MFSA MALTA FINANCIAL SERVICES AUTHORITY

14 September 2026

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

**Outcomes-Based Review on Outsourcing (including by way of secondment) by Fund Managers, self-managed schemes authorised as AIFs, UCITS and PIFs (collectively referred to as "Fund Managers"), of the critical functions of investment management, risk management, valuation, compliance, AML and internal audit (where applicable)**

**Dear Management Body and Compliance Officer,**

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

**BACKGROUND AND METHODOLOGY**

As part of its supervisory mandate, the MFSA conducts supervisory interactions to assess the compliance of regulated entities with relevant laws and regulations.

This Outcomes-Based Review assessed the extent Fund Managers comply with the requirements of the Alternative Investment Management Directive 2011/61/EU (AIFMD) and the Undertakings for Collective Investment in Transferable Securities Directive 2009/65/EC (UCITS Directive), as amended by Directive (EU) 2024/927, and as transposed in the applicable investment services rules, in terms of outsourcing. The Outcomes-Based Review also aimed to assess the level of adherence with internal processes with respect to *inter alia* the decision-making process as to which function is to be outsourced, the selection process of an outsourced service provider including the due diligence undertaken and the ongoing oversight of such outsourced service providers until the termination of the relationship ("the outsourcing process life-cycle").

Outsourcing is a critical risk area that Fund Managers must carefully manage to ensure smooth operations and protect investors' interests. Many Fund Managers outsource critical functions such as, portfolio management and risk management to third-party service providers in order to reduce costs and benefit from specialised professional expertise. While outsourcing can improve efficiency and allow Fund Managers to focus on core investment activities, it also introduces significant risks that must be managed diligently. These risks include operational failures, data security breaches, inadequate level of service, regulatory non-compliance, and business continuity issues if the service provider is somehow unable to perform as expected.

Fund Managers remain fully accountable for outsourced activities, even though the tasks are performed by external parties. Therefore, robust documented due diligence before selecting service providers is essential, along with clear contracts, defined service-level agreements, and ongoing monitoring of performance. Effective oversight helps ensuring that outsourced functions meet regulatory requirements and maintain high standards of accuracy and reliability. In addition, firms must have contingency plans in place to manage disruptions or terminate outsourcing arrangements if necessary for any reason. The Authority acknowledges that under the appropriate conditions, including pre-appointment checks on the chosen service provider, outsourcing provides expertise in the case of small Fund Managers.

To assess the adequacy of outsourcing arrangements, the Authority carried out this Outcomes-Based Review on a sample basis and covered approximately 16% of the authorised Fund Managers. The reviews were held throughout 2025 in three phases:

i) The first phase involved the collation of information through a self-assessment questionnaire to all selected Fund Managers with a definite period of time given to submit their responses.

ii) The second phase comprised a review of the responses and any supporting documentation provided, such as:
   - the outsourcing policy;
   - due diligence undertaken on outsourced service providers; and
   - minutes of board meetings where outsourcing was discussed.

iii) In the third and final phase, the Authority carried out an on-site interaction with a number of respondents where interviews with key officials, such as the governing body and the compliance officer were held.

During the review, the Authority aimed to focus on the following key areas:

- Actions taken prior to the appointment of the outsourced service provider
- Regulatory implications of outsourcing
- Conflict of interest that arises from outsourcing arrangements
- Initial and ongoing due diligence on the outsourced service provider
- Reporting obligations
- Contingency planning

The purpose of this 'Dear CEO' letter is to share the main findings of the Outcomes-Based Review, as well as to communicate the Authority's expectations and any recommendations related to the area of outsourcing. Therefore, this communication should not be construed as a complete and exhaustive review of all requirements arising from the applicable regulatory frameworks.

**KEY FINDINGS**

## 1. Pre-selection criteria for outsourced service providers

*Observations*

Based on a review of the replies, we note that while most Fund Managers have an element of pre-selection criteria for outsourced service providers, these frameworks are often not tailor-made to the operations and business model of the respective Fund Manager, and in practice rely on informal processes. In several instances, Fund Managers referred to high-level outsourcing policies containing broad, all-encompassing criteria, which provide limited practical guidance on how providers should be consistently evaluated or compared. This is further compounded by gaps in the depth and scope of information gathered, with some Fund Managers focusing disproportionately on specific areas such as operational risk, while giving limited or no attention to other critical elements.

In particular, assessments of a provider's operations are often of a high-level nature without delving sufficiently into key operational risk sub-categories, such as cyber security, information security, data protection, business continuity and disaster recovery, which are instead analysed under general criteria rather than evaluated independently. Additionally, most responses indicated a lack of differentiation in the application of criteria based on the criticality of the outsourced function. Similar approaches were applied irrespective of the potential impact on licensable activities or regulatory obligations in the event of a failure by the outsourced service provider.

As a result, risks associated with outsourcing critical functions such as investment management or risk management may not be adequately identified or assessed at the pre-appointment stage. This lack of detailed risk-based assessment, increases the likelihood of inconsistent decision-making and may expose Fund Managers to significant operational and regulatory risks, suggesting that existing pre-selection frameworks are not always aligned with regulatory expectations.

*Expectations*

Having documented pre-defined selection criteria and a clear understanding of the information to be obtained from prospective outsourced service providers is critical for Fund Managers, given the operational, regulatory, and reputational implications that outsourcing key functions has. The Authority expects Fund Managers to implement a structured, risk-based, and properly documented pre-selection process that ensures the suitability of service providers throughout the lifecycle of the outsourcing arrangement. This includes clearly defining the functions to be outsourced, distinguishing between critical and non-critical activities, and establishing objective and proportionate criteria aligned with regulatory expectations, industry standards, and best governance practices.

Robust pre-defined criteria provide the foundation for a consistent, transparent, and well-informed selection process, reducing reliance on ad hoc or subjective decision-making and ensuring alignment with the Fund Manager's strategic objectives and risk appetite. They also enable Fund Managers to identify in advance the essential capabilities and characteristics required for the outsourced activity, such as appropriate authorisation and regulatory standing, financial soundness, technical expertise, operational resilience, governance frameworks, and experience with similar funds or asset classes. The competence of the appointed service provider shall satisfy the required expertise in the context of the nature, operations and investment strategy of the fund.

In this context, Fund Managers should obtain comprehensive and comparable information from potential providers, including details on organisational structure, key personnel, internal controls, risk management frameworks, data protection and cyber-security measures, business continuity planning, sub-delegation arrangements, and conflict of interest management. In addition, the Fund Manager shall carry out checks to ensure that the service provider is of sufficient repute and integrity.

Fund Managers should assess whether the provider has sufficient and competent personnel to meet current and anticipated business needs, maintains strong internal controls and governance arrangements, and is able and willing to grant appropriate audit and access rights to support ongoing oversight. Clear exit and termination arrangements should also be in place to ensure the orderly transfer of outsourced functions without disruption to operations, funds under management, or investors. Establishing such structured criteria and information requirements not only strengthens due diligence and enables like-for-like comparison of providers, but also enhances efficiency, reduces delays in sourcing or replacing providers, and supports the Fund Manager's ability to demonstrate to the competent authority that outsourcing decisions are well-taken, consistent, and compliant. Overall, these elements form the cornerstone of a robust and effective outsourcing framework.

## 2. Distinction between 'in-house' and 'outsourced' function

*Observations*

An element that was observed among nearly all Fund Managers in the sample was the lack of understanding regarding the distinction between an 'in-house' function and an 'outsourced service', particularly in relation to employment (including secondment arrangements) and contractual arrangements. In several cases, functions were described as being carried out in-house despite the individuals performing those activities not being employees of the Fund Manager but instead engaged through service agreements with third-party entities. The finding suggests that some respondents equated 'in-house' with familiarity with the entity and local presence, rather than with an employment relationship governed by an employment contract.

In many instances, the existence of a service agreement in lieu of an employment agreement was not recognised as tantamount to outsourcing, even where the service provider is a separate legal entity. This appears to obscure the boundaries between internal and outsourced functions, potentially leading to inconsistent classifications across Fund Managers of which function is 'in-house' or 'outsourced'. The responses suggest that Fund

Managers are focusing more on how work is performed in practice, neglecting the underlying contractual arrangements. In some cases, this had serious implications as Fund Managers had both the investment management and risk management function outsourced, resulting in a letter-box entity structure.

*Requirements*

An in-house service is generally understood to exist when a function is performed by an individual who is directly employed by the Fund Manager under an employment contract or by way of secondment agreement. On the contrary, where a function is carried out pursuant to a service agreement rather than an employment agreement, the activity should be regarded as outsourced, irrespective of how closely and integrated the concerned individual is within the day-to-day activities of the Fund Manager.

The legal and contractual basis of the engagement is key to the differentiation between 'in-house' and 'outsourced'. Service agreement generally reflects the involvement of a sole practitioner or a separate legal entity that through one or more of its employees provide the service contracted for. Deeming such arrangement as 'in-house', despite the absence of an employment relationship, risks compromising the Fund Manager's compliance with Article 13(2) of the UCITS Directive which inter alia states that, '*The management company shall not delegate its functions to the extent that it becomes a letterbox entity.*' and Article 20(3) of the AIFMD which inter alia states, '*...nor shall the AIFM delegate its functions to the extent that, in essence, it can no longer be considered to be the manager of the AIF and to the extent that it becomes a letter-box entity.*' If a Fund Manager mis-classifies its 'in-house' and 'outsourced' functions, it may allude itself as having in-house capabilities while in essence it would be relying on third-party service providers, lacking sufficient internal resources and substance which ultimately results in being a letter-box entity.

Having critical functions in-house is of utmost importance for a Fund Manager, as regulatory frameworks require Fund Managers to retain decision-making powers, expertise, and oversight over its core activities. Such principle will be strengthened further with the AIFMD II (Directive (EU) 2024/927) which has come into effect as from 16 April 2026. Letter-box entities undermine the objectives of the mentioned Directives by obscuring where functions are actually performed and by whom, potentially weakening accountability and oversight. The MFSA requires that at least one from the investment management and risk management functions is undertaken in-house i.e. by at least an individual employed by the Fund Manager. If the Fund Manager opts to have an in-house investment management function, all portfolio managers have to be employed by the Fund Manager. If on the other hand, the Fund Manager goes for an in-house risk management function, the individual undertaking day-to-day risk management shall be employed. In the cases where investment/risk management committee members assume the portfolio or risk management function collectively and directly, the majority of the committee members of the function deemed to be in-house, are expected to be employees of the Fund Manager.

## 3. Conflict of Interest

*Observations*

From the responses collated, it was observed that in practice, the assessment of conflict of interest on outsourced service providers is largely limited to compliance with the relevant rules and documented policies. Case in point, the majority of the Fund Managers seem to ensure that individuals involved in the investment management function are not involved in the risk management function and the valuation function. On the other hand, there was limited evidence on analysis of other areas of conflict of interest which are important to be assessed for the well functioning of a Fund Manager.

In particular, no consideration is given to situations where the Fund Manager outsources various functions to the same service provider. Despite each function is carried out by different individuals, no assessment is being done on whether effective separation between each function can be achieved and maintained in the provider's organisation. Another notable gap identified is the lack of conflict of interest assessment on the fact that certain service providers service multiple Fund Managers and routinely deliver identical or similar services to competing clients.

*Expectations*

A thorough conflict on interest policy that also addresses conflict of interest that arises from outsourcing, is critical for the Fund Manager's outsourcing framework. The following are some key components that should be included in a conflict of interest policy:

- Clear definition of what constitutes a conflict of interest
- Identification of who is responsible to identify, monitor and approve (if deemed acceptable) such conflict of interest
- Monitoring process of such conflict of interest including escalation procedures

The Authority requires that in an outsourced service provider relationship, conflict of interest is adequately identified, mitigated and if not possible, alternative arrangements should be sought. As observed, certain deficiencies were found in the responses. The Authority expects that Fund Managers consider the conflict of interest that arises from service providers that are providing identical service to competing Fund Managers. Although the Authority acknowledges that this market structure is common and not inherently problematic, it can give rise to several potential conflicts that go beyond those covered by rules and regulations. These may include risks related to:

- Preferential allocation of resources to one client over the other – During peak periods or particular market/economic scenarios, the service provider may face competing demands from its client base which could lead to advertent or inadvertent preferential treatment of certain clients.

- Information leakage – Despite having confidentiality clauses in the respective service agreements, having the same service provider serving a large client base of the same industry, increases the risk of inadvertent sharing of information directly or indirectly that may have serious impact on the sustainability of the Fund Manager.
- Standardisation of services – The service provider may be incentivised to standardise the service being offered to its clients which eventually will overlook the specific needs of each and every Fund Manager with the consequence that the service is not provided with the required level of quality.

The Authority also expects that Fund Managers take into consideration the conflict of interest that arises from a service provider that through different individuals, provide various services to the Fund Manager. Whilst acknowledging that when such arrangement is in place, it does not automatically imply the presence of conflict of interest, it is highly likely that such conflict will arise and the Fund Manager is expected to take this into consideration when assessing a proposed service provider.

Fund Managers are required to scrutinise whether effective separation can be achieved and maintained in practice, rather than merely relying on oral confirmation provided in the negotiations at pre-appointment stage. Whilst respecting the privacy of the outsourced service provider, the Fund Manager has to understand the reporting lines, polices and "Chinese Walls" of such service provider. In service providers that are relatively small, such controls may be constrained and difficult to be fully implemented as individuals may hold multiple roles lacking proper independent oversight, leading to a situation where conflict of interest cannot be mitigated. Despite such small set-up, the MFSA requires that compliance officers and other control functions are fully independent and maintain the necessary independence of mind to carry out their role effectively and free from any judgement, at all times.

It is important for Fund Managers to move away from merely a formalistic exercise and adopt a more realistic approach when assessing conflict of interest, taking into consideration *inter alia*, section 2.1.8 *Conflicts of Interest and Confidentiality* of the MFSA Corporate Governance Code. This will enhance the effectiveness of such exercise and will further contribute to good corporate governance.

## 4. Due Diligence

*Observations*

It was observed that some Fund Managers failed to undertake appropriate due diligence, if done at all, on the proposed outsourced service providers. A concerning approach was observed on several licence holders that instead of undertaking appropriate due diligence, they relied on the reputation in the industry of the provider. In this regard, the pre-selection assessment focused on whether the provider is well-known, widely referenced in the industry, or has an established client base, rather than on a detailed evaluation of its operations, governance structures, risk management process and compliance history, among other important criteria.

*Expectations*

The due diligence process is not merely a formal checklist approach. It is a substantive assessment designed to ensure that the provider can perform the outsourced function reliably, competently, and in accordance with all applicable regulatory obligations. The absence of thorough due diligence increases the probability that the Fund Manager will oversee critical issues related to the outsourced service provider's financial stability, staffing adequacy, internal control environment, cybersecurity posture, business continuity arrangements, and regulatory compliance history, all of which are key elements to ensure that outsourced functions are performed to the level required and in accordance with the relevant regulatory requirements.

By fulfilling these expectations, both at pre-appointment stage and on an ongoing basis, Fund Managers would be able to demonstrate proactive oversight over outsourced functions, reduce operational and compliance risks, and strengthen its investors'/clients' confidence in the service being delivered. In this regard, the Authority emphasises the importance that Fund Managers have a robust ongoing due diligence framework for their outsourced service providers, that includes periodic onsite inspections to the providers' premises. Onsite inspections are key because they allow Fund Managers to corroborate the information found in policies and off-site questionnaires, observe internal controls in real time, interview key personnel, review technological safeguards, and assess the actual as opposed to the expected performance of the outsourced function. In this regard, the Authority expects a Fund Manager to include in the compliance monitoring plan the timely review of outsourced service providers. Although off-site reviews are important, on-site reviews provide a more profound understanding of the operations of the service provider. The frequency shall be determined in accordance with the criticality of the service provided, and in line with the nature, scale and complexity of operations of the Fund Manager.

Due diligence is a critical process through which licence holders seek to ensure that outsourcing arrangements do not compromise the ability of the funds being managed to act in the best interests of investors, act in compliance with the applicable regulatory requirements and positively contribute to the reputation of the sector.

## 5. Reporting

*Observations*

From the review conducted on the collated questionnaires, we identified that generally there is no proper reporting to the governing body regarding the outsourced service providers engaged by Fund Managers, this despite that several Fund Managers rely heavily on outsourced service providers. In many cases, the governing body of the Fund Manager only receives high-level information that lack the necessary operational detail and the essential features of the outsourcing relationship. As a result, there is limited evidence of formal documentation demonstrating how the governing body is evaluating prospective outsourced service providers and exercising their oversight duties on the appointed outsourced service providers.

*Expectations*

It is of utmost importance that, within a Fund Manager, a comprehensive written report on each outsourced service provider covering *inter alia* performance, costs, due diligence findings, risk rating, compliance matters, conflict of interest and operations, is formally presented to the governing body in a timely manner in line with the schedule of inspections/ reviews carried out. At lease once a year the governing body shall carry out a documented performance assessment of all key outsourced service providers. Such reporting enhances the corporate governance of the Fund Manager as among other aspects, it increases the board's oversight on outsourced service providers which given that under the AIFMD and UCITS Directive, delegation of functions does not transfer the liability from the Fund Manager to the outsourced service provider but the governing body retains full responsibility for the proper performance of the delegated activities.

Reporting at the governing body meetings ensures that oversight of outsourcing arrangements is given its due importance, enabling the governing body to exercise informed judgment and challenge where necessary. Ultimately it will allow the governing body to determine whether the outsourced service provider continues to deliver services in line with contractual and regulatory expectations. Sufficient time should be dedicated within each meeting of the governing body to the discussion on outsourcing matters as the depth and quality of oversight are directly linked to the time afforded for meaningful review of the report when reviewing the pack prior to the meeting and also to the challenging and deliberation during the meeting. Outsourcing arrangements should not be regarded as minor administrative topics especially when they concern the outsourcing of core functions such as but not limited to portfolio management, compliance and risk management. This comprehensive perspective enables early identification of concentration risks, operational deficiencies, or emerging regulatory issues, easing a timely intervention on potential issues before resulting into material breaches or detrimental outcomes to investors.

## 6. Contingency planning

*Observations*

Based on the responses collected through the survey, the majority of the Fund Managers indicated that their primary contingency measure to mitigate the potential failure of an outsourced service provider consists of ensuring that the provider maintains appropriate business continuity and operational resilience arrangements. Respondents noted that, at least on an annual basis, they review and verify that outsourced service providers have adequate business continuity and disaster recovery plan in place. This review process generally includes assessing that the service provider has procedures in place to ensure the continuity of critical services in the event of operational disruptions, system failures, cyber incidents, or other unforeseen events that could affect the provision of outsourced activities. This is reviewed by verifying the existence of data backup mechanisms and recovery procedures, intended to maintain data storage and availability uninterruptedly.

Our findings suggest that Fund Managers place significant reliance on the internal resilience frameworks of their outsourced service providers as a key element of their contingency planning. Instead of establishing back-up arrangements independent from the outsourced service providers, Fund Managers generally seek to ensure that the service provider itself has implemented sufficient safeguards to maintain service continuity and to minimize operational risks. Limited attention is placed on the transition to new service providers and the procedures related to such change, that will contribute to ensuring a seamless uninterrupted transfer of service.

*Expectations*

While the approach described above shows that Fund Managers are aware of the importance of operational resilience in outsourcing arrangements, relying solely on the annual verification that outsourced service providers maintain business continuity and disaster recovery plans, and data backup procedures, may present certain shortcomings. Such approach may pose certain shortcomings as Fund Managers may focus on the existence of continuity arrangements of outsourced service providers rather than on their effectiveness or its' own ability to respond to a disruption by the outsourced function that affects the service provided.

This approach may create an overreliance on the service provider's internal contingency arrangements. The Authority expects that effective outsourcing oversight generally requires not only verifying the resilience of the service provider but also ensuring that the Fund Manager has developed its own contingency strategies, including the identification of alternative service providers and internal fallback procedures in the event that the outsourced provider becomes unable to deliver the service for an extended period. This will ensure that the Fund Manager's service in continued interruptedly even when the outsourced service provider is facing significant operational disruption. In this regard, Fund Managers should enhance their contingency plans by *inter alia* simulating stress testing scenarios periodically and take the necessary measures/ corrective action to address any deficiencies observed. The Authority expects that such contingency plans and oversight of the outsourced service provider are duly included in the outsourcing policy and risk management framework of the Fund Manager.

**CONCLUSION**

The findings arising from this Review 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 outsourcing. In this regard, the Authority wishes to highlight that amongst the key areas of improvements identified during this Review, Fund Managers should focus on having clear pre-defined criteria in their approach in the selection of outsourced service providers and taking into consideration the substance requirements. The Authority would like to also stress the importance of managing conflict of interest that arises from outsourcing relationships, having proper and effective due diligence process in place (including properly documenting the ongoing reviews conducted), frequently reporting to the governing body that enhances its visibility on the outsourced service providers and a

MFSA MALTA FINANCIAL SERVICES AUTHORITY

contingency plan in place that ensures uninterrupted service to clients in case the outsourced service provider fails to deliver the contracted service.

We remind you that the outsourcing of critical operational functions shall neither weaken the quality of the Fund Manager's internal controls nor the ability of the MFSA to monitor the Fund Manager's compliance with its regulatory obligations. The Fund Manager shall retain full responsibility for all outsourced functions and the agreements with outsourced service providers shall clearly allow the Authority to access any information related to the respective Fund Manager. The governing body of the Fund Manager remains liable for ensuring that outsourced activities are properly performed in compliance with the applicable requirements and delivered in the best interests of the entity and the underlying funds' investors.

**All Fund Managers are expected to conduct a gap analysis based on the findings and recommendations of this Outcomes-Based Review. This analysis should be documented and made available to the Authority upon request and may be subject to verification during future supervisory engagements. Fund Managers 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, Fund Managers are encouraged to contact the Authority.**

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

Yours Sincerely,
**Malta Financial Services Authority**

Christopher P. Buttigieg | Digitally signed by Christopher P. Buttigieg Date: 2026.09.14 09:24:10 +02'00'

Ian MELI (Signature) | Digitally signed by Ian MELI (Signature) Date: 2026.09.14 07:30:57 +02'00'

**Prof. Christopher P. Buttigieg**
Chief Officer Supervision

**Ian Meli**
Head – Investment Services Supervision

*The MFSA ensures that any processing of personal data is conducted in accordance with Regulation (EU) 2016/679 (General Data Protection Regulation), the Data Protection Act (Chapter 586 of the Laws of 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.*