# MFSA: Thematic Review on Governance and the Compliance Function in relation to Trustees and Company Service Providers

## GOVERNANCE

### 1. The Board of Directors (the 'Board')

Findings:

- The Authority noted that TCSPs often lacked the formality of retaining detailed minutes of such discussions. From a review of Board meeting minutes provided, the Authority observed instances where such minutes did not extend to discussions relating to the key matters impacting the authorised business, such as client onboarding, risk and compliance, and instead discussions appeared to be restricted to formal operational matters of the business.

- In other instances, whilst Board meeting minutes did include reference to integral matters, the said minutes did not include sufficient detail on the discussions leading to decisions taken by the Board. This was due to the fact that the directors often engaged in informal discussions relating to the authorised business which discussions were, however, not subsequently documented.

- Certain Board members lacked a comprehensive understanding of the workings of key functions and processes of the Authorised Person.

- One Director held multiple other roles, such as also being the Company Secretary, and Compliance Officer and/or MLRO of the Authorised Person, and possibly also one of the shareholders, without implementing adequate mitigating measures and controls.

Regulatory Requirements:

- Authorised Persons are required to maintain Board meeting minutes which provide a true and accurate record of discussions held, decisions taken, and resolutions made, especially those relating to significant and strategic matters concerning the authorised business.

- Where any key decisions are taken by Board members outside of formal Board Meetings, such decisions should be duly recorded in the form of resolutions. Board minutes and resolutions should enable external parties to understand Board discussions and decision-making processes.

- Adequate Board packs should also be retained, including any supporting documentation referred to in such minutes.

- All members of the Board are expected to have a general understanding of the workings of key functions and processes of the Authorised Person.

- TCSPs are to ensure that structures where one person is holding multiple roles, do not give rise to any issues relating to, for example, time management and conflicts of interest.

## 2. Policies and Procedures

Findings:

- Authorised persons did not have in place certain policies or procedures, including:

  (i) a governance policy outlining reporting lines and decision-making procedures;
  (ii) an outsourcing policy;
  (iii) compliance-related procedures; and/or
  (iv) cybersecurity policies/procedures.

- Governance policy did not include decision-making procedures and fell short of extending to the specific responsibilities of the directors, reporting lines and the manner in which the Authorised Person applies the dual control principle.

- The Business Continuity Plan did not include procedures to provide for the continuity of functions in circumstances of long periods of absence of any of the key officers of the Authorised Person, including the Directors and the Compliance Officer.

Regulatory Requirements:

- Authorised Persons are expected to ensure that policies and procedures are reviewed at least annually.

## 3. Client Onboarding & Ongoing Monitoring

*Client Onboarding Decision-Making*

Findings:

- The Authority noted governance structures whereby the Board of Directors did not have the final determination in terms of client onboarding.

- Client onboarding was not being carried out in line with the dual control principle. For example, having only one Director, or the Money Laundering Reporting Officer alone, responsible for the final determination as to whether a client should be onboarded, or otherwise.

Regulatory Requirements:

- Should any of the core functions of the Board be delegated to any other person, committee or body, the Authorised Person should obtain prior approval from the Authority for any intended changes to be made to the approved governance structure. Furthermore, in such instances the Authorised Person should also have in place a

formal delegation framework clearly outlining this arrangement which should also be approved by the Authority.

- Authorised persons set up as legal persons are required to ensure that all decisions relating to the regulated business, including client onboarding, are effectively taken by at least two directors or by a director and another senior official of the Authorised Person duly approved by the Authority.

*Client Agreements*

Findings:

- Shortcomings in client agreements reviewed in terms of missing key elements, such as omitted reference to the specific licensable service/s being covered by the agreement.

- Where a group of entities are servicing a common client, the common client agreement in place failed to specifically indicate the specific entity providing the respective licensable service, which may be misleading to the client, or even possibly raise concerns as to whether the licensable services are being provided through the duly authorised entity.

- Client agreements and/or letters of engagement were found to have deficiencies such as missing signatures for one or more parties to the agreement, or failure to identify the role of the signatory, as well as agreements not being duly dated.

Regulatory Requirements:

- To ensure that client agreements clearly outline the licensable services being provided and covered by the agreement, and in the case of a group of companies or related entities providing multiple services to the client, an indication as to which licensed entity is offering the respective licensable services.

*Resource Sharing & Outsourcing Agreements*

Findings:

- The Authority observed that an Authorised Person forming part of a group of companies shared resources and outsourced certain key functions to third parties, without having any underlying resource sharing and/or outsourcing agreements in place.

Regulatory Requirements:

- Authorised Persons are required to have in place the necessary underlying agreements governing sharing of resources or outsourcing of services. Such agreements are required to be set out in a formal, clear, written contract which establishes the respective rights and obligations of the parties.

*Regulatory Registers*

Findings:

- Authorised Person did not have in place a risk register required by the applicable regulatory framework. In other instances, albeit having the relevant registers in place, the Authority noted a lack of certain key details recorded in such registers, such as in the complaints, conflicts of interests, risk, and/or breaches registers. Such omissions included a reference to the client in question when noting details in the complaints register and a description of the breach recorded in the breaches register, or the remedial action taken.

Regulatory Requirements:

- Authorised persons are requested to ensure to record all key information in registers which are required to be in place. This information should also extend to any mitigating and/or remedial action undertaken in such circumstances.

*Filing of Regulatory Submissions*

Findings:

- The Authority raised issues relating to late filings of regulatory submissions by Authorised Persons, such as the Annual Compliance Return and Financial Statements. Such conduct, apart from amounting to breaches of regulatory requirements, reflects poor governance practices being adopted in ensuring that the necessary checks and balances are being implemented to ensure compliance with all applicable requirements.

Regulatory Requirements:

- Authorised persons are expected to have robust systems and controls in place to ensure that regulatory submissions are filed within the stipulated deadlines. Authorised Persons are also expected to have systems to monitor any updates or communications issues by the Authority.

## 4. Authorised Persons providing Directorship Services

Findings:

- Where Authorised Persons offered directorship services, Board meetings were not being held on a regular basis and observed a lack of detail being kept thereon for those held. In one instance, this also resulted in significant delays in the approval of statutory documentation and subsequent late filing with the relevant authorities (e.g. late filing of audited financial statements and annual returns with the Malta Business Registry).

- The Authority noted instances where Authorised Persons were arranging for corporate entities to act as directors/company secretaries for their clients. This is not in line with the CSP Rulebook which sets out that CSPs may only arrange for the appointment of

their officers or employees (natural persons) to act as director or secretary, or a similar position, in client entities.

Regulatory Requirements:

- Authorised Persons providing directorship services are reminded of their general fiduciary duties of loyalty, care, and skill, owed to client companies. All Authorised Persons acting as directors, are expected to act in the best interest of the client company, and to carry out their duties in an honest and transparent way.

- Authorised Persons are to ensure that regular client Board meetings are being held and any decisions taken during such meetings are duly documented.

- Directors are to ensure that there are no unnecessary delays in the approval and submission of statutory filings, especially for those instances where delays may result in client companies incurring penalties.

## 5. Transparency & Cooperation with the Authority

*Notifications of Resignations and Appointments of Approved Persons*

Findings:

- The Authority noted a few instances where Authorised Persons did not inform the Authority, in a timely manner, of resignations of persons holding approved positions. Prolonged vacancies in these roles consequently led to a breach of the legal and/or regulatory obligations relating to the minimum board composition or the obligation to appoint a compliance officer.

- The Authority also noted instances where Authorised Persons failed to seek necessary approvals of the Authority for the appointment of officers prior to submitting the necessary forms to the Malta Business Registry or prior to such persons taking on their respective functions.

Regulatory Requirements:

- Authorised Persons are to ensure that resignations are communicated to the Authority in a timely manner.

*Provision of Information to the Authority*

Findings:

- Authorised Persons are expected to co-operate with the MFSA, and any other relevant authorities, in an open and honest manner. They are expected to provide the Authority with any information it may require in the exercise of its supervisory role.

Regulatory Requirements

- Authorised Persons are expected to co-operate with the Authority and any other relevant regulatory authorities in an open and honest manner and shall provide the Authority with any information it may require.

## MATTERS RELATING TO THE COMPLIANCE FUNCTION

### 6. Documentation of the Work Carried out by the Compliance Function

Findings:

- The Authority noted instances where work carried out by the compliance function was not being documented, which led to the Authority not being in a position to assess the matters identified and the checks carried out by the compliance function.

- The Authority noted numerous deficiencies in client file reviews and could not determine whether these shortcomings had also been identified and communicated by the compliance function, or whether in fact such deficiencies were being addressed, due to this lack of recording of such work.

- The Authority noted instances whereby, albeit compliance reports had been drawn up, the recorded compliance work only extended to regulatory updates. Such reports failed to extend to any compliance checks carried out by the compliance officer, such as: client file reviews, updates on testing/reviews carried out in terms of the Compliance Monitoring Programme, and any weaknesses identified therefrom.

Regulatory Requirements:

- Authorised persons are to ensure that the work of the compliance function is adequately documented, in line with good governance and record keeping practices.

- The compliance function should be guided by the compliance monitoring programme.

- Compliance reports should include any testing/checks carried out, any deficiencies encountered and any corresponding recommendations and/or mitigating measures recommended by the compliance function. Compliance reports should subsequently be duly presented to the Board.

### 7. Compliance Monitoring Programme (the 'CMP')

Findings:

- Common issues identified included: lack of a set methodology and frequency of testing to be carried and certain missing regulatory checks to ensure compliance with all the applicable legislative and regulatory requirements.

Regulatory Requirements:

- Authorised persons are to have in place and/or strengthen their CMP to ensure that it includes the methodology of the reviews/tests as well as the timeframe by when such tests/reviews are to be carried out.

- For an effective CMP, the compliance function must conduct a proper risk assessment and mapping exercise to identify and prioritise compliance risk factors prior to the drafting (and updating) of a CMP. The risk assessment should identify areas of high, medium, low compliance risks, identify any gaps in the compliance programme and test the controls in place to mitigate the identified risks. This risk assessment exercise should be data driven (not theoretical), and properly documented and reviewed on a periodic basis.

- The CMP should be an ongoing programme aimed at monitoring the overall operations and procedures to ensure all aspects of the business are adequately monitored (including all services provided by the Authorised Persons as part of their authorisation) and includes as part of the CMP, such as complaints handling, systems and controls, conflicts of interests, training, breaches, business continuity and its testing, monitoring of critical service providers, capital requirements and professional liability risks, segregation of funds, sampling transactions, AML, Compliance and Due Diligence, record keeping and regulatory calendar submissions.

- For each area to be tested, it is recommended that the CMP provides, inter alia:
    - a description of the area to be tested;
    - the relevant procedure explaining how such areas are tested;
    - the finding and/or recommendations; and
    - the period of when the testing will be/was carried out.

- The CMP should state the period during which the reviews/tests will take place and once drafted, the program should be presented to the Board for consideration and approval, which should in turn be ensuring effective compliance function monitoring and oversight.

## 8. Carrying out of Compliance Client File Reviews

Findings:

- In instances, compliance-related client file reviews were being carried out sporadically rather than on a pre-set periodical or systematic risk-based basis. The Authority noted that the compliance officer of such Authorised Persons was often reviewing the same clients due to their high-risk rating or only reviewing newly engaged clients. In a few instances, the Authority noted that, albeit certain deficiencies being noted by the Authority relating to missing client documentation kept on file, as required by the Authorised Person's own internal procedures and checklists, such deficiencies did not feature in the compliance reports prepared by the compliance function.

- In other instances, compliance reports fell short of including any recommendation to address these gaps.

Regulatory Requirements:

- Authorised Persons are to ensure that the compliance function is carrying out effective and independent checks on client files, following a set methodology, and ensuring that applicable legislative and regulatory requirements, including internal policies and procedures and those relating to record-keeping, are being adhered to.

- Authorised persons are to ensure that such compliance client file reviews are duly documented, including any weaknesses or breaches identified together with recommendations on the remedial action to be undertaken.

### 9. Independence of the Compliance Officer

Findings:

- Compliance officers' involvement in the client onboarding process should only extend to providing guidance with respect to compliance issues, and only if this is deemed necessary.

Regulatory Requirements:

- Compliance Officers should not be involved in the performance of services or activities which they monitor, particularly the process of onboarding of clients, nor should they be client facing.

### 10. Access to all Relevant Information

Findings:

- Any hindered access to relevant information may result in impeding the compliance officer to carry out the necessary compliance work in an effective manner, resulting in Authorised Persons adopting a weak Three Lines Model which could in turn result in governance weaknesses.

Regulatory Requirements:

- Authorised Persons are not only requested to ensure that compliance officers have unhindered access to all relevant documentation, but also that they have adequate resources to carry out their duties.

### 11. Matters relating to Record Keeping

*Client Data and Correspondence not Centrally Saved*

Findings:

- The Authority noted instances where client data and correspondence were not saved centrally. Records such as client correspondence, were saved in email inboxes of

employees, some of whom had left their employment. This led to the inability of Authorised Persons to provide information to the Authority in a timely manner.

Regulatory Requirements:

- Authorised Persons are r to ensure that client data and correspondence is centrally saved. Authorised Persons are to ensure that records are adequately stored, irrespective of whether these are stored digitally or physically, as long as the method adopted is consistent and conducive to timely retrieval of such records.

*Failure to Segregate Records from Records of Related Entities*

Findings:

- An Authorised Person failed to segregate its client records from the records of its related entity. Such practices are not regarded to be in line with adequate governance practices given that they may result in either the Authorised Person not having all necessary records on file or having client files which include records pertaining to a separate legal entity, which may lead to a risk of breach of confidentiality or legal risk.

- The Authority noted a common practice of related Authorised Persons forming part of a group of entities holding common Board meetings and recording common Board meeting minutes. The Authority noted that no indication was made as to which company was servicing the clients discussed in such meetings.

Regulatory Requirements:

- Authorised Persons are reminded of the importance of segregation of records from any other entity, including related entities. In the instance where clients are being serviced by the Authorised Person and a related entity, separate records must be duly kept.

- In instances where client data and documentation are shared or relied on, appropriate underlying agreements must be in place governing this arrangement.

- With respect to common Board meeting minutes being kept, Authorised Persons are requested to ensure that a clear indication is made as to which related authorised entity is servicing the client/s being discussed in such meetings, and that the Board meeting clearly delineate where specific issues discussed relate a particular authorised entity.

*Non-Recording of Decisions relating to Clients*

Findings:

- The Authority noted instances where decisions, or key information, relating to clients or review of client documentation were not being documented. For example, in a number of instances, particularly those where the Authorised Persons adopted an automated CRA system, the Authority could not find evidence of a system of preparer and reviewer of client documentation, such finding was particularly noted in client risk assessment reviewed.

- Authorised persons are reminded to ensure that the preparer/s and reviewer/s of documentation should be duly recorded, as part of the Authorised Person's internal controls.

- In relation to client risk assessments, the Authority also noted instances where key deliberations and information, such as the reason/s leading to a manual lowering of a risk score by the Authorised Person, and/or mitigating measures to be applied to that particular client, were not duly documented. In other instances, it was noted that Authorised Persons onboarded clients which fell outside the Authorised Persons' risk appetite and did not appropriately document the client onboarding decision, nor the implementation of any mitigating measures.

Regulatory Requirements:

- Authorised persons are reminded of the importance of the adoption of adequate record keeping practices, and the retention of records which are sufficient to enable the Authority to monitor compliance with the applicable legislative and regulatory regimes.

## GAP ANALYSIS EXERCISE

- Authorised persons are expected to carry out a gap analysis with respect to the practices and processes of their authorised business and take prompt action to address any identified shortcomings accordingly.

- This gap analysis should be duly documented and made readily available, to the Authority, upon request.