MFSA MALTA FINANCIAL SERVICES AUTHORITY

Feedback Statement

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

Ref: 04-2020

Date: 11 December 2020

# Table of Contents





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

communications@mfsa.mt
www.mfsa.mt

# Feedback Statement

On 30 June 2020, the Malta Financial Services Authority ('MFSA' or 'the Authority') published a Consultation Document on the Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements.

During the consultation period, expiring on 28 August 2020, the MFSA received substantial feedback from the industry. This document is the outcome of the feedback review process.

The Guidance document has been welcomed in general and the feedback has been both constructive and encouraging. The Authority reviewed all the feedback received and the conclusion of the feedback review process, is provided in Section 2 of this document.

In parallel with the issuance of this Feedback Statement the final version of the Guidance document is also being published.



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

# 1. Introduction

On 30 June 2020, the Malta Financial Services Authority ('MFSA' or 'the Authority') published a Consultation Document on the Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements. The Authority, through this consultation process, proposed 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 for:

- 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 AIFMs, 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

The proposed Guidance document contains five Titles. Title 1 is divided into two Sections. The first section outlines the Scope and Application of the Guidance document, whilst the second section provides a number of definitions of key terms used within the document. Title 2 defines the four Principles, on which the Guidance document is based. Title 3 provides guidelines on Technology Arrangements such as Cloud Computing. Title 4 provides guidance on ICT and Security Risk Management and lastly, Title 5 contains guidelines on Outsourcing Arrangements.

During the consultation period, expiring on 28 August 2020, the MFSA received substantial feedback from the industry. This document is the outcome of the feedback review process.



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

The Guidance document has been welcomed in general and the feedback has been both constructive and encouraging. The Authority reviewed all the feedback received and the conclusion of the feedback review process, is provided in Section 2 of this document. The feedback has been categorized as follows:

1. Definitions
2. Artificial Intelligence and Machine Learning
3. Principle of Proportionality
4. Complexity
5. Three Lines of Defence Model
6. Standards, Technologies and Best Practices
7. Interactions with the Authority
8. Business Managed Applications
9. Outsourcing in General
10. Intra-group Outsourcing and Sub-Outsourcing
11. Cloud Services
12. Changes in Text deriving from European Supervisory Authorities' Guidelines
13. Rewording and Restructuring
14. Generic and other Considerations
15. Alignment with EIOPA Guidelines on Information and Communication Technology Security and Governance
16. Other Feedback

Each feedback category is covered in a dedicated subsection. For each feedback category, a summary of the feedback received, as well as the position taken by the Authority on the feedback, is provided. The position taken by the Authority includes where applicable, whether the feedback resulted into any amendment/s to the Guidance document.

Wherever in the document, the feedback statement mentions a respondent, such respondent may be an individual respondent, or a representation made by a group of respondents who chose to provide feedback collectively (e.g. as an association).

In parallel with the issuance of this Feedback Statement the final version of the Guidance document is also being published.

This Guidance document should be considered as a live document due to the dynamic nature of regulatory developments, technology evolution, and related opportunities and risks. It will be updated from time to time to reflect any relevant developments.

The Authority would like to remind the industry that in the event of any inconsistency or conflict between this 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.



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

# 2. Feedback Statement

## 2.1 Definitions

Section 2 of Title 1 provides definitions for a number of key terms used within the Guidance document. The Guidance document further explains a number of terms, in-line within the main text.

### Feedback Received

Two respondents made recommendations for additional definitions as well as for minor amendments on an element of definitions in place.

The following additional definitions were recommended:

- Algorithmic bias;
- Cloud-agnostic containerisation;
- eDiscovery;
- Exploits;
- Greenfield deployment;
- Open Source (components/software);
- Red Team Exercise;
- Software entropy;
- Technical debt;
- Thin Client Interface;
- Threats;
- Virtual Machine;
- Vulnerabilities.

The following definitions were recommended to be amended:

- Authentication;
- Data Governance;
- Non-repudiation;
- Significant Sub-outsourcer.

### MFSA Position

The recommended additional definitions were included except for:

- **Thin Client Interface** – the definition of 'Thin Client' was provided instead;
- **Cloud-agnostic containerisation** – the definition of 'Containerisation' was provided instead;
- **Red Team Exercise** – the definition of 'Red Team' was provided instead.



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

The recommended minor amendments were also carried out except for "Significant Sub-outsourcer". This definition together with the term has been removed altogether in line with the EIOPA Guidelines on Outsourcing to Cloud Service Providers (EIOPA-BoS-20-002).

## 2.2 Artificial Intelligence and Machine Learning

Due to the proliferation of Artificial Intelligence and Machine Learning, MFSA considered providing an element of guidelines in this field in Title 3, Section 10.

### Feedback Received

A respondent recommended additional provisions to mitigate discrimination risks in line with the principle and legal obligation of equality and non-discrimination.

Another respondent recommended the addition of language regarding the detection of malicious AI and AI malfunctions

### MFSA Position

MFSA supports equality and non-discrimination. Whilst discrimination risks are not necessarily endemic to the financial services industry only, but may be pertinent horizontally across multiple industries, the recommended additional provisions were incorporated in paragraph 3.10.9 of the Guidance document.

On the detection of malicious AI and AI malfunctions, (b) and (d) of Paragraph 3.10.6, were updated accordingly.

## 2.3 Principle of Proportionality

The guidelines within the Guidance document are subject to the principle of proportionality. Their application should take into consideration the size, internal organisation and individual risk profile, as well as the nature, scope, complexity and riskiness of the Licence Holder's operation and of the services and products provided or intended to be provided.

### Feedback Received

A number of respondents recommended that MFSA issues precise definitions, criteria, specifications, and/or thresholds for levels of proportionality.

### MFSA Position

In line with the European Supervisory Authority (ESA) Guidelines and without prejudice to all applicable Acts, Regulations, rules or any other sector specific guidelines, Licence Holders listed in section 1.1.9, are expected to comply with the Guidance document in such a way that is proportionate to, and takes into account, the size, internal organisation and individual



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

risk profile, as well as the nature, scope, complexity and riskiness of the Licence Holders' operation and of the services and products provided or intended to be provided. These characteristics vary from one organization to another and every organization has its own specific characteristics. The guidelines within the Guidance document should be applied in a manner that is tailored to the risks and needs of these specific characteristics.

In a similar response made to the European Banking Authority (EBA) on the EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04) which is the basis of Title 4 of the Guidance document, the EBA's analysis to the response was:

*"The application of these guidelines is not for competent authorities' needs but for institutions to ensure that they manage their ICT and security risks proportionately. Furthermore, using a graded approach would limit the implementation of principle-based guidelines and it is the right of the management body to establish proportionate application".*

Within their Guidelines on Internal Governance (EBA/GL/2017/11) the EBA provides criteria that should be taken into account by institutions and competent authorities for the purpose of the application of the principle of proportionality.

This principle is expected to persist within the Digital Operational Resilience Regulation for the Financial Sector. This Regulation is in legislative proposal stage as at the time of writing and amendments (including possibly in this regard) may be expected.

## 2.4 Complexity

The Guidance document refers to 'complex' Technology Arrangements in paragraphs 3.8.1 and 3.9.2.

### Feedback Received

A respondent recommended a definition of what constitutes a 'complex' Technology Arrangement, referring to requirements in: Paragraph 3.8.1 on SOAR and Cyber AI as an augmentation to SIEM in complex Technology Arrangements; and Paragraph 4.7.12 (on FIM integration with SIEM).

The same respondent contended that a substantial investment is required to purchase File Integrity Monitoring (FIM) tools. Furthermore, the same respondent suggested that it would require enhanced experience to set the alerts at an optimal level for detecting the right changes and avoid false positives.

### MFSA Position

On the definition of 'complex' Technology Arrangements, there are different approaches and academic research available to measure technology complexity.

The complexity of a Technology Arrangement is typically relative to the processes it entails, the technology components involved and the human resource intensity required as well as



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

their required level of competence. The same Technology Arrangement may thus be more complex for one organisation than for another, whilst complexity may change over time. The relevance of automation through SOAR, Cyber AI, SIEM and FIM technologies (if adequately planned, contracted, implemented and maintained) is expected to increase as technology complexity increases.

Investment in technology such as FIM is subject to the principle of proportionality. Unless security monitoring solutions are set up correctly (adequately planned, contracted, implemented and maintained, as explained above) they will not achieve the respective security objectives outlined by the Licence Holder effectively.

## 2.5 Three Lines of Defence Model.

Paragraph 4.6.4 in Section 6, ICT Risk Management, states that Licence Holders should identify and manage their ICT risks according to the Three Lines of Defence model or similar internal control framework.

### Feedback Received

A respondent made reference to an update to the Three Lines of Defence model (the Three Lines Model) released by the Institute of Internal Auditors on 20 July 2020 (during the consultation period of the Guidance document).

The same respondent recommended that Paragraph 4.6.5 is shifted above Paragraph 4.6.2 for consistency purposes.

The same respondent recommended that, in conjunction with Paragraph 4.6.14, the Guidelines Document can be enhanced if mapping to business processes explicitly states that business process mapping must identify relationships to information systems (and processes) and that the maps must be maintained current and updated at least annually, which will in turn help Licence Holders keep and maintain a current view of ICT risks and the risks associated with technology-enabled financial services and solutions.

Another respondent proposed that Paragraph 4.7.5 is worded as a recommendation rather than a requirement. The same respondent posits that separation between IT Security and the general ICT Operations is not always compatible with entities' security structures.

### MFSA Position

MFSA thanks the respondent for referring to the Three Lines Model, which feedback is herewith being acknowledged and relayed to the industry.

Paragraphs 4.6.1 to 4.6.3 are introductory paragraphs, that lead the way for the main body of the ICT Risk Management section. It provides references to the Three Lines of Defence Model from various Financial Services Principles and Guidelines.



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

On business process mapping, the identification of relationships to Information Systems and Processes is contemplated in Paragraph 4.6.15. The requirement for regularly updating mappings is covered within Paragraph 4.6.14.

Paragraph 4.7.5 has been reworded to include the Principle of Proportionality. This Paragraph is in line with the ESA Guidelines and best practices. The Security Function is deemed to be a Control Function and should be segregated from standard/normal ICT Operations.

## 2.6 Standards, Technologies and Best Practices

The Guidance document refers to a number of specific standards, technologies and best practices.

### Feedback Received

In conjunction with Paragraph 4.7.1, one respondent enquired whether the Authority is expecting Licence Holders to acquire certifications such as ISO/IEC 27001 or whether adhering to specific certifications is enough. The respondent further holds that the implementation and/or alignment with ISO 38500:2015, COBIT 5, PCI DSS, 27001:2017, 27002:2013, 27017:2015, NIST and CIS is commendable but requires a good amount of investment to get qualified and aligned, as well as the subsequent maintenance of the certification. The respondent stated that it is not always feasible to implement standardized frameworks in full as this also depends on the principle of proportionality.

The same respondent recommended that Paragraph 4.7.8 is rephrased to allow different varying authentication mechanisms for APIs and not just the two listed. Whilst agreeing that a benchmark on security standards should be set, the respondent felt that limiting the actual mechanism can be very costly to organisations who have a similar mechanism which is just as secure.

In conjunction with Paragraphs 3.8.2, another respondent expressed a concern that Data Loss Prevention (DLP) products are not always compatible with data subjects' rights in terms of the General Data Protection Regulation, providing an example of a particular solution. On Paragraph 3.8.3, the same respondent remarked that the decision about whether to supplement DLP with User and Entity Behaviour Analytics (UEBA) should be a matter to be determined by Licence Holders, in the light of their needs and IT framework and this should not be a requirement.

The same respondent expressed disagreement with Paragraph 4.9.11, pointing out that in practice, it is unlikely that an entity obtains OWASP 4.0 Verification Level 3 verification for every application used or developed.



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

MFSA Position

Paragraphs 4.7.1 and 4.7.8 have been reworded.

On Paragraphs 3.8.2, the Authority would like to clarify that these Guidelines are principle based and technology neutral and do not favour any type of solution over another. The responsibility for compliance with the relevant Acts, Regulations, Rules or Sector Specific Guidelines (including the General Data Protection Regulation) rests with the Licence Holder. Paragraph 3.8.3 describes Data Loss Prevention and User and Entity Behaviour Analytics, both of which are recommended solutions. The decision whether to implement or not and to what extent lies with the Licence Holder based on the principle of proportionality and without prejudice to the relevant Acts, Regulations, Rules or Sector Specific Guidelines.

In Paragraph 4.9.11 OWASP 4.0 Verification Level 3 (Advanced) is being recommended for a critical or important business function or service involving personal, financial data or transactional data, or where a Licence Holder's operation could be jeopardised.

## 2.7 Interactions with the Authority

The Guidance document makes reference to a number of situations where Licence Holders need to interact with the Authority.

Feedback Received

On Paragraph 4.6.22, a respondent requested a clarification as to whether reporting to the Management Body is enough or is a separate report of risk assessment results to the authorities expected.

Another respondent enquired whether Licence Holders are expected to formally report on [cyber resilience] to the MFSA or whether this will be covered during onsite visits. In addition, the same respondent enquired about whether any potential remedial actions are to be discussed with the Authority.

MFSA Position

Paragraph 4.6.22 has been amended. This paragraph takes into consideration reporting obligations, inter alia, reporting obligations in Article 11A (2) of the Financial Institutions Act and Article 19C (2) of the Banking Act.

On the feedback provided by the other respondent, without prejudice to all applicable Acts, Regulations, rules or sector specific guidelines, Licence Holders should approach the Guidance document with a view to align with the Authority's expectations therein. As stated within the Consultation Document, MFSA plans to conduct thematic reviews on a sectoral basis, on key aspects of the Guidance document. Licence Holders may also interact with the Authority to discuss any potential remedial actions and/or any clarifications required.



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

## 2.8 Business Managed Applications

Paragraphs 4.9.18 and 4.9.19 speak about Business managed applications or end user computing applications, such as spreadsheet or desktop database software. These may end up being used by business functions to fill gaps in critical or important business processes that are not addressed by enterprise application software.

### Feedback Received

A respondent commented that the acceptable level of end user computing is not clear. There would be potentially significant resourcing implications for IT/operational/compliance areas if one had to take a more aggressive stance: a) on replacing end user computing with enterprise applications; and/or b) on policing these activities across the organisation.

The same respondent remarked that "Business managed applications" should be more clearly defined in the document. The respondent explained that it is normal for certain "power users" outside of IT to be able to make business configuration changes within applications, while IT look after the technical configurations and the hosting environment.

### MFSA Position

The level and extent of business managed applications or end user computing applications is an assessment that the Licence Holder needs to conduct, based on risk. The rationale of Paragraph 4.9.18 is that an organisation should not end up in a situation where it relies on the fragility and fragmentation of such applications (and the pertinent data) which may not have the same level of controls as enterprise application software.

## 2.9 Outsourcing in General

Title 5 of the Guidance document covers the 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.

The responsibility for regulatory compliance rests with the Licence Holders and is not outsourceable.

### Feedback Received

On Paragraph 3.7.1, one respondent requested that:

- MFSA clarifies whether Licence Holders and service providers should specifically establish this formally within contractual arrangements for non-EU service providers, and whether EU-based service providers are, through regulation, already subject to this requirement hence not requiring specific contractual arrangements.



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

- Guidance should also be provided as to whether this type of arrangement is specifically required when a "right to audit" by the Licence Holder in relation to service provider services and systems has already been contractually stated.
- Guidance should also be provided as to expectations e.g. frequency and scope.

Referring to Paragraph 5.10.10, the same respondent claimed that this paragraph is transposing paragraph 70 of the EBA Guideline on Outsourcing Arrangements. The transposition of this paragraph leaves out the EBA reference to the "critical and important functions" which means that whilst the EBA is adopting the principle of proportionality in the implementation of due diligence, the MFSA is extending this requirement to all contracts which is deemed to be burdensome. As a result, it is proposed that the MFSA Final Guidance includes reference to "critical and important functions".

MFSA Position

On the feedback provided on Paragraph 3.7.1, clarifications and guidance are available in Title 5, Outsourcing Arrangements, largely in Section 11.

Paragraph 5.10.10 has been amended. Without prejudice to all applicable Acts, Regulations, rules or sector specific guidelines, due diligence as part of an outsourcing process, whether it relates to a critical or important function or not, is widely considered as a good practice and is recommended across, for the benefit of the Licence Holder.

## 2.10 Intra-group Outsourcing and Sub-Outsourcing

Intra-group outsourcing is essentially a form of outsourcing and is subject to expectations provided by the Guidance document on outsourcing. Licence holders should also ensure that they have the necessary oversight on sub-outsourcing which can have a risk bearing especially within the context of outsourcing entailing critical or important functions. Licence Holders should be particularly careful when large and/or complex chains of service providers are involved.

Feedback Received

On Paragraph 5.10.3, one respondent enquired on the applicability of the requirement in the context of a Licence Holder having a relationship with a global group establishment also referred to by the same respondent as the main provider (not necessarily a Licence Holder and not necessarily established in Malta) which in turn offshores (possibly within the European Union and/or in third countries) within the group.

On Paragraph 5.10.11, another respondent enquired whether the respective requirements apply to intra-group outsourcing.

A respondent argued that although sub-outsourcing gives rise to higher risks in case they are not properly monitored, sub-outsourcing can be a result of a company being more technically capable/specialized in particular areas. The same respondent enquired whether Licence Holders are expected to formally report on [sub-outsourcing] to the MFSA or



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

whether this will be covered during onsite visits. In addition, the same respondent enquired about whether any potential remedial actions are to be discussed with the Authority.

MFSA Position

On the query about Paragraph 5.10.3, as provided by Paragraph 5.10.7, where the outsourcing arrangement includes the possibility that the service provider sub-outsources critical or important functions to other service providers, Licence Holders should take into account:

a) The risks associated with sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country from the service provider;
b) The risk that long and complex chains of sub-outsourcing reduce the ability of Licence Holders to oversee the outsourced critical or important function and the ability of competent authorities to supervise them.

Paragraphs 5.11.3 to 5.11.7 provide further requirements that are applicable to this context. Licence Holders may contact the authority for any further clarifications related to their particular outsourcing contexts and/or arrangements.

On the second query, intra-group outsourcing is a form of outsourcing and therefore Paragraph 5.10.11 applies.

On the feedback provided by the third respondent, Licence Holders should approach the Guidance document with a view to align with the Authority's expectations therein. As stated within the Consultation Document, MFSA plans to conduct thematic reviews on a sectoral basis, on key aspects of the Guidance document. Licence Holders may also interact with the Authority to discuss any potential remedial actions and/or any clarifications required.

## 2.11 Cloud Services

The Guidance document makes several references to cloud computing and cloud services providers throughout the whole document, but especially in Title 5 on Outsourcing Arrangements.

Feedback Received

Referring to The Accountability Principle in Paragraph 2.4.6, a respondent claimed that the accountability principle or changing some responsibilities or enforcing additional controls with Big Tech companies is a very difficult principle to attain.

The same respondent claimed that cloud services could be challenging given that in the cloud a service/provider might be present at some point in time and close the business or disappear or go bankrupt. The guidelines also make reference to having contingency plans to cover such risks. At the end, it might be worthwhile to keep the system on premise or develop or outsource software house to create a new system.



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

The same respondent highlighted that the migration of a system from cloud to (on-premise or a different cloud) might require some effort, especially if there are communication deficiencies (with Big Tech company) to be reached. Regional/International authorities for cooperation/communication would be needed to get in touch with Big Tech bodies when financial institutions fail to do so.

MFSA Position

On the first comment it would be worth noting that Big Tech Companies are reportedly engaging in compliance programs within the Financial Services realm. It is also worth noting that the proposed Digital Operational Resilience Regulation for the Financial Sector intends to implement an oversight framework for critical ICT third-party service providers. This Regulation is in legislative proposal stage as at the time of writing and amendments (including possibly in this regard) may be expected.

The second and third comment increase the relevance of the Guidance document which puts forward requirements related to risk management in general and exit strategies in particular.

## 2.12 Changes in Text deriving from European Supervisory Authorities' Guidelines

This section addresses feedback with recommendations to change text within the Guidance document that derives directly from European Supervisory Authorities' (ESA) Guidelines.

Feedback Received

The following changes were recommended:

Paragraph 4.4.2
Text: *"the ICT strategy which should be reviewed and updated on a regular basis"*.
Recommendation: *"the ICT strategy which should be reviewed and updated on a regular basis and at least annually"*.
Rationale: Similarly, to the Risk Framework and other matters discussed in this guidance document, the ICT strategy should be reviewed at least annually to ensure continued relevance and alignment with ICT and Business strategies.

Paragraph 4.6.9
Text: *"d) monitor the effectiveness of these measures as well as the number of reported incidents affecting the ICT related activities, taking timely actions to correct the measures where necessary and track their implementation"*.
Recommendation: *"d) monitor the effectiveness of these measures as well as the number of reported incidents affecting the ICT related activities, taking timely actions to correct or further enhance the measures where necessary and track their implementation"*.



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

Rationale: Updates to mitigating measures may not only be necessary to correct existing deficiencies, but also to further enhance existing controls and bring them in line with the Corporate Risk Appetite.

Paragraph 4.6.25
Recommendation: The paragraph can be enhanced if it includes a provision through which the IT auditors can note area(s) for improvement, even if the control itself passes the audit.
Rationale: Self-explanatory.

Paragraph 4.6.10
Text: *"The framework should be documented and continuously improved with 'lessons learned' during its implementation and monitoring"*.
Recommendation: *"The framework should be documented and continuously improved with 'lessons learned' during its ~~implementation and monitoring~~ lifetime"*.
Rationale: A Risk Framework exists beyond the setup/implementation and monitoring phases, primarily including use of [no further text provided by the respondent].

Paragraph 4.7.2
Text: *"b) should be based on the relevant results of the risk assessment process, as well as sector-specific compliance requirements"*.
Recommendation: *"b) should be ~~based on~~ aligned with the relevant results of the risk assessment process, as well as sector-specific compliance requirements"*.
Rationale: The mentioned sentence is essential in order to highlight the interconnectedness of ICT and security risk management and information security but inferring that the security policy should be based on the risk assessment process is misguiding.

Paragraph 4.7.6
Text: *"e) ensure that all employees and third parties accessing information and systems are adequately informed of the information security policy, for example through information security training and awareness sessions"*.
Recommendation: To waive this requirement for third parties whereby there is an agreement in place that security awareness training is provided [by the same third party].
Rationale: Third parties undergoing formal security training can be waived from this requirement. If a particular company agrees to the External ISP [Information Security Policy] document where conditions are specified that security awareness training is to be provided to all staff.

Paragraph 4.7.6
Recommendation: To add *"g) ensure that all ICT initiatives and projects include sound security architecture from their early stages"*.
Rationale: We recommend adding this text, possibly earlier in the list, to remind of the importance of involving Information Security in the early design stages of ICT projects.

Paragraph 4.7.18
Text: *"Furthermore, Licence Holders should consider good practices such as source code reviews (see 4.9.8), vulnerability assessments, penetration testing, and red team exercises"*.



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

Recommendation: *"Furthermore, Licence Holders should consider good practices such as source code reviews (see 4.9.8), vulnerability assessments, penetration testing, compromise assessment, and red team exercises"*.
Rationale: Compromise Assessment focuses on identifying previously unknown, successful, or ongoing compromises.

Paragraph 4.9.5
Recommendation: (project management methodology) can be enhanced if it includes an additional item [(g)] Project Financial Tracking.
Rationale: Licence Holders will benefit greatly if they track budgeted cost of work scheduled against actual cost of work performed for projects.

Paragraph 5.3.1
Text: *"that would, or could, realistically be performed by Licence Holders"*.
Recommendation: Given that the Guidance document is specifically on Technology Arrangements, we believe that the phrase could be further expanded upon to provide greater clarity.
Rationale: The text is helpful however still leaves a lot of room for interpretation. Most of the Licence Holders are nowadays resorting to external arrangements and in a number of instances, there are grey areas as to whether this is outsourced or not.

Paragraph 5.3.5
Recommendation: To add *"(f) any other outsourced function, if compromised and made public, would result in a negative public perception of the Licence Holder, or otherwise damage the Public Trust in the Licence Holder or the financial system at-large"*.
Rationale: As a catch-all for all other critical functions.

Paragraph 5.8.2
Recommendation: We believe that sections 5.8.2 (b) and (c) should more clearly set out that the internal auditor should ensure that the processes are robust, and controls are effective rather than, in some way, approving (or otherwise) the matters set out therein.
Rationale: The internal audit function has an important role in within the governance and risk management frameworks of entities. We should however appreciate that the governing bodies are the decision-makers within the enterprise.

Paragraph 5.9.3
Recommendation: The paragraph can be enhanced if it included an item (j). For example: (j) the register should identify the responsible executive in the Management Body of the Licence Holder, and the name and contact information of primary and secondary contacts in the outsourcing service provider.
Rationale: Self-explanatory.

Paragraph 5.9.4
Recommendation: With reference to item (i), please consider adding an explicit statement that the list of alternate service providers must be kept current and reviewed and updated (annual reviews are recommended).
Rationale: Self-explanatory.



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

Paragraph 5.11.18
Recommendation: The licensed entity is able to also consider/rely upon reports carried out by the service provider's internal auditor working in line with industry practice and the IIA's or ISACA's (or equivalent's standards). The other requirements, for instance, the considerations in 5.11.20 would also apply.
Rationale: Self-explanatory.

Paragraph 5.12.1
Text: *"outsourcing and sub outsourcing of…functions including that the availability, integrity, and security of data"*.
Recommendation: *"outsourcing and sub outsourcing of…functions including that the confidentiality, integrity, and ~~security~~ availability of data"*.
Rationale: Please consider harmonizing the vocabulary related to information security.

MFSA Position

MFSA acknowledges the feedback received and appreciates the effort put in by the respective respondents. The recommendations reflect changes in text that derives directly from ESA Guidelines following extensive consultation processes and the Authority would have a preference to preserve the text as originally derived in these particular cases.

On the feedback provided in Paragraph 4.7.18, the identification of a compromise is captured in Paragraphs 4.7.14 to 4.7.17.

On the feedback provided in Paragraph 5.11.18, the understanding is that (b) of Paragraph 5.11.18 includes "third-party or internal audit reports made available by the service provider".

## 2.13 Rewording and Restructuring

Some respondents provided recommendations for rewording of certain paragraphs as well as an element of restructuring to consider in the immediate term or in future versions of the Guidance document.

Feedback Received

Feedback Part 1

Paragraph 3.8.7
Recommendation: The paragraph needed rewording for more clarity.
Rationale: Self-explanatory.

Paragraphs 4.3.3 and 4.7.29
Text: *"Records of trainings carried out should be kept"*.



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

Recommendation: *"Records of trainings carried out and evidence of attendance should be kept"*.
Rationale: As auditors, we often come across companies keeping excel lists of trainings carried out, without any evidence of proof to confirm attendees. Indeed, the original text as proposed would allow this practice to continue without achieving the objective that the MFSA is targeting.

Paragraph 4.6.11
Text: *"Before any major change, that is a high risk and high impact change"*.
Recommendation: *"Before any major change, that is a high ~~risk~~ likelihood and high impact change"*.
Rationale: Risk is typically defined as a computation between likelihood and impact.

Paragraph 4.6.22
Text: *"Risk Assessment results should be reported to the Management Body in a timely manner, and to the Authority on an annual basis, or at shorter intervals if so determined by the Authority"*.
Recommendation: *"Risk Assessment results should be appropriately documented and reported to the Management Body in a timely manner, and to the Authority on an annual basis or at shorter intervals if so, determined by the Authority"*.
Rationale: Appropriate documentation is an essential part of Risk Assessment.

Paragraph 4.6.26
Text: *"Without prejudice to the provisions of 4.6.19 to 4.6.27"*.
Recommendation: *"Without prejudice to the provisions of 4.6.19 ~~to 4.6.27~~"*.
Rationale: We note that section 4.6.27 is not included in the guidance document.

Paragraph 4.9.3
Recommendation: The paragraph can be enhanced if it includes an organization approach addition [item (g)] which requires post-project lessons learned and, if necessary, a periodic risk review of the product or service resulting from projects.
Rationale: Self-explanatory.

Paragraph 4.10.2
Recommendation: The paragraph can be enhanced if this wording is added to the second paragraph: "Licence Holders should put BCPs in place to ensure they can react to potential failure and cyber-attack scenarios...".
Rationale: Self-explanatory.

## Feedback Part 2

Title 3, Section 6
Recommendation: The recommendations and flow of the Guidance document can be improved if Section 7 (Unrestricted Audit, etc.) is placed after Section 10 (Artificial Intelligence, etc.).
Rationale: Self-explanatory.



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

Title 3: Section 8
Recommendation: In subsequent Guidance Documents, please consider expanding on these topics.
Rationale: Self-explanatory.

Paragraph 3.8.5
Recommendation: Still, more detail on the relationship between a Licence Holder's internal Investigative Service Department, ICT teams, and Legal teams will be of tremendous value.
Rationale: Self-explanatory.

Paragraphs 3.8.6 and 3.8.7
Recommendation: Licence Holders can benefit from more direct guidance on the high levels of cross-functional collaboration needed to meet these challenges.
Rationale: Self-explanatory.

Paragraph 4.3.1
Text: *"The Management Body of the Licence Holder should ensure that there is an adequate internal governance"* (and others).
Recommendation: "The Senior Management Body of the Licence Holder should ensure that there is an adequate internal governance".
Rationale: Replace 'Management Body' with 'Senior Management Body' every time Accountability for Governance and Assurance is mentioned, and retain 'Management Body' every time that Responsibility or Action are mentioned. A segregation and distinction between the accountability of the board and responsibility of executive management should be promoted.

Paragraph 4.4.1
Text: *"c) clear information security objectives, focusing on people, process and technology (i.e. ICT systems and ICT services)".*
Recommendation: *"c) clear information security objectives, focusing on people, process and technology (i.e. ICT systems and ICT services) in line with general security and governance policies established by the Licence Holder".*
Rationale: Objectives should not be set in a vacuum, but aligned with the governance policies set out by the board.

Paragraph 4.7.4
Recommendation: To enhance by specifying that Licence Holders must properly fund the ICT risk mitigation measures.
Rationale: A lack of adequate funding can easily place a Licence Holder in a state of non-compliance and lead to negative and damaging issues resulting from materialized risk.

Paragraph 4.7.12
Text: *"System hardening should occur before any new device or application is added to the Licence Holders production environment using pre-configured hardened images".*
Recommendation: *"System hardening should occur before any new device or application is added to the Licence Holders production, testing, staging, corporate or other ICT environment*



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

*using pre-configured hardened images, established hardening configuration procedures or similar".*
Rationale: Breaches occur not only through production equipment but also non-production setups such as testing, staging or corporate environments. These should therefore be allowed the same level of care, although different configurations will be applicable according to the needs.
Furthermore, hardening may occur not only through the use of pre-configured hardened images, but also through the use of configuration procedures, scripts or automated tools.

Paragraph 4.7.18
Recommendation: To enhance by specifying the use of cyber incident simulations and desktop activities before a Licence Holder is subjected to Red teaming activities.
Rationale: Red team activities are very effective for a variety of reasons. Aggressive red teaming activities often cause the Management Bodies of Licence Holders to experience shock, awe, and discomfort. Licence Holders' capacity to perform better under pressure are improved with incremental activities designed to improve their ability to respond. Cyber Crisis Scenarios (and red team activities) can also contribute to more robust Technology Arrangements and outsourcing relationships.

Paragraph 4.7.24
Text: *"The Licence Holder's network at OSI Layers 2 and 3 and any virtualised network infrastructure in the cloud".*
Recommendation: *"The Licence Holder's production network at OSI Layers 2 and 3 and any virtualised network infrastructure in the cloud".*
Rationale: In context of the paragraph in which this is contained, we understand that this bullet point is referring specifically to the production network.

Paragraph 4.7.29
Recommendation: To enhance by explicitly referencing the strengthening of risk, compliance and security culture.
Rationale: Explicit references to additional training and security measures for work-from-home conditions, as we are now experiencing with the current pandemic, can also enhance this part of the Guidance document.

Chapter 4, Section 7
Recommendation: As Licence Holders move forward with the development of technology-enabled financial services, enablers, and solutions, a paragraph on Intellectual Property Protection at the end of Section 7 can enhance this section.
Rationale: Licence Holders will do well to perform periodic risk review assessments of technology-enabled enablers, solutions and services to assure that the security and performance of these services will be maintained throughout the product or service lifecycle.

Paragraph 4.8.8
Recommendation: The paragraph can be enhanced if it includes a reference that Licence Holders should be able to identify the last known safe state for restoration.
Rationale: According to FireEye, the average dwell time (the time during which a cyber intruder can infiltrate and navigate a victim's information systems without being detected)



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

is 56 days. The same statistic was 416 days in 2011. Still, malicious cyber intruders can go undetected for longer periods of time, depending on the cyber security maturity level of the Licence Holder.

Paragraph 4.9.8
Recommendation: The paragraph can be enhanced if it mandates the review of the open source components (Open Source Software, OSS), so that the Licence Holder properly licences the software and mitigates the risk of losing intellectual property rights and avoids potential violations of open software licences.
Rationale: Violations of OSS terms and conditions are known to result in legal action from the open software provider against the Licence Holder.

Paragraph 5.4.11
Text: (f) (Transfer, Reintegrate, or Discontinue).
Recommendation: This is very difficult for many organizations who lack well thought-out plans. In future versions of this Guidance, perhaps this topic can be expanded.
Rationale: Self-explanatory.

Title 5, Section 9
Recommendation: To consider adding a Subsection dedicated to Human Resource Security.
Rationale: The Human Resource Security subsection would require the Licence Holder to have documentation that shows the performance of security due diligence with regard to outsourced staff with access to critical systems or data. Indicative points are that; (a) the outsourced staff has undergone a thorough background check, (b) the outsourced staff's educational history has been confirmed as accurate, (c) the outsourced staff members are not insolvent, (d) the outsourced staff does not have a criminal record, and (e) that all outsourced and sub-outsourced staff agree to abide by the Licence Holder's Code of Conduct/Ethics (or equivalent code).Self-explanatory.

Paragraph 5.10.6
Recommendation: The paragraph can be enhanced if it explicitly states that a Licence Holder, as part of the risk assessment, periodically conducts a third-party information security assessment in harmony with Malta local requirements, EBA published guidelines, or other references.
Rationale: Self-explanatory.

Paragraph 5.11.24
Recommendation: We believe that the guidance note should clarify whether it is expected that the Licence Holder be in a position to terminate agreements immediately. We believe that the contracts entered into would consider a transition period.
Rationale: Self-explanatory.

MFSA Position

MFSA thanks the industry for the feedback provided and welcomes the recommendations in Feedback Part 1 which were taken on board and the respective paragraphs amended.



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

The Authority thanks the industry for the feedback provided in Feedback Part 2. The recommendations on Title 3, Section 8 and Paragraph 5.4.11 are duly noted. The other recommendations are acknowledged but no changes were affected in this regard. The Authority is herewith providing feedback on an element of recommendations made.

On the feedback provided on Paragraph 4.7.4, the understanding is that the recommendation is covered in Paragraph 4.3.4.

On the feedback provided on Paragraph 4.7.18, the understanding is that the recommendation is addressed in Paragraph 4.10.5.

On the feedback provided on Paragraph 4.7.29, the understanding is that the content is broad enough to cover the recommendation.

On the feedback provided on Chapter 4, Section 7, and Paragraph 4.9.8, Intellectual Property is not covered within the scope of this release of the Guidance document.

On the feedback provided on Paragraph 4.8.8, the Authority believes that this is a valid point, and the understanding is that the recommendation is addressed through a combination of requirements within the Guidance document, including inter alia, Title 4, Section 7 (ICT Operations Security, Security Monitoring, Disaster Response and Recovery Plans), as well as Title 3, Section 8. The ability to identify the last known safe state for restoration (and indeed the ability to move to that state) is a function of different individual capabilities that need to be in place, including, inter alia: the capability to go back in time with event monitoring; digital forensic investigation capabilities that can yield precise facts and timelines; the quality and granularity of the backup process as well as backup retention periods vis-à-vis the dwell-time of the particular incident.

On the feedback provided on Title 5, Section 9, the Authority believes that this is also a very valid point. The outsourcing model being mentioned by the respondent also falls within the scope of Outsourcing within Title 5 and subject to the same requirements including Due Diligence requirements (Paragraphs 5.10.9 to 5.10.13).

On the feedback provided on Paragraph 5.10.6, the understanding is that this requirement is broadly addressed in Paragraphs 5.11.12 to 5.11.23 and 5.12.3.

On the feedback provided on Paragraph 5.11.24, without prejudice to all applicable Acts, Regulations, rules or any other sector specific guidelines, Licence Holders should approach the Guidance document with a view to align with the Authority's expectations therein.



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

## 2.14 Generic and other Considerations

The following recommendations were put forward by a few respondents for consideration.

Feedback Received

A respondent recommended giving a short paragraph under each Title Section to describe the contents and purpose of the Title and its Sections and Subsections. The Guidance Document will be easier to follow with short subsection descriptions. Short descriptions appear in some subsections (4.6.16 and others). The same respondent also recommended to add an index at the end, for key or defined terms.

On Title 4, Section 1, the same respondent envisions that while the scope of this section is limited to the management of ICT risk, there will come a time where Licence Holders will face security incidents that will require extremely close cooperation with other stakeholders

in Business Continuity, Disaster Recovery, and Cyber Resilience (Section 4.1.4) spheres. Perhaps the topic of cross-functional cooperation within a Licence Holder will contribute to a future version of this Guidance Document.

Another respondent observed that once the guidance notes have been issued, Licence Holders will be expected to review their business to confirm which aspects apply to them, and to the extent that a paragraph applies to them the Licence Holder will be expected to show how the matter has been considered and the outcome. The respondent claims that given the thoroughness of the guidance, such review would be long and time consuming, regardless of the size of the business. The respondent recommends that this is considered by the MFSA. In line with this observation, another respondent recommended that the MFSA ought to refer to a reasonable, agreed timescale by which firms are expected to have completed their proportionate review that reflects the size of the business and its resources.

MFSA Position

The first recommendations will be considered in subsequent iterations of the Guidance document.

The observation related to cooperation, is a valid contribution but may be more attributed to the cohesiveness of the functions of an organization (which is critical in the course of an incident). Information Security Testing and Disaster Recovery Testing exercises are good opportunities to test such cohesiveness under incident conditions. The Management Body of an organization is also responsible to set the right tone and climate for the different functions of an organization to work cohesively.

Without prejudice to all applicable Acts, Regulations, rules or any other sector specific guidelines, Licence Holders should approach the Guidance document with a view to align with the Authority's expectations therein. Whilst it is acknowledged that the Guidance document has a comprehensive coverage, it is primarily in the interest of the Licence Holders to adopt its principles proportionately.



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

## 2.15 Alignment with EIOPA Guidelines on Information and Communication Technology Security and Governance

On 8 October 2020, the European Insurance and Occupational Pensions Authority (EIOPA) released Guidelines on information and communication technology security and governance (EIOPA-BoS-20/600). The EIOPA Guidelines are applicable as of 1 July 2021 to insurance and reinsurance undertakings. The Authority aligned the Guidance document with the EIOPA Guidelines. In particular, minor amendments were made in Paragraphs 4.7.5, 4.7.7, 4.9.6, 4.10.5 and 4.10.6 in this regard.

In the event of any inconsistency or conflict between this Guidance document and these sector-specific guidelines, the provisions of the sector-specific guidelines prevail.

## 2.16 Other feedback

Licence Holders may request further feedback or clarifications in relation to the Guidance document by sending an email to the Supervisory ICT Risk and Cybersecurity function within MFSA on sirc@mfsa.mt.



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