MFSA: Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements

Synopsis of the technical guidance

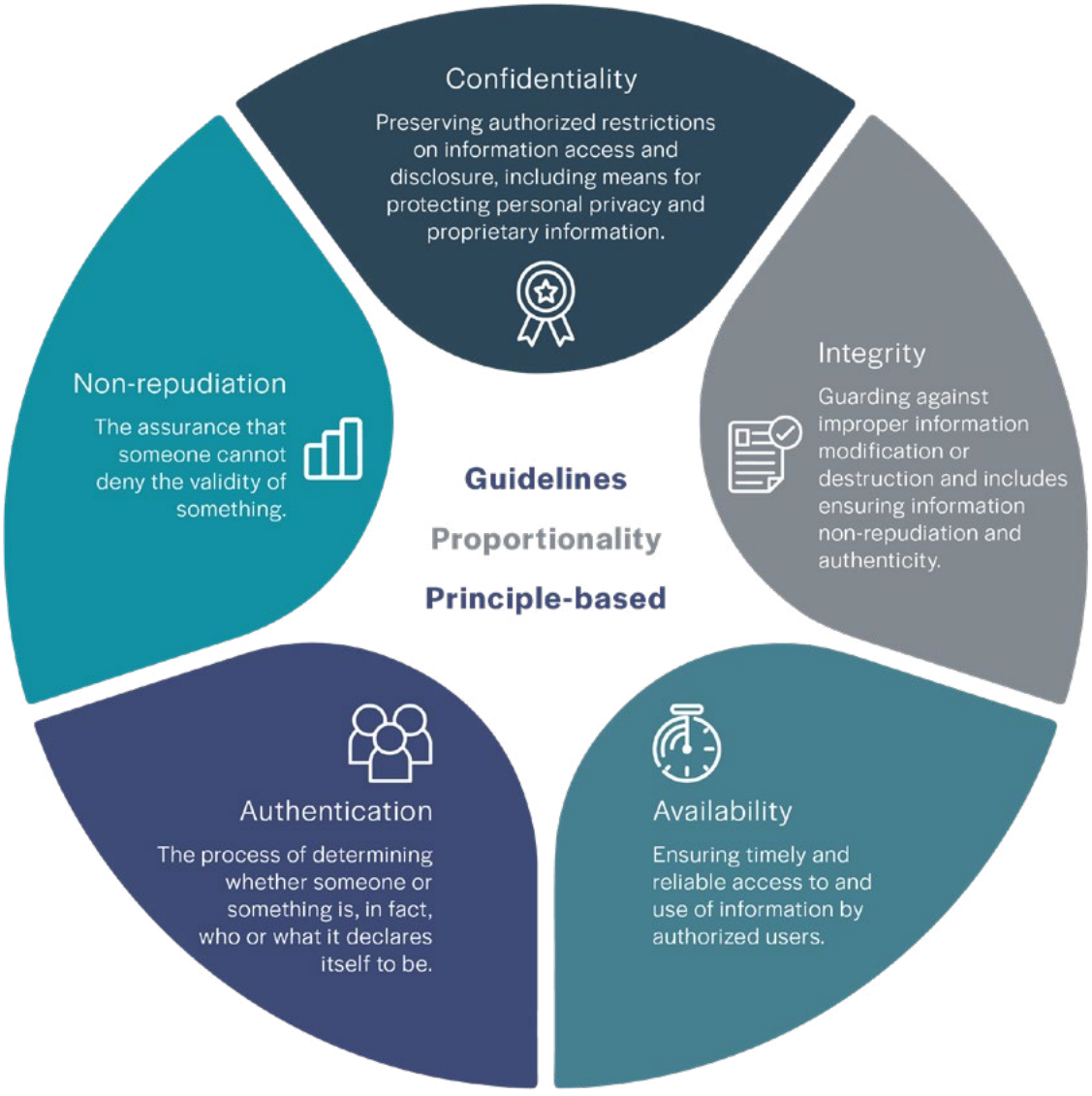
mazars

mazars

Synopsis of the technical guidance

On the 11th December 2020, the Malta Financial Services Authority (the "MFSA") issued cross-sectoral guidelines titled: Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements (the "Guidance").

The Guidance establishes a number of risk mitigation factors emanating from increased reliance on technological arrangements that need to be adequately mitigated. This includes the establishment of a comprehensive ICT governance framework. The MFSA Guidance also includes extensive guidance on the outsourcing of IT to third parties. The below sections provides detailed explanations on the areas covered by the Guidance document.



mazars

Technology Arrangements

Unrestricted audit by MFSA on technology arrangements

Technology Arrangements should be implemented in a way that guarantee all legal and regulatory compliance requirements, including competent authorities' rights to information gathering, right of access and right to audit (remote and on premises) irrespective of deployment method, to fulfil their legal obligations.

Cloud arrangements

The Guidance document elaborates on various types of Cloud arrangements and recommends to Licence Holders to carefully consider Cloud portability in general. Furthermore, MFSA draws the attention to number of risks that License holders face with Cloud arrangements such as:

- Combining Microservices with a well-established, mature container orchestration platform and application packaging framework if heading towards a loosely coupled architectural pattern;
- Placing reliance on any vendor proprietary software offered as PaaS and integrated in a Technology Arrangement serving a critical or important function, and where such software or middleware may not be readily offered as PaaS by other Cloud providers. This includes, but is not limited to, databases as a service (DBaaS); Recommendation on the use of Identity and Access Management as a Service (IAMaaS/ IDaaS), including Just-In-Time Privileged Access Management (JIT PAM) and Disaster recovery architecture in the Cloud which may include cloud-provider-specific elements embedded in the overall design of the Technology Arrangement.

Security Monitoring, DLP, eDiscovery, and forensic capabilities

Subject to the overarching provisions of proportionality, Licence Holders should make use of Security Incident and Event Management (SIEM) tools for round-the-clock real-time analysis of logs and security alerts generated by applications and network infrastructure, whether on premises or in the cloud, and for correlation of security events which enables Licence Holders to get the bigger picture of cyber threats and indicate a security issue.

For complex Technology Arrangements, License holders should augment their security information and event management setup with Security Orchestration Automation and Response (SOAR) and Cyber AI technology to improve security incident management by automating responses to low-level incidents, streamlining security operations and achieve higher efficiency and effectiveness.

Furthermore, the implementation of Data Loss Prevention (DLP) technology within a Technology Arrangement as part of a data governance framework is critical for effective regulatory compliance and protection of data in use, in motion and at rest. DLP should be augmented with eDiscovery capabilities to efficiently and effectively facilitate the identification, preservation, collection, processing, review, analysis, production and presentation of Electronically Stored Information (ESI), comprising both structured or unstructured data, when responding to internal, due diligence, litigation or regulatory requests in a timely and comprehensive manner.

Technology Arrangements include the necessary tools (e.g. for taking forensically sound virtual machine images, or cloud-based storage snapshots), some of which may need to be provided by Cloud Service Providers, infrastructure or middleware vendors, that facilitate such activities under an appropriate governance structure and documented procedures.

mazars

ICT and Security Risk Management

ICT governance / ICT strategy

The Management Body of the Licence Holder should ensure that there is an adequate internal governance and internal control framework in place covering ICT risk management as part of an overarching operational risk management framework, in accordance with all applicable legal and regulatory requirements, and sector-specific guidelines.

The Management Body should set clear roles and responsibilities on ICT management, cybersecurity/ information security management, as well as business continuity management.

ICT risk management

Licence Holders should identify and manage their ICT risks according to the three lines of defence model or similar internal control framework in use at their organisation that is approved by the Authority, and that ensures similar outcomes without prejudice to the Principle of Proportionality, applicable Acts, Regulations, rules or sector-specific guidelines.

The management framework governing ICT risk should include processes in place to:

a) enable management to determine an appropriate risk appetite for ICT risks;

b) identify and assess the ICT risks to which the Licence Holder is exposed via an ICT risk assessment;

c) define mitigation measures, including controls, to mitigate ICT risks;

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;

e) report to the Management Body on the ICT risks and controls;

f) identify and assess whether there are any ICT and security risks resulting from any major change in ICT system or ICT services, processes or procedures, and/or after any significant operational security incident.

The framework should be documented and continuously improved with "lessons learned" during the implementation and monitoring

Cyber security

Licence Holders should, under the principle of proportionality, consider internationally recognised standards and frameworks such as ISO/IEC 27001:2017 (particularly in conjunction with 27002:2013 and/or 27017:2015), the NIST Cybersecurity Framework, or CIS Critical Security Controls and their security objectives, when implementing their security control framework.

A person should be designated as the person responsible for the Information Security function

- Information Security policy – needs to define the high-level principles and rules to protect the confidentiality, integrity and availability of the License Holder's and its customers' information. Furthermore, this policy should be based on the relevant results of a risk assessment as well as sector specific compliance requirements.
- Logical security policy – needs to address a number of security risks, including segregation of duties, users accountability, privileged access rights, remote access, logging of user activities, access management, user access reviews, user access revocation and user authentication methods.
- Physical security policy - Physical access to ICT systems should be permitted only for authorised individuals. Authorisation should be assigned in accordance with the staff's tasks and responsibilities limited to individuals who are appropriately trained and monitored. Physical access should be regularly reviewed to ensure that unnecessary access is promptly revoked when not required.
- ICT operations security – License holder need to implement procedures to identify potential vulnerabilities, ensure secure configuration baselines, network segmentation, protection of endpoints, systems to ensure integrity of software, firmware and data, and encryption of data at rest and in transit, based on the data classification.
- Security monitoring - Licence Holders should implement appropriate and effective capabilities for detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets. The continuous monitoring and detection process should cover:

a) Relevant internal and external factors, including business and ICT administrative functions;

b) Transactions to detect misuse of access by third parties or other entities and internal misuse of access; and

c) Potential internal and external threats.

- Information security reviews, assessment and testing - Licence Holders should establish and implement an information security testing framework that validates their cybersecurity posture and ensure that this framework considers identified threats and vulnerabilities, identified through threat monitoring and the ICT risk assessment process. Licence Holders should perform ongoing and repeated tests of the security measures. All critical ICT systems should be subjected to vulnerability assessments and penetration testing by an independent party at least on an annual basis. Non-critical systems should be tested regularly on a risk-based approach, but at least every three years instead of annually provided that such systems are fully in scope of the processes and procedures covered and such non-critical systems are logically isolated from critical systems and there is no interdependence or information exchange between.
- Information security training and awareness - Licence Holders should ensure that staff members occupying key roles receive targeted information security training at least annually. Licence Holders should establish and implement periodic security awareness programmes to educate their staff, including the Management Body, on how to address information security risks.

ICT operations management

Licence Holders should manage their ICT operations based on documented and implemented processes and procedures. These should include as minimum:

- Technical documentation (including up to date asset inventory)
- Implement logging and monitoring procedures for critical ICT operations to allow for detection, analysis and correction of technical faults and errors.
- Backup and restoration procedures
- Incident management procedures

Business continuity management

Licence Holders should have business continuity arrangements as part of their operational risk management framework, in accordance with all applicable Acts, Regulations, rules or sector-specific guidelines, and having regard to the nature, scale and complexity of their business. As part of sound business continuity management, Licence Holders should:

- Conduct business impact analysis (BIA)
- Licence Holders should put BCPs in place to ensure that they can react appropriately to potential failure and cyber-attack scenarios. The license holder should be able to recover the operations of their critical business activities after disruptions within a recovery time objective (RTO, the maximum time within which a system or process must be restored after an incident) and a recovery point objective (RPO, the maximum time period during which it is acceptable for data to be lost in the event of an incident).
- Testing of DR plans
- Crisis communications

ICT Project and Change management

Subject to the Principle of Proportionality, Licence Holders should establish and implement an ICT projects portfolio management (also known as programme management) framework, which at a minimum, defines the organisation's approach to:

a) Programme Management i.e. structure, roles and responsibilities e.g. through a Project Management Office (PMO);

b) Projects pipeline management and change control;

c) Project management methodology;

d) Resource management;

e) Risk management taking into consideration the project management methodology;

f) Programme reporting, performance metrics, dashboards, update frequencies and escalation policy;

g) Post-project lessons learnt.

Licence Holders should establish and implement an ICT project management policy that includes as a minimum:

a) project objectives;

b) roles and responsibilities;

c) a project risk assessment;

d) a project plan, timeframe and steps;

e) key milestones;

f) change management requirements,

and ensures that information security requirements are analysed and approved by a function that is independent from the development function.

Licence Holders should develop and implement a process governing the acquisition, development and maintenance of ICT systems in order to ensure the confidentiality, integrity, availability of the data to be processed are comprehensibly assured and the defined protection requirements are met. This process should be designed using a risk-based approach.

Outsourcing Arrangements

Outsourcing

The MFSA guidance document includes on whole section on outsourcing, specifically addressing issues about governance, risks and responsibilities surrounding the phenomena of IT outsourcing.

The guidance document defines what constitutes outsourcing and what not. Furthermore, the guidance document states:

- Outsourcing within the same group companies does not exonerate the License holder from its responsibilities, since the guidance document clearly states that the responsibility still lies within license holder.
- The License holder should receive appropriate reports (including independent audit reports) from the outsourced service provider.
- Risk assessment for outsourced services (guidance document also lists the factors to be included in the risk assessment). This should take into consideration issues relating to conflict of interests.
- Outsourcing policy should be in place (guidance document also lists of areas to be included in the outsourcing policy)
- Business continuity plans need to factor in outsourcing arrangements.
- Areas to be covered by internal audit
- Register of outsourced services (guidance document also list what this register should include)
- Outsourcing process
  - Pre-outsourcing analysis
  - Contractual phase
  - Monitoring and oversight of outsourcing arrangements
  - Exit strategies

mazars

What do you need to do?

- Familiarise yourself with the MFSA guidance document and how this may impact your firm.
- Consider setting up a team/task force, including your IT team, to take a systematic approach to ensure compliance with the Guidance document. Engage external expertise if required.
- Understand the categories of data your firm processes, the medium through which they are processed, and where and how they are stored.
- Determine the inherent IT risk exposure that your firm faces.
- Identify the controls and safeguards implemented within your firm and their effectiveness to mitigate risk.
- Establish what remedial actions are required in order to ensure compliance to the MFSA Guidance.
- Establish a framework to ensure that IT risk is effectively and efficiently managed in an on-going manner.
- Take reasonable measures to be in a position to demonstrate that your entity complies to the MFSA guidance document.

How can we assist?

Mazars in Malta can guide and assist you through the different phases of this journey by working closely with you and your team. Our areas of assistance include the following:

1. Provide assurance on your firm's compliance with the MFSA Guidance document.
2. Identification of risks through an IT risk assessment, taking into consideration the size and complexity of your entity, including data sensitivity.
3. Draw up and/or assist in the implementation of a scalable remediation plan tailor-made for your firm.
4. Assist in the setting up and/or review of an ICT governance framework.
5. Assist with IT business continuity planning.
6. Assistance in setting up Security Incident and Event Management platforms.
7. Vulnerability assessments and penetration testing.
8. Provide cybersecurity training tailor-made to Board level members, Management level (including c-level management), executive members, and support staff.
9. Assist established internal audit functions to conduct IT Audit and cyber security services.
10. Assistance in setting up Computer Incident Response Teams and incident handling procedures.

Get in touch

Alan Craig, Partner
alan.craig@mazars.com.mt

Ramon Cutajar, Director
ramon.cutajar@mazars.com.mt

Mazars
32, Sovereign building
Zaghfran road
Attard ATD9012
Malta

www.mazars.com.mt

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws

mazars