Firm.

The role of a Compliance Officer is of vital importance and must operate independently to monitor and, on a regular basis, to assess the adequacy and effectiveness of the measures and procedures put in place and the actions taken to address any deficiencies in the Licence Holder's compliance with its obligations. Furthermore, the compliance function should advise and assist the relevant persons responsible for carrying out investment services and activities to comply with the Licence Holder's legal and regulatory requirements.

Compliance Officers are to ensure that their compliance manuals and CMP are updated and are considered as live documents. In this regard, any major changes to the CMP should be discussed and presented to the Board for consideration. This, in turn, proves effective compliance monitoring and oversight.

Investment Firms shall ensure that the work of the compliance function is adequately documented, in line with good corporate governance and record keeping practices. The ESMA Guidelines *on certain aspects of the MiFID II compliance function requirements* provide various information in relation to the compliance function and on what is expected by a Compliance Officer and delves into the responsibilities of the compliance function and the compliance risk assessment.

The ESMA Guidelines referred to above further highlight that the compliance function should ensure that compliance monitoring is carried out through a structured and well-defined compliance monitoring programme and that a compliance policy is observed. The findings of the compliance function should be taken into account by the management body and the risk management function in decision making processes.

The compliance function is to establish a risk-based monitoring programme on the basis of the compliance risk assessment with the aim to determine the compliance priorities and the focus of monitoring. The compliance risk assessment should set the work programme of the compliance function with the aim of allocating the compliance resources efficiently. The compliance risk assessment should be reviewed on a regular basis and when necessary.

The aim of the monitoring programme should be to evaluate whether the firm's business is conducted in accordance with the respective Rules and obligations. The risk-based approach to compliance should determine the appropriate tools and methodologies used by the compliance function and the respective frequency of monitoring activities, which may be recurring or ad/hoc.

The CMP needs to be detailed and delve into all aspects of the entity clearly documenting in detail the checks to be carried out and the respective findings. It is also considered as a good practice to circulate the CMP to the Board of Directors.

In this regard, for each area tested, it is recommended that the CMP provides, *inter alia:*

- a Risk assessment to identify the compliance risks;
- a description of the area to be tested;
- the relevant procedure explaining how such areas are tested;
- the findings and / or recommendations;
- the plan should explain how the overall operations and procedures will be tested and, if they are not tested within a specific period, a justification needs to be included; and
- the timelines of the testing period.

Compliance reports are suitable tools to warrant the necessary management attention. The reports should cover all business units involved in the provision of investment services and ancillary services provided by the Investment Firm. In this regard, Guideline 3 (28) of the ESMA Guidelines on certain aspects of MiFID II Compliance Function requirements lists down some of the information the compliance reports should include, such as *inter alia* i) information on the adequacy and effectiveness of the firms policies and procedures with the relative obligations and ii) a summary of the compliance function structure.

Compliance reports should be detailed and clearly document what checks have been carried out during the respective reporting period, including a summary of any on-site inspections or desk-based reviews carried out. The reports should also document a summary of major findings, breaches or deficiencies on

the tests carried out together with the compliance officer's respective recommendations. Moreover, compliance reports should formally document any important discussions ensued during the quarter period under review.

6. *Investment Firms Regulation / Directive (IFR/D)*

During the course of the introduction and subsequent implementation of the IFR/D, the Authority has over the years issued various IFR Briefings and published a series of Circulars on various aspects of the IFR/D such as those relating to: i) the classes of Investment Firms; ii) capital requirements and K Factors; iii) reporting requirements including the XBRL testing phase; vi) information on the various Implementing Technical Standards and ITS validation rules; and v) liquidity requirements. The aim of these Briefings and Circulars was to keep the industry updated on developments and provide guidance of what is required and expected in terms of *inter alia* capital and reporting requirements.

The engagements served as an opportunity to verify the knowledge of Board Members and the Compliance Officer on the IFR/D requirements. Some Licence Holder officials were aware of the requirements and familiar with the data reported and included within the EBA XBRL returns, others showed lack of knowledge on the subject, particularly when the compilation of returns was outsourced.

It was also further noted that some Compliance Officers were not involved in reviewing the EBA XBRL reports. The MFSA also came across situations when some Investment firms were unaware that they had to re-submit the EBA returns when the audited figures deviated from the submitted unaudited figures as per Article 2 (4) of the Commission Implementing Regulation (EU) 2021/2284 which states that *"Investment Firms may submit unaudited figures. Where audited figures deviate from submitted unaudited figures, the revised, audited figures shall be submitted without undue delay."*

As a result of this, the MFSA was not always being provided with the correct figures.

Regulatory Requirement & Guidance

1. Investment Firms Directive ("IFD")
2. Investment Firms Regulations ("IFR")
3. Part BI of the Investment Services Rules for Investment Services Providers
4. Commission Implementing Regulation (EU) 2021/2284

The IFR/D regime has now been in force since June 2021. Whilst we understand that the requirements which emanate from the respective Rules and Regulations may seem formidable, they are specific to Investment Firms, as compared to the previous requirements under the CRD and CRR. We therefore expect and encourage Licence Holders to ensure they familiarise themselves further with the requirements to ensure proper prudential oversight of the entities.

Regardless of the individuals responsible for preparing the EBA XBRL returns, it is expected that senior management, namely Board Members and the Compliance Officer are familiar with the requirements and can interpret the conclusions drawn from the respective XBRL returns. These returns provide a general oversight of the Company's main risks and respective capital to ensure safeguarding.

We take this opportunity to remind entities to ensure that when submitting the EBA returns, the data is factual, free of any misstatement or errors and that returns are duly re-submitted accordingly should the audited figures deviate from the unaudited figures submitted. In this regard, kindly refer to the latest Circular issued by the Authority on 22 January 2024, which provides further insight in relation to their submission.

Throughout these months, the MFSA has identified recurring data quality issues. It is pertinent to note that even though a submission may be reported as accepted by the EBA, Licence Holders are to download the submission report and ensure that there are no warnings. Should there be any warnings, Licence Holders are required to investigate the issue, clear the issue and resubmit accordingly. Going forward the MFSA will be carrying out further data quality checks. Any recurring data quality issues could lead to action from the Authority depending on the severity of the case.

7. Notifications and Approvals

During the course of the meetings, we came across instances when some Licence Holders were not aware of the requirements of when they are required to notify the Authority on specific circumstances and when the Authority's approval is required. As an example, we came across firms who were not aware of the requirement to notify the Authority of a change in shareholding or a change in registered address.

Regulatory Requirement

Investment Firms are to ensure that the necessary notifications are made as listed in R1-1.7.1 of Part BI of the Investment Services Rules for Investment Services Providers within the stipulated time frame and that the necessary approval is sought whenever required.

CONCLUSION

THE AUTHORITY'S EXPECTATIONS ON INVESTMENT FIRMS

The observations, findings and conclusions arising from the engagements conducted during the period 1 July 2022 to 31 July 2024 are being outlined in this letter with the aim and intention of sharing the key findings encountered and highlighting the areas we believe may be of interest to Investment Firms.

In general, the MFSA expects authorised Investment Firms to abide by high level of standards and corporate governance, and whilst acknowledging that certain rules are not granular, it remains the responsibility of the Board of Directors to introduce appropriate policies and procedures to ensure a robust corporate governance culture. Whilst the Rules and Regulations provide a high degree of proportionality, it is pertinent to understand that certain basic requirements shall be implemented, irrespective of the size, nature and complexity of operations. It is also critical to ensure that certain decisions are adequately documented and that an audit trail is kept within the Company's records in the interest of proper data governance.

We strongly advise Investment Firms to review and take note of this letter and identify those areas deemed relevant to your business operations. Subsequently, it is expected that your firm conducts a thorough gap analysis with respect to the practices, processes and procedures, followed by prompt action to rectify and address any identified deficiencies or shortcomings accordingly. Please be aware that it is the responsibility of all Investment Firms to fulfil their obligations in accordance with the respective requirements. In the future, the Authority may interact with individual Investment Firms regarding the issues outlined in this letter to verify compliance.

Should you require any clarification on the above, please do not hesitate to contact the Authority's Investment Services Supervision Function on investmentfirms@mfsa.mt.

Yours faithfully,
Malta Financial Services Authority

Christopher Peter BUTTIGIEG (Signature)
Digitally signed by Christopher Peter BUTTIGIEG (Signature)
Date: 2024.11.21 10:57:49 +01'00'

Christopher P. Buttigieg
Chief Officer Supervision

Doris (Maria Dolores) K/A Doreen BALZAN (Signature)
Digitally signed by Doris (Maria Dolores) K/A Doreen BALZAN (Signature)
Date: 2024.11.21 09:51:53 +01'00'

Doreen Balzan
Head Investment Services Supervision

(+356) 2144 1155
info@mfsa.mt
www.mfsa.mt

Malta Financial Services Authority
Triq l-Imdina, Zone 1
Central Business District, Birkirkara, CBD 1010, Malta