17 February 2025

To: The Authorised Person,

To: The Management Body,

To: The Compliance Officer

Thematic Review on the Compliance Function of Company Service Providers

You are receiving this letter as the Authorised Person, the Management Body and/or the Compliance Officer of a Company Service Provider ("Authorised Person" or "CSP") supervised by the Malta Financial Services Authority (the "MFSA" or "Authority").

BACKGROUND AND METHODOLOGY

The Authority's Supervisory Priorities for 2024[1], as per previous years, identified the area of compliance as one of the key supervisory priorities to continue focusing on during 2024 vis-à-vis all sectors regulated by the MFSA, including therefore for Company Service Providers. This also aligns with the MFSA's Strategic Statement[2] where one of the Authority's strategic objectives is in fact to promote good governance and compliance. In order to achieve focused goals, the Authority regards the carrying out of thematic reviews as one of the most effective tools in view of the fact that common issues are analysed and expectations are communicated to the industry as a whole, as opposed to specific authorised persons only.

In this regard, as part of its supervisory work plan for 2024, the Trustees and Company Service Providers Supervision ("TCSPs") Function through the TCSPs Supervision Team carried out a thematic review focussing on the compliance function (the "Thematic Review"), in order to assess the effectiveness and resilience of this key role and area of the regulated business of CSPs. This Thematic Review was launched in the form of a detailed questionnaire which touched upon various themes relating to the Compliance Function including: the role and independence of the Compliance Officer, policies and procedures, the work of the Compliance Officer, reporting lines, breaches, and complaints handling. For the purposes of this Thematic Review, the Authority selected, on a risk-based approach, a sample of 49 CSPs holding different types of classes of CSP authorisation in terms of the Company Services Act (Chapter 529 of the Laws of Malta) ("CSP Act"), consisting of both legal persons and natural persons. In fact, the sample of 49 CSPs comprised of 8 CSPs (16% of the sample) who are natural persons, and 41 CSPs (84% of the sample) constituted as legal persons. In this regard, in view of certain intrinsic differences which stem from the legal structure of both types of CSPs, findings which are not applicable to natural persons are indicated accordingly

[1] https://www.mfsa.mt/wp-content/uploads/2024/02/MFSA-Supervision-Priorities-2024.pdf
[2] https://www.mfsa.mt/wp-content/uploads/2023/02/MFSA-Strategic-Statement.pdf

in the relevant sections below. Following the assessment of the responses received, the Authority also selected six CSPs with whom further engagement was undertaken in the form of a supervisory meeting, to obtain further clarifications on the responses received.

The purpose of this letter is to inform the industry about the main findings of this Thematic Review and to communicate the Authority's expectations whilst encouraging CSPs to enhance their Compliance Function where gaps are identified. As an overall observation, the Authority positively noted that importance is indeed being given by CSPs to having in place an effective compliance function and to implement thorough checks, in the spirit of ensuring that CSPs are operating in line with applicable legislative and regulatory requirements. However, the Authority also identified certain areas, as highlighted in detail below, which require further improvement. These include gaps relating to the implementation of written alternative arrangements in the absence of the Compliance Officer, the broadening of the scope of client file reviews and frequency of testing for the purposes of identification of any breaches. The Authority's supervisory expectations vis-à-vis CSPs are aimed at strengthening and maintaining stability within Malta's financial sector, in recognition of the key role which these service providers play as gatekeepers to Malta's financial system as a whole. In this regard the MFSA is also duty-bound to ensure compliance with Malta's international commitments whilst simultaneously adopting a proportionate regulatory approach, taking into account the nature, size and complexity of the authorised business of the Authorised Person. In fact, this proportionality can be seen in the varying extents of applicability of the CSP Rulebook to the different classes and legal forms of CSPs. With this principle of proportionality in mind, the questions included in this Thematic Review were also tailored to take into consideration the varying nature of the business of CSPs holding different classes of authorisation and the different set ups which such CSPs may have, and the selection of CSPs targeted for the purpose of this exercise was also made on the basis of these considerations, in keeping with the Authority's spirit of a risk-based approach to supervision. CSPs are reminded that compliance obligations and standards are expected to be adhered to and implemented by all. However, the Authority does take into account the size and business model of the Authorised Person in reaching its determination as to whether such compliance obligations are being adequately adhered to.

The Authority's commitment to drive the strengthening of the compliance culture of Authorised Persons is evident from its continuous outreach and guidance activities on the subject matter. In fact, this Thematic Review follows the Thematic Review on Governance and the Compliance Function in relation to Trustees and Company Services Providers[3] (the "Thematic Review on Governance and the Compliance Function") issued by the Authority in 2024 which also touched upon some of the themes related to the Compliance Function, which have also effectively emerged from this Thematic Review. In this regard, for the purposes of alignment of the Authority's position on common themes covered by both thematic reviews, the Thematic Review on Governance and the Compliance Function will also be duly referred to in this Thematic Review for guidance, where necessary and applicable.

[3] https://www.mfsa.mt/wp-content/uploads/2024/04/Dear-CEO-Letter-Thematic-Review-on-Governance-and-the-Compliance-Function-in-relation-to-Trustees-and-Company-Service-Providers.pdf

KEY FINDINGS

1. Role of the Compliance Officer

1.1. Reporting Lines[4]

As part of this Thematic Review, CSPs were asked to confirm the reporting line of their respective compliance officers within their governance structure. In this regard, the Authority positively noted that the majority of CSPs constituted as legal persons indicated that the Compliance Officer reports directly to the Board of Directors. The Authority noted that in two instances CSPs indicated that the Compliance Officer reports to the senior manager in charge of the Risk and Compliance Function whilst two other CSPs indicated that the Compliance Officer reports to the Risk and Compliance Committee. In the latter case, the Authority noted that in one instance all the Board Members sat on the Committee responsible for Compliance whilst in the other case the Compliance Committee is composed of some of the CSP's Board Members. In another case, a CSP indicated that the Compliance Officer reports to the compliance function of the international group which it forms part of.

Regulatory Requirements

CSPs should ensure that the Compliance Officer has the necessary authority and independence to be able to discharge the role. In this regard, CSPs should ensure that the Compliance Officer's reporting line does not impinge, or in any way diminish, this authority and independence. Therefore, it should be ensured that the Compliance Officer has a direct line of communication with the Board of Directors to be able to effectively report on the compliance matters of the CSP. CSPs are reminded that the Board of Directors remains ultimately responsible for the implementation of any necessary action plan to address any compliance findings.

Furthermore, the Authority noted that there are instances wherein CSPs establish committees to deal with certain functions of the regulated business, including compliance, and having the Compliance Officer reporting to such committee. In this regard, CSPs should ensure that the entire Board, particularly those Board members not forming part of such committee, are continuously updated on the compliance matters discussed by such committees. With respect to CSPs forming part of a group of companies, whilst the Authority understands that a line of communication with the group is indeed necessary to ensure group-wide alignment, such CSPs are to ensure that the Board of Directors of the Authorised Person is duly kept updated on all compliance-related matters of the CSP and takes an active role vis-à-vis decisions impacting the CSP's business in Malta.

[4] This section does not apply to individual CSPs in view of them being permitted to carry out the role of compliance officer in relation to their own regulated business.

Authorised Persons are reminded of their obligation in terms of R3-11.1.1 of the Company Service Providers Rulebook (the 'CSP Rulebook') of having established, appropriate and transparent reporting lines to mitigate any conflicts of interest. Furthermore, they are also referred to R2-6.1 and R3-8.2 of the CSP Rulebook[5] with respect to the establishment and maintenance of an effective compliance function.

1.2. Time Commitment

The Authority noted a variety of replies provided by CSPs in relation to the time dedicated by the Compliance Officer to the carrying out of the said role. The most common response in this regard was that the Compliance Officer dedicates 1-2 hours on a weekly basis which was closely followed by an indication of 4-6 hours on a weekly basis. The Authority noted that in five instances the respondents were unable to indicate the time dedicated by the Compliance Officer to the role held specifically with the CSP, particularly where a compliance officer may possibly be appointed to hold the compliance officer role for a number of related entities, or else indicated that the time allocated would be 'as necessary'. The Authority positively noted that, with the exception of some outliers, Compliance Officers, in general are dedicating sufficient time for their role commensurate with the nature, size and scale of business of the CSP.

Regulatory Requirements

In accordance with R2-5.10.1 of the CSP Rulebook, Compliance Officers, are expected to dedicate sufficient time to ensure the efficient and effective performance of their functions. In fact, the assessment of time commitment is one of the four assessment criteria of the MFSA's fitness and properness assessment carried out prior to approving any person, as further explained under Section 5 'Time Commitment' of the MFSA's Guidance on the Fitness and Properness Assessments Applied by the Authority[6] , and which criteria should be satisfied on an ongoing basis throughout the tenure of any approved role.

The Authority also refers to Section 1.1 'Time Commitment' of the Guidance Note on the Fulfilment of Post-Authorisation Requirements[7] (the "Guidance Note") issued by the Authority. The Guidance Note lays down that in determining the time commitment which the Compliance Officer should dedicate to the role, one should consider, amongst others the nature, scale and complexity of the activities of the Authorised Person for which it holds such appointment, as well as any other commitments held by the Compliance Officer.

[5] https://www.mfsa.mt/wp-content/uploads/2021/03/Company-Service-Providers-Rulebook.pdf
[6] GUIDANCE ON THE FITNESS AND PROPERNESS ASSESSMENT APPLIED BY THE AUTHORITY
[7] https://www.mfsa.mt/wp-content/uploads/2023/10/Publication-of-Guidance-Note-on-the-Fulfilment-of-Post-Authorisation-Requirements.pdf

1.3. Staff assisting the Compliance Officer

With regards to staff assisting the Compliance Officer, 65% of the CSPs forming part of this Thematic Review indicated that the Compliance Officer has staff assisting them with the role as opposed to the 35% which indicated that the Compliance Officer has no staff assisting them. In the latter case, the majority of the respondents were individuals authorised as CSPs. The Authority noted that most commonly, the Compliance Officer was supported by other staff in those instances where the Compliance Officer role was outsourced, and assistance was provided by the staff of the service provider engaging the Compliance Officer.

In relation to the allocation of duties to staff assisting the Compliance Officer, the Authority noted an array of different duties mentioned. Amongst the most commonly mentioned duties, CSPs indicated: support with the execution of the Compliance Monitoring Programme ("CMP"), assistance with regulatory reporting, client file reviews and keeping abreast with the updates issued by the Authority in relation to regulatory developments. In a number of instances, CSPs indicated that staff assist with prevention of money laundering compliance-related duties such as, client-onboarding, client screening and ongoing monitoring. In one instance, it was provided that the Managing Director of the Authorised Person assists the Compliance Officer with the CMP.

Regulatory Requirements

CSPs are reminded that whilst Compliance Officers may have staff assisting with the execution of their role, and this is in fact regarded positively if it ensures a more effective compliance function, the individual appointed as the Compliance Officer remains ultimately responsible for all aspects of compliance of the Authorised Person in line with R2-6.1.5 (a) of the CSP Rulebook. In this regard, the Compliance Officer should exercise proper day to day oversight over such staff to ensure that compliance staff are effectively and adequately carrying out any tasks assigned to them and that ultimately the activities of the CSP are carried out in accordance with the applicable laws and regulations including the CSP Act and CSP Rulebook.

1.4. Alternative Arrangements for the performance of the role of the Compliance Officer

When queried about alternative arrangements in case of the absence of the Compliance Officer, the Authority positively noted that the majority of CSPs indicated that such arrangements have in fact been put in place. The Authority only noted one instance where the CSP, an individual, indicated that no such arrangements had been catered for.

Whilst most of the Authorised Persons indicated that there had not been any instances where the Compliance Officer was absent for a prolonged period of time, they indicated that in such circumstances the role would be primarily assumed by the Board of Directors. Some CSPs referred to the MLRO assuming such role, whilst those CSPs having an internal compliance team in place supporting the Compliance Officer indicated that such team members would perform the duties in the Compliance Officer's absence. In those instances where the Compliance Officer is outsourced, the Authorised Persons indicated that a team member of the service provider engaging the Compliance Officer would fill in to perform the required duties.

The Authority positively noted that more than half of the CSPs, constituting 56% of the sample, indicated that such alternative arrangements are documented.

Regulatory Requirements

Authorised Persons are reminded of their obligation under R3-8.2 of the CSP Rulebook to establish and maintain a permanent and effective Compliance Function tasked with ensuring the CSP's compliance with applicable laws and regulations at all times. Authorised Persons are also referred to R3-2.2 and R3-6.4 of the CSP Rulebook which requires Authorised Persons to maintain adequate systems and procedures to ensure compliance with the applicable legal and regulatory requirements. In this regard, CSPs are expected to ensure that such procedures should also cover alternative arrangements to ensure the fulfilment of the duties of the Compliance Officer in their absence.

1.5. Access to information[8]

The Authority positively noted that in almost all cases, CSPs forming part of this Thematic Review indicated that the Compliance Officer has access to the necessary information to be able to carry out their role. In one instance the Authority noted that the CSP indicated that whilst the Compliance Officer has access to client-related information, access to internal information is subject to the Board's prior approval. In other instances, the Authority noted that the access to the necessary information by the Compliance Officer was included as a condition in the service contract of the Compliance Officer, which the Authority noted as a best practice.

Regulatory Requirements

CSPs are expected to ensure that in terms of R3-8.3(i) of the CSP Rulebook Compliance Officers have access to all the relevant information of the CSP to be able to effectively carry out their duties. The Authority would like to highlight that such provision of access to all relevant information should not be hindered in any manner, which hindrance may be inferred from practices such as requiring the prior approval of the Board of Directors. Therefore, as a best practice, CSPs are reminded that Compliance Officer's access to information should not be subject to, or dependent, on any other approval. Additionally, access to the necessary information for the Compliance Officer to be able to carry out the relevant compliance checks reinforces the proper application of the Three Lines Model and ensure that the Authorised Person has the proper checks and balances in place.

Authorised Persons are also referred to Section 2.5 of the Thematic Review on Governance and the Compliance Function issued by the Authority for further guidance.

[8] This section does not apply to individuals who are authorised to carry out the role of compliance officer in relation to their own regulated business.

1.6. Independence of the Compliance Officer[9]

The Authority noted a number of best practices which were reported in relation to the manner in which Authorised Persons ensure the Compliance Officer's independence from the Board of Directors. Most commonly, Authorised Persons provided that Compliance Officers have the necessary authority to carry out their duties without hindrance and that compliance matters are presented directly to the Board for consideration and decision-making. In one case, the Authorised Person indicated that the Compliance Officer reports to the compliance function of the group of companies the CSP forms part of, although maintaining a direct line of communication with the local Board of the Authorised Person. Some CSPs provided that the Compliance Officer is outsourced which helps to strengthen their independence from the Board of the Authorised Person. Other CSPs mentioned the fact that the Compliance Officer was not one of the directors, which was deemed to strengthen the Compliance Officer's independence to carry out the role.

With regards to involvement in client on-boarding, the Authority positively noted that 65% of CSPs which formed part of this Thematic Review indicated that the Compliance Officer is not involved in the client on-boarding process of the CSP. With regards to the 16 CSPs who indicated that the Compliance Officer is involved in the client on-boarding process, the majority provided that the involvement relates to the provision of advice to the Board on compliance issues related to onboarding and/or the carrying out of the client risk assessment when also holding the role of Money Laundering Reporting Officer of the CSP.

When asked whether the Compliance Officer holds any other role within the CSP, 26 out of 49 Authorised Persons answered in the affirmative. The majority of these referred to the Compliance Officer also holding the roles of Money Laundering Reporting Officer ('MLRO') and Risk Officer. The Authority also noted a number of instances where the Compliance Officer is also a director of the CSP. In the latter case, Authorised Persons indicated that the said director would not be involved in any decisions relating to client matters and in view of holding the role of Compliance Officer their remuneration is not linked to the business performance of the Authorised Person.

Regulatory Requirements

CSPs are expected to ensure that in terms of R3-8.4 of the CSP Rulebook, Compliance Officers are not involved in any activities which they are required to monitor and should not hold any client facing roles in order not to impinge upon their impartiality and independence of judgement. Additionally, CSPs should ensure that the determination of the remuneration of the Compliance Officer does not hinder their independence in performing their role. Authorised Persons are also referred to Section 2.4 of the Thematic Review on Governance and the Compliance Function for further guidance.

When the Compliance Officer holds any other role within the Authorised Person, the Authorised Person should ensure that this is complementary to the role of Compliance Officer and more importantly adequate controls should be implemented to avoid any potential conflicts of interest which may arise pursuant to the Compliance Officer holding such additional role/s. Particularly, the Authority would like to highlight that in those instances where the Compliance Officer is also a director of the CSP, proper

[9] This section does not apply to individuals who are authorised to carry out the role of compliance officer in relation to their own regulated business.

measures are to be implemented to ensure such director is not client-facing and that such director is not one of only two parties who are involved in the implementation of the CSP's compliance with the dual control principle in terms of R3-6.6.2 of the CSP Rulebook, as this is likely to increase the possibility of a conflict of interest situation arising.

1.7. Involvement of the Compliance Officer in Committees of the Authorised Person[10]

The Authority noted that 9 CSPs which formed part of this Thematic Review indicated that the Compliance Officer is involved in committees of the Authorised Person. In this regard, most commonly, Authorised Persons indicated that the remit of such committees extended to risk and compliance matters. One Authorised Person indicated that the Compliance Officer attends also the business committee of the CSP, however having no voting rights in such committee.

Regulatory Requirements

Once again, CSPs are expected to ensure that Compliance Officers are not involved in the performance of activities which they are required to monitor, including the participation in committees tasked with such matters.

Authorised Persons are reminded that in the instances of establishment of any committees which would not have been communicated to the Authority at authorisation stage, Authorised Persons should notify the Authority prior to the setting up of such committees, for the Authority to assess whether any additional approvals may be required with respect to the proposed members. Authorised Persons are also reminded to ensure that in cases of changes to the remit of such committees or to members of the previously notified committees, the Authority is also to be notified. In this regard, Authorised Persons may contact the Authority on cspsauthorisations@mfsa.mt.

2. Policies and Procedures

2.1. Frequency of Review of Policies and Procedures

The Authority positively noted that the majority of Authorised Persons indicated that their policies and procedures are reviewed at least annually to ensure that these are in line with their internal practices and CSPs' applicable legislative and regulatory requirements. In a number of instances CSPs provided that the review is carried out on a 'needs' basis.

Regulatory Requirements

CSPs are expected, in accordance with R3-6.5 of the CSP Rulebook, to review the adequacy of their policies and procedures at least annually. The said review should not simply take into account any

[10] This section does not apply to individual who are authorised to carry out the role of compliance officer in relation to their own regulated business.

changes in the legal and regulatory framework of CSPs but should also take into account any changes in the systems and internal controls of the Authorised Person. Furthermore, CSPs are to ensure that their staff, where applicable, are also regularly trained on such policies and procedures, in line with R3-6.2, R3-6.6.5 and R3-6.6.6 of the CSP Rulebook.

2.2. Adaptation of the Group-wide Policies and Procedures to Local Requirements

The Authority positively noted that Authorised Persons forming part of international groups have all indicated that group-wide policies and procedures are adapted to the local legal and regulatory requirements.

Regulatory Requirements

Whilst the Authority understands that Authorised Persons forming part of an international group adopt group-wide policies for the purposes of consistency throughout the group, CSPs are expected to ensure that such policies and procedures are adapted and aligned with the applicable local legal and regulatory obligations, in accordance with R3-6.4 of the CSP Rulebook.

2.3. Written Procedures on the Compliance Function

When asked whether Authorised Persons have written procedures in place with regards to their Compliance Function, the Authority positively noted that 82% of the respondents confirmed that these are indeed in place.

Regulatory Requirements

CSPs are expected, in line with R3-8.1 of the CSP Rulebook, to have in place adequate policies and procedures to ensure compliance with the applicable legal and regulatory framework. In this regard it follows that CSPs are required to have in place procedures with respect to the Compliance Function which should be commensurate with the size and level of the authorised business of the CSP. Amongst others, it is considered best practice that these procedures should lay down: the duties of the Compliance Officer, the allocation of any duties to any staff assisting the Compliance Officer, the testing to be carried out by the Compliance Officer, a description of any tools used by the Compliance Officer such as the Compliance Monitoring Programme, the manner in which the work of the Compliance Function will be documented and presented to the Board, the reporting lines of the Compliance Function as well as the arrangements in place to ensure continuity in case of absence of the Compliance Officer as indicated under Section 1.4 above.

2.4. Ensuring Adherence with Internal Policies and Procedures

With respect to the manner in which the Compliance Officer ensures that the Authorised Person is adhering to its policies and procedures, a variety of measures were indicated by CSPs. These included: the attainment of a written confirmation from staff that they have read and understood the internal policies, training, testing through the compliance monitoring programme and file reviews. The Authority positively noted that CSPs adopt a variety of internal controls and measures to ensure that their staff are adhering to internal policies and procedures.

Regulatory Requirements

CSPs are expected to ensure that in terms of R3-6.2 (ii), R3-6.5 and R3-6.6.5 of the CSP Rulebook, inter alia, adequate procedures are put in place with regards to the carrying out of the authorised activities of the CSP in compliance with the applicable legal and regulatory requirements. This is also considered as best practice vis-à-vis having robust internal controls and measures in place, to ensure that staff are made duly aware of such procedures and that testing is carried out to ensure that staff are carrying out their duties in compliance with the said procedures.

3. Compliance Monitoring Programme ('CMP')

3.1. Implementation of the CMP

i. Establishment and Frequency of Review of the CMP

With regards to the implementation of a CMP, the Authority positively noted that 92% of the CSPs forming part of this Thematic Review have a CMP in place. The Authority noted that four of the CSPs who indicated that they do not have a CMP in place, were individuals. In this regard, whilst all CSPs are expected to have in place a CMP, the Authority acknowledges and accepts that the level of depth and complexity of a CMP should vary and would be commensurate with the nature and size of a CSP's authorised business and business model. Nevertheless, the Authority positively noted that a high percentage of CSPs already have a formal CMP in place.

In relation to the frequency of updating of the CMP, the Authority noted that 63% indicated that this is updated on annual basis with other popular replies being on a quarterly and bi-annual basis. With regards to the updating of the CMP in terms of the compliance risk factors identified, CSPs are expected to ensure that these are aligned with any changes to their business model, operations or practices adopted by the CSP in the day-to-day running of the authorised business.

With respect to the methodology of testing of the CMP, the Authority positively noted that 89% of the Authorised Persons indicated that this is documented.

ii. Process involved in the drafting of the CMP

The Authority positively noted that all CSPs which are legal persons, and those CSPs who are natural persons having another individual appointed as a Compliance Officer, with the exception of three, indicated that discussions are held with the Board of Directors or the Authorised Person respectively, prior to the drafting of the CMP.

As a means to align the areas for testing based on the data compiled by the Compliance Officer, most respondents indicated that they carry out a risk assessment or analysis on an annual basis or on a quarterly basis. In case of one CSP, it was explained that the Authorised Person looks at the results of the previous CMP and adapts the CMP based on the findings of the said previous CMP. The Authority also noted a few instances where the CSPs indicated that the CMP refers to testing of all applicable requirements under the CSP Rulebook and other applicable laws and regulations.

When asked whether the compliance risk factors included in the CMP are selected on a risk-based approach, 93% of the Authorised Persons replied positively. Authorised Persons indicated various types of compliance risks usually considered in the CMP including: breaches, capital requirements, complaints, conflicts of interests, anti-money laundering related risks, governance, regulatory filings, segregation of funds and record-keeping. The Authority noted very few instances where reference was made to outsourcing and disaster recovery-related risks whilst however positively noted that other Authorised Persons referred to other types of risks which go beyond compliance risks, including: operational risks, human resources, technology and cybersecurity, reputation and financial risks.

In one particular case, the CMP is not drafted by the Compliance Officer of the Authorised Person itself but by the group's compliance function. In such case the Authority draws the attention of CSPs to ensure that any CMP implemented at group level is adapted by the local CSP to cater for all the requirements applicable to it under Maltese law as these may be different to those applicable to other entities forming part of an international group. Reference to Section 2.2 of this letter is made.

Regulatory Requirements

CSPs are required, in terms of R3-8.5 of the CSP Rulebook to ensure that a CMP is put into place to monitor and test the compliance of the CSP with the applicable legal and regulatory framework. Additionally, the Compliance Officer is also required to provide regular updates on the progress of the CMP to the Board of Directors in case of CSPs which are legal persons. With regards to natural persons who are authorised as CSPs and who have appointed a third party individual as Compliance Officer, the latter is to ensure that periodic updates are provided to the CSP.

Authorised Persons are also referred to Section 2.2 of Thematic Review on Governance and the Compliance Function for detailed guidance and best practices in relation to the process of drafting and implementation of the CMP.

3.2. Documentation of the testing of the CMP

The Authority positively noted that when Authorised Persons were requested to confirm whether the outcome of the testing carried out under the CMP is documented, 91% confirmed that this is indeed

documented. With regards to the manner in which the said outcome is documented, CSPs largely indicated that this is done through compliance reports. Some Authorised Persons indicated that this is done in the CMP itself whilst a few others indicated that this is done through *ad hoc* reports. The Authority therefore positively noted the high percentage of CSPs which document the testing carried out in terms of the CMP, which is an obligation posed on all CSPs in terms of good governance and good record-keeping practices.

The Authority positively further noted that 37 out of the sample of 49 Authorised Persons indicated that recommendations are set out by the Compliance Officer with respect to the findings of the testing of the CMP. With regards to the type of recommendations made by the Compliance Officer the Authority noted frequent reference to updating of the policies and procedures and internal systems of the CSP.

Regulatory Requirements

CSPs are expected, in terms of R3-8.5 of the CSP Rulebook, to ensure that the testing carried out under the CMP is duly documented, together with the remedial actions to be undertaken in order to bring the Authorised Person in line with internal policies and procedures and applicable legislative and regulatory requirements. Furthermore, Compliance Officers are to ensure that any recommendations are brought to the attention of the Board of Directors or the Authorised Person, as applicable. In turn, CSPs are expected to ensure that the recommendations set out by the Compliance Officer are duly addressed in a timely manner.

4. Handling of Complaints

With regards to complaints handling procedures, the Authority noted that only one CSP indicated that these were not in place. Furthermore, the Authority positively noted that all Authorised Persons indicated that a complaints register is in place. On this point, the Authority therefore positively noted the importance being given by CSPs to complaints handling with respect to their authorised business.

Authorised Persons were requested to indicate whether the Compliance Officer is involved in the handling of complaints, with 70% confirming the Compliance Officer's involvement. Authorised Persons indicated an array of ways in which the Compliance Officer is involved including: provision of guidance, analysis of the complaint received, updating of the complaints register and overseeing that the complaint is processed in accordance with the internal complaints procedure.

Regulatory Requirements

CSPs are required to ensure that, in accordance with R3-11.9 of the CSP Rulebook, a complaints handling procedure and a complaints register are implemented with regards to the handling of complaints received from their clients. Additionally, whilst Compliance Officers are not necessarily expected to deal with complaints themselves, they are expected to exercise oversight over this process to ensure that the complaints received by the Authorised Person are handled in accordance with the internal procedure and that any follow-up action to improve the CSP's systems and/or procedures, as may be necessary, is duly undertaken.

The Compliance Officer is to ensure that the complaints are duly recorded in the CSP's complaints register and duly reported to the Authority in its annual compliance return.

5. Compliance Testing

5.1. Compliance testing for identification of breaches

The CSPs forming part of this Thematic Review were asked to specify the type of testing that is carried out to identify any breaches of the applicable legal and regulatory framework. Most commonly, CSPs indicated that testing is carried out through the CMP with some indicating the particular themes such as: reviews of the policies and procedures, client file reviews, reviews of agreements in case of outsourced functions, review of the bank accounts of the CSP to verify segregation of funds, and review of the regulatory calendar to ensure that the regulatory filings are done with competent authorities in a timely manner. The Authority positively noted the variety of areas of regulatory compliance areas captured by testing carried out by CSPs through their CMP, indicating a good level of understanding of their compliance obligations.

The Authority noted two instances where the Authorised Persons indicated that no testing for the purposes of identifying breaches is carried out.

Regulatory Requirements

CSPs are expected, in terms of R3-10.1-R3-10.3 of the CSP Rulebook to establish and maintain appropriate policies and procedures for the identification of breaches, together with a breaches log to record any breaches identified. The Authority would like to stress the importance of carrying out testing as part of the CMP to target specifically the identification of any breaches committed by the CSP in terms of all applicable legislative and regulatory requirements.

5.2. Client File Reviews

i. <u>Basis and Scope of Client File Reviews</u>

The Authority noted that 80% of the Authorised Persons indicated that the Compliance Function carries out client file reviews. With respect to those which indicated that they do not, nine are legal persons and one is an individual authorised as a CSP. All CSPs are expected to carry out client file reviews in terms of their ongoing obligations in order to ensure compliance with all their applicable legal and regulatory obligations, both vis-à-vis the duties owed to their clients as well as regulatory compliance.

CSPs were asked to indicate the basis on which the sample of the client file review is chosen, with the most common response being on a risk-based approach, followed by the response that the sample is selected on a random selection basis. Authorised Persons with a small client base indicated that they carry out a review of all their clients on an annual basis.

In relation to the types of checks carried out as part of the client file review the Authority noted that the absolute majority indicated checks carried out in relation to anti-money laundering related obligations vis-a-vis the attainment of updated due diligence documentation from clients, client screening and updating client risk assessments. The Authority noted that only 8 out of 49 CSPs specifically indicated that the review of the client files extends also to the requirements set out under the CSP Rulebook. In this regard, the Authority would like to highlight the distinction between carrying out client file reviews from an AML/CFT perspective and those from a compliance perspective. Whilst the importance of carrying out client file reviews from an AML/CFT-compliance perspective remains paramount in view of the gatekeeper role held by CSPs, such CSPs are also expected to ensure that client files are reviewed with a focus on any other applicable legislation and regulations, and that any follow up actions or procedures required by their own internal procedures, are also adhered to.

ii. Documentation of the Findings of the Client File Reviews

With regards to the documentation of the findings of the client file reviews, the Authority positively noted that 98% of the CSPs which had indicated that they carry out client file reviews, provided that the findings are documented. Authorised Persons indicated various ways in which such findings are documented, commonly through *ad hoc* reports and the compliance reports. Reference was also made, in a few instances, to recording of the findings on the CSP's system. In one particular instance, the CSP provided that findings are not recorded formally but rather through email with the relevant team members.

Authorised Persons were also asked to indicate whether remedial actions are also documented together with the findings of the client file reviews, however in the absolute majority of the replies no reference to the documentation of the remedial action was made.

The Authority noted the different forms in which CSPs document the work done by the Compliance Function in terms of client file reviews. In this regard, CSPs are expected to ensure that all such compliance work, including the remedial action taken by the CSP, is documented in a manner which allows accessibility for future reference by both the CSP, and the Authority upon request including, but not limited to, any such request made in the course of a supervisory interaction.

Regulatory Requirements

CSPs are expected to carry out client file reviews on a regular basis and in terms of their ongoing monitoring obligations. Through client file reviews, Compliance Officers should ensure that client files are maintained in line with the CSP's internal policies and procedures and to identify any weaknesses or deficiencies accordingly. Furthermore, through client file reviews, CSPs would be kept abreast of any current and potential risks posed by their clients and would be able to implement any necessary mitigating measures accordingly.

With respect to the frequency of the carrying out of client file reviews, CSPs are expected to implement a set methodology to determine the frequency of client file reviews, which should be driven by risk. This has been observed as a best practice to ensure that the risk-based approach is properly implemented vis-à-vis ongoing monitoring. CSPs are to ensure that the Compliance Function

documents any relevant findings, recommendation/s and action/s to be undertaken in order to remedy any identified shortcomings. The Compliance Function should further ensure that the Board of Directors, where applicable, is kept updated with the compliance work carried out and that an adequate action plan on how to address any findings is put in place without undue delay. CSPs are further reminded that such checks should not only extend to obligations emanating from AML/CFT applicable legislation and regulation however, CSPs should also ensure they are adhering to their CSP obligations and their own policies and procedures.

CSPs are also referred to Section 2.3 of the Thematic Review on Governance and the Compliance Function for guidance with regards to the carrying out of the client file reviews.

6. Compliance Reports

Authorised Persons were asked whether a compliance report is prepared by the Compliance Officer. All respondents, except for one CSP who is a natural person, indicated that they do prepare a compliance report. When asked about the frequency of preparation of compliance reports, the majority indicated that these are prepared on a quarterly basis. The next most popular responses indicated that compliance reports were prepared on a bi-annual and annual basis respectively. The Authority noted that two respondents did not provide a concrete indication, but simply indicated that compliance reports are prepared "as necessary".

CSPs were also requested to indicate the typical contents of the compliance reports prepared, and some common areas mentioned included: updates on the testing carried out in terms of their CMP, regulatory updates from competent authorities, communication with competent authorities, updates on staff training, breaches, regulatory reporting and complaints. The Authority noted a few instances where the contents mentioned were limited to anti-money laundering related areas such as updates on new clients, due diligence and changes in the clients' risks.

Regulatory Requirements

The Authority draws the attention of CSPs who are natural persons, and who are permitted to act as Compliance Officers themselves in relation to their own business, to R2-6.1.3 of the CSP Rulebook which requires such CSPs to draw up an annual compliance report providing the confirmations stipulated therein. The Authority acknowledges that the nature, size and business model of CSPs falling within the above-mentioned criteria would generally not be significant or complex and therefore compliance work reporting may be more simplified and streamlined in line with the spirit of proportionality. The minimum set of confirmations required by the applicable Rule, are therefore intended to act as guidance and to provide a benchmark of the minimum requirements which such CSPs are to monitor adherence thereto. On the other hand, with regards to all other CSPs not falling within the said category, such CSPs are required, in terms of R3-8.5 of the CSP Rulebook, to prepare compliance reports recording the compliance work carried out by the Compliance Officer for the relevant reporting period. Compliance reports should include any testing/checks carried out, which should as best practice be driven by the CSP's CMP, as well as 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, in the case of a CSP

who is a legal person, or to the CSP himself in the case of a natural person who falls within a class which requires the appointment of an independent compliance function.

Authorised Persons are referred to Section 2.1 of the Thematic Review on Governance and the Compliance Function for further guidance.

7. Provision of Updates to the Board of Directors

Authorised Persons were asked to specify the manner in which the Board is updated with compliance matters, with the absolute majority indicating in their responses that this was done through the presentation of compliance reports. The Authority noted that 93%[11] of the respondents indicated that the Compliance Officer attends Board Meetings. It should be noted that out of the three CSPs who indicated that the Compliance Officer does not attend Board Meetings, compliance reports are still presented to the Board whilst in the other case compliance reports are presented by the Compliance Officer to the risk committee.

The Authority positively noted that all CSPs indicated that the Board of Directors follows-up on any recommendations and/or action points specified in the compliance reports. Most commonly, CSPs indicated that the documentation of such follow-up action is done through recording of action points in Board minutes which remain open until fully resolved. Some Authorised Persons indicated that the Board follows up through updates in the subsequent compliance reports presented.

CSPs were also required to indicate the manner in which the Compliance Officer ensures that the Board of Directors follows up on any findings identified. In this regard, a variety of responses were provided, with the majority of CSPs indicating that the Compliance Officer would raise pending action points in subsequent compliance reports until resolved, whilst others indicated that this is done through testing and monitoring of pending action points.

Regulatory Requirements

The Board of Directors of CSPs collectively remains ultimately responsible for the compliance of the Authorised Person with all applicable legal and regulatory requirements. In this regard, the Board of Directors is required to ensure that it obtains regular updates from the Compliance Function and that it follows up on any pending matters raised by the Compliance Officer to enhance the Authorised Person's overall compliance with the applicable laws and regulations. Authorised Persons are also referred to R3-6.2(iii) and R3-6.5 of the CSP Rulebook.

[11] The statistical data provided under this section is based solely on the sample portion of legal persons.

8. Training

8.1. Staff Training

The Authority noted that when requested to indicate the manner in which the Authorised Person ensures that the staff attends training, CSPs commonly referred to the maintenance of a training log. The Authority positively noted that a number of CSPs indicated having specific training plans in place for their staff. CSPs are expected to undergo ongoing training on various aspects of the authorised business in order to keep abreast of legislative and regulatory developments.

CSPs made frequent reference to the holding of annual training which however focused solely on anti-money laundering obligations with very few references to training in relation to the CSP's activities and the CSP legal and regulatory regime. The Authority noted that even fewer references were made to training on the CSP's internal policies and procedures.

With regards to the involvement of the Compliance Officer in identification of the training plan for staff, the absolute majority of respondents indicated that the Compliance Officer is involved in identifying the training needs of staff with particular reference to their role within the Authorised Person.

Regulatory Requirements

CSPs are expected, in terms of R3-6.6.5 and R3-6.6.6 of the CSP Rulebook, to ensure that adequate training plans are implemented with respect to their staff, taking into account the role carried out within the CSP by the particular staff member. Therefore, CSPs are expected to undergo ongoing training on various aspects of the authorised business in order to keep abreast of legislative and regulatory developments applicable to the CSP, particularly with regard to its regulated activities. Therefore, whilst the Authority commends CSPs on the training efforts vis-à-vis their anti-money laundering obligations, in recognition of the vulnerability of this sector to money laundering and terrorist financing, CSPs are reminded to ensure that training also extends to all other applicable obligations. Authorised Persons are further reminded of the importance of holding training on their internal policies and procedures, with a view to ensuring that staff carry out their duties in accordance with such policies and procedures.

Furthermore, the Compliance Officer, as the person responsible for the Compliance Function of the Authorised Person, is expected to at least be involved in identifying the training needs of the staff members commensurate with their role.

8.2. Training attended by the Compliance Officer

The Authority noted that 5 out of 49 CSP respondents indicated that the Compliance Officer did not attend any training in the past 12 months in relation to the licensable activities carried out by the CSP.

With regards to those CSPs which indicated that the Compliance Officer attended training, the Authority noted that training covered the CSP regime, regulatory reporting, anti-money laundering and counter-terrorism financing, sanctions, corporate governance, tax and data protection.

The Authority also noted the training indicated was organised by different types of training bodies, ranging from competent authorities including by the MFSA, associations of various professions and advisory service providers.

Regulatory Requirements

The Authority draws the attention of Authorised Persons to Section 8.1 above, particularly with respect to those Authorised Persons who indicated that the Compliance Officer did not attend any training relating to the CSP's activities in the past 12 months. CSPs are expected to undergo ongoing training as part of their ongoing fitness and properness.

Additionally, the Compliance Officer, as the person responsible to ensure compliance by the Authorised Person with all applicable legislative requirements, should ensure that they keep themselves updated at all times with all the legal and regulatory developments. This is to be achieved at least in part through the attendance of relevant training.

CONCLUSION

The findings arising from this Thematic Review are being highlighted in this letter with the aim of sharing experiences, best practices indicated by Authorised Persons themselves and drawing attention to potential weaknesses identified in relation to the compliance function of CSPs. This is in turn ultimately aimed at further strengthening not only the compliance function, but also the overall governance culture of all CSPs. Pursuant to the feedback provided through the Thematic Review questionnaire, the Authority noted a commendable improvement by CSPs in respect of the implementation of their Compliance Function however the Authority encourages CSPs to continuously strive to continue enhancing their Compliance Function in line with the Authority's expectations and recommendations put forward in this Thematic Review.

In this regard, the Authority wishes to highlight that amongst the salient recommendations made in this Thematic Review, CSPs should in particular focus on taking the necessary measures to safeguard the independence of Compliance Officers in the execution of their role. Another area of focus should be the carrying out and documentation of testing in terms of the CMP, covering also breaches as an area for testing. Additionally, CSPs are expected to follow-up and act upon any recommendations made by the Compliance Officer pursuant to the findings emanating from testing carried out in terms of the CMP in a timely manner. The Authority would like to stress the importance of the provision of updates by the Compliance Officer to the Board of Directors on compliance matters which should be duly discussed and minuted.

The Authority would like to highlight the importance that all CSPs, not merely those which formed part of the sample of this Thematic Review, **carry out a gap analysis** in relation to their Compliance Function to take into account all the findings and recommendations made in this Thematic Review. The gap analysis should be duly documented and made readily available to the Authority upon

request. The Authority may verify the said gap analysis during future supervisory interactions with CSPs.

CSPs are expected to ensure that they take the necessary actions to align the set up and operations of their Compliance Function with the MFSA's expectations, leading to the enhancement of one of the Authorised Persons' key functions. In taking the necessary corrective actions to align their position with the MFSA's expectations, CSPs are expected to adopt a proportionate approach taking into account the nature, size and complexity of their authorised business. This would in turn strengthen the application of the Three Lines Model adopted by CSPs.

Should anything remain unclear or further guidance on achieving the Authority's expectations in practice be required, authorised persons are invited to contact the Authority, accordingly. The MFSA remains committed to continue providing guidance on best practices to continuously improve the compliance and governance culture in the financial services sector.

Yours faithfully,

Malta Financial Services Authority

Christopher Peter BUTTIGIEG (Signature)

Digitally signed by Christopher Peter BUTTIGIEG (Signature)
Date: 2025.02.17 12:24:41 +01'00'

Christopher P. Buttigieg
Chief Officer Supervision

Petra Camilleri
Deputy Head - Trustees and Company Service Providers Supervision Function

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.