MFSA MALTA FINANCIAL SERVICES AUTHORITY

Consultation Document

Consultation Document on the Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements

Ref: 04-2020

Date: 30 June 2020

Closing Date: 28 August 2020

NOTE: The documents circulated by the MFSA for the purpose of consultation are in draft form and consist of proposals. Accordingly, these proposals are not binding and are subject to changes and revisions following representations received from Licence Holders and other involved parties. It is important that persons involved in the consultation bear these considerations in mind.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155

communications@mfsa.mt
www.mfsa.mt

1.0.0 Introduction

1.0.1 Exercising proper governance and control over technology arrangements and their outsourcing, as well as having an effective cybersecurity framework, have become key priorities for any organisation.

1.0.2 Technology developments, coupled with an increased reliance on Information and Communications Technology (ICT) within the Financial Services industry, typically involving combinations of on-premise and cloud-based arrangements, have created challenges both for the industry and the regulators. The opportunities and scope of outsourced services widened, and such services may be provided, virtually, from any location. This means that certain aspects of outsourced activities may be unregulated and may thus result in adverse risk, impairing Licence Holders' oversight capability and the ability of the MFSA to monitor the Licence Holders' compliance with their obligations to ensure the continuous and satisfactory service to their clients.

1.0.4 The MFSA is proposing to issue principle-based cross-sectoral guidelines ("Guidance document") in the areas of Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements, setting out the MFSA's expectations. The Guidance document draws from, and references, several sources, primarily European Supervisory Authorities' (ESAs) Guidelines, but also International Standards and established Frameworks. The MFSA plans to make cross-references within the respective prudential rules of the applicable industry sectors listed in Section 2.2 to the Guidance document.

1.0.5 The Guidance document is without prejudice to all applicable Acts, Regulations, rules or sector-specific guidelines. In the event of any inconsistency or conflict between the Guidance document and any applicable Acts, Regulations, rules or sector-specific guidelines, the provisions of the said Acts, Regulations, rules or sector-specific guidelines shall always prevail.

1.0.6 This Guidance document should be considered as a live document due to the dynamic nature of technology evolution. It will therefore be updated from time to time to reflect any developments.

1.0.7 The proposed Guidance document contains five Titles. Title 1 is divided in two Sections. The first section outlines the Scope and Application of the Guidance document, whilst the second section provides a number of definitions used within the document. Title 2 defines the four Principles, on which the Guidance document is based. Title 3 provides guidelines on Technology Arrangements including, for instance, Cloud Computing. Title 4 provides guidance on ICT and Security Risk Management. Finally, Title 5 contains guidelines on Outsourcing Arrangements. Section 2.0.0 provides further information on the Guidance document.

1.0.8 Following the consultation period, as part of its off-site supervision, the MFSA plans to conduct thematic desk-based reviews on a sectoral basis, on key aspects of the Guidance document.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

2.0.0 The Guidance Document

2.1.0 Title 1 – Scope and Application

2.1.1 Given the need, on the one hand, to provide clarity and more specific guidance to Licence Holders and prospective applicants regarding Technology Arrangements, particularly those involving outsourcing arrangements, and on the other hand, the need for unhindered supervisory oversight in the context of evergrowing reliance on cloud services and geographically dispersed hosting arrangements, the Authority is providing guidelines on Technology Arrangements to authorised entities listed in Section 2.2 below, without prejudice to sector-specific legislation, including delegated measures, sector-specific guidance, and all other EU and national legislation.

2.1.2 The Guidance document is addressed to the following entities licensed by the Authority:

- Credit Institutions
- Financial Institutions
- Insurance Undertakings and Reinsurance Undertakings
- Insurance and Reinsurance Undertakings which are part of a group in line with Article 212 of Directive 2009/138/EC
- Captive Insurance Undertakings and Captive Reinsurance Undertakings
- Insurance Intermediaries
- Ancillary Insurance Intermediaries
- Retirement Pension Schemes (Occupational Retirement Schemes and Personal Retirement Schemes)
- Pension Service Providers (Retirement Scheme Administrator, Investment Manager and Custodian)
- Investment Services Licence Holders
    - Investment Firms Categories 1 to 3
    - Custodians of Collective Investment Schemes – Categories 4a and 4b
    - Fund Managers: De minimis AIFMSs, full scope AIFMs and UCITS Management Companies
    - Self-managed Collective Investment Schemes (including Professional Investment Funds, UCITS and Alternative Investor Funds)
    - Recognised Fund Administrators
- Trading Venues
- Central Securities Depositories
- Trustees and other Fiduciaries
- Company Service Providers
- Virtual Financial Assets

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

2.2.0 Title 2 - High Level Principles

2.2.1 The Guidance document is based on four high level principles which are Proportionality, Principles-based consistency of outcomes, Information Assurance (IA) in Technology Arrangements and Approach to cloud computing.

2.3.0 Title 3 – Technology Arrangements

2.3.1 This section covers the essential characteristics of cloud computing; cloud computing service models; cloud computing deployment models; shared responsibilities for different cloud service models; isolation in virtualised environments; monolithic, microservices and serverless architectures; unrestricted audit, on-site and remote access, and information gathering and investigations; security monitoring, DLP, eDiscovery and forensic capabilities; consumption of cloud services over the internet; and artificial intelligence and machine learning.

2.4.0 Title 4 – ICT and Security Risk Management

2.4.1 Title 4 covers internal governance and risk management measures that should be taken into account when managing risks associated with Technology Arrangements, their operations, and the data therein. This section encompasses aspects of ICT strategy, ICT Risk Management, Information Security, ICT Operations Management, and ICT Project and Change Management. Further guidelines are also provided on Business Continuity Management, which should form part of the Licence Holders' operational risk management framework to ensure that ICT systems and services and their interdependencies within the Technology Arrangements are designed for a level of operational resilience commensurate with their criticality.

2.5.0 Title 5 – Outsourcing Arrangements

2.5.1 Guidelines under Title 5 cover internal governance arrangements, including sound risk management, that Licence Holders should implement when they outsource functions, in particular the outsourcing of critical or important functions, in a Technology Arrangement or an outsourced business function or process that is delivered as a Cloud Service. This section provides guidance on assessments of outsourcing arrangements; guidance on sound governance arrangements including an outsourcing policy, the management of conflicts of interest, business continuity planning, internal audit function expectations, and documentation requirements; and guidance on the outsourcing process including pre-outsourcing analysis, the contractual phase, monitoring and oversight of outsourcing arrangements, and exit strategies.

3.0.0 Consultation Period

3.0.1 Any comments or feedback in relation to the Guidance document are to be addressed to the Supervisory ICT Risk and Cybersecurity function within MFSA by sending an email to sirc@mfsa.mt, referring to this Consultation, not later than Friday 28 August 2020.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt