23 February 2026

To: The Management Body
The Compliance Officer/Person in charge of the compliance function

Thematic Review on Compliance and Internal Audit Functions of Management Companies of AIFs and UCITS funds

Dear Sirs and Madams,

You are receiving this letter as the Management Body and/or Compliance Officer and/or the person responsible for the compliance function of an Alternative Investment Fund Manager or UCITS Manager, including self-managed AIFs and UCITS (collectively referred to as "**Management Company/ies**"), falling within the supervisory remit of the Malta Financial Services Authority (the "**MFSA**" or "**Authority**").

BACKGROUND

The MFSA will continue to prioritise its supervisory activities on ensuring that authorised entities maintain robust second and third lines of defence through effective internal controls, governance, and risk management frameworks supported by strong internal controls, sound governance and robust risk management frameworks. This is to ensure that Management Companies carry out their activities in a prudent and orderly manner, that the first line of defence operates effectively and in compliance with regulatory requirements and that applicable licensing conditions are met in the best interests of investors.

In this context, and as part of the Common Supervisory Action on Compliance and Internal Audit Functions launched by the European Securities Market Authority ("**ESMA**") in February 2025, the MFSA carried out a thematic review to assess the adequacy of control functions of Management Companies.

The MFSA assessed compliance with the requirements laid down in Directive 2009/65/EC ("**UCITS Directive**") and Directive 2011/61/EU ("**AIFMD**"), as further transposed in Part BII of the Standard Licence Conditions applicable to Investment Services Licence Holders which qualify as UCITS Management Companies, Part BIII of the Standard Licence Conditions applicable to Investment Services Licence Holders which qualify as AIFMs, Appendix VIII to Part BII of the Standard Licence Conditions

applicable to Retail Collective Investment Schemes and Part B of Standard Licence Conditions applicable to Alternative Investment Funds ("**the Rules**").

METHODOLOGY

The MFSA circulated a self-assessment questionnaire (the "**CSA Questionnaire**") to a pre-selected sample of Management Companies covering approximately 16% of the total population.

A number of respondents within this sample were also identified to be in scope of a thematic supervisory meeting, enabling the MFSA to obtain a more detailed understanding of their policies, procedures, systems and controls. In addition, follow-up supervisory interactions were also held with all Management Companies after the submission of the CSA Questionnaire to obtain further information or clarifications.

The purpose of this Dear CEO letter is to communicate the Authority's main findings and observations along with its supervisory expectations and any resulting recommendations in relation to the Compliance and Internal Audit functions. However, please note that this communication should not be interpreted as a complete and exhaustive review of all requirements, arising from the applicable regulatory frameworks.

KEY FINDINGS AND OBSERVATIONS

1. COMPLIANCE FUNCTION

1.1. Compliance Function Responsibilities

General Comment

Management Companies are required, taking into account the principle of proportionality, to establish and maintain a compliance function that operates with an appropriate degree of independence from the business and other control functions. The Authority notes that, in certain cases, independence may be constrained where the same individual performs multiple roles, however in such circumstances, adequate controls to mitigate conflicts should be implemented to ensure effective challenge and preserve the ability of the compliance function to escalate material compliance matters, including disagreements with other functions, to the Board without undue influence. Clear reporting lines should also be in place when it comes to reporting critical information to the Board and the MFSA, as necessary.

1.1.1. Policies and Record Keeping

Observations

Based on a review of the compliance policies and procedures provided during the course of the thematic review, the MFSA Officials noted that the escalation of breaches and follow-up of open compliance issues were not always properly documented.

In particular, a number of Management Companies had either not established a formal breaches escalation procedure or had procedures in place that did not clearly define how disagreements or unresolved compliance issues between the compliance function and other functions were to be escalated, monitored and resolved. In such cases, the Authority noted a certain reliance on informal communication rather than on a clearly defined and structured internal escalation framework.

Expectations

With respect to policies and procedures, SLC 2.03 of Part BII of the rules applicable to UCITS Management Companies, SLC 1.26 of Part B of the rules applicable to AIFMs, SLC 16.7 of Part BII of the rules applicable to self-managed UCITS and SLC16.18B of Part B of the rules applicable to self-managed AIFs require Management Companies to establish, implement and maintain policies and procedures, which are adequate to enable the detection of any risk of failure to comply with their obligations.

Management Companies are reminded that absence of clearly outlined escalation procedures for breaches or other compliance deficiencies may impede their timely identification, reporting and establishment of remedial actions, potentially resulting in delayed resolution and closure of such issues.

Furthermore, policies and procedures as well as systems and internal controls should be reviewed regularly and at least on an annual basis with a view to reflect new regulatory developments and changes in the organisation's nature, scale and complexity of its operations.

1.1.2. Conflicts of Interest ("COI")

Observations

The MFSA further identified cases where policies were outdated, noting in particular, that the Conflicts of Interest Register was not maintained as a dynamic document. New conflicts arising after the engagement of relevant persons were not always recorded in a timely manner, and in some cases the details of identified conflicts were either unclearly defined or not documented at all.

Additionally, such registers often lacked sufficient detail regarding the specific mitigating measures implemented to manage and, where possible, prevent identified conflicts.

Expectations

Management Companies should ensure that the COI policy is updated and reflects current activities. Reviews should be carried out regularly, at least annually. Furthermore, logs should be updated promptly whenever new conflicts are identified or existing conflicts change. Each conflict should be clearly and sufficiently

documented, specifying, at a minimum, the nature of the conflict, the parties involved, when the conflict has occurred and identified, affected roles or functions and any related financial, personal, or professional interests.

In addition, mitigating measures should be in place for each identified conflict and how such measures are implemented and monitored to ensure effective management and, where possible, prevention of conflicts. It is also a good practice to include conflicts of interest as a standard agenda item during Board and Committee meetings.

1.1.3. Training

Observations

In a number of instances, Management Companies had not implemented a coordinated and structured internal compliance training programme. As a result, officials were not consistently provided with training on relevant local and international regulatory developments, nor on their individual responsibilities in relation to regulatory compliance.

The Authority also observed that certain compliance reports were found to be incomplete, lacking significant compliance related information, such as breaches related to investment and borrowing restrictions and material valuation errors exceeding 0.5% of NAV.

Expectations

A lack of adequate training opportunities to officials directly engaged in day-to-day activities on regulatory developments and any applicable changes internal policies and procedures may increase eventual risks of non-compliance. Management Companies are therefore encouraged to ensure that regulatory changes and updates to policies and procedures are communicated to the operational stuff via appropriate training in a timely manner.

1.1. Compliance Monitoring

Observations

In the context of the monitoring role of compliance functions, the MFSA has identified a few deficiencies. In particular, it was noted that in some cases the compliance

monitoring plan ("CMP") was not supported with a clear risk assessment of all relevant business activities nor with an assessment of the effectiveness of internal policies/procedures to mitigate identified risks. Consequently, compliance monitoring activities, as well as the frequency of compliance checks, were not clearly set based on their inherent and residual compliance risks, resulting in a lack of comprehensive and risk-sensitive compliance monitoring plans. Moreover, compliance monitoring checks and testing methodologies were not always clearly defined.

Nearly half of the Management Companies omitted certain business activities and regulatory obligations as part of their monitoring activities. For example, the Authority found no evidence that the Management Companies authorised to passport their services abroad had reviewed their cross-border activities on a regular basis to confirm alignment with the passporting notifications and regulatory obligations in that Host Member State. Similarly, no checks on the Management Company's websites and marketing material were found to be carried out to ensure that these were accurate and updated as per the latest compliance approval. Likewise, checks on delegated functions, cyber-security and sustainability risks and disclosures were either omitted or only partially covered in the CMP.

Additionally, the MFSA noted that some entities relied predominantly on a reactive approach to assess and monitor deficiencies and breaches which could result in certain compliance deficiencies either not identified at all or identified with a substantial delay.

The MFSA also noted a lack of adequate documentation of remediation plans, as well as insufficient records of testing carried out under the CMP. In several cases where deficiencies have been identified during compliance monitoring, no formal remediation plan was drawn up with clear recommendations and timelines for remedial actions. In other instances, the remedial actions were not followed up and closed in timely manner.

Expectations

The effectiveness of internal control arrangements should be underpinned by a thorough and ongoing assessment of the nature and magnitude of the risks, to which they are exposed to.

Management Companies are, therefore, encouraged to adopt and maintain a clearly articulated risk-based approach to compliance monitoring. To this end, the CMP should be supported by a documented and sufficiently granular compliance risk assessment, which should form the basis for determining the scope, frequency and prioritisation of compliance monitoring and oversight activities across all operational activities, including ancillary services as well as delegated and cross-border activities as applicable.

While the principle of proportionality may be applied, any decision to focus the CMP on selected areas only must be appropriately justified. Such justification should not be based solely on proportionality considerations but should also clearly demonstrate the relevance of the selected areas to the business activities and, in particular, reflect the level and nature of the compliance risks identified. Areas assessed as higher risk or of greater regulatory significance are expected to receive commensurate attention within the CMP. A holistic long-term plan should be devised ensuring that all risks that the Management Company is exposed to are mitigated.

The outcomes of the compliance risk assessment are expected to be used to set the work programme of the compliance function, ensuring that adequate resources are allocated in a manner that is proportionate to the nature, scale and complexity of activities.

Compliance functions are further expected to review their compliance risk assessments on a regular basis and, where warranted, also on an ad-hoc basis, particularly where there are material changes to the business model, organisational structure, delegated arrangements or the applicable regulatory framework. When heightened risks are identified, the compliance risk assessment and the corresponding CMP should be updated to ensure that the objectives, focus and the scope of compliance monitoring remain appropriate, effective and aligned with supervisory expectations. Compliance functions should be able to pre-empt, rather than react to compliance issues and to ensure that additional operational and reputational risks or extra costs for investors are avoided. Compliance functions should have the necessary support, expertise and authority to carry out the compliance functions effectively.

Remediation plans are also expected to be developed, ensuring that a root cause analysis of any non-compliance matter is performed and internal controls and

procedures are properly updated. Separately, targeted training or any other identified mitigating measures should be taken to prevent recurrence of non-compliance.

1.2. Oversight of the Board

Observations

The Authority notes that the Board minutes did not consistently reflect discussions on the compliance reports or other significant updates, including the progress of the monitoring activities carried out by the compliance function. In several cases, key compliance or governance related discussions were discussed verbally between the Compliance officer and the Board but were not properly documented, impairing an audit trail of relevant decisions taken. Moreover, follow-up on identified compliance deficiencies by the Board was in some instances delayed, resulting in prolonged unresolved compliance matters.

The MFSA also noted instances where Boards were not provided with progress reports from the compliance function on its compliance monitoring activities.

One Management Company confirmed that documents before Board meetings are circulated without a password or any other encrypting measures, potentially exposing the Management Company to data breaches.

Expectations

The Authority reminds Boards of their ultimate responsibility for the overall direction and strategy of the Company, as well as for ultimately ensuring compliance with the applicable regulatory requirements. Boards are encouraged to play a proactive and prominent role in ensuring that all regulated business activities are carried out in line with the applicable regulatory requirements.

Management Companies are required to maintain adequate records, including Board minutes that accurately and comprehensively reflect discussions held, decisions taken and resolutions made concerning their authorised business activity. Where key compliance or governance discussions occur outside formal Board Meetings, these should be duly recorded and documented, to preserve a clear audit trail.

It is considered best practice for compliance reports to be circulated to the Board on a quarterly basis. These reports should, at a minimum, outline the checks conducted by the compliance function, highlight any findings or breaches, provide recommendations or proposed remedial actions, include annexed reports from onsite or offsite assessments and summarise any escalated compliance issues along with the required follow-up measures.

1.3. Delegated compliance functions

Observations

The Authority noted that, in a number of instances, Management Companies exercised limited oversight over delegated compliance functions. In particular, certain companies lacked a structured process in place to ensure that the performance of delegated compliance function was regularly reviewed and documented, as required under SLC 4.01(c) of the rules applicable to UCITS Management Companies and SLC 4.01(f) of the rules applicable to AIFMs.

Management Companies are required to maintain effective oversight of delegated compliance functions, ensuring that the service provided is up to the required standards and applicable regulatory standards. Adequate contingency arrangements to address the potential termination of delegated compliance services should also be established. In practice, in some cases these expectations have not been fully met. For example, the Authority noted cases where the early termination of a delegate's service agreement, arising from a disagreement with the Management Company, occurred without sufficient handover or arrangements for a replacement compliance officer, resulting in an interruption to the continuity of the compliance function.

Expectations

Management Companies shall be responsible for deciding on, adopting and implementing all the arrangements and organisational decisions which are necessary to ensure compliance with the applicable rules and obligations.

Management Companies remain fully responsible for the performance of delegated compliance functions and should implement robust procedures to manage any transitions between individuals occupying the role of Compliance Officer effectively, ensuring that their regulatory obligations continue to be met without interruption.

In the event of the resignation or unavailability of a delegated Compliance Officer, Management Companies should ensure that adequate contingency plans are in place to maintain continuity of the outsourced compliance function. This includes taking timely steps to appoint a replacement before the effective date of resignation or ensuring that alternative interim arrangements are in place to avoid gaps in carrying out compliance tasks.

Such safeguards should also include clear communication lines between the outsourced Compliance Officer and the Board of ongoing and pending compliance checks, as well as proper documentation and handover of ongoing compliance activities.

2. INTERNAL AUDIT FUNCTION

Observations

In cases where an Internal Audit function was in place, the MFSA noted that, the internal audit plan was not always treated as a dynamic document, with limited tracking of whether planned tests were carried out or delayed.

Moreover, a number of the entities falling within the scope of this thematic review reported having a derogation from establishing a separate and independent Internal Audit function. In such cases, the MFSA noted very limited detail on the alternative arrangement in place to compensate for the absence of independent assurance by an Internal Audit function, such as a Board-approved internal audit plan or ad-hoc thematic reviews of key operational areas. This raises concerns regarding the robustness of internal governance and the effectiveness of the second line of defence in monitoring and challenging risks and controls.

Expectations

The Management Company' Boards are reminded that internal audit function plays a crucial role by providing independent internal oversight, evaluating and improving the effectiveness of the entity's risk management, internal controls and governance processes.

Therefore, in the absence of an independent internal audit function, the board should ensure that alternative arrangements are in place that provide sufficient assurance and oversight, equivalent to ones typically coming from an internal audit function but on a smaller scale. In particular, the Authority expects that an internal audit plan is in place and approved by the Board, ensuring that ad-hoc thematic audits on key operational areas are carried out. To ensure the independence of the reviews performed, Management Companies may also rely on outsourced independent experts in targeted areas.

Internal Audit Functions are also expected to document which areas were completed, enabling them to track the remediation of the findings identified and report progress to the Board on a regular basis. If, following a risk assessment exercise, it has transpired that a particular area has become riskier, it is expected that the frequency is adjusted to cover all the material risks adequately. The rationale behind such an adjustment should be documented and presented to the Board for approval. Once the internal auditor is satisfied that a finding has been addressed and the corrective actions implemented, the status or score of the finding should be updated to reflect its remediation.

CONCLUSIONS

The findings arising from the CSA exercise are being highlighted in this letter with the aim of sharing best practices within the asset management industry and drawing attention to potential weaknesses identified in relation to the Compliance and internal audit oversight processes.

In this regard, the Authority wishes to highlight that amongst the key areas of improvements identified during this Review, Management Companies should focus on properly capturing all critical aspects of business operations within its compliance monitoring activities, assessing the level of Board of Directors oversight, adequate documentation of ongoing monitoring checks as well as the establishment of clear follow-up processes for open compliance concerns.

The Authority would also like to emphasise the importance of the timely rectification to the compliance deficiencies, for which clear mitigating measures and timelines shall be established. Management Companies are reminded that the Board of Directors remains ultimately responsible for ensuring compliance with all applicable rules and obligations. Delegating tasks to service providers does not transfer this

responsibility. The Board should ensure that appropriate oversight, controls, and governance are in place, and that its fiduciary duties to the investors of the funds under management are fully met. Although the nature, scale and complexity of operations should be carefully considered, certain basic requirements need to be implemented in order to ensure not only compliance with regulatory requirements, but more importantly, the sustainability of the business.

All Management Companies are expected to conduct a gap analysis based on the findings and recommendations of this review. This analysis should be documented and made available to the Authority upon request and may be subject to verification during future supervisory engagements. Management Companies should take necessary steps to align their processes, policies, and procedures with the MFSA's expectations using a proportionate approach based on their nature, size, and complexity.

For any clarifications or further guidance on the contents of this Dear CEO letter, Management Companies are encouraged to contact the Authority.

Yours sincerely,

Christopher P. Buttigieg
Digitally signed by Christopher P. Buttigieg
Date: 2026.02.23 19:02:26 +01'00'

Dr Christopher P. Buttigieg
Chief Officer Supervision

Ian MELI (Signature)
Digitally signed by Ian MELI (Signature)
Date: 2026.02.23 19:09:02 +01'00'

Ian Meli
Head – Investment Services Supervision

The MFSA ensures that any processing of personal data is conducted in accordance with Regulation (EU) 20161679 (General Data Protection Regulation), the Data Protection Act (Chapter 586 of the laws at Malta) and any other relevant European Union and national law. For further details, you may refer to the MFSA Privacy Notice available on the MFSA webpage www.mfsa.mt.