MFSA MALTA FINANCIAL SERVICES AUTHORITY

Guidance Note on the Fulfilment of Post-Authorisation Requirements

Company Service Providers

CONTENTS

REVISIONS LOG

VERSION	DATE ISSUED	DETAILS
1.00	04 October 2023	Guidance Issued

A. Introduction

Through the amendments made to the Company Service Providers Act [CAP. 529 of the Laws of Malta] (the 'Act') by Act L of 2020 which came into force on 16 March 2021, any person providing Company Service Provider services ("CSP") to third parties by way of business, as further defined in the amended Company Service Providers Rulebook, was required to submit an application for authorisation as a Company Service Provider, specifically bringing into scope certain service providers which were previously exempt from obtaining authorisation. Applications for authorisation by such persons were to be submitted within a transitory timeframe prescribed by law.

Following completion of the application process, successful applicants were granted an authorisation in terms of the Act by the issuance of an Authorisation Letter and a Certificate of Authorisation. As per Article 5(3) of the Act, as also supplemented by Section 3.4.2 of the Authorisation Process Service Charter[1], the Authority is empowered to subject applicants to any restrictions or conditions it may deem appropriate. In fact, during the authorisation process carried out during 2021 and 2022, the Authority imposed specific post-authorisation requirements on identified Authorised Persons via means of a written letter, which requirements were to be complied with, or addressed, within the stipulated timeframe.

As set out in the 'Authorisation Process Service Charter', adherence to, and ongoing internal monitoring in relation to post-authorisation requirements, remains the primary responsibility of the Authorised Person. Authorised Persons are reminded that during the authorisation process they were duly informed of the post-authorisation requirements being imposed and they had duly signified their acceptance to such requirements. Therefore, failure to comply with the post-authorisation requirements within the stipulated timeframes, may lead to the withdrawal of the authorisation issued by the Authority. Lastly, it is the responsibility of the Authorised Person to immediately notify the Authority in a timely manner, and preferably before the expiration of the given timeframe, if any difficulties are encountered in implementing any of these post-authorisation requirements.

In this regard, whilst this Guidance Note is focused on providing further insight of the post-authorisation requirements imposed on newly authorised CSPs, this guidance, specifically that set out in Section D below, provides guidance to all CSPs.

[1] Issued by the Authority on 30 June 2021 - https://www.mfsa.mt/wp-content/uploads/2021/06/MFSA-Authorisation-Process-Service-Charter.pdf

B. Purpose

The Malta Financial Services Authority (hereafter referred to as 'MFSA' or 'the Authority') is publishing this Guidance Note outlining the Authority's expectations in terms of the fulfilment of the post-authorisation requirements imposed on those persons authorised to act as Company Service Providers in terms of the Act in November 2022. Furthermore, this guidance is also intended to act as guidance for all CSPs issued with an authorisation and which are subject to a number of post-authorisation requirements, and in general to act as a reference point for best practices expected by the Authority vis-à-vis all CSPs.

C. Targeted Post-Authorisation Requirements

1. Governance

As part of the authorisation process, the Authority assesses the applicant's systems and controls by which its business is managed and operated as well as the suitability of all key personnel involved. In this regard, below are the main themes emanating from the post-authorisation requirements imposed by the Authority to address some gaps in relation to the governance matters, which were identified during the processing of certain applications.

1.1 Time Commitment

All approved persons must be able to commit sufficient time to perform their functions efficiently and effectively. 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 in the MFSA's Guidance on the Fitness and Properness Assessments.

Persons must ensure that their time commitment is adequate for their role and more importantly that this commitment does not diminish following the granting of the authorisation. Factors which may affect a person's time commitment include: the number of commitments held, the size and situation of the entities where the commitments are held, the nature, scale and complexity of the activities and any other professional or personal commitments and circumstances[2].

In this regard, Authorised Persons subject to post-authorisation requirements which required any of their officers to strengthen their time commitments, as set forth in the

Authorisation letter and Annex attached thereto, are to ensure that a quantitative and qualitative reassessment was undertaken following the issuance of the Authorisation Letter, and that it is undertaken on a regular basis thereafter to ensure ongoing compliance with these expectations.

1.2 Dual Control

The principle of dual control is set out in R3-6.6.2 of the Company Service Providers Rulebook (the 'CSP Rulebook') and requires that legal persons shall be effectively directed or managed by at least two directors. In the case wherein more than two persons are directing the business, a minimum of two persons' judgments must be engaged. In this regard, both persons must have sufficient experience and knowledge of the business[2] and where a single individual is particularly dominant, this will raise doubts concerning the fulfilment of this criterion.

Therefore, the expectation is for Authorised Persons to have taken the necessary action to ensure active participation of at least two individuals. In this regard, Authorised Persons are also expected to maintain adequate records to demonstrate adherence to this principle, which may be assessed and tested by the Authority in a supervisory interaction.

1.3 Yearly Assessments vis-à-vis Staff Complement

The Authority noted that a significant number of applicants had submitted business models wherein it was indicated that the CSP activities of the Authorised Person were to be provided as ancillary to the main line of business. In such instances, wherein the staff complement of the applicant was sufficient at the time of application stage, the Authority required the comfort that this would be adequate if the level of the business were to increase. In such cases, the Authority requested Authorised Persons to undertake an assessment on a yearly basis to determine whether an increase in staff complement is required.

In this regard, Authorised Persons subject to such post-authorisation requirement are required to ensure to undertake an assessment to determine whether its staff complement is still adequate in view of any increase level of business, which assessment should be duly documented.

[2] R3-6.6.4 of the CSP Rulebook.

2. Compliance Function

A CSP is required to establish and maintain a permanent and effective compliance function which operates independently. The Compliance Officer role is an onerous role necessitating adequate time and resource commitment and should therefore be carried out by persons who fully understand the extent of their responsibilities with adequate skill, knowledge and experience in both compliance and company service providers. This responsibility mainly revolves around ensuring that the business of the Authorised Person is being carried out in line with the applicable legislative and regulatory frameworks. In this regard, below are themes and respective guidance relating to some of the post-authorisation requirements imposed by the Authority, specifically targeting the compliance function.

2.1 Independence[3]

Compliance Officers are expected to demonstrate independence of judgement in order to ensure the effectiveness of their role within the organisational structure of the Authorised Person. CSPs should ensure that the Compliance Officer operates effectively, impartially and as a means of checks and balance over the rest of the operations of the regulated business. For example, a Compliance Officer should act independently of other officers or functions of a corporate CSP. In this respect, the Compliance Officer may not be involved in the performance of services or activities which s/he is required to monitor[4]. Particularly, the Compliance Officer should not form part of the dual control principle, vis-a-vis client onboarding decisions, and should be sufficiently independent from the client onboarding process[5] unless consulted to provide guidance with respect to compliance issues, if this is deemed necessary.

Therefore, in some instances certain CSPs were required to appoint, within the stipulated timeframe set out in the Authorisation Letter, an alternative Compliance Officer from the person approved at authorisation stage to enhance the independence element of the Compliance Function. ***To satisfy this requirement Authorised Persons are to identify an alternative compliance officer and ensure to submit a duly filled in Personal Questionnaire, prior to the expiration of the stipulated timeframe, so that the Authority carries out the fitness and properness test on the proposed individual.***

[3] This does not apply to authorised individuals who were authorised to carry out the roles of compliance officer and money laundering reporting officer of their own regulated business.
[4] R3-8.4(i) of the CSP Rulebook
[5] R3-8.4(i) of the CSP Rulebook

2.2 Compliance Work Carried Out and the Documentation thereof

Authorised Persons should ensure that the compliance function is properly trained and equipped to detect any risk of failure by the CSP to comply with its obligations under the applicable legislative and regulatory frameworks. This includes, *inter alia*, and as highlighted in some post-authorisation requirements imposed, the review of the CSP's policies and procedures and the testing of the CSP's systems. Furthermore, this function should ensure that adequate remedial action and proposals are set forth in order to ensure that any failures are duly rectified and sufficient measures are implemented to ensure that such instances are prevented from re-occurring.

In furtherance to the above, the compliance function is expected to document all the testing and monitoring carried out in terms of the Compliance Monitoring Programme drafted. From its supervisory interactions, the Authority notes that a common deficiency in the CSP industry relates to a lack of documentation of the work carried out by this Function.

In the case of individual CSPs, such persons are required to prepare an annual report which includes compliance-related matters. Further guidance on the contents of this report is set out in R2-6.1.3 of the CSP Rulebook.

In relation to corporate CSPs, the compliance function is expected to draw up an annual compliance monitoring programme (Refer to Section 2.3 below) and provide the Board with regular compliance updates in the form of compliance reports. Furthermore, the Board shall then be responsible to rectify any deficiencies identified by the Compliance Function, and all remedial action undertaken should also be documented. Following this, once deficiencies are addressed, the Compliance Function should ensure that adequate controls and tests are in place and implemented to ensure the effectiveness of any such measures taken.

Therefore, in order to address any imposed post-authorisation requirements in relation to the work carried out by the compliance function, and the documentation thereof, Authorised Persons are expected to have in place the necessary tools in order to carry out the respective compliance work, including but not limited to a compliance monitoring programme as outlined above (and as also further expanded upon in the following section), and to draw up compliance reports in the applicable form, addressing all the matters outlined in the CSP Rulebook, as applicable to the respective class of authorisation granted to the CSP.

2.3 Compliance Monitoring Programme

The Compliance Monitoring Programme ('CMP') is one of the tools used by a Compliance Officer in the performance of their work, as required in terms of R3-8.5 of the CSP Rulebook. This programme should set out the testing and monitoring to be carried out by the Compliance Officer in ensuring that the CSP's regulated business is being carried out in terms of the applicable legislative and regulatory frameworks. A CMP should be proportionate to the nature and size of the regulated business however generally, for an effective CMP, the MFSA expects the following elements to feature as a minimum set of criteria:

- that the Compliance Officer conducts a **proper risk assessment and mapping exercise to identify and prioritise compliance risk factors to the drafting and updating of the CMP**. The risk assessment should identify areas of high, medium and low compliance risk, identify any gaps in the compliance programme and test the controls in place to mitigate the identified risks. This risk assessment exercise should be data driven (not just theoretical), properly documented and reviewed on a periodic basis;

- the CMP should not merely be a tick-box exercise but should be **an ongoing programme aimed at monitoring the overall operations and procedures specific to the regulated entity, to ensure all aspects of the business are adequately monitored** (including all services being provided as part of the CSP's authorisation) and included as part of the CMP, such as, but not limited to: governance, policies and procedures, complaints handling, conflicts of interest, training, breaches register, delegation of powers, business continuity plan testing, monitoring of critical service providers, capital requirements and professional liability risks, segregation of funds, sampling transactions, AML Compliance and Customer Due Diligence, record-keeping and regulatory calendar of submissions;

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

- the CMP should state **the period during which the reviews/tests will take place**. In the case of entities, once drafted, the CMP should be presented to the Board/Management Body for consideration and approval, which should in turn ensure that the Company has in place effective Compliance Function monitoring and oversight.

Authorised Persons who were imposed with a post-authorisation requirement to submit a copy of the CMP are to be guided by the above, accordingly.

2.4 Mentoring

As part of the fitness and properness test applied by the Authority, the nature, size and business model of the applicant is taken into consideration when assessing whether the proposed Key Function Holder is suitable for the proposed role. During the processing of applications, the Authority noted that there were instances wherein applicants proposed individuals to act as Compliance Officer without having the combined expected level of knowledge and experience. In this regard, in some cases, and after having undertaken a holistic assessment of the systems and controls in place, the Authority approved the appointment of the Compliance Officer, qualified with a requirement to engage an external compliance consultant to mentor and guide the Compliance Officer for a specific time period. Upon expiration of the mentoring period, a further assessment may be held by the Authority through an interview with the Compliance Officer to assess the effectiveness of such mentoring.

Where such a post-authorisation requirement was imposed, Authorised Persons are expected to prepare a report setting out: the details of the individual who provided the mentoring and all integral information on the mentoring process, specifically on the areas focused on and the Compliance Officer's performance during this period. This report should be endorsed by the mentor and be readily available for review upon request by the Authority.

2.6 Compliance Officer Outsourcing Agreement

In instances wherein an Authorised Person has outsourced the compliance function, a post-authorisation requirement was imposed requesting the provision of the related outsourcing agreement. Reference is made to 'Title 9 – Outsourcing' of the CSP Rulebook which governs the information which should be included in such outsourcing arrangements by CSPs. ***To satisfy this requirement Authorised Persons are therefore expected to submit to the Authority the respective outsourcing agreement underlying this arrangement within the timeframes stipulated in the Authorisation Letter.***

3. Risk Management Function

As set out in R3-7.2 of the CSP Rulebook, Class C CSPs are required to establish and maintain an independent risk management function. The Authority undertakes a comprehensive assessment prior to making a determination as to whether a proposed individual shall be approved or otherwise as an independent Risk Officer. In some

instances, for the purposes of finalising the application process in line with the legislative deadline, the Authority approved the person proposed to hold the risk management function only for a temporary period, who was to be subsequently replaced. ***Authorised Persons imposed with a post-authorisation requirement to identify and propose an alternative person responsible for the risk management function should be duly guided by the below and should ensure to do so within the stipulated deadline set out in the Authorisation Letter.***

The independent risk officer should be sufficiently unconnected to the business units and should not be involved in revenue generation. An independent risk officer should therefore not be involved in other roles which may give rise to conflicts of interest (eg. executive director responsible for business generation, ultimate beneficial owners of the licensed entity etc). At the same time, the risk officer should have access to all business lines that have the potential to generate material risk to the Authorised Person and should therefore also be well aware of any risks which may be posed by other subsidiaries, affiliates or related entities whose activities could have an impact of the business of the Authorised Person.

Apart from the independence criteria, risk officers are also expected to have the knowledge and competence in the area of risk management, and to undertake any additional training, as necessary. A thorough understanding of the Authorised Person's risk management framework and policies is also expected in order for the risk officer to communicate and co-ordinate and administer risk management through strong relationships with key personnel across the organisational structure.

Should the Authorised Person deem that, in terms of R3-7.3 of the CSP Rulebook, it is not appropriate and proportionate to appoint an independent risk officer in view of the nature, scale and complexity of its business and the nature and range of the CSP services and activities undertaken in the course of that business, the Authorised Person may request a derogation from the Authority. In such instances, the Authority shall assess the request and make a final decision as to whether to grant such derogation or otherwise. During the application process, in certain instances, where the Authority regarded the derogation request as a borderline case, the Authorised Person was requested to provide further information in terms of the volume of business and number of clients for the coming three years of operation, in order to determine whether such derogation was still justifiable. Authorised Persons imposed with this post-authorisation requirement are to provide the requested data at the intervals and by the deadlines set out in the Authorisation Letter.

4. Professional Indemnity Insurance

Rules R3-5.1–R3-5.4 of the CSP Rulebook set out the requirement and necessary detail in relation to CSP's obligation of taking out and maintaining a full professional indemnity

insurance (PII) cover. The Authority notes that there were instances wherein CSPs had not yet obtained this PII cover at application stage and were imposed with a post-authorisation requirement to obtain this PII cover within a stipulated timeframe.

In this regard, CSPs imposed with this post-authorisation requirement are expected to provide a declaration, signed by the individual CSP or by two directors in the case of corporate CSPs, confirming that a PII cover was obtained in line with the CSP Rulebook within the timeframes stipulated in the authorisation letter. This declaration may be sent to the Authority in soft copy and signed in line with the 'Use of Electronic Signatures' Circular issued by the Authority on 15 November 2022 on tcspsupervision@mfsa.mt.

5. External Reviews

CSPs are expected to have in place the necessary controls in order to ensure that all the functions within its organisational business structure operate independently and effectively. In certain set-ups, the Authority noted a lack of independence and a high degree or interconnection between the functions, particularly where the same person was proposed to carry out multiple roles within the same business structure. In such instances, the Authority imposed post-authorisation requirements on Authorised Persons to engage an external third party to carry out an independent audit/review.

Authorised Persons imposed with this post-authorisation requirement are expected to have undertaken the independent audit within the timeframe set out in the Authorisation letter, and following this audit, Authorised Persons are to ensure to address any deficiencies noted. The remedial action taken should also be duly documented.

6. Training & Qualification

As part of the competence criteria forming part of the fitness and properness assessment, the Authority shall assess and determine whether the proposed person has an appropriate level of knowledge, professional expertise and experience in the relevant field. In this regard, where the Authority deems that the proposed person does not fully meet the competence criteria to the level expected, the Authorised Person shall be requested to demonstrate that such person has undergone relevant training or has obtained a qualification in relation to their proposed role. These may include, *inter alia*, training and qualification requirements relating to risk management, CSP Regulatory Framework, AML/CFT and compliance training.

6.1 Training

In instances wherein the Authority noted that a proposed person had a relevant background in relation to the proposed role but nevertheless lacked direct experience or formal qualifications, training was imposed in order to ensure that the proposed person is kept up to date on matters relating to the relevant area. ***Where such a post-authorisation requirement was imposed, evidence of the person having completed such training is to be duly provided to the Authority, where requested in the Authorisation Letter, or made available upon request thereafter.***

6.2 Qualification

In other instances, the Authority noted that the proposed person did not hold the necessary qualifications in relation to the proposed role and the individual's experience was not deemed to be up to the level expected. In such cases the Authority looked holistically at the governance set-up of the Authorised Person and where it was determined that adequate systems and controls were in place, despite the individual officer not fully meeting the qualifications criteria, Authorised Persons were conditionally approved subject to the attainment of such qualification by identified persons prior to the stipulated deadline as set out in the post-authorisation requirement. Such persons were also encouraged to keep abreast of developments in specific areas, for example AML/CFT, through the attendance of relevant training courses. ***Where such a post-authorisation requirement was imposed, evidence of the attainment of such qualification is to be duly provided to the Authority, where requested in the Authorisation Letter, or made available upon request thereafter.***

D. General Post-Authorisation Requirements

As outlined above in this Guidance Note, the Authority may grant authorisations which are subject to post-authorisation requirements where it deems that certain aspects of the proposed conduct of business or certain qualities of any proposed person of the applicant do not meet the Authority's expectations at authorisation stage. These requirements, together with the Authority's expectations in terms of their fulfilment, are set out below.

1. Compliance Officer

Authorised Persons should ensure that the Compliance Officer familiarises himself/herself thoroughly with the applicable laws, regulations, rules, directives and

any other enforceable measures or guidance, or any other legal requirement in whatever form, in force in Malta at any time, and with all obligations applicable to it arising therefrom. The MFSA requires that the Compliance Officer demonstrates independence of judgement and exercises proper day to day supervision and control over the activity of the Authorised Person as the licence holder. The MFSA requires that the Compliance Officer does not breach, or permit breaches by others, of internal control procedures and systems or licence conditions imposed upon the business of the Authorised Person. In the event that the Compliance Officer becomes aware of such breaches, they are expected to notify the person concerned and, where appropriate, the Management Body. All such breaches and actions taken as a result should be recorded in writing. Furthermore, the Compliance Officer is expected to notify the MFSA of any breach of the conditions of the Authorised Person's authorisation upon becoming aware of such breach.

The MFSA also expects the Compliance Officer to ensure, so far as they are able, that incorrect or misleading information is not provided deliberately or recklessly to the MFSA either in supervisory returns or in any other manner.

A Compliance Officer is usually the officer tasked with keeping the Authorised Person's Corporate Profile updated, as well as the responsibility to upload regulatory submissions through the MFSA's LH Portal. In order for access to be granted to the Corporate Profile and File Uploads section of the Authorised Person on the LH Portal, the Compliance Officer must ensure that an account has been set up first. The following link provides guidance on how such an account can be set up: https://lhportal.mfsa.mt/Files/2FAManual.pdf. The corporate email address is to be used when setting up this account. Once the account is set up the Compliance Officer should provide the Authority with the email address in order for access to be granted accordingly.

2. Money Laundering Reporting Officer

Authorised Persons should ensure that the Money Laundering Reporting Officer ('MLRO') familiarises themselves thoroughly with the Prevention of Money Laundering Act (Chapter 373 of the Laws of Malta), the Prevention of Money Laundering and Funding of Terrorism Regulations (S.L.373.01) and any relevant procedures and guidance issued by the Financial Intelligence Analysis Unit ('FIAU') which can be found on the MFSA website under the Anti-Money Laundering section. Furthermore, Authorised Persons should ensure that the FIAU is notified of the details of the appointed MLRO pursuant to Regulation 15(1)(e) of the above-mentioned Regulations. In this regard, the appointed MLRO will need to register with the FIAU website and contact Compliance at the FIAU for guidance on the required Compliance and Supervision Platform for Assessing Risk ('CASPAR') registrations.

The appointed MLRO should ensure that s/he familiarises himself/herself thoroughly with the Act, the Regulations, the National Interest Act ('NIA'), the Criminal Code and any relevant procedures and guidance issued by the FIAU and that s/he thoroughly understands the requirements and responsibilities of their role as MLRO. The primary responsibilities of the MLRO are those set out in Section 5.1.1 of the Implementing Procedures – Part I (and any amendments thereto) issued by the FIAU as further elaborated upon in Chapter 5 of the said Implementing Procedures and/or through sector specific Implementing Procedures. The said responsibilities are:

a) Receiving and evaluating in a timely manner any internal reports of transactions or activities giving rise to a possible suspicion of ML/FT, and submitting Suspicious Transaction Reports to the FIAU within the applicable timeframes whenever s/he believes that there are reasonable grounds to suspect, suspicions or knowledge of ML/T, even in the absence of any internal report; and

b) Replying within the applicable timeframes to requests for information received from the FIAU.

The MLRO may also be entrusted with additional responsibilities which include:

- Carrying out regular reviews of the Authorised Person's business activities and evaluating any activities to assess any potential risks;

- Providing recommendations for systems and procedure enhancements in regard to countering money laundering and funding of terrorism risks;

- Assisting in the development and implementation of an effective Anti-Money Laundering compliance programme and creating sound internal controls to ensure that all controls are adhered to;

- Drafting and revising (as necessary) the Authorised Person's internal policies and procedures;

- Proactively monitoring processes, practices and the Authorised Person's documents and procedures to identify weaknesses;

- Rolling out Anti-Money Laundering training to all new employees and provide providing training on any changes to relevant laws/ regulations and how such changes are effectively implemented within the Authorised Person's internal controls. From time to time existing all current employees should be offered refresher training on a periodic basis;

- Liaising with the Regulatory Authorities and with the Authorised Person's external auditors, as necessary; and

- Keeping the Authorised Person's Board and Senior Executive Management/high ranking functionaries informed about any concerning issues that might arise.

Where the MLRO has not been entrusted with these additional responsibilities, the MLRO is still expected to contribute thereto, liaising and communicating with the responsible officer/s as may be necessary so as to ensure the effective detection and reporting of transactions and activities that give rise to suspicion, knowledge or reasonable grounds to suspect ML/FT.

The MLRO is also reminded to notify the FIAU of his/her details pursuant to Regulation 15(1)(e) of the Regulations. In this regard, the applicant as the appointed and approved MLRO should proceed to register himself/herself on the FIAU's CASPAR platform which is accessible via the FIAU website.

3. Operational Office

The Authorised Person is to ensure that it has in place measures to safeguard the confidentiality and segregation of all information pertaining to its CSP activities and its clients.

4. Outsourcing Agreements

If the Authorised Person is outsourcing any of its services, it must ensure that an agreement is in place to reflect such outsourcing arrangements.

5. Resource Sharing Agreements

The Authorised Person is to ensure that a resource sharing agreement is in place if it is sharing resources (such as human resources, IT systems, offices etc.) with a third party.

With respect to the different types of agreements referred to above, the Authority expects that these are comprehensive so as to cover all the services to be provided, as well as any reporting obligations and safeguards that the parties thereto are to put in place to ensure that the Authorised Person is not exposed to any unnecessary risks.

6. Business Continuity Policy and Disaster Recovery Plan

Authorised Persons are to ensure that they have in place measures which cover critical aspects of the business and the risk factors that would have the greatest impact on the

Authorised Persons' service offering and operations, in the event that they should materialise. Authorised Persons are to ensure that they identify a person who is responsible for the implementation of the business recovery plan and that employees within the Authorised Person are aware that they should report to him/her in the event of a business interruption incident.

7. IT Systems and Cyber Security

Authorised Persons are to ensure that data is backed up as part of its business continuity policies and ensure that such back-ups are held frequently. An Authorised Person is to have in place cyber security policies and measures so as to safeguard the integrity and confidentiality of its data as well as protect it against any cyber-attacks.

8. AML Policies and Procedures

Authorised Persons, as subject persons under the relevant AML/CFT legislation, are to ensure that the AML Manual is in line with the provisions of the Prevention of Money Laundering Act and any rules and regulations issued thereunder as well as with the FIAU Implementing Procedures. It is expected that such policies are tailor made to the business model and the services provided by the Authorised Person.

9. Client Acceptance Policy

An Authorised Person is to ensure that it has in place a Client Acceptance Policy to mitigate ML/FT risks and to ensure that it is in line with the requirements emanating from Part I of the FIAU Implementing Procedures.

10. Business Risk Assessment ('BRA') and Customer Risk Assessment ('CRA')

In terms with the FIAU Implementing Procedures the Authorised Person is to ensure that it has in place a Business Risk Assessment and a Customer Risk Assessment which should be proportionate to the Authorised Person's nature, complexity and size of its business and which should be regularly reviewed and updated. The BRA should not only cover ML/FT risks but all risks pertaining to the Authorised Person's business model. Likewise, the CRA should cover the risks that the Authorised Person will be exposed to in providing its services either in the course of a business relationship or as a one-off transaction.

11. Marketing

An Authorised Person is to ensure that any marketing strategies implemented for the promotion of CSP services should clearly state that the services are provided by the Authorised Person and not by any related entities. The Authority expects full transparency in this regard and all marketing material should be duly scrutinised prior to publication, to ensure that it provides an accurate representation and does not provide misleading information to clients or other stakeholders.

12. Capital Requirements

Authorised Persons, especially sole practitioners, are reminded that the capital requirement is to be maintained for as long as the Authorised Person remains authorised under the Act. Moreover, where an Authorised Person who is a sole practitioner opts to provide the Authority with a bank guarantee, the Authorised Person is reminded that the Authority is to be provided annually with the renewed guarantee.

E. Conclusion

Having regard to the guidance provided in this document, Authorised Persons who were subject to post-authorisation requirements, are expected to carry out a **gap analysis** to verify whether the imposed requirements have been duly fulfilled in accordance with the guidance provided in this Guidance Document. **Furthermore, this gap analysis, together with the action points taken to fulfil such requirements, should be duly documented and readily available to be provided to the Authority upon request.** The Authority may also verify the effectiveness of this gap analysis, and the resulting outcome, in any supervisory interaction with the Authorised Person.

Malta Financial Services Authority

Triq L-Imdina, Zone 1

Central Business District, Birkirkara, CBD 1010, Malta

communications@mfsa.mt

www.mfsa.mt