25 November 2025

To: The Authorised Person,

To: The Management Body,

To: The Risk Officer

Thematic Review on the Risk Management Function of Company Service Providers

You are receiving this letter as the Authorised Person, the Management Body and/or the Risk 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 2025[1] identified the area of risk management as one of the key supervisory priorities to focus on during 2025 vis-à-vis 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, including risk management. Company Service Providers' residual risk level in the latest National Risk Assessment ('NRA')[3] published in 2023 was that of medium-high risk, with the provision of offering of registered office service alone, being rated as posing the highest risk in terms of ML/FT risks. The NRA examined how CSPs are often misused in creating Maltese registered legal persons with no sufficient links to Malta, for money laundering or concealment of beneficial ownership, or of having clients abusing of complex corporate structures for the same reasons. Therefore CSPs, as gatekeepers of the financial services industry, are expected to build strong risk cultures within their organisations and ensure a comprehensive understanding of all risk/s they face or may face, including those relating to money laundering and terrorist financing, and beyond and to ensure that they have in place robust controls to mitigate such risks. This is exacerbated by the constant evolution of the legal, regulatory and business environment in which they operate it. In this regard, the Authority will continue to ensure that CSPs are adequately managing their risks and that they operate in a sound manner, safeguarding overall market integrity.

The foundations of risk management in the CSP industry are built upon CSPs' understanding of their business environment especially in an environment wherein risks are constantly changing, which may have deteriorating effects on their systems, operations, reputation and ultimately their business continuity and client service. The Board of Directors is responsible for developing and fostering a risk-awareness culture at all levels of the CSP whilst also encouraging communication and accountability. CSPs are reminded that the aim of risk management is not to eliminate risk but rather

[1] MFSA Supervisory Priorities 2025
[2] https://www.mfsa.mt/wp-content/uploads/2023/02/MFSA-Strategic-Statement.pdf
[3] PublicNRA_Dec2023.pdf

to take a proactive approach to scenarios which could lead to detrimental effects on the regulated business. In order to build a robust risk management function, the CSP Rulebook imposes upon all CSPs to have a risk management framework in place be able to identify, analyse and evaluate risk, accordingly. When applying the bowtie analysis method, CSPs are expected to ensure they are aware of the risk/s they face and assess their current controls which act as preventive controls to the happening of such risk/s. On the other hand, CSPs should also have in place recovery controls which mitigate the negative effects of risks which have occurred or which most likely will occur. CSPs are encouraged to take on a proactive rather than a reactive approach to risk management to sustain business resilience.

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 2025, the Company Service Providers Supervision ("CSPs") Function carried out a thematic review focussing on the effectiveness and resilience of CSPs' risk management function (the "Thematic Review"). This Thematic Review was launched in the form of supervisory meetings held with identified CSPs having an independent risk management function and therefore having an appointed Risk Officer in place. For the purposes of this Thematic Review, the Authority selected, on a risk-based approach, a sample of ten out of sixty-one CSPs authorised as Class C CSPs in terms of the Company Services Act (Chapter 529 of the Laws of Malta) ("CSP Act") and having an independent risk management function, representing 16.4% of the population. The sample of ten CSPs comprised of nine CSPs (90% of the sample) constituted as legal persons, and one CSP (10% of the sample) being a natural person.

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 Risk Management Function where gaps are identified. As an overall observation, the Authority positively noted the importance being given by CSPs to the risk management function which was introduced by the issuance of the CSP Rulebook back in 2021. It was observed that CSPs indeed comprehend the importance of analysing risks faced in their day-to-day operations, including both those ML/FT in nature and also non-ML/FT risks. In fact, the Authority noted an array of non-ML/FT risks identified by CSPs, some of which were specific to their business models whilst others were faced by all CSPs. Furthermore, it was also noted that at times, past events have led CSPs to identify new risks which they then took into account in their risk assessment models.

On the other hand, whilst it was observed that all CSPs ensured to have in place a separate function which operates independently, certain deficiencies in the effectiveness of such risk management functions were noted. Most prominently, the Authority noted a lack of identification of various non-ML risks which the individual CSPs face, for example, reputational risk, risk related to lost contact clients, outsourcing risk and risks relating to cybersecurity. Furthermore, the Authority further noted that ineffective controls were being implemented for the wide range of risk/s identified by CSPs and which do not effectively mitigate the risks emerging from such risks identified. Additionally, the Authority noted instances wherein CSPs did not document the testing of such controls in place. Lastly, whilst all CSPs had a risk register in place, such registers lacked certain regulatory requirements, as shall be described in further detail below.

In assessing the effectiveness of CSPs' risk management functions, the Authority took into account the nature, size and complexity of the authorised business of the CSPs in question. In fact, the business model of the CSPs was a starting point in analysing their risk management function. With this principle of proportionality in mind, the Authority ensured that its expectations are well-aligned with the size, nature and the different setups and arrangements in place by the CSP, including whether it outsources any functions, its risk appetite and the level of complexity of IT systems utilised, for example. Therefore, whilst risk management obligations are applicable to all CSPs, the Authority does take into account the size and business model of the Authorised Person in reaching its determination as to whether such risk management obligations are being adequately adhered to.

The Authority is committed to strengthening the risk culture of CSPs by engaging in further outreach and guidance on the subject matter. In fact, as identified in MFSA' Supervisory Priorities of 2025, the assessment of CSPs' risk management function is part of the Authority's outcomes-based supervision. Therefore, the Authority will be focusing on the intended results from the supervisory meetings carried out and will derive an efficient way to achieve them.

KEY FINDINGS

1. Role of the Risk Officer

1.1. Time Commitment

On average, the Authority noted that Risk Officers of the CSPs forming part of this Thematic Review allocated 3.5 hours per week to their role. It was communicated that there are specific periods throughout the year wherein more hours need to be dedicated, and which time allocation also depends on the type and amount of testing to be carried out during a particular period. Furthermore, in instances wherein the Risk Officer held other roles within the CSP's organisational structure, such as also being the compliance officer and/or money laundering reporting officer, very often the Authority noted that such individual had a team assisting him/her in the performance of such roles. When taking into account the nature and size of the CSPs in question, the Authority noted that in general, Risk Officers are dedicating sufficient time to carry out their role.

Regulatory Requirements

In accordance with R2-5.10 of the CSP Rulebook, Risk Officers must be able to commit sufficient time to perform their functions efficiently and effectively and in terms of R4-4.4 of the CSP Rulebook, CSPs must ensure that such person is capable of committing sufficient time and are expected to conduct both a qualitative and quantitative assessment of their officials' time commitment. 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[4], and which criteria should be satisfied on an ongoing basis throughout the tenure of any approved role.

2. Policies and Procedures

2.1. Risk Management Policies and Procedures

The Authority positively noted that 90% of the CSPs forming part of this Thematic Review had a risk management policy and procedure in place. Overall, the risk management policies reviewed established the basic principles of risk management with respect to the identification, assessment, monitoring and management of the risks faced by CSPs. Whilst the Authority assessed the respective policies in line with the CSPs' business model and principle of proportionality, the Authority noted a number of policies failed to include certain key detail about their risk management frameworks. These included: the risk appetite of the CSP, the role of the Risk Officer and the manner in which the Risk Officer carries out his/her role including any tools used, the manner of reporting to the Board of Directors or the Authorised Person, the different risk assessments carried out by the CSP a description of controls in place to mitigate risk identified.

Regulatory Requirements

In terms of R3-7.1(ii) of the CSP Rulebook, CSPs are required to establish, implement and maintain adequate risk management policies and procedures, which identify risks relating to the CSP's activities, processes and systems and set the level of the CSP's risk appetite.

By way of guidance the Risk Management Policy should, *inter alia*, include:

- Objective and scope of policy;
- The role of the Risk Officer and the Board in terms of oversight of the Risk Management Function;
- The CSP's risk culture and the role of the Risk Management Framework within the CSP's structure;
- Risk Appetite Statement;
- The manner in which the CSP identifies, analyses, evaluates and treats risk;
- A description of the different risk assessments carried out by the CSP, including the Business Risk Assessment, the assessment in terms of R3-7.1 of the CSP Rulebook (where applicable) and the customer risk assessment, including any trigger events which would require a risk re-analyses;
- Reference to other policies which may already embed risk-related matters;
- Establishment of the Risk Register and its contents;
- Description of controls in place, including testing thereof;
- Reference to risk owners;
- Reporting to the Board, including the contents of risk reports presented;
- Internal risk reporting, such as internal escalations; and
- Training and Awareness.

[4] GUIDANCE ON THE FITNESS AND PROPERNESS ASSESSMENT APPLIED BY THE AUTHORITY

2.2. Frequency of Review

The Authority positively noted that the majority of CSPs indicated that their risk management policies and procedures are reviewed at least annually, or upon the happening of a trigger event to ensure that these are in line with both internal and external factors and also with their internal practices.

Regulatory Requirements

CSPs are expected, in accordance with R3-6.5 of the CSP Rulebook, to review the adequacy of their risk management policies and procedures at least annually. The said review should not simply take into account any changes in the legal and regulatory framework of CSPs but should also take into account any changes to their internal or external factors. Furthermore, CSPs are to ensure that their staff are also regularly trained on such policies and procedures, in line with R3-6.2(ii), R3-6.6.5 and R3-6.6.6 of the CSP Rulebook.

2.3. Adherence with Risk Management Policies and Procedures

CSPs were questioned on the manner in which they ensure adherence by their staff to their risk policies and procedures. In this regard, a variety of measures were indicated by CSPs, including: testing employees on such policies and procedures, provision of yearly training, the attainment of a written confirmation from staff that they have read and understood the internal policies and oversight carried out by a senior employee. 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 and that 9 out of 10 CSPs indicated that specific training is provided to staff on such policies and procedures, including the Board of Directors.

Regulatory Requirements

CSPs are expected to ensure, in terms of R3-7.1(v)(b) of the CSP Rulebook, to monitor the level of compliance by its approved persons and staff members with its risk management policies and procedures. Furthermore, in terms of R3-7.1(v)(c) of the CSP Rulebook, CSPs are also expected to monitor the adequacy and effectiveness of measures taken to address any deficiencies in those policies and procedures, including failure by the relevant persons to comply with therewith.

3. Business Risk Assessment

3.1. Identification and Assessment of ML/FT Risks

The Authority positively noted that all CSPs which formed part of this Thematic Review had a Business Risk Assessment in place and which accounted for several ML/FT risks, including the four risk pillars, in line with applicable AML/CFT legislation and regulation. All CSPs described in detail the methodology used behind the drafting of their Business Risk Assessment and the qualitative and quantitative assessments carried out together with their assessment of the likelihood and impact of such risks.

The Authority noted however that very often, CSPs failed to assess the risks of the provision of CSP services for which they are authorised to provide in view of the fact that at the time of the supervisory meeting, they were not providing such a service. These included for example provision of corporate directorship services and provision of registered office services. Furthermore, the Authority noted that at times, CSPs failed to assess the risks emanating from the provision of registered office services alone, when having clients to whom they only offered registered office services.

On the other hand, as a good practice the Authority noted that CSPs are analysing the risk emanating from the provision of a combination of CSP services rather than only assessing them individually, as shall be described in the following section.

Regulatory Requirements

In terms of R3-6.4 and R3-7.1(i) of the CSP Rulebook, CSPs are required to undertake an assessment with the purpose of understanding and identifying all the risks associated with their business model and target markets. Such assessment should not be limited to ML/FT risks and should be duly documented and reviewed regularly in line with the changing environment within which the CSP is operating. This assessment should be carried out particularly considering all the CSP services CSPs are authorised to provide. Furthermore, the carrying out of such assessment taking into account the contextual environment in which such CSP services are being provided and any changes thereto is also in line with the recommendations made by the NRA.

3.2. Controls Implemented in terms of ML/FT Risks

The Authority positively noted that the majority of CSPs implement controls to mitigate the ML/FT risks identified. However, the Authority also noted that, in a few instances, identical control measures were applied across the board for the different CSP services assessed, which controls did not adequately reflect the risks emanating from the respective CSP services. For instance, a few CSPs indicated ‘scrutiny of transactions of the customer relationship’ as a control measure implemented in terms of the provision of formation services, arranging for another person to act as a company secretary and the provision of registered office services.

As stated in the previous section, the Authority positively noted that at times, CSPs considered the provision of a combination of CSP services to act as a control measure to mitigate risks which arise from the provision of a singular CSP service. For example, providing directorship services with registered office services, with the latter providing minimal insight into the business activity of the client than the former. However, when assessed together, CSPs deemed the risk of providing such services together to be lower than providing the service of registered office alone, for example.

Regulatory Requirements

In terms of R3-7.1(iv) of the CSP Rulebook, CSPs are expected to adopt effective controls, processes and mechanisms to manage and mitigate the risks relating to the CSP’s activities, processes and system, in light of that level of risk tolerance. In this regard, CSPs should ensure to implement applicable, effective and robust control measures in order to mitigate the risks emanating from their

CSP business. Such controls should directly address the nature of the risks they are intended to mitigate.

4. Risk Register

The risk register is one of the tools utilised by CSPs in order to ensure that CSPs are kept abreast of current and emergent risks. In essence, the risk register should provide a snapshot of the CSPs' clients together with the risks inherent to their business models and should also include an assessment of risks which go beyond ML/FT in nature, together with their likelihood and impact, whilst also outlining mitigation strategies to control such risk. In terms of the CSP Rulebook, the risk register shall, as a minimum, consist of the below criteria which are hereby being described and explained below. The Authority positively noted that all the CSPs forming part of this Thematic Review had a risk register in place. However, considerable divergencies from the requirements of the CSP Rulebook were also noted.

4.1. Clients' Risk Rating and Risks Inherent to their Business Model

The majority of the risk registers reviewed did include a list of CSPs' clients together with the risk rating attributed to them respectively. However, the most common deficiency noted related to the lack of identification of the risks inherent to the business model of CSPs' clients. In most cases, a few of the risk factors were identified, such as the services provided to the client, which however did not comprise all the risk factors which led to the final risk rating of the client. On the other hand, there were also instances wherein this part of the risk register was left out completely.

Regulatory Requirements

In terms of R3-7.6(a) and (b) of the CSP Rulebook, in the first part of their risk register, CSPs are expected to (i) list all their CSP clients together with the relevant risk rating awarded and also include (ii) an identification of the risks inherent to the business model of each client which led to the final risk rating. It is important to note that the aim of the risk register is for CSPs to have a snapshot of the risks which their clients pose in order to determine whether the necessary controls are in place in order to mitigate such risk/s. This is also in alignment with the recommendations made by the NRA to ensure, in this case CSPs, are fully aware of the risks associated with their clients particularly in the context of legal persons.

4.2. Non-ML/FT Risk Assessment carried out in terms of R3-7.1(i) of the CSP Rulebook

4.2.1 Identification and Assessment of Non-ML/FT Risks

CSPs are required to identify and assess non-ML/FT risks they face in their day-to-day operations. The Authority noted that the majority of CSPs forming part of this Thematic Review carried out a separate assessment of non-ML risks from their Business Risk Assessment whilst only a few CSPs identified and assessed both ML/CFT and non-ML/FT risks in their Business Risk Assessment.

The Authority positively noted an array of non-ML/FT risks which the CSPs forming part of this Thematic Review identified. These included those risks relating to: outsourcing, legal, regulatory & compliance, conflicts of interest, recruitment, marketing, capital adequacy requirements, internal controls, record-keeping, employees, complaints, IT failure, cyber security, physical security, environmental and pandemic, financial, reputational, health & safety, strategic and those related to lost contact clients. Consequently, this portrayed CSPs' understanding the importance of such type of risks and which could, similar to ML/FT risks, have detrimental effects on their regulated business. However, most CSPs individually failed to assess a number of these non-ML risks which they were facing or could potentially face. The most common risks which were not considered by the individual CSPs were risks related to outsourcing and reputational risks related to lost contact clients.

The Authority positively noted as a good practice that non-ML/FT risks identified in the risk register were quantitatively and qualitative assessed in terms of their probability and impact on the CSP and the residual risk of such risks was also determined. A good practice noted during the review of risk registers provided was the identification of risk owners of the risks identified. In this regard, CSPs explained that such risk owners would assume the function contingent to that risk category and be aware of their responsibilities where any risks that could pose any threat to the CSP would have to be brought to the Board of Director's attention. In this regard, the Authority noted one instance where one risk owner was identified by the CSP for all risks identified in the risk register despite the differing nature of the risk categories. The Authority would like to highlight the importance that the risk owner identified for the particular risk should be well versed in the specific category particularly to identify any potential threats to the CSP. This is especially the case with respect to risks which are of more technical nature such as cybersecurity risk and financial risk.

The Authority further positively noted that all CSPs indicated that this assessment is reviewed at least on annual basis or upon the happening of a trigger event which would merit a re-assessment of the risks identified. Furthermore, the Authority positively noted that all the CSPs forming part of this Thematic Review confirmed that they assess the causes and consequences of both actual and potential risks which they may face. In this regard, it was noted that CSPs take on a proactive rather than a reactive approach to risk management and understand the benefits of being equipped with the necessary controls in view of any emerging risk/s which they may face.

As a good practice, the Authority noted the practice of carrying out one-to-one meeting by the Risk Officer with the different risk owners in order for the Risk Officer to gain a thorough understanding of existing controls, identify any gaps and introduce additional risk areas which are already not accounted for by the CSP in view of new and emerging risks.

4.2.2. Controls Implemented

Whilst the majority of CSPs have identified controls in order to mitigate risks arising from such non-ML/FT risks, most of these controls solely referred to policies and procedures adopted by the CSP without adequately describing the practical aspect of the mitigating measure implemented. For example, in terms of IT failure and cybersecurity risk, very often reference to the IT and cybersecurity policy was made without, for example, naming whether there is regular and effective communication with the IT providers or whether independent reviews on the IT system are carried out. In terms of IT connectivity breakdown, one CSP simply made reference to the fact that the risk of nationwide electricity outages remains high without describing an actual control in place. Nevertheless, during the supervisory meeting held, the CSP then described how it has in place a dual internet connection which is tested together with a power generator. However, such controls were not included as part of the risk register.

On the other hand, other CSPs included various control measures in place such as IT disaster recovery arrangements in place, server room secured and arrangements to provide back-up recovery site with respect to business continuity risks. With respect to the risk of inadequate information technology systems, as control actions CSPs identified appraisal of system needs and options, appraisal of security and authorisation procedures, implementation of measures to secure and protect data etc. With respect to the risk of exceeding budgets, the controls included the regular analysis of actual spend versus budget and reviews of spending by the Chief Financial Officer, regular reporting and review of budgetary position to Senior Management. In relation to the risk of being under insured and having inadequate insurance the controls mentioned related to the immediate communication to the insurance provider on any changes in activities, appointment of reputable insurance providers, insurance products and risks reviewed annually, and the insurance policy reviewed annually.

Furthermore, on two occasions the Authority noted that risks were identified in risk management policies of the CSP which however were not then subsequently assessed in any risk assessment carried out by the CSP. Consequently, the CSPs in question failed to identify the residual risk of such risks identified and also failed to have in place robust controls to mitigate the risk/s. In a few instances, the Authority also noted that CSPs had no controls in place for certain risks identified.

Regulatory Requirements

CSPs face a diverse range of risks which go beyond ML/FT in nature. In this regard, they are expected to carry out a thorough assessment of such risks by referring to both internal and external factors. In terms of R3-7.6 of the CSP Rulebook, the risk register shall contain an assessment, based on the assessment carried out in terms of R3-7.1(i) of the CSP Rulebook outlining other risks, typically non-ML/FT risks which the CSP is exposed to or may potentially be exposed to. As outlined above, there were CSPs which amalgamated this assessment into their Business Risk Assessment and therefore this assessment was not required. However, the majority of CSPs indeed carried out a separate assessment of such non-ML/FT risks and which assessment formed part of their risk register.

In this regard, CSPs are expected to ensure that a qualitative and quantitative assessment of non-ML risks which they face, or may potentially face, is carried out. By devising key risk indicators, CSPs will ensure that the likelihood and probability of a risk materialising and its consequences does not exceed their risk appetite. The type of risks to be assessed here should reflect the CSPs' IT technologies used, governance structure and reporting lines, any reputational risks which they may face, staff complement etc. Therefore, CSPs are expected to ensure that any risks emerging from any aspect of their business is duly included in this assessment, or in their Business Risk Assessment, as applicable.

In furtherance to the identification of non-ML/FT risks, CSPs are also expected, as part of this assessment, to ensure they have in place robust controls in order to mitigate such risks. Such controls should adequately target the risk/s emanating from the respecting risks identified by the CSP and should be adequately described in the risk register. Furthermore, CSPs are also required to assess the effectiveness of such controls in place in order to determine whether any deficiencies need to be addressed.

5. Cybersecurity

Amongst the various risks which were identified and discussed with the CSPs forming part of this Thematic Review were risks relating to cybersecurity. The most common examples of cybersecurity risks which CSPs face were described as being phishing, hacking and loss of sensitive data. Very often, CSPs expressed their lack of expertise in this area and their complete reliance on outsourced IT professionals in terms of not only in the identification of new and emergent cybersecurity risks, but also in the testing and addressing of any deficiencies in controls in place. In fact, during the supervisory meetings held, a number of CSPs struggled to describe the measures in place with respect to identification of cybersecurity risks and testing.

Apart from the reliance on outsourced IT professionals, CSPs also mentioned other controls in place to mitigate cybersecurity risks such as having strong firewalls in place, two-factor authenticators, holding of different servers for each department of the CSP to minimise risk of loss of all data, Chinese walls, access rights provided on a needs-based basis and the carrying out of audits by third parties.

CSPs were also queried on the procedure in place should employees face a cybersecurity attack. In this regard, the majority of CSPs indicated that they have an internal escalation procedure in place and that the CSPs' outsourced IT provider will be notified immediately. In this regard, the Authority noted 3 out of 10 instances where the internal escalation procedure was not formally documented in any of the CSPs' policies. In fact, one of the said three CSPs explained that such procedure is contained in an email circulated to staff.

The Authority positively noted that only one CSP indicated that it does not have any cybersecurity policies or procedures documented and another CSP which indicated that such policy is not tested. Furthermore, the Authority also positively noted that all CSPs which formed part of this Thematic Review were aware of the Guidance on Technology Arrangements, ICT and Security Risk Management and Outsourcing Arrangements[5] which was issued by the Authority on 30 June 2020 (the 'Guidance').

Regulatory Requirements

CSPs are required to ensure that they have the necessary knowledge to identify, assess and mitigating risks relating to cybersecurity. Lack of awareness may lead to weak systems in place and a higher degree of probability of attacks. Therefore, in terms of R3-6.6.6 of the CSP Rulebook, CSPs, including employees at all levels, are expected to undergo necessary training to ensure they are kept abreast with latest developments.

CSPs are required to have in place robust systems and procedures dealing with cybersecurity in light of the detrimental effects which could affect their regulated business in their day-to-day operations should they face a cyber-attack. In this regard, in terms of R3-12.8 of the CSP Rulebook, CSPs are

[5] Guidance on Technology Arrangements ICT and Security Risk Management and Outsourcing Arrangements

expected to take into account the size, nature, scale and complexity of their business and on a best effort basis refer to the Guidance to ensure they are well-equipped in terms of cyber security risks. In this regard, CSPs should ensure they have in place policies and procedures dealing with cybersecurity together with robust controls in place in order to mitigate any cyber security risks. Furthermore, in terms of R3-11.6.4 of the CSP Rulebook, CSPs are expected to test their systems in place at least annually, which testing should be duly documented.

6. Documentation of Risk Control Testing

During the review of the risk reports provided, the Authority noted that the majority of the reports reviewed failed to indicate the testing carried out, and the outcome thereof, by the Risk Officers on existing controls the CSPs have in place to mitigate current or emergent risks. In this regard, whilst the majority of CSPs verbally confirmed that testing is in fact carried out by the Risk Officer, this is not being documented in risk reports, despite very often this being mandated in risk management policies.

In a few instances, CSPs noted that testing carried out on existing controls was described in risk reports however, this testing lacked detail with respect to the method of testing and the outcome thereof. Therefore, the Authority was not in a position to assess the adequacy of such testing carried out or identify any gaps in the CSP's controls. Furthermore, the Authority further noted that very often, no follow-ups on the deficiencies identified in risk reports on such testing was noted in subsequent reports.

Regulatory Requirements

In terms of R3-7.1(iv) of the CSP Rulebook, CSPs are requested to adopt effective controls, processes and mechanisms to manage and mitigate the risks relating to the CSP's activities, processes and systems. Furthermore, in order to ensure the effectiveness of such controls, CSPs are expected to carry out regular testing on the controls implemented in order to ensure whether amendments or enhancements are deemed necessary, especially in light of any new risks identified. In this regard, CSPs are expected to set out a description of such testing, the outcome thereof and any recommendations set forth by the Risk Officer in risk reports prepared, which should be duly forwarded to the Board of Directors for their consideration. Furthermore, Risk Officers should ensure that the Board of Directors duly take onboard the recommendations and/or take the necessary action in order to address any deficiencies identified in the existing controls or implemented new controls required.

7. Provision of updates to the Board of Directors[6]

All Risk Officers forming part of this Thematic Review confirmed that they report directly to the Board of Directors of the CSPs in question forming part of this Thematic Review. The Authority positively noted that 90% of Risk Officers of the selected CSPs provide regular updates to the Board of Directors in the form of risk reports. It was also noted that another Risk Officer only prepared an annual risk report and kept the Board verbally updated on risk-related matters throughout the year.

[6] This section is based on data relating to CSPs constituted as legal persons.

The majority of risk reports reviewed included an overview of the Risk Officers' observations in terms of current risks faced by the CSP and the current controls in place. The Authority positively noted a good practice that such reports also included the identification of new and emergent risks however this was not widely applied by the CSPs forming part of this Thematic Review. Furthermore, the Authority noted that only a few reports included recommendations on existing and potentially new controls required to be implemented by the CSPs. Also, at times, reports lacked detail as to how particular risks identified in such reports were identified and what mitigating measures were implemented to control any emerging risks.

As discussed in Section 6 of this letter, the Authority was concerned to note that the majority of risk reports reviewed lacked a description of the testing carried out by the Risk Officer on the controls in place. In this regard, the Authority was not in a position to assess the level of effectiveness of the CSPs' controls in place for the risks identified.

Regulatory Requirements

In terms of R3-7.2(ii) of the CSP Rulebook, CSPs holding a Class C authorisation having an independent risk management function are required to provide reports and advice to senior management. Whilst the detail and frequency of such reports is not determined in the CSP Rulebook, CSPs are expected to provide updates to the Board of Directors on a regular basis in order to ensure that the CSP is well-aware of new and emergent risks, any changes in the effectiveness of any current controls in place or any new controls which need to be implemented. The Authority's expectation is that the frequency is determined by the business model and the risk appetite of the Authorised Person. The Authority expects that the higher the risk appetite the more controls should be in place and the higher the frequency of the risk reports. Furthermore, the contents of such risk reports should provide an adequate overview of any assessments carried out by the Risk Officer in the period being covered by the report, including an assessment of current/new risks, any new controls implemented, any changes to the CSP's risk appetite, detail on testing of controls carried out, including the outcomes thereof and recommendations put forward by the Risk Officer.

The Board of Directors of CSPs collectively remains ultimately responsible for the compliance of the Authorised Person with all applicable legal and regulatory requirements, including risk management requirements. In this regard, Board of Directors are required to ensure that they obtain regular updates from the Risk Management Function and that they follow up on any pending matters raised by the Risk Officer to enhance the Authorised Person's overall risk culture and compliance with the applicable laws and regulations, including risk management requirements. The Authority's expectation is that these reports, mitigating factors and follow ups are formally discussed during Board Meetings and such discussions are duly documented.

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 risk management function of CSPs. Following the carrying out of the supervisory meetings with the identified CSPs and the review of all documentation provided, the Authority was pleased to observe the importance being given to the risk management function by CSPs. The Authority noted an appetite for consideration of various risks albeit the need for further training with respect to particular risks, especially those relating to IT and cybersecurity.

In this regard, the Authority wishes to highlight that amongst the salient recommendations made in this Thematic Review, CSPs should in particular focus on ensuring that non-ML/FT risks are taken into consideration in their risk assessments and that robust controls are put in place in order to mitigate risks emerging thereof. Additionally, Risk Officers are expected to provide detailed reports to the Board of Directors, including an assessment of all testing carried out and recommendations put forward in order to ensure that the Board of Directors is being kept abreast of any new and emergent risks. Finally, the Authority would like to stress on the importance of the requirements of the contents of the risk register, as set out in the CSP Rulebook and described in detail in this letter.

The Authority would like to highlight the importance that all CSPs, not merely those which formed part of the sample of this Thematic Review or those required to appoint a Risk Officer, **carry out a gap analysis** in relation to their Risk Management 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 Risk Management 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 risk management culture in the financial services sector.

Yours faithfully,

Malta Financial Services Authority

Christopher Peter BUTTIGIEG (Signature)

Digitally signed by Christopher Peter BUTTIGIEG (Signature)
Date: 2025.11.25 14:55:13 +01'00'

Christopher P. Buttigieg
Chief Officer Supervision

Alison CORTIS (Signature)

Digitally signed by Alison CORTIS (Signature)
Date: 2025.11.25 14:27:30 +01'00'

Alison Cortis
Head - 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.