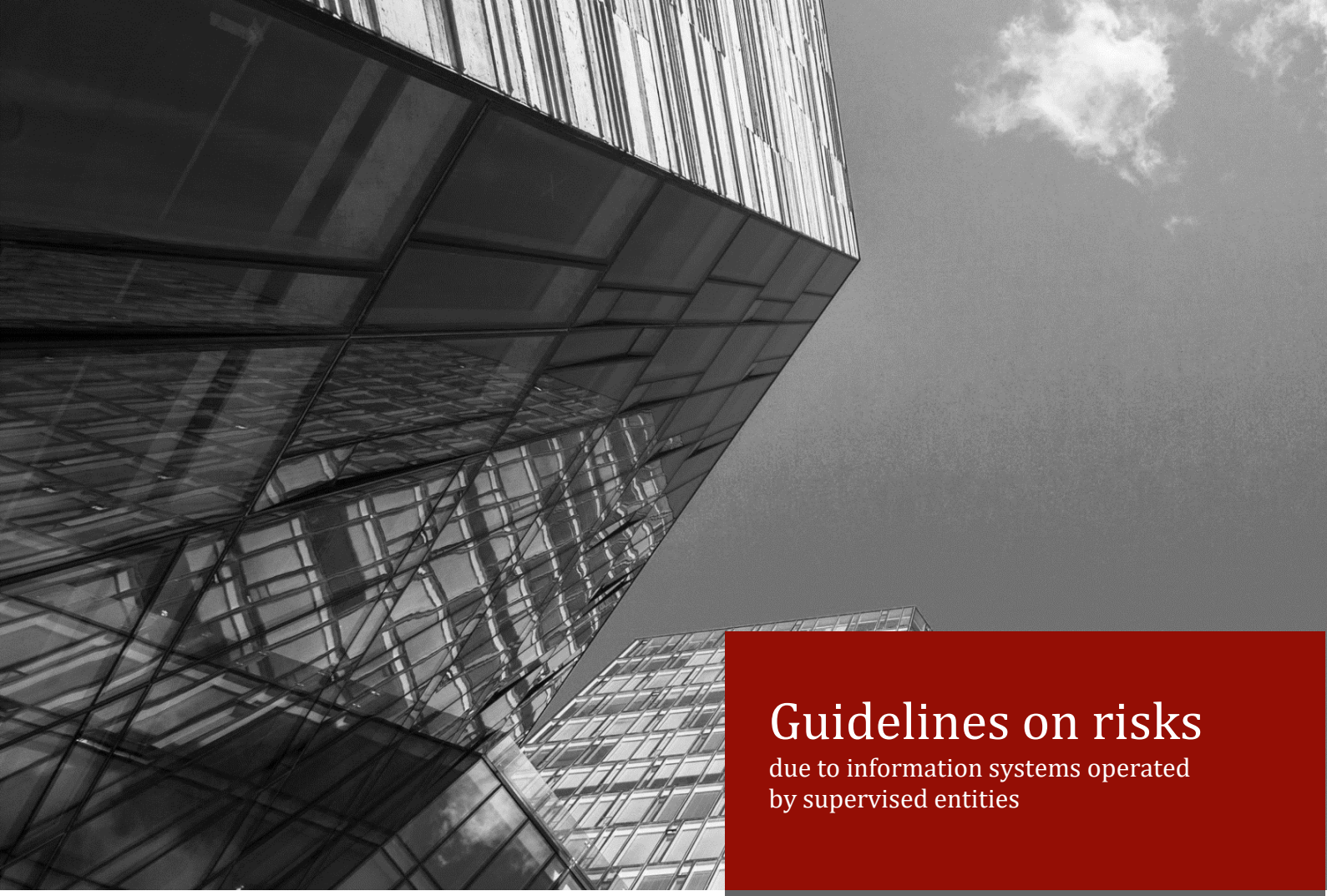

Guidelines on risks

due to information systems operated by supervised entities

No. 1/2019

This is a translation of the authoritative Icelandic text. In the event of any discrepancies between the translation and the original Icelandic text, the original text shall prevail.

This document is issued in accordance with Article 8, Paragraph 2 of the Act on the Official Supervision of Financial Activities, no. 87/1998.

11 March 2019

FJÁRMÁLAEFTIRLITIÐ
THE FINANCIAL SUPERVISORY AUTHORITY, ICELAND

Table of Contents

Introduction

The Financial Supervisory Authority supervises the work practices of supervised entities on the basis of the Act on Official Supervision of Financial Activities, no. 87/1998, and special legislation applying to their activities. An element in such supervision is ensuring that supervised entities monitor the risk stemming from information system operations and minimise it insofar as is possible.

These Guidelines are intended to present and harmonise the criteria used to assess supervised entities' compliance with the provisions of the law and Governmental directives pertaining to operational risk, with emphasis on operation of information systems and use of information and communications technology (commonly referred to as IT or ICT) in this context. It should be noted that the Guidelines are not intended to replace the provisions of the law and Governmental directives pertaining to personal data protection, cybersecurity, or other aspects of information system operations.

Minimisation of risk in the operation of information systems entails, among other things, adopting measures aimed at managing operational risk. It is also necessary to guarantee that information is secure; i.e., by ensuring that access is limited to authorised parties on an as-needed basis and that the information is correct and has not been tampered with.

The scope of measures to safeguard the security of information systems must be commensurate with the scope of the supervised entity's operations and the risks associated with them. Because of this, the Financial Supervisory Authority makes more stringent follow-up requirements of supervised entities with extensive and complex operations than it makes of smaller entities with simple operations; cf. Points 51-53 of the Guidelines.

These Guidelines contain criteria further explaining the requirements provided for in statutory and regulatory instruments concerning operational risk, with emphasis on operation of information systems. The Financial Supervisory Authority uses the criteria as a basis for its evaluation of compliance with statutory and regulatory instruments, including sound and appropriate business practices. If the Financial Supervisory Authority concludes that a violation of laws or rules has taken place, the Authority demands remedial action; cf. Article 10, Paragraph 1 of Act no. 87/1998, and assesses whether there is reason to take other measures in response to the violation.

1. Scope

1. These Guidelines apply to all supervised entities according to Article 2 of the Act on Official Supervision of Financial Activities, no. 87/1998.
2. These Guidelines apply to those information systems[1] that are operated by supervised entities and are important to or have an impact on the entities' activities.
3. When a supervised entity is part of a conglomeration, the Guidelines apply to the operation of the information systems of companies in the conglomeration together with the supervised entity, if those systems are important to or have an impact on the supervised entity's activities.

2. Management and responsibility[2]

4. The board of the supervised entity is responsible for ensuring that the entity's information system operations meet the criteria laid down in these Guidelines.[3] The board of the supervised entity is required to adopt appropriate measures to ensure that all information systems, cf. Point 2, that are relevant to or have an impact on the supervised entity's activities are operated in accordance with the Guidelines.
5. The responsibilities of the board according to Point 4 apply irrespective of whether information system operations are outsourced, either wholly or in part. Responsibility for information system operations and management of risks associated with outsourcing always rests with the board of the supervised entity and cannot be outsourced. In executing the partial or complete outsourcing of information system operations, the board must conduct monitoring to ensure that the criteria laid down in Section 3 of these Guidelines, on *Outsourcing*, are satisfied in full.
6. The board of the supervised entity is responsible for ensuring that a contingency framework is in place; cf. Section 2.3 on *Contingency framework* in these Guidelines.

[1] The term *information systems* refers to those digital systems that are involved in information processing, together with all connections to, from, and between them.

[2] In assessing compliance with Points 4-9 in these Guidelines, consideration will be given, among other things, to the criteria presented by the European Banking Authority (EBA/GL/2017/05) in its Guidelines on ICT Risk Assessment (referred to hereinafter as the EBA Guidelines). For further information, see: https://www.eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-on-ict-risk-assessment-under-the-srep. Points 20-34 therein will be used for guidance and will be adapted for supervised entities, in accordance with their activities.

[3] Such responsibility follows from various provisions of special legislation on the financial market: cf. Article 17, Article 54, Paragraph 1 and Article 78(g) of the Act on Financial Undertakings, no. 161/2002; cf. also Article 6 of the Act on Securities Transactions, no. 108/2007; cf. Article 38, Article 39, and Article 44, Paragraph 5 of the Act on Insurance Activities, no. 100/2016; cf. also Articles 4-6 of the Regulation on Insurance Activities, no. 585/2017; cf. Article 29, Paragraph 1 and Article 36(e) of the Act on Mandatory Insurance of Pension Rights and on Activities of Pension Funds, no. 129/1997; cf. also Article 3 and Article 6, Paragraph 2 of the Regulation on Risk Monitoring Systems for Pension Funds, no. 590/2017; cf. Article 10, Paragraph 2, Items 2-5 and Article 11 of the Act on Stock Exchanges, no. 110/2007; cf. Article 13 of the Act on Electronic Registration of Title to Securities, no. 131/1997; and cf. Article 17, Paragraph 1, Item 3 of the Act on Mutual Funds, Investment Funds, and Institutional Investment Funds, no. 128/2011; cf. also Articles 8 and 11 of the Regulation on Organisational Requirements for Investment Fund Management Companies (including on conflicts of interests, business conduct, risk management, and the substance of agreements between custodians and fund management companies), no. 471/2014.

7. It is important that the board of the supervised entity ensure that information system operations including maintenance are stable and consistent with policies and, where applicable, with timetables, and that they follow documented procedures; cf. Point 9. The board is required to ensure that adequate inputs are on hand, such as equipment and personnel, including the necessary knowledge and skills.

2.1 Policies and procedures[4]

8. The board of the supervised entity formulates policy or, as applicable, policies, which specify, among other things, the objectives and security requirements for information system operations. Such policy or, as applicable, policies must cover outsourcing; i.e., which elements of information system operations may be outsourced and to whom they may be outsourced.
9. In order to minimise operational risk, supervised entities need to have documented protocols that are used as a basis for information system operations, including procedures laid down in writing.[5] An element in such protocols is the maintenance of a daily log on, among other things, the grant of access to systems and changes to access. The procedures must take into consideration the criteria set forth in these Guidelines as regards:
    - Risk analysis and risk assessment; cf. Section 2.2
    - Contingency framework, cf. Section 2.3[6]
    - Change management, cf. Section 2.4[7]
    - Outsourcing and cloud services; cf. Section 3[8]
    - Security matters, including training and education; cf. Section 4
    - Notifications and documentation of incidents, cf. Section 5.1.

[4] As regards the role of the board, formulation of policy for information system operations, preparation of documented procedures, and regulated entities' obligations relating to operational risk, reference is made to the same statutory provisions as those relating to Point 4 of these Guidelines.
[5] Supervised entities' procedures must state clearly who is responsible for individual activities. The documentation of the procedure must also be dated for traceability purposes, and its text must be clear.
[6] In assessing compliance with Section 2.3 (*Contingency framework)* and Section 4 (*Security)* of these Guidelines, consideration will be given, among other things, to the criteria set forth by the European Banking Authority in the aforementioned EBA Guidelines for ICT Risk Assessment. The criteria listed on pages 25-27 and 29 in the EBA Guidelines will be examined.
[7] In assessing compliance with Section 2.4 (*Change management*) of these Guidelines, consideration will be given, among other things, to the criteria set forth in the EBA Guidelines for ICT Risk Assessment. The criteria listed on pages 28-29 in the EBA Guidelines will be examined.
[8] In assessing compliance with Section 3 (*Outsourcing and cloud services*) of these Guidelines, consideration will be given, among other things, to the criteria set forth in the EBA Guidelines for ICT Risk Assessment. The criteria listed on pages 29-30 of the EBA Guidelines will be examined.

2.2 Risk analysis and risk assessment[9]

10. As part of analysing and assessing operational risk, supervised entities must analyse and assess risk due to information systems. As a result, they must have procedures in place for monitoring the risk and minimising the probability that it will materialise.

11. The board of the supervised entity determines the limits of acceptable information technology-related risk based on the entity's operations and the scope of its activities. The risk limits must be reviewed on a regular basis.

12. The board of the supervised entity shall ensure that risks associated with the use of information technology in the entity's operations is assessed at least once a year, and more often if changes occur that affect information security. The assessment shall be prepared so as to ensure that risk is within the limits set by the board in accordance with Point 11. The execution and results of the risk assessment shall be documented, together with: i) recommended remedial action, where needed; and ii) follow-up on remedial action as laid down in Point 13.

13. Following the risk assessment, the supervised entity must define clearly the actions that must be taken to address the risk that has been identified. It must be ensured that responsibility for the remedial actions is clear and that the actions are followed up.

2.3 Contingency framework

14. As part of ameliorating or minimising operational risk, supervised entities are required to plan for potential shocks that could compromise the performance capacity of their information systems. To this end, the boards of supervised entities must also adopt a comprehensive contingency framework in which roles, responsibilities, tasks, and risk factors are defined, in order to respond to such shocks.

15. On the basis of the risk assessment, cf. Section 2.2, the supervised entity must determine which information systems are important for its operations. The contingency framework is intended to cover all important information systems.

16. The framework must include the following measures, among others:

    - Responses to those elements that, according to the risk assessment, could fail, and actions that must be taken;
    - Information for the board, employees, customers, and other parties that need to know of a stoppage of operations;
    - Clear criteria on when alternative solutions shall be activated;
    - Recovery processes.

17. The framework must be reviewed and updated annually; cf., however, Point 53.

[9] In assessing compliance with Section 2.2 of these Guidelines, consideration will be given, among other things, to the criteria set forth in the EBA Guidelines for ICT Risk Assessment. Points 35-62 therein will be used for guidance and will be adapted for supervised entities, in accordance with their activities.

2.3.1 Business continuity plan

18. Supervised entities that are required to have in place a business continuity plan or other comparable plan[10] shall document their responses to shocks that could lead to a stoppage of information system operations.
19. The plan shall be deemed by the Financial Supervisory Authority to cover the following points, among others:
    - An overview of the information systems covered by the plan;
    - A description of the responses to various shock scenarios;
    - Clear criteria for the activation of shock response measures;
    - Acceptable time limits for operational stoppages before shock response measures are activated;
    - Procedures for re-launching information systems;
    - An overview of areas of responsibility and activation procedures for shock response measures;
    - Information disclosure to the board, employees, suppliers, customers, public authorities, and the media.
20. It is important that the plan be followed up, as applicable, with training, exercises, and testing of alternative solutions so as to ensure that they function as intended. Furthermore, testing and test results should be documented so that execution and performance can be assessed.

2.4 Change management

21. The party (or, if applicable, parties) authorised to take important decisions about information system operations should give their consent for changes and/or implementation of changes to the information systems concerned before the changes are executed.
22. The supervised entity must have written procedures, cf. Point 9, for procurement, development, implementation, maintenance, and testing of information systems. The procedures should cover risks related to development, testing, and the approval process for changes to information systems, including development of or modifications to software before it is brought into use.
23. The procedures described in Point 22 must provide for the separation of the development and testing environment from the actual operating environment. Furthermore, such procedures must document the grant and revocation of authorised access to the computer environments that contain actual data if the data are used for development or testing.
24. Records must be kept of all incidents that occur when systems are brought into use or changes are made to the actual operating environment; cf. Points 46 and 47.

[10] Cf. Article 78(g), Paragraph 2 of the Act on Financial Undertakings, no. 161/2002, and Article 39, Paragraph 5 of the Act on Insurance Activities, no. 100/2016.

3. Outsourcing[11]

25. If a third party[12] is engaged to carry out tasks relating to a supervised entity's information systems, it must be ensured that this third party is informed of the substance of these Guidelines and follows them as a representative of the supervised entity. Outsourcing[13] in connection with information systems should always be carried out on the basis of a written contract between the supervised entity and the third party, or on the basis of a comparable arrangement that ensures that communications between the parties are documented and that the tasks entrusted to the external contractor are described.

26. In order to minimise the supervised entity's operational risk, the written contract with the external contractor, or the comparable arrangement provided for in Point 25, shall include the following provisions:

    - Provisions specifying which services the external contractor shall provide.
    - Provisions authorising the supervised entity to supervise the activities falling under the scope of the contract, including access by the supervised entity's external and internal auditors.
    - Provisions obliging the external contractor and its employees to observe confidentiality provisions comparable to those governing the supervised entity.
    - Provisions authorising the Financial Supervisory Authority to access data and information owned by the supervised entity and in the contractor's possession.
    - Provisions authorising the Financial Supervisory Authority to conduct on-site inspections of the external contractor's premises if the Authority considers such inspections necessary for its supervision of the supervised entity.
    - Provisions on whether chain outsourcing is authorised and, if so, to what extent, and what limitations the supervised entity imposes on chain outsourcing by the external contractor.
    - Provisions on how these Guidelines shall be followed, including storage and handling of data and notifications of incidents.
    - Provisions on regular reviews of the contract. Reviews in this context should take place at least every two years; cf., however, Point 53.
    - Provisions on an exit strategy for the supervised entity.

[11] Supervised entities' obligations in connection with outsourcing follow from the provisions on operational risk and outsourcing in special financial market legislation: cf. Article 54, Paragraph 1 and Article 78(g) of the Act on Financial Undertakings, no. 161/2002; cf. also Article 7 of the Act on Securities Transactions, no. 108/2007; cf. Articles 33 and 49 of the Act on Insurance Activities, no. 100/2016; cf. also Article 21 of the Regulation on Insurance Activities, no. 585/2017; cf. Article 39(a) of the Act on Mandatory Insurance of Pension Rights and on Activities of Pension Funds, no. 129/1997; cf. also Article 4 of the Regulation on Risk Monitoring Systems for Pension Funds, no. 590/2017; cf. Article 10, Paragraph 2, Items 2-5 of the Act on Stock Exchanges, no. 110/2007; cf. Article 13 of the Act on Electronic Registration of Title to Securities, no. 131/1997; and cf. Article 18 of the Act on Mutual Funds, Investment Funds, and Institutional Investment Funds, no. 128/2011.

[12] The term *third party* refers to a party that carries out outsourced work and is not an employee of the supervised entity.

[13] The term *outsourcing* refers to an arrangement between a supervised entity and a service provider, where the service provider carries out or executes, wholly or in part, tasks, services, or actions that would otherwise be carried out by the supervised entity concerned.

27. It is important that the service contract with the external contractor specify a representative from the supervised entity who is responsible for ensuring that the provisions of Point 26 are satisfied. Furthermore, the responsible party ensures that the external contractor satisfies the requirements made of it in the service contract and assesses the risk associated with the outsourcing. The Financial Supervisory Authority is of the opinion that it is desirable to designate the responsible party by title or position within the supervised entity; i.e., that the responsible party not be a named individual.
28. If data hosting is outsourced, the supervised entity must ensure that the Financial Supervisory Authority can obtain data and information from the third party in the same way as it would if it were seeking data from the supervised entity itself.
29. The Financial Supervisory Authority requires that it be informed in advance of outsourcing arrangements, irrespective of whether the third party is established in Iceland or abroad, and of where the Authority may obtain data if the need arises. In this context, necessary information includes, for instance, information on the external contractor, the contractor's address and venue, where the data will be stored, information on the contractor's contact personnel, and a confirmation that the contractor is aware that the Financial Supervisory Authority is authorised to have access to the data in question; cf. Point 31.
30. With reference to the objectives laid down in Article 9, Paragraph 1 of the Act on Official Supervision of Financial Activities, no. 87/1998, cf. also the discussion in Point 35, the Financial Supervisory Authority considers it preferable that supervised entities do not chain outsource the hosting of information systems and data, either wholly or in part, further than to a fourth party.[14] The Financial Supervisory Authority instructs supervised entities to avoid, in general, chain outsourcing to parties outside the European Economic Area, and then only if the statutory environment in the country to which the function is chain outsourced does not prevent the Financial Supervisory Authority from having access to the data.

3.1 Cloud services[15]

31. Supervised entities that intend to implement cloud solutions must assess whether the outsourcing complies with the criteria laid down in these Guidelines, with reference to the requirements specified in the law and Governmental directives concerning operational risk. Such an assessment entails, among other things, completing a checklist[16] and returning it to the Financial Supervisory Authority no later than thirty (30) days before the cloud solution is to be brought into use.

[14] Chain outsourcing to a fourth party refers to outsourcing by the supervised entity to a third party, which then outsources to another party, referred to as the fourth party. The Financial Supervisory Authority does not object to such outsourcing but is of the opinion that the chain should not extend to fifth parties or more. Outsourcing within the same conglomeration is not considered chain outsourcing.

[15] In assessing compliance with Section 3.1 in these Guidelines, consideration will be given, among other things, to the criteria set by the EBA in its Recommendation on the use of cloud services. For further information, see: https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers. The EBA Recommendation will be used for guidance and will be adapted for supervised entities, in accordance with their activities.

[16] The checklist can be found on the Financial Supervisory Authority website. For further information, see: https://www.fme.is/media/leidbeiningar/Gatlisti-vegna-innleidingar-skyjalausna.pdf.

32. The supervised entity must assess the risk associated with the cloud solution, including with reference to the checklist according to Point 31. Furthermore, the supervised entity must ensure that satisfactory security measures are in place in connection with the outsourcing.

4. Security

33. In order to ensure security in information system operations, the Financial Supervisory Authority is of the view that the supervised entity should introduce and maintain documented procedures, cf. Point 9, with the aim of protecting information, documents, data, and data media[17] from unauthorised disclosure, alteration, and destruction. Documented protocols shall be used as a foundation for security defences. Furthermore, there shall be documented protocols for allocation, review, and revocation of authorised access to supervised entities' systems.

4.1 Data storage and handling

34. The procedures according to Point 33 shall specify that users of supervised entities' information systems cannot delete documents, entries, messages, or communications histories from the information systems concerned during the period of time specified in Point 36.

35. According to Article 9, Paragraph 1 of the Act on Official Supervision of Financial Activities, no. 87/1998, supervised entities must grant the Financial Supervisory Authority access to all of their accounts, minutes, documents and other data that are in their possession, that pertain to their activities, and that the Financial Supervisory Authority considers necessary. In order for the objective of this provision to be achieved, it is important that the data the Authority may request be available immediately when a request is made for access to them or to information contained therein. As a result, and considering the main purpose of these Guidelines as regards minimising operational risk, the Financial Supervisory Authority is of the view that supervised entities' data storage and handling should include taking backup copies of data and information systems.[18] Copies are necessary so that the Financial Supervisory Authority can recreate each important step in specific transaction processes. Such recreations are an important element in the Authority's supervisory role, according to both Article 8, Paragraph 1 of the Act on Official Supervision of Financial Activities, no. 87/1998, and the supervision provisions found in certain special legislation.

36. Security backups must satisfy the following requirements:

[17] Data media include, for instance, smartphones, tablets, laptops, tape recordings, magnetic disks, memory keys, memory cards, external hard drives, compact discs, digital video disks, built-in memory units in tech equipment, and other comparable items.

[18] Such systems include all of the supervised entity's information systems that contain records and data pertaining to business information and/or transaction orders, irrespective of whether they are stored at the supervised entity itself or outsourced. This refers to all information and communications systems relating to business transactions; i.e., e-mail, telephone systems, mobile phones, fax machines, messaging systems, or other types of communications systems, as well as other systems that may contain data pertaining to transaction orders.

- The arrangements and protocols for the copying process must be well organised, in the Financial Supervisory Authority's opinion, and must entail active monitoring to ensure that copying is carried out in accordance with documented procedures. The protocols should specify, among other things, the storage period for backup copies, the storage location, and the equipment needed to recover them.
- Backup copies of information systems that contain business information[19] must be available for at least two (2) years from the original data entry date.
- Backup copies of information systems that contain transaction orders[20] must be available for at least five (5) years from the original data entry date.
- Copies of accounting systems shall be available for at least seven (7) years from the original data entry date, pursuant to Articles 19 and 20 of the Accounting Act, no. 145/1994, including the equipment and systems needed to recover the data.
- Copies must be available to supervisory bodies at short notice, and specified data must be readily accessible.

37. In order to ensure the security and credibility of the business information and transaction orders stored in security backups, it is important that:
    - Copies that are taken contain all trading system entries, documents, telephone logs, e-mails, messages, or comparable data in a continuous and traceable time series, provided that the data contain business information and/or transaction orders.
    - The copies and the information contained in them must be protected so as to make it impossible to delete them or alter them in error in any way. Furthermore, backup copies and backup equipment must be protected satisfactorily against the risk of mistreatment and risks in the environment.
    - Access to backup copies should be restricted insofar as is possible.
    - It should be ensured that backup copies remain legible until the end of the storage period.

4.2 Cybersecurity

38. In carrying out the risk assessment described in Section 2.2 and in connection with the contingency framework according to Section 2.3, supervised entities must give particular consideration to cybersecurity so as to minimise losses due to cyberattacks.
39. It is important that supervised entities protect systems and information against cyberthreats and fraud – such as unauthorised access, data theft, viruses, and malicious code – with appropriate monitoring, cyberdefences, and security training (see Point 40).

[19] The term *business information* refers to all information and data on customers and their position vis-à-vis the supervised entity concerned.
[20] The term *transaction orders* refers to communications that entail binding decisions between parties, such as instructions to carry out certain trades, confirmation of contracts, etc.

4.3 Security training and education

40. Supervised entities must bolster and maintain employees' knowledge of best practice in connection with information security and responses to imminent threats. An element in this is to increase employees' knowledge of cyberattacks and attempted fraud. Risks of this type could be directed at supervised entities via such channels as e-mail, communications media, and text messages.

41. It is important to have in place a security training plan (including cyber security training), present it regularly, and update it systematically. Holding contingency exercises is an important element in supervised entities' security training and education; cf. Section 2.3.

5. Internal monitoring and incidents

42. Supervised entities are required, cf. Points 4, 8, and 10, to maintain active internal monitoring that includes checks on compliance with the criteria laid down in these Guidelines. Carrying out checks on compliance with the criteria in Point 43 is one element in such internal monitoring, and furthermore, incidents must be handled and reported to the Financial Supervisory Authority as is provided for in Section 5.2.

5.1 Checks on compliance with the Guidelines

43. The Financial Supervisory Authority directs supervised entities to entrust internal auditor or an impartial party with conducting a check on compliance with these Guidelines. It is important that the appraiser execute the process in an organised and systematic way, following generally acknowledged and accepted methods.

44. The compliance check according to Point 43 shall be conducted annually; cf., however, Point 53.

45. With reference to Article 9, Paragraph 1, of the Act on Official Supervision of Financial Activities, no. 87/1998, the Financial supervisory Authority requires that the execution and outcome of the compliance check according to Point 43, together with recommendations for improvements where necessary, be documented and submitted to the Authority annually, in accordance with instructions, via the Authority's service portal.

5.2 Incident notifications and progress reports[21]

46. Supervised entities must have in place written procedures for the handling of incidents occurring in information system operations, including notifications of incidents to the

[21] In connection with incident notifications and progress reports, the Financial Supervisory Authority will rely on a new classification of incidents so as to harmonise with the EBA Recommendations (EBA/REC/2017/03) concerning incident reporting. For further information, see: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incident-reporting-under-psd2. The EBA Recommendation will be used for guidance and will be adapted for supervised entities, in accordance with their activities.

Financial Supervisory Authority; cf. Points 48 and 49. Incidents shall be handled[22] by determining their cause, returning operations to normal, and preventing incidents from reoccurring.

47. It is important that supervised entities maintain electronic incident records and that incidents be traceable and measurable.

48. The Financial Supervisory Authority requires that all incidents occurring in information system operations be reported to the Authority as soon as possible, and no later than four (4) hours after the incident is discovered. Incident reports must be submitted, in accordance with the instructions accompanying the appropriate forms, via the Financial Supervisory Authority's service portal. The scope of the incident report is determined by the activities of the supervised entity concerned.

49. Supervised entities must submit progress reports in connection with incidents as described in Point 48, in accordance with the instructions accompanying the appropriate forms, via the Financial Supervisory Authority's service portal. Progress reports must be submitted as soon as possible, but no later than three (3) days after the incident is discovered. The scope of progress reports is determined by the type of incident concerned.

6. Proportionality and sanctions

50. This section of the Guidelines discusses the principle of proportionality and how it is applied during the supervisory process. It also covers the relationship between sanction provisions in special legislation and the operational risk assessment criteria that appear in the Guidelines.

6.1 Proportionality during the supervisory process

51. In carrying out supervision in connection with these Guidelines, the Financial Supervisory Authority takes into account the size, nature, and scope of the supervised entity's information system operations, as well as the complexity of the systems concerned; cf. Points 52 and 53.

52. Without exception, the following supervised entities must comply with the criteria laid down in these Guidelines:

- Payment service providers; cf. Article 8 of the Payment Services Act, no. 120/2011.
- Insurance conglomerates; cf. Article 3 of the Act on Insurance Conglomerates, no. 60/2017.
- Securities exchanges and other regulated securities markets; cf. Articles 1 and 2 of the Act on Stock Exchanges, no. 110/2007.
- Central securities depositories; cf. Article 2 of the Act on Electronic Registration of Title to Securities, no. 131/1997.

[22] The term *incidents* refers to unforeseen events that occur in the operation of information systems and either curtail the service provided by the supervised entity in excess of defined benchmarks or affect confidentiality, integrity, or availability of information systems.

- Pension funds; cf. Article 1, Paragraph 1 of the Act on Mandatory Insurance of Pension Rights and on Activities of Pension Funds, no. 129/1997, when net assets for the payment of pension benefits exceed 100 m.kr. and the combined number of active pension fund members and pension income recipients exceeds 10,000.
- UCITS management companies; cf. Article 4, Paragraph 1, Item 7 of the Act on Financial Undertakings, no. 161/2002, when combined assets under management exceed 100 b.kr.

53. Supervised entities, other than those specified in Point 52, are required to satisfy the criteria in these Guidelines in the same manner as those specified in Point 52, but with adaptations as regards the following:
    - Risk assessments according to Section 2.2 shall be carried out on a regular basis, and at least every three (3) years.
    - The contingency framework according to Section 2.3 shall be updated on a regular basis, and at least every three (3) years.
    - Reviews of outsourcing contracts according to Point 26 shall be conducted on a regular basis, and at least every four (4) years.
    - Impartial compliance checks according to Point 43 shall be carried out on a regular basis, and at least every three (3) years.
    - Incident notifications and progress reports according to Section 5.2 shall be based on the activities of the supervised entities concerned.

6.2 Sanctions

54. These Guidelines contain criteria that the Financial Supervisory Authority sets forth and relies on in its supervision of operational risk, with emphasis on information system operations. The criteria are set forth in order to explain more fully the requirements provided for in the law and Governmental directives as regards supervised entities' operational risk. The requirements and the criteria form the foundations for the Financial Supervisory Authority's assessment of compliance with provisions on operational risk in special legislation concerning supervised entities' activities. The Financial Supervisory Authority determines sanctions for violations of provisions on operational risk in accordance with the penalty provisions in the special legislation that is relevant in each instance.

7. Entry into effect

55. These Guidelines shall take effect upon publication, whereupon the current Guidelines on Information Technology Systems of Supervised Entities, no. 2/2014, shall cease to apply. Notifications of incidents, cf. Section 5.2, will not be sent in updated form, however, until after 1 January 2020.