FMA

Finanzmarktaufsicht
Liechtenstein

FMA Guidelines 2021/3 – ICT Security Guidelines

Guidelines on the Monitoring of Information and Communications Technology (ICT) Risks

Reference:	FMA Guidelines 2021/3
Addressees:	– Banks under the Liechtenstein Banking Act (*Bankengesetz, BankG*; hereinafter referred to as the "BA") – Investment firms under the BA – E-money institutions under the Liechtenstein E-Money Act (*E-Geldgesetz, EGG*) – Payment institutions under the Liechtenstein Payment Services Act (*Zahlungsdienstegesetz, ZDG*) – Insurance undertakings under the Liechtenstein Insurance Supervision Act (*Versicherungsaufsichtsgesetz, VersAG*) – Insurance intermediaries under the Liechtenstein Insurance Distribution Act (*Versicherungsvertriebsgesetz, VersVertG*) – Pension schemes under the Liechtenstein Occupational Pensions Act (*Gesetz über die betriebliche Personalvorsorge, BPVG*) – Pension funds under the Liechtenstein Pension Funds Act (*Pensionsfondsgesetz, PFG*) – Management companies and undertakings for collective investment in transferable securities (UCITS) under the Liechtenstein Act on Certain Undertakings for Collective Investment in Transferable Securities (*Gesetz über bestimmte Organismen für gemeinsame Anlagen in Wertpapieren, UCITSG*) – Management companies and investment undertakings under the Liechtenstein Law on Investment Undertakings (*Investmentsunternehmensgesetz, IUG 2015*) – Alternative investment fund managers under the Liechtenstein Alternative Investment Fund Managers Act (*Gesetz über die Verwalter alternativer Investmentfonds, AIFMG*) – Asset managers under the Liechtenstein Asset Management Act (*Vermögensverwaltungsgesetz, VVG*)
Publication:	Website
Adoption:	19 May 2021
Entry into force:	1 January 2022
Last amended on:	–
Legal bases:	Article 4 of the Liechtenstein Financial Market Supervision Act (*Finanzmarktaufsichtsgesetz, FMAG*; hereinafter referred to as the "FMA Act") and Article 25(1) of the FMA Act

Landstrasse 109 • P.O. Box 279 • 9490 Vaduz • Liechtenstein
Telephone +423 236 73 73 • Fax +423 236 73 74 • www.fma-li.li • info@fma-li.li

FMA

Contents

1. Principles and legal basis

1. These Guidelines are based on Articles 4 and 25 of the FMA Act. This underlying legislation is supplemented by special statutory regulations.
2. These ICT Security Guidelines are to be read in the light of the principle of proportionality. Implementation of these Guidelines shall depend on the respective risk structure, complexity and size of the particular financial intermediary, as well as on the scope and nature of its business. The financial intermediary must ensure that these Guidelines are implemented appropriately.
3. Alongside the requirements set out in these Guidelines, financial intermediaries must also observe the supervisory requirements (as from time to time in force) that are applicable to them. Information on their specific applicability can be found in the FMA Communications, which are published on the FMA website, on the application of the guidelines and recommendations issued by the European Supervisory Authorities.
4. Requirements relating to functions for which there is no underlying statutory basis need not be implemented. If, for example, a special law should provide that a financial intermediary is not required to establish an internal auditing system, the corresponding requirements relating to internal auditing need not be implemented.
5. For information purposes, with regard to the specific implementation of an information security management system (ISMS) and risk management system by financial intermediaries, reference is made to the following international standards; however, these standards are not binding for financial intermediaries:
    - ISMS: ISO 27001, NIST Cybersecurity Framework, COBIT, BSI Grundschutz (Basic Security)
    - Risk management system: NIST SP 800-53, ISO 27005

2. Definitions

Information and communications technologies (ICT)

The term “information and communications technologies (ICT)” covers all technical media used for handling information and supporting communications. This includes, inter alia, computer and network hardware as well the associated software.

ICT and security risks (including cyber risks)

This means the risk of loss due to a breach of confidentiality; loss of integrity of systems and data; an inadequate availability, or a lack of availability, of systems and data; or an insufficient capability to change information technology (IT) within a reasonable time frame and at a reasonable cost if the environmental or business requirements should change (i.e. agility). This also includes security risks arising from inadequate or defective internal processes, or external events, including cyberattacks or inadequate physical security measures.

ICT systems

ICT components forming part of a network or interconnected network that supports the operational activities of a financial institution.

ICT services

Services that are provided by ICT systems for one or more internal or external users. Examples include services in the areas of data collection, data storage, data processing and reporting, as well as monitoring services, and business and decision-making support services.

ICT assets

The inventory of software and hardware used by a financial intermediary in order to provide its ICT services in a business context.

ICT projects

All projects or partial projects to change, replace, discard or implement ICT systems and services. ICT projects may form part of a larger ICT or business transformation programme.

ICT operational incidents or ICT security incidents

An individual incident or a series of interrelated incidents not planned by the financial intermediary that have, or could have, a negative impact on the integrity, availability, confidentiality and/or authenticity of ICT services.

Management body

The body or bodies of an institution that is/are appointed and authorised to determine the strategy, objectives and general policy of the institution as well as to control and monitor the decisions of the executive board, and whose members include the persons who actually manage the business of the institution.

Patch

A patch is a small program for fixing software errors such as security loopholes in application software or operating systems.

Penetration tests/Red Team exercises/threat-led penetration tests

A penetration test is a targeted – and usually simulated – attempt to attack an IT system. It is used to test the effectiveness of existing security measures.

Red Team exercises involve the simulation of an attack on a friendly infrastructure by a group (Red Team) operating under realistic conditions, with the aim of testing the security and defence mechanisms. Another group inside the infrastructure (Blue Team) attempts to ward off the intruders from the other side.

A threat-led penetration test is a controlled attempt to compromise the cyber resilience of a company by simulating the tactics, techniques and methods of real-life hackers. It is based on targeted threat intelligence and focuses on the employees, processes and technologies of a company with minimal prior knowledge and impact on business operations.

ICT system landscape

The ICT system landscape describes the entirety of the IT and communications systems used within an ICT environment, including the applications and all of the infrastructure components within a network, as well as the electronic data to be managed and the interfaces between the components.

Important ICT services and/or ICT systems (in an outsourcing context)

ICT services and/or ICT systems that are critical or essential under the supervisory and statutory regulations (as from time to time in force) that apply to financial intermediaries. In the absence of any more-extensive supervisory or statutory regulations that define ‘importance’ for financial intermediaries, outsourced ICT

services and/or ICT systems shall be deemed important if an assessment conducted autonomously by the financial intermediary identifies them as critical or important for the provision of its services.

3. ICT strategy

6. The management body of a financial intermediary is responsible for determining, approving and continuously monitoring the implementation of the ICT strategy as part of its overall business strategy. It is also responsible for establishing an effective risk management framework for the ICT and security risks. In this respect, financial intermediaries must put in place appropriate procedures for monitoring the implementation of their ICT strategy and measuring its effectiveness. The management body must review the ICT strategy on a regular and ad hoc basis in order to ensure that it is up to date; any necessary adjustments must be implemented.

7. The ICT strategy is to be coordinated with the overall business strategy. It gives substance to the ICT architecture development by providing an overview of the ICT system landscape, including dependencies on third parties. As a minimum, the ICT strategy must address and include the following points:

   a) How the financial intermediary's ICT needs to be developed in order to effectively implement and support the business strategy, including development of the organisational structure, the ICT system changes (new systems [internally or externally developed] and changes to existing systems) and important dependencies on third parties.
   b) Whether or not outsourcing of the ICT systems and/or ICT services is desired. If so, to what extent and what are the factors that will need to be considered?
   c) Clear and measurable information security objectives, with a focus on ICT systems and ICT services, personnel and processes.

8. To this end, financial intermediaries must establish action plans for achieving the objectives of their ICT strategies. These action plans must be communicated to all relevant employees, as well as contractors and third-party suppliers (where applicable and relevant), and be reviewed regularly to ensure their relevance and adequacy. In the case of outsourced ICT services and/or ICT systems, the relevant actions are delegated to the service provider as part of the outsourcing arrangement; the process by which the financial intermediary is to monitor attainment of the objectives must be defined.

4. ICT governance

9. The financial intermediary's IT governance must ensure that the ICT strategy is measurable and that it is implemented effectively. The management body shall ensure that the financial intermediary has an appropriate internal governance structure and an adequate internal control framework for managing ICT and security risks, which must also cover outsourced ICT services and/or ICT systems. In this respect, the management body shall define clear duties and responsibilities for ICT functions, information security risk management and business continuity, including those of the management body and its committees.

10. The management body shall ensure that the financial intermediary's staff are professionally qualified to a sufficiently high standard. It must also ensure that they have sufficient resources to continuously support the ICT operational requirements, and the ICT and security risk management processes, as well as to ensure the implementation of their ICT strategy. The management body must furthermore ensure that the allocated budget contains adequate funds to enable the above requirements to be fulfilled. Financial intermediaries shall also ensure that all employees, including holders of key functions, are provided with adequate training at least once per year on ICT and security risks, including information security.

11. The financial intermediary's internal audit shall also give due consideration to the ICT and security risks during the course of the audit planning, taking into account the risk analysis in connection with its multi-year planning.

5. ICT and information security risk management

5.1 Organisation and objectives

12. The financial intermediary shall have an adequate and effective ICT and information security risk management concept, which is integrated into the financial intermediary's company risk management concept.

13. Financial intermediaries shall identify, assess and manage their ICT and security risks, including those arising from outsourcing arrangements. The ICT roles or organisational units responsible for the ICT systems, processes and security functions shall be provided with appropriate processes and control mechanisms to enable them to ensure that all risks can be identified, analysed, measured, monitored, managed, reported and kept within the limits of the financial intermediary's risk tolerance level. In addition, the projects they implement, the systems they provide and the functions they perform must be compliant with external and internal requirements.

14. The financial intermediaries shall assign responsibility for the control and monitoring of ICT and security risks to the risk management unit. The risk management unit shall ensure that the ICT and security risks are identified, measured, assessed, managed, monitored and reported; it has operational responsibility for monitoring and controlling compliance with the ICT security risk management framework. Financial intermediaries shall guarantee the independence and objectivity of their risk management units and ensure that there is appropriate separation of ICT operational processes; they shall also ensure that their risk management units are not assigned responsibility for the internal audit functions. This risk management unit shall be directly accountable to the executive board and shall be responsible for monitoring and controlling compliance with the ICT and security risk management framework.

15. With the aid of a risk-based approach, the internal audit process must be capable of independently reviewing, and objectively assessing, all ICT and security-related functions and departments within a financial institution, in order to verify their compliance with both the principles and procedures of the financial institution and with the external requirements. Financial intermediaries shall define and assign important and relevant roles, responsibilities and corresponding reporting obligations in a manner that ensures the ICT and information security risk management frameworks will be effective.

16. The ICT and information security risk management frameworks shall include processes to enable the following:

a) Determination of a risk tolerance level for ICT and security risks that is consistent with the financial intermediary's risk tolerance level
b) Identification and assessment of the ICT and security risks to which the financial intermediary is exposed
c) Specification of measures, including control measures, to minimise ICT and security risks and thus ensure that they remain within the risk tolerance level and the limits specified in supervisory requirements
d) Monitoring of the effectiveness of these measures and recording of the number of reported incidents that impact upon ICT-related activities, and the introduction of appropriate measures where necessary
e) Reporting to the management body on the ICT and security risks and control measures
f) Identification and assessment of whether or not there are any ICT and security risks arising from a major change in the ICT system or the ICT services, processes or procedures, and/or following a major operational or security incident

17. Financial intermediaries shall ensure that the ICT and information security risk management frameworks are complied with, documented and continuously improved on the basis of the knowledge gained during the implementation and monitoring processes. The ICT and information security risk management frameworks are to be reviewed and approved by the management body at least once per year.

5.2 Determination of functions, processes and ICT assets

18. The financial intermediaries shall prepare an updated overview of their business functions, duties, business processes and support processes and keep these up to date, in order to determine the significance of their interdependencies with respect to ICT and security risks.

19. In addition, the financial intermediaries shall prepare, and keep up to date, an inventory of ICT assets that shows their business functions and support processes, such as the ICT systems, as well as their dependencies on other internal and external systems. The financial intermediary shall also maintain, and keep up to date, current lists of employees, contractors and third parties, in order to be able to manage, as a minimum, the ICT assets that support the critical functions and processes.

5.3 Criticality grading and risk assessment

20. Financial intermediaries shall grade the business functions, support processes and ICT assets identified in accordance with Section 5.2 Determination of functions, processes and ICT assets in terms of their criticality.

21. In order to assess the criticality of these identified business functions, support processes and ICT assets, financial intermediaries shall take into account, as a minimum, the confidentiality, integrity and availability requirements. The competencies and responsibilities for the ICT assets shall be clearly assigned.

22. When the risk assessment is carried out, financial intermediaries shall review the adequacy of the criticality gradings for the ICT assets, as well as the corresponding documentation.

23. Financial intermediaries shall identify the ICT and security risks that impact upon the identified business functions, support processes and ICT assets in terms of their criticality. This risk assessment shall be carried out and documented annually or, if necessary, at shorter intervals. Such risk assessments shall also be carried out in the case of all major changes to infrastructure, processes or procedures affecting the business functions, support processes or ICT assets, and the financial intermediary's risk assessment shall then be updated accordingly.

24. Financial intermediaries shall ensure that the threats and vulnerabilities concerning business functions, support processes or ICT assets are continuously monitored and shall regularly review the risk scenarios affecting these.

5.4 Risk reduction

25. On the basis of the risk assessments, the financial intermediaries shall determine the measures necessary to ensure that the identified ICT and security risks are kept within acceptable limits; they shall also determine whether any changes to the existing business processes, control measures, ICT systems and ICT services are necessary. The financial intermediary shall give consideration to the implementation period that will be necessary in order to implement these changes and shall take appropriate interim measures to minimise the resulting ICT and security risks, and thus keep within the financial intermediary's ICT and security risk tolerance level.

26. The financial intermediaries shall determine and implement measures to minimise the identified ICT and security risks, as well as to protect ICT assets on the basis of their classification according to Section 5.3 Criticality grading and risk assessment.

5.5 Reporting

27. Financial intermediaries shall inform their management body of the findings of the risk assessment in a clear and timely manner.

5.6 Internal auditing

28. The management body of a financial intermediary shall approve the audit plan, including any ICT audits and major changes to these. The audit plan and manner of its implementation, including the frequency of the audits, must reflect the inherent ICT and security risks to which the financial intermediary is exposed, taking into account proportionality, and must be updated regularly.

29. A formal process with clear responsibilities for the follow up and rectification of critical ICT audit results must be defined; this shall also include time limits for the rectifications.

6. Information security management

6.1 Information security guidelines

30. Financial intermediaries shall develop and document information security guidelines in which the overarching principles and rules for protecting the confidentiality, integrity and availability of the data and information belonging to the financial intermediary and its clients are defined, elaborated upon and documented. The information security guidelines must be consistent with the financial intermediary's information security objectives and be based on the relevant results from the risk assessment process. The guidelines shall be approved by the management body.

31. The guidelines shall include a description of the information security management unit's most important roles and responsibilities. They shall also set out the information security requirements concerning employees, service providers, processes and technologies. The guidelines must guarantee the confidentiality, integrity and availability of the financial intermediary's critical, logical and physical ICT assets and resources, as well as sensitive stored data (data at rest) and sensitive data in transit (data in transit). The information security guidelines shall be communicated to all employees of the financial intermediary; they must also be communicated to the relevant staff of the financial intermediary's contractors in the case of important ICT outsourcing arrangements, unless the relevant information security information has been adequately provided to the contractor in the outsourcing guidelines.

6.2 ICT monitoring and information security

32. Financial intermediaries shall define and implement rules and procedures to enable them to identify anomalous activities that may affect their information security and to respond appropriately to such events. Within the framework of this continuous monitoring process, financial intermediaries shall implement appropriate and effective measures for detecting and reporting physical intrusions, hacker attacks, unauthorised data outflows and violations of the confidentiality, integrity and availability of the ICT assets. The continuous monitoring and detection processes shall cover the following:

    a) Relevant internal and external factors, including business and ICT administration functions
    b) Transactions and processes for identifying access misuse by third parties or other entities, as well as internal access misuse
    c) Potential internal and external threats

33. Financial intermediaries shall establish and implement processes and organisational structures to enable identification and continuous monitoring of security threats that may have a significant impact on their ability to provide their services. Financial intermediaries must ensure that institution-specific potential threats from cyberattacks can be identified, particularly in relation to critical and/or sensitive data and ICT systems. Financial intermediaries must actively keep abreast of technological developments to ensure they are aware of the security risks. Financial intermediaries shall establish detection measures to enable the identification of potential data leaks, malicious code and other security threats, and publicly known security loopholes in software and hardware, as well as to identify relevant new security updates (see Section 8.1 ICT operations security).

34. The security monitoring process helps the financial intermediary to understand the nature of the operational or security incidents, for the purposes of identifying trends and assisting investigations.

6.3 Inspection, evaluation and testing of information security measures

35. Financial intermediaries shall inspect, evaluate and test ICT systems, ICT services and information security measures in order to ensure the effective identification of security breaches, security incidents and vulnerabilities in their ICT systems and ICT services (see Section 8.1 ICT operations security). By means of good practice approaches such as vulnerability management with regular vulnerability analyses, penetration tests, Red Team exercises and other appropriate measures, financial intermediaries shall check for security loopholes and thus protect sensitive data and ICT systems.

36. Financial intermediaries shall design and implement an information security testing framework for assessing the robustness and effectiveness of their information security measures; it must be ensured that this framework takes into account the threats and vulnerabilities identified during the threat monitoring and the information risk management processes.

37. The framework for the information security tests must ensure that the tests

    a) are conducted by independent testers with adequate knowledge, skills and competencies in the field of testing information security measures, who are not involved in the development of the information security measures; and
    b) include extensive vulnerability and penetration tests (including threat-led penetration tests where necessary and appropriate) that reflect the identified risk level of the business processes and systems.

38. Financial intermediaries shall repeat the tests of the security measures on a regular basis. For all critical ICT systems, these tests must be carried out at least once per year. Non-critical systems are to be tested periodically, and at least once every five years, using a risk-based approach.

39. Financial intermediaries shall ensure that testing of the security measures is carried out promptly in the event of changes to the infrastructure, processes or procedures, or in the event of changes due to major operational and security incidents, or following the approval of new critical applications that are linked to the Internet, or any major modifications to such applications.

40. Financial intermediaries shall monitor and assess the results of the security tests, implement appropriate adjustments to the security measures, and update the security measures for their critical ICT systems appropriately and without delay.

41. Based on the observed security threats and the implemented changes, tests shall be carried out under scenarios involving relevant and known potential attacks.

6.4 Training and awareness raising in relation to information security

42. Financial intermediaries shall introduce a training programme, including a regular security awareness-raising programme, for all employees and relevant persons in order to ensure that they are trained to fulfil their duties and responsibilities in manner consistent with the relevant information security guidelines and procedures, and thus minimise the potential for human errors, theft, fraud, misuse or losses; it must also be ensured that they are trained in how to respond appropriately to information security risks. Financial intermediaries shall ensure that training is carried out at least once per year for all employees and relevant persons. The training may be delivered by employees or by affiliated or external specialists.

7. User authorisation management

7.1 Logical security/access protection

43. Financial intermediaries shall define, document and implement procedures for logical access controls (identity and access management). These procedures must be put into practice, enforced, monitored and regularly reviewed. The procedures must also include control measures for monitoring anomalies. As a minimum, these procedures must implement the following elements, for the purposes of which the term “user” also refers to technical users:

    a) Need-to-know, principle of least privilege, and separation of functions: Financial intermediaries shall manage the access rights to ICT assets and their support systems, including for remote access, on a need-to-know basis. Users shall be granted the minimum set of access rights that is strictly necessary for them to perform their duties (principle of least privilege), this is to prevent unauthorised

access to a large volume of data, as well as to avoid access rights being assigned in combinations that would enable control mechanisms to be bypassed (principle of separation of duties).

b) User accountability: financial intermediaries shall limit the use of generic and commonly used user accounts as far as possible, and shall ensure that users performing actions in the ICT systems can be identified.

c) Privileged access rights: Financial intermediaries shall ensure that privileged system access is subject to strict controls by strictly limiting and closely monitoring accounts with higher levels of system access rights (e.g. administrator accounts). To ensure secure communications and minimise risks, remote administrative access to important ICT systems must take place only on a need-to-know basis, using strong authentication solutions.

d) Logging of user activity: All activities performed by privileged users must be logged and monitored. Access logs must be stored for an appropriate period based on the criticality of the identified business functions, support processes and ICT assets, according to Section 5.3 Criticality grading and risk assessment, without prejudice to the retention obligations under EU and national law. The appropriate period shall be determined by reference to the general retention periods under the Liechtenstein Law on Persons and Companies (*Personen- und Gesellschaftsrecht, PGR*). Financial intermediaries shall use this information to aid the identification and investigation of anomalous activities occurring during the provision of services.

e) Access management: Access rights are to be granted, revoked or changed promptly (immediately after occurrence/awareness of the event) on the basis of pre-defined approval workflows, which involve the owner of the information. Access rights must be revoked immediately upon termination of an employment relationship.

f) Access certification: access rights shall be checked regularly to ensure that users do not have any excessive privileges and that access rights are revoked if they are no longer necessary.

g) Authentication methods: Financial intermediaries shall implement authentication methods that are sufficiently robust to ensure adequate and effective access controls that are compliant with the rules and procedures. The authentication methods must adequately reflect the criticality of the ICT systems, ICT information or the relevant access process. As a minimum, this must include complex passwords or strong authentication methods (e.g. two-factor authentication) that are based on the relevant risk.

44. Electronic access by applications to data and ICT systems is to be kept to the minimum level necessary for provision of the relevant service.

7.2 Physical security

45. The physical security measures of financial intermediaries shall be defined, documented and implemented in a manner that ensures their premises, data centres and sensitive areas are protected against unauthorised access and environmental hazards.

46. Physical access to ICT systems shall be granted only to authorised persons. Authorisations shall be issued in line with the individual's duties and responsibilities and shall be limited to persons who are adequately trained and supervised. Physical access rights shall be reviewed regularly to ensure that any unnecessary access rights are revoked as soon as they are no longer required.

47. Appropriate measures for protecting against environmental hazards reflect the importance of the buildings and the criticality of the activities or ICT systems housed within them.

8. ICT operational management

48. Financial intermediaries shall manage their ICT activities on the basis of documented and implemented processes and procedures that have been defined by the management body. These documents shall define how the financial intermediaries are to operate, monitor and control their ICT systems and ICT services, including documentation of critical ICT processes, and must enable them to maintain an up-to-date ICT inventory.

49. Financial intermediaries shall ensure that the output of their ICT activities is aligned to their business requirements. Financial intermediaries shall improve and, where possible, maintain the efficiency of their ICT activities; this includes, but is not limited to, the need to minimise potential errors arising from the execution of manual activities.

50. Financial intermediaries shall implement logging and monitoring procedures for critical ICT activities that will enable the identification, analysis and rectification of errors.

51. Financial intermediaries shall maintain an up-to-date inventory of their ICT assets (including ICT systems, network devices, databases, etc.). To enable a proper configuration and change management process, the ICT system inventory shall include the configurations of the ICT systems, as well as the connections and dependencies between the various ICT systems.

52. The ICT system inventory must be sufficiently detailed to enable the immediate identification of a system and its location, security classification and ownership. Interdependencies between systems must be documented to aid responses to security incidents and operational disruptions, including cyberattacks. Effective processes for procuring and disposing of ICT assets must be established in order that the inventory can be updated promptly and without any omissions.

53. Financial intermediaries shall monitor and manage the life cycles of their ICT systems to ensure that they continue to meet and support the business and risk-management requirements. Financial intermediaries shall monitor whether their ICT systems are supported by their external or internal suppliers and developers and whether all relevant patches and upgrades have been installed on the basis of documented processes. Risks arising from outdated or unsupported ICT systems shall be assessed and mitigated.

54. Financial intermediaries shall implement processes to facilitate performance and capacity planning as well as performance monitoring, in order that important performance problems and ICT capacity bottlenecks can be identified, responded to promptly and prevented.

55. Financial intermediaries shall define and implement backup and recovery procedures for data and ICT systems in order to ensure that these can be recovered and restored when necessary. The scope and frequency of the backup operations must be consistent with the business recovery requirements and the criticality of the data and the ICT systems, and shall be assessed with the aid of the completed risk assessment. The backup and recovery procedures must be tested periodically.

56. Financial intermediaries shall ensure that data and ICT system backups are stored securely and are located far enough away from the primary location to ensure that they will not be exposed to the same environmental risks.

8.1 ICT operations security

57. Financial intermediaries shall implement procedures to prevent the occurrence of security problems in ICT systems and ICT services, minimise their impact on the provision of ICT services and ensure the management of infrastructure and network security. These procedures must incorporate the following measures:

    a) Identification of potential vulnerabilities, which must be assessed and remedied by ensuring that software and firmware (including the software provided by financial intermediaries to their internal and external users) are kept up to date through the installation of critical security patches, if available, or by implementing alternative measures to ensure that they are adequately protected
    b) Definition, implementation and regular monitoring of secure basic configurations for all network components
    c) Implementation of a network segmentation system, a system for preventing data losses and a system for encrypting network traffic outside of protected network zones (data in transit) (according to the data classification)
    d) Implementation of solutions for protecting end points, including servers, workstations and mobile devices; before allowing end points to access the company network, financial intermediaries shall evaluate whether or not the end points meet the security requirements specified in the security standards they have defined
    e) Ensuring that mechanisms are available for monitoring the integrity of software, firmware and data (particularly security relevant settings)

58. Furthermore, the financial intermediaries shall continuously monitor whether changes in the existing operating environment affect the existing security measures, or if such changes necessitate the implementation of additional measures in order to adequately mitigate the associated risks. These changes form part of the financial intermediaries formal change management process, which ensures that changes are properly planned, tested, documented, authorised and put into effect.

8.2 Management of ICT incidents and problems

59. Financial intermediaries shall implement and put into effect an incident and problem management process for monitoring and logging operational and security-relevant ICT incidents; in the event of disruptions, this must enable them to take prompt action to maintain or restore important business functions and processes, in accordance with Section 11 Disaster recovery plan and business continuity management. Financial intermediaries shall define suitable criteria and thresholds for the classification of events as operational or security incidents; they shall also establish early warning indicators to provide warnings that will enable early detection of such incidents.

60. In order to minimise the impact of adverse events and enable a timely recovery, financial intermediaries shall establish appropriate processes and organisational structures to ensure coherent and integrated monitoring, handling and follow-up of operational and security incidents; they must also enable the identification and elimination of the main causes so as to prevent repetition of the incidents. The incident and problem management process shall specify:

    a) The procedure for identifying, tracking, logging, categorising and classifying incidents according to a prioritisation system that is based on the business criticality
    b) The roles and responsibilities for the various incident scenarios (e.g. errors, malfunctions, cyberattacks)

c) Problem management procedures for identifying, analysing and resolving the underlying causes of one or more incidents. Financial intermediaries shall analyse operational or security incidents which they are likely to have been affected by, which have actually been identified, or which have occurred within and/or outside the organisation; they must then take account of the important findings from these analyses and update their security measures accordingly.
d) Important internal communication plans, including incident reporting and escalation procedures – which also covers security-related client complaints – in order to ensure that:
    i. Incidents with potentially severe adverse effects on critical ICT systems and ICT services are reported to the management level of the ICT department and the management body responsible for ICT.
    ii. The management body is informed on an ad hoc basis in the event of serious incidents; as a minimum, this must include details of the effects, the response and the additional controls that will need to be defined as a result of the incidents.
e) Procedures for responding to incidents in order to mitigate the effects associated with the incidents and ensure that the service is promptly restored to an operational state and made secure
f) Specific external communication plans for critical business functions and processes to:
    i. Collaborate with relevant stakeholders, e.g. service providers, in order to provide an effective response and ensure a recovery following an incident.
    ii. Inform external parties (e.g. clients, other market participants or supervisory authorities), where necessary, within the prescribed time limits, in accordance with the applicable regulations.

9. ICT projects and change management

9.1 ICT project management

61. The financial intermediary shall implement a programme and/or a project governance process, which must define roles, responsibilities and competencies, in order to effectively support implementation of the ICT strategy.

62. The financial intermediary shall adequately monitor and minimise the risks associated with its portfolio of ICT projects (programme management), taking into account the risks that may arise from the dependencies between different projects, as well as the risks arising in cases where multiple projects are dependent on the same resources and/or specialist knowledge. In this respect, the financial intermediary shall also take account of any projects involving major changes to ICT systems, as well as projects that will have significant effects on the risks relating to ICT security.

63. The financial intermediary shall prepare and implement a set of ICT project management guidelines which must, as a minimum, cover the following:

    a) Project objectives
    b) Roles and responsibilities
    c) A project risk assessment
    d) A project plan, a time frame and project steps
    e) Important milestones
    f) Change management requirements
    g) Acceptance criteria for the handover of new ICT functions to the company

64. The ICT project management guidelines must stipulate that the information security requirements are to be analysed and approved by a unit that is independent of the development unit.

65. The financial intermediary shall ensure that all divisions affected by an ICT Project are represented in the project team and that the project team has the necessary knowledge (including the relevant functions and competencies from the different ICT areas, based on the risk level), in order to guarantee a secure and successful project implementation.

66. The management body must be informed, regularly or ad hoc, of the initiation and progress of ICT projects and the associated risks, on either an individual or a collective basis depending on the significance and size of the ICT projects. Financial intermediaries shall integrate project risks into their risk management system.

9.2 Purchasing and development of ICT systems

67. Financial intermediaries shall develop and put into effect a process for regulating the purchasing, development and maintenance of ICT systems. This process shall be developed using a risk-based approach.

68. The financial intermediary shall ensure that, prior to purchasing or developing ICT systems, the functional and non-functional requirements (including information security requirements) have been clearly defined and approved by the relevant management body.

69. The financial intermediary shall ensure that measures are taken to minimise the risk of unintended changes to, or intentional manipulations of, the ICT systems during development and implementation in the production environment.

70. Financial intermediaries shall have a methodology for testing and approving ICT systems prior to their first use. This methodology must take into account the criticality of the business processes and assets. The tests must ensure that the new ICT systems function as intended. They must also use testing environments that adequately reflect the production environment.

71. Financial intermediaries shall implement separate ICT environments in order to minimise functional disruptions and the effects of non-verified changes to the production systems. In particular, they must ensure the separation of production environments from development, testing and other types of non-production environments. Financial intermediaries shall ensure the integrity and confidentiality of production data within non-production environments. Access to production data shall be limited to authorised users. Data in the testing environment must be made subject to the same protection requirements as data in the production environment as soon as productive data are used in the testing environment.

72. Financial intermediaries shall take measures to protect the integrity of the source code for ICT systems that have been developed in-house. They shall also document the development, implementation, operation and/or configuration of the ICT systems comprehensively in order to reduce any unnecessary dependencies on technical experts. Where applicable, the documentation for the ICT systems shall include, as a minimum, user documentation, technical system documentation and work instructions.

73. The financial intermediary’s processes for the purchasing and development of ICT systems shall apply also in respect of ICT systems that are developed or managed outside of the ICT organisation by the end-users of the business function (e.g. end-users of computer applications), subject to a risk-based approach. The financial intermediary shall maintain a list of the applications that support important business functions or processes.

9.3 ICT change management

74. Financial intermediaries shall prepare and implement an ICT change management process in order to ensure that all changes to ICT systems – including, in particular, security-related configuration changes – are recorded, tested, assessed, approved, implemented and reviewed in a controlled manner. When making changes in emergency situations (i.e. changes which need to be introduced as quickly as possible), financial intermediaries shall follow procedures that include appropriate security precautions.

75. Financial intermediaries shall determine whether or not changes in the existing operating environment affect the existing security measures, or if such changes will necessitate new measures to minimise the associated risks. Such changes must be compliant with the financial intermediary's formal change management processes.

10. Outsourcing (including cloud)

10.1 Principles

76. The outsourcing of ICT services and/or ICT systems shall not result in delegation of the financial intermediary's responsibilities. Financial intermediaries shall remain fully responsible and accountable for fulfilling their regulatory obligations, including the ability to supervise the outsourced ICT services and/or ICT systems. They shall remain responsible to the FMA for the outsourced ICT services and/or ICT systems in the same manner as if they operated these themselves.

77. When outsourcing ICT services and/or ICT systems, financial intermediaries shall:

    a. Clearly assign responsibilities for the documentation, management and control of outsourcing agreements:
        i. As part of their risk management function, financial intermediaries shall set up a separate outsourcing unit or– insofar as this is permissible under statutory regulations – designate a manager. In the latter case, the manager must be directly subordinate to the management body (e.g. a holder of a key function in relation to a control function). As part of the financial intermediary's internal control framework, the outsourcing unit or manager shall be responsible for monitoring and controlling the risks associated with outsourcing agreements, as well as for monitoring the documentation associated with the outsourcing agreements.
        ii. Financial intermediaries may, after taking proportionality principles into account, delegate the outsourcing function to a member of their executive board. Duties and responsibilities for the management and control of outsourcing agreements must be clearly separated.
    b. Assign sufficient resources to ensure compliance with all legal and supervisory requirements, including these Guidelines, and to ensure the documentation and monitoring of all outsourcing agreements.
    c. Define how they will reduce dependencies on service providers to an acceptable level by means of risk assessments, Business Continuity Management and exit strategies.

78. Before entering into an outsourcing agreement, financial intermediaries must:

    a. Check whether the outsourcing agreement concerns important ICT services and/or ICT systems
    b. Identify and assess all relevant risks associated with the outsourcing agreement
    c. Carry out appropriate due diligence auditing of the potential service provider
    d. Assess whether the supervisory requirements that apply to them are being complied with
    e. Identify and assess any conflicts of interest that may arise in connection with the outsourcing arrangement

79. For the purposes of the risk assessment and the due diligence audit, financial intermediaries shall adopt an approach that is appropriate to the nature, scope and complexity of the risks associated with the ICT services and/or ICT systems that are being outsourced to the service provider.

80. The financial intermediary's internal audit must independently verify, by means of a risk-based approach, that its outsourcing framework has been properly and effectively implemented. In particular, the audit plan should encompass the outsourcing agreements for important ICT services and/or ICT systems.

10.2 Outsourcing guidelines

81. Outsourcing guidelines address the practical implementation of the requirements set out in the outsourcing strategy. Financial intermediaries must have written outsourcing guidelines in place that have been approved by the governing body which is authorised to determine the financial intermediary's strategy, objectives and general policy and to scrutinise the decisions of the executive board. They shall review and update the written outsourcing guidelines regularly and ensure that they are being implemented. The outsourcing guidelines must cover the key life cycle phases of the outsourcing agreements and include definitions of the principles, responsibilities, role descriptions, tasks and processes associated with outsourcing arrangements. They must take account of the nature of the outsourcing arrangement (managed services, hosting, cloud, etc.). In addition, the outsourcing guidelines must define decisive criteria and factors for selecting and collaborating with a service provider. They must also specify whether or not service providers are permitted to sub-outsource important outsourced ICT services and/or ICT systems to subcontractors and, if so, under what conditions.

10.3 Important ICT services and/or ICT systems

82. Before entering into an outsourcing agreement with a service provider, financial intermediaries must check whether or not the outsourcing agreement involves important ICT services and/or ICT systems. When conducting this check, financial intermediaries must, if appropriate, consider whether or not the ICT services and/or ICT systems have the potential to become important in the future. Furthermore, financial intermediaries must conduct a further review of the ICT services and/or ICT systems that have already been outsourced to a service provider in the event of any significant changes to the nature, scope or complexity of the risks associated with the outsourcing agreement.

10.4 Risk assessment

83. Financial intermediaries must ensure that decisions relating to the outsourcing of ICT services and/or ICT systems to a service provider are taken on the basis of an in-depth risk assessment, which must also take account of all relevant risks arising in connection with the outsourcing agreement. The ICT and security risks arising in connection with outsourcing must be assessed as part of the ICT and information security risk management (see also Section 5.1 Organisation and objectives).

84. During the course of the risk assessment, financial intermediaries shall take account of the expected benefits and costs of the planned outsourcing agreement; this shall include weighing up any risks that may be reduced or better managed against the risks that may arise as a result of the planned outsourcing agreement.

85. When outsourcing important ICT services and/or ICT systems, financial intermediaries shall consider the following factors in the course of their risk assessment:

    a) The form of outsourcing (e.g. nature of the outsourcing, service model)
    b) The impact on business continuity management

c) concentration risks, if multiple ICT services and/or ICT systems are outsourced to a single service provider, or if a service provider is not easily replaceable
d) Risks associated with the process of migrating the data, as well as the ICT services and/or ICT systems
e) Risks associated with the sensitivity of the outsourced ICT services and/or ICT systems, the sensitivity of the data associated with them and the security measures that are therefore necessary
f) Risks relating to the country in which the service provider has its place of business, as well as in relation to countries in which the outsourced ICT services and/or ICT systems will be provided, and/or in which data will be stored or processed:
    i. Concerning the political and security situation
    ii. Concerning the applicable laws, including the data protection regulations
    iii. Concerning the applicable law enforcement regulations
    iv. Concerning the insolvency regulations that could be applied in the event that the service provider should suffer a failure, or concerning any restrictions that could affect, in particular, the urgent recovery of the service provider's data
    v. Concerning supervisory restrictions
g) Risks associated with sub-outsourcing (including risks resulting from long and complex outsourcing chains)

86. Financial intermediaries must ensure the implementation and effectiveness of the risk management measures defined in their risk management frameworks.

87. The risk assessment must be carried out before entering into an outsourcing agreement and then be subsequently reviewed on a regular basis. If financial intermediaries become aware of significant defects and/or significant changes to the provided services, or the situation of their service providers, the risk assessment must be reviewed without delay, or a new risk assessment must be carried out. If an outsourcing agreement is renewed but with modifications to its content and scope (e.g. expansion of its scope, or the incorporation into the agreement of important ICT services and/or ICT systems that were not previously included) a new risk assessment must be carried out.

10.5 Due diligence auditing

88. Financial intermediaries shall define a process for selecting and approving service providers in order to ensure that the service providers are suitable for providing the ICT services and/or ICT systems that they are planning to outsource (due diligence auditing).

89. By means of their due diligence auditing process, financial intermediaries shall ensure that service providers meet the criteria stipulated in their written outsourcing guidelines (see also Section 10.2 Outsourcing guidelines).

90. When outsourcing important ICT services and/or ICT systems, financial intermediaries shall ensure that service providers have the business reputation, appropriate and sufficient capabilities, specialist knowledge, capacities, resources (e.g. human, financial and IT resources), infrastructure, organisational structure and, if applicable, the necessary licences issued by, or registrations with, supervisory authorities, so as to provide the ICT services and/or ICT systems in a reliable and professional manner and thus comply with their obligations throughout the term of the outsourcing agreement. Service providers must guarantee to provide the services in a secure and durable manner; they must furthermore have an adequate ICT change management policy that conforms, by analogy, with Section 9 ICT projects and change management.

91. If the outsourcing includes the processing of personal or confidential data, financial intermediaries must satisfy themselves that service providers will either be unable to gain access to the data (e.g. by encrypting the data independently of the service provider) or by implementing adequate technical, personnel and organisational measures to protect the data. This applies in particular in cases where the service provider provides its services to multiple companies. The confidentiality of the data must be ensured not only vis-à-vis third parties but also between the different outsourcing client companies.

92. To support the findings of the due diligence audit, financial intermediaries may, where applicable, have recourse to certifications that are based on international standards, as well as audit reports prepared internally or by recognised third parties.

93. Due diligence audits in respect of service providers must be carried out prior to outsourcing the ICT services and/or ICT systems. If financial intermediaries should enter into a second agreement with a service provider that has already been audited, they shall apply a risk-based approach in order to determine whether or not a second due diligence audit is necessary.

94. If financial intermediaries should become aware of significant defects and/or significant changes in relation to the provided services or the situation of their service providers, the due diligence audit must be reviewed without delay, or a new due diligence audit must be carried out.

10.6 Conflicts of interest

95. Financial intermediaries shall identify, assess and manage any conflicts of interest that may arise in connection with their outsourcing agreements. Where outsourcing arrangements lead to significant conflicts of interest, including between entities forming part of the same group, financial intermediaries shall take appropriate measures to manage these conflicts of interest.

10.7 Register of outsourcing agreements

96. As part of their governance and risk management systems, financial intermediaries shall maintain a continuously updated register of their outsourcing agreements. Taking into account the statutory retention periods, financial intermediaries shall continue to retain in the register, for an appropriate period, those documents concerning terminated outsourcing agreements, including any accompanying documentation.

10.8 Outsourcing agreement

97. The rights and obligations of the financial intermediary and the rights and obligations of the service provider must be clearly allocated and recorded in a written agreement. Interfaces, responsibilities, liabilities and competencies of the financial intermediary and the service provider must be precisely defined and delineated, and governed by a contract. In particular, the terms must stipulate which technical and organisational security measures are being outsourced and how the financial intermediary is to monitor the effectiveness of the outsourced control measures.

10.9 Sub-outsourcing

98. The outsourcing agreement must specify whether or not sub-outsourcing of important ICT services and/or ICT systems is permissible. If sub-outsourcing is permitted, the relevant terms governing this must also be included in the outsourcing agreement. Furthermore, it must be contractually ensured that the outsourcing agreements between the service provider and its subcontractors will be consistent with the contractual arrangements under the primary outsourcing agreement.

99. If the service provider sub-outsources to a subcontractor, the service provider shall remain subject to its obligation to report to the outsourcing financial intermediary. If important ICT services and/or ICT systems are outsourced, the service provider must be placed under an obligation to monitor the ICT services and/or ICT systems that it is sub-outsourcing, so as to ensure that all contractual obligations between the service provider and the financial intermediary continue to be complied with.

100. If important ICT services and/or ICT systems are outsourced, the subcontractor must contractually agree to comply with all applicable laws and contractual obligations and shall grant the financial intermediary the same contractual access, information and auditing rights that were granted to it by the service provider.

10.10 Data security

101. Financial intermediaries shall ensure that service providers comply with appropriate ICT security standards.

102. As part of the planned outsourcing arrangement, financial intermediaries shall establish an appropriate level of protection to ensure the confidentiality of data, the availability of outsourced ICT services and/or ICT systems and data, as well as the integrity and retraceability of data and systems; this must conform to their information security guidelines (Section 6.1 Information security guidelines). Where necessary in order to protect data in transit, data in storage or data at rest, financial intermediaries shall also consider implementing special measures, such as the use of encryption technologies in combination with a suitable key management architecture.

103. To guarantee the confidentiality, availability and integrity of outsourced ICT services and ICT systems, financial intermediaries shall ensure that the outsourcing agreements (for both normal operation as well as in the event of disruptions (see also Section 11.2 Business continuity planning) entered into with service providers for the outsourcing of important ICT services and/or ICT systems cover the following:

    a. Appropriate and proportionate objectives and measures relating to information security, including requirements such as:
        i. Minimum cyber security requirements, taking into account, by analogy, the measures set out in Section 8.1 ICT operations security
        ii. Requirements for the financial intermediary's data lifecycle specifications
        iii. Data encryption requirements (at rest and in transit)
        iv. Requirements for procedures to monitor network security, for security monitoring processes, and for the location of data centres. Financial intermediaries shall ensure that service providers monitor the outsourced ICT services and ICT systems analogously in accordance with Section 6.2 ICT monitoring and information security.
        v. Requirements for procedures to ensure logical access controls/access protection and physical security measures. Financial intermediaries shall ensure that service providers protect the outsourced ICT services and ICT systems analogously in accordance with Section 7 User authorisation management through the use of logical and physical security procedures.
        vi. Requirements for information security monitoring procedures. Financial intermediaries shall ensure that service providers monitor the information security of the outsourced ICT services and ICT systems analogously in accordance with Section 6.3 Inspection, evaluation and testing of information security measures.
        vii. Requirements for training programmes. Financial intermediaries shall ensure that service providers train their employees analogously in accordance with Section 6.4 Training and awareness raising in relation to information security.

b. Processes for handling operational and security incidents analogously in accordance with Section 8.2 Management of ICT incidents and problems, including escalation and reporting to the financial intermediary. Financial intermediaries and service providers shall conduct joint testing of these processes on a periodic basis.
c. Backup and recovery procedures and procedures to facilitate testing of their effectiveness by the financial intermediary, analogously in accordance with Section 8 ICT operational management.

104. With the aid of contractually defined key performance indicators, financial intermediaries shall monitor compliance with these specifications and shall ascertain the service provider's level of compliance with the security objectives, measures and performance targets. Financial intermediaries shall contractually ensure that service providers are subject to an obligation to inform them of any developments that may compromise the proper execution of the outsourced activities and processes.

10.11 Data protection

105. In the case of outsourcing arrangements involving the handling or transmission of personal or confidential data, financial intermediaries shall apply a risk-based to selecting the data storage and data processing location(s) (i.e. country or region).

106. Financial intermediaries shall ensure that they comply with all of the requirements under the data protection laws that are applicable to them, including in respect of outsourced ICT services and/or ICT systems. When outsourcing abroad, appropriate technical and organisation measures shall be implemented to ensure compliance with the data protection requirements under the data protection laws that apply to them.

107. The financial intermediary must be aware of the data storage and data processing location(s), including the location of the relevant data centre(s).

10.12 Access, information and auditing rights

108. As part of the outsourcing agreement, the financial intermediary shall ensure, at least for important ICT services and/or ICT systems, that the service provider grants the financial intermediary, its internal and external auditors, and the FMA, the access, information and auditing rights necessary for monitoring the outsourcing agreement and to comply with all of the applicable supervisory requirements. The foregoing shall be deemed subject to any more extensive statutory requirements that may be applicable to financial intermediaries. Financial intermediaries must ensure the above, even if the important ICT services and/or ICT systems are outsourced to a service provider that is domiciled abroad, or if they are provided abroad as a result of the outsourcing arrangement.

109. When outsourcing important ICT services and/or systems, financial intermediaries shall ensure that neither the outsourcing agreement nor any other contractual provisions prevent or restrict the access, information and audit rights from being effectively exercised by the financial intermediary, its internal or external auditors, or the FMA.

110. In the event of any sub-outsourcing of important ICT services and/or ICT systems, financial intermediaries shall ensure that they, or their internal or external auditors, or the FMA, are also able to exercise the access, information and audit rights against the subcontractors.

111. When outsourcing important ICT services and/or systems, financial intermediaries may have recourse to conveniences such as the use of third-party certifications, internal or external audit reports and collective audits, providing that this is permitted under the supervisory requirements to which they are subject.

112. Financial intermediaries shall ensure that the outsourcing agreement makes provision for the internal auditor to audit the outsourced ICT services and/or ICT systems using a risk-based approach.

10.13 Monitoring

113. Using a risk-based approach, financial intermediaries shall regularly monitor their service providers' execution of the activities, implementation of the security measures, and their compliance with the agreed service quality. Financial intermediaries shall apply procedures to monitor compliance with the security control measures that have been outsourced to the service provider.

114. The management body must be updated regularly on the latest situation with respect to the risks identified in connection with the outsourcing of important ICT services and/or ICT systems. The financial intermediary's internal procedures must ensure appropriate internal reporting in relation to the outsourcing and sub-outsourcing of ICT services and/or ICT systems.

115. For monitoring purposes, the financial intermediary shall establish monitoring and control mechanisms which take into account the fact that important ICT services and/or ICT systems, or parts thereof, have been outsourced. The monitoring and control mechanisms shall include indicators for events that could trigger activation of the exit strategy. If any deficiencies are identified, the financial intermediary shall take appropriate corrective action or implement appropriate workaround measures.

116. Financial intermediaries shall agree rights of instruction in the outsourcing agreement which ensure that all required instructions necessary for the performance of the agreed service can be issued, in order that the financial intermediary has the possibility to exert influence and control over the outsourced ICT services and/or ICT systems.

10.14 Business continuity for outsourced ICT services and/or systems

117. Financial intermediaries shall, analogously in accordance with Section 11 Disaster recovery plan and business continuity management, prepare, maintain, and regularly test appropriate business continuity plans in respect of important outsourced ICT services and/or ICT systems. In doing so, they shall take into account scenarios such as a deterioration in the quality of provision of the important outsourced ICT services and/or ICT systems to an unacceptable level, or a failure to provide them, or the potential impact that would result from the insolvency or another type of failure of the service provider, and, if applicable, any political risks in the service provider's jurisdiction.

10.15 Exit strategies

118. When outsourcing important ICT services and/or ICT systems, financial intermediaries must have a documented exit strategy that is consistent with their outsourcing guidelines and business continuity plans and which has been subjected to a feasibility verification.

119. As a minimum, the exit strategy must take into account the following possibilities:

a. Termination of the outsourcing agreement (ordinarily or without notice)
b. A failure of the service provider
c. A deterioration in the quality of the provided service, and actual or potential operational disruptions due to inadequate provision of the service or a failure to provide the service
d. The emergence of major risks relating to the appropriate and continuous application of the service

120. Financial intermediaries shall agree a clearly formulated clause in the outsourcing agreement that enables them to terminate the outsourcing agreement and which specifies reasonable notice periods. As a general rule, it must be possible to terminate the outsourcing of important ICT services and/or ICT systems without adversely affecting the continuity and quality of the services provided by the financial intermediary to its clients.

121. Financial intermediaries must ensure, bearing in mind any system and data-format compatibility issues, that it is possible to bring outsourced important ICT services and/or ICT systems back in house. Financial intermediaries must also ensure that service providers will provide them with appropriate assistance during the transfer of outsourced important ICT services and/or ICT systems, data or applications to either a different service provider or directly to the financial intermediary, and that the service provider will erase the financial intermediary's data fully and securely following the (re-)transfer.

11. Disaster recovery plan and business continuity management

122. Financial intermediaries shall establish a business continuity management (BCM) system in order to maximise their ability to continuously provide the services and limit losses in the event of severe operational disruptions.

123. The BCM procedures shall be adequately taken into account in the audit plan for the internal audit.

11.1 Business impact analysis (BIA)

124. As part of the BCM system, financial intermediaries shall carry out business impact analyses (BIAs), in which they quantitatively and qualitatively analyse their exposure to severe business disruptions, and evaluate the potential impact (including in relation to confidentiality, integrity and availability) using internal and/or external data (e.g. data made available by the service provider that is relevant for a business process, or publicly accessible data that may be relevant for the purposes of the BIA) as well as scenario analyses. The financial intermediary shall ensure that the scenario analyses cover all of the business areas, internal units and processes, as well as the outsourcing arrangements. The BIA must also take into account the criticality of the identified and classified business functions, support processes, third parties and ICT assets, as well as their interdependencies according to Section 5.3 Criticality grading and risk assessment.

125. The financial intermediary must ensure that the BIA is carried out appropriately and regularly. The financial intermediary shall also define the criteria for conducting ad hoc BIAs outside of the normal update cycle.

126. Financial intermediaries shall ensure that their ICT systems and ICT services are designed and aligned to the BIA in such manner that, by way of example, specified critical components (see also Section 5.3 Criticality grading and risk assessment) are redundantly laid out in order to prevent disruptions occurring due to incidents that impact upon these components.

11.2 Business continuity planning (BCP)

127. On the basis of their BIA, financial intermediaries shall prepare plans to guarantee their business continuity (business continuity plans, “BCPs”), which must be documented and approved by the management body. These plans must take into account, in particular, risks that could adversely affect continuation of the business activities. The plans support the protection and, where necessary, recovery of the confidentiality, integrity and availability of their business functions, support processes and ICT assets. When preparing these plans, financial intermediaries shall coordinate, were necessary, with relevant internal and external stakeholders.

128. Financial intermediaries shall establish BCPs in order to ensure that they are able to respond appropriately to potential failure scenarios, and that they have the capability, following a disruption, to restore their critical business activities to an operational state within a prescribed recovery time (recovery time objectives, “RTO”, the maximum time within which a system or process must be restored after an incident) and to a prescribed recovery point (recovery point objective, “RPO”, the maximum time period within which a data loss is acceptable in the event of an incident). The RTO and RPO must also be agreed with service providers in respect of outsourced important ICT services and/or systems. In cases of severe operational disruptions that trigger specified BCPs, financial intermediaries shall prioritise measures to maintain the business operations using a risk-based approach that draws upon the risk assessment referred to in Section 5.3 Criticality grading and risk assessment.

129. The financial intermediary’s BCP shall take into account a range of different scenarios, including any extreme but plausible scenarios to which they may be exposed, as well as scenarios involving cyberattacks. They must also assess the possible impact of such scenarios. On the basis of these scenarios, the financial intermediary shall specify how it will ensure the continuity of its ICT systems and ICT services and the security of its information.

130. The financial intermediary shall provide its employees with training on the disaster recovery plans.

11.3 Response and recovery plans

131. Financial intermediaries shall develop response and recovery plans on the basis of the BIAs and plausible scenarios. These plans must specify the conditions under which the plans can be activated and the measures that are to be taken in order to ensure the availability, continuity and recovery of, as a minimum, the financial intermediary’s critical ICT systems and services. The response and recovery plans must be designed to achieve the financial intermediary’s recovery targets.

132. The response and recovery plans shall include both short-term and long-term recovery options. The plans:

a) Concentrate on restoring critical business functions, support processes, ICT assets and their interdependencies to an operational state, in order to avoid adverse effects on the functionality of the financial intermediary’s operations and the financial system
b) Shall be documented and made available to the business and support units and must be easily accessible in the event of an emergency
c) Shall be updated to reflect knowledge gained from incidents, tests, newly identified risks and threats, as well as changed recovery targets and priorities

133. The plans must also allow for alternative options in cases where a recovery may not be possible in the sort-term due to costs, risks, logistics or unforeseen circumstances.

134. As part of their response and recovery plans, financial intermediaries shall also consider and establish continuity measures to minimise the impact in the event that any of their service providers that are of critical importance to the continuity of their ICT services should suffer a failure.

11.4 Testing of plans

135. Financial intermediaries shall test their BCPs regularly. In particular, they must ensure that the BCPs for their critical business functions, support processes, ICT assets and their interdependencies (including, where applicable, those provided by third parties) are tested on a regular and, if necessary, incremental basis.

136. The BCPs must be updated at least once per year on the basis of the test results, the current threat intelligence and lessons learnt from past events. The departments and employees concerned shall be informed of the update. Where relevant, any changes to the recovery targets (including RTOs and RPOs) and/or changes to the business functions, support processes and ICT assets shall also be taken as a basis for updating the BCPs.

137. The BCP testing carried out by the financial intermediaries must demonstrate that they have the capability to maintain the functionality of their business operations until the critical operations are restored. In particular:

a) They must test an appropriate range of severe but plausible scenarios, including those taken into account during development of the BCPs (including, where applicable, testing of systems provided by third parties); this includes migrating critical business functions, support processes and ICT assets to the disaster recovery environment and demonstrating that they can be run and executed in this manner for a period of time that adequately reflects typical recovery times, after which normal functioning can then be restored.
b) They must be designed to challenge the assumptions on which the BCPs are based, including the governance regulations and the crisis communications plans.
c) They must include procedures for testing the ability of their employees, contractors, service providers, ICT systems and ICT services to respond appropriately to the defined scenarios.

138. The test results shall be documented and all deficiencies identified during the tests must be analysed, addressed and reported to the management body.

11.5 Crisis communication

139. In the event of a disruption or emergency situation, and during implementation of the BCPs, financial intermediaries shall ensure that they have appropriate and effective crisis communications measures in place so that all relevant internal and external stakeholders, including the competent authorities – if provided for under national regulations – and relevant service providers, are kept promptly and appropriately informed.

140. Furthermore, the FMA expects financial intermediaries to inform the FMA of severe cyberattacks, or cyberattacks that disrupt business operations, within seven (7) days of becoming aware of them.

12. Data protection

The FMA processes personal data exclusively in accordance with the general data processing principles of the General Data Protection Regulation (Regulation (EU) No. 2016/679 of the European Parliament and of

the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) and in line with applicable data protection law.

All information regarding the processing of personal data, including details about the purpose of processing, the data controller and the rights of data subjects can be found in the FMA Privacy Policy, accessible at: www.fma-li.li/en/fma/data-protection/fma-privacy-policy.html

13. Entry into force

These Guidelines were approved by the FMA Executive Board on 19 May 2021 and shall enter into force on 1 January 2022.

Please contact the FMA for further information.
Telephone: +423 236 73 73
E-Mail: info@fma-li.li