Regulations and guidelines 8/2014

Management of operational risk in supervised entities of the financial sector

J. No
FIVA 22/01.00/2019

Issued
4.11.2014

Valid from
1.2.2015

Further information from
Digitalisation and Analysis /
Digitalisation and Banking Services

FINANCIAL SUPERVISORY AUTHORITY
tel. +358 9 183 51
firstname.surname@fiva.fi
fin-fsa.fi

FIN-FSA
FINANCIAL SUPERVISORY AUTHORITY

Legal nature of regulations and guidelines

Regulations

Financial Supervisory Authority (FIN-FSA) regulations are presented under the heading ‘Regulation’ in the FIN-FSA's regulations and guidelines. FIN-FSA regulations are binding legal requirements that must be complied with.

The FIN-FSA issues regulations only by virtue of and within the limits of legal provisions that entitle it to do so.

Guidelines

FIN-FSA interpretations of the contents of laws and other binding provisions are presented under the heading ‘Guideline’ in the FIN-FSA's regulations and guidelines.

Also recommendations and other operating guidelines that are not binding are presented under this heading, as are the FIN-FSA’s recommendations on compliance with international guidelines and recommendations.

The formulation of the guideline shows when it constitutes an interpretation and when it constitutes a recommendation or other operating guideline. A more detailed description of the formulation of guidelines and the legal nature of regulations and guidelines is provided on the FIN-FSA website.

fin-fsa.fi > Regulation > Legal framework of FIN-FSA regulations and guidelines

Contents

1 Scope of application and definitions

1.1 Risk management

Chapters 4–7, 8.2, 9.1 and 9.2 of these regulations and guidelines apply to the following supervised entities as referred to in the Act on the Financial Supervisory Authority: (Issued on 29 January 2018, valid from 1 March 2018)

- credit institutions
- Finnish branches of third country credit institutions
- investment firms governed by chapters 9, 10 and 11 of the Credit Institutions Act in accordance with chapter 6, section 2 of the Investment Services Act
- fund management companies engaged in activities referred to in section 5, subsection 2 of the Mutual Funds Act
- alternative investment fund managers (AIF managers) providing investment services
- holding companies of credit institutions and investment firms as well as holding companies of conglomerates as referred to in the Act on the Supervision of Financial and Insurance Conglomerates
- central bodies of amalgamations of deposit banks
- payment institutions

Chapters 4–6, 8.2 and 9.1(2) of these regulations and guidelines apply to the following supervised entity:

- the stock exchange.

In addition, the Financial Supervisory Authority (FIN-FSA) recommends that Finnish branches of third country investment firms comply with chapters 4–7, 8.2, 9.1 and 9.2 of these regulations and guidelines. (Issued on 29 January 2018, valid from 1 March 2018)

Chapter 7 on payment systems only applies to supervised entities providing money transmission services.

Chapters 7 and 9.1 apply to persons providing payment services without authorisation, including account information service providers, applying the parts specified in more detail in the said chapters. (Issued on 29 January 2018, valid from 1 March 2018)

Section 9.3 (annual assessment of operational and security risks of payment services) and 9.4 (reporting of fraud data related to payment instruments) applies to supervised entities providing payment services, persons providing payment services without authorization and also to domestic credit institutions and Finnish branches of foreign credit institutions providing payment services in Finland. (Issued on 23 September 2019, valid from 1 January 2020)

Chapter 9.5 (Applying for an exemption from maintaining a contingency mechanism for a PSD2 dedicated interface) applies to account servicing credit institutions and payment institutions. (Issued on 23 September 2019, valid from 1 January 2020)

1.2 Contingency planning

Section 8.3 of these regulations and guidelines applies to the following supervised entities and foreign supervised entities, which are obliged to prepare for contingencies as referred to in the Emergency Powers Act (1552/2011):

- credit institutions
- payment institutions
- investment firms providing custody of financial instruments as an ancillary service (Issued on 29 January 2018, valid from 1 March 2018)
- fund management companies
- alternative investment fund managers providing investment services
- Finnish branches of foreign credit institutions
- Finnish branches of foreign payment institutions
- Finnish branches of foreign investment firms
- Finnish Central Securities Depository (APK).

In addition, FIN-FSA recommends that the stock exchange comply with the guidelines in section 8.3 on contingency planning. (Issued on 29 January 2018, valid from 1 March 2018)

1.3 Principle of proportionality

These regulations and guidelines apply to different supervised entities and different governance models. In its application of these regulations and guidelines a supervised entity may take into account the nature, scope, complexity and risks of its operations as well as other possible corresponding factors affecting the assessment, when it considers how to implement the regulations and guidelines in an appropriate and effective manner.

1.4 Definitions

Supervised entity means all supervised entities and foreign supervised entities referred to in the Act on the Financial Supervisory Authority and presented above in section 1.1 on the scope of application of the regulations and guidelines.

Operational risk means the risk of loss associated with

- inadequate or failed internal processes
- staff
- systems
- external events.

Operational risk also includes legal risk, whereas strategic risk is here excluded from operational risk.

Controls mean procedures for ensuring that operational goals are reached. Controls include all measures taken to prevent, detect and mitigate disruptions, shortcomings, faults and misuse.

Typically, controls comprise reconciliations, the four eyes principle, and comparison of counterparties' confirmations with the supervised entity's own contract documentation.

Executive management means the supervised entity's CEO and all persons who report directly to the CEO or hold the top managerial posts in the supervised entity or effectively direct the operations of the entity.

2 Legal framework and international recommendations

2.1 Legislation

These regulations and guidelines relate to the following statutes: (Issued on 29 January 2018, valid from 1 March 2018)

- the Credit Institutions Act (610/2014, below also the CIA)
- the Investment Services Act (747/2012, below also the ISA)
- the Mutual Funds Act, (48/1999, below also the MFA)
- the Act on Alternative Investment Fund Managers (162/2014, below also the AIFMA)
- the Act on the Amalgamation of Deposit Banks (599/2010)
- the Payment Institutions Act (297/2010, below also the PIA)
- the Act on Supervision of Financial and Insurance Conglomerates (699/2004)
- the Act on Trading in Financial Instruments (1070/2017)
- the Act on the Book-Entry System and Settlement Systems (348/2017)
- the Payment Services Act (290/2010)
- the Emergency Powers Act (1552/2011)
- the Government Decree on Objectives of Maintenance Readiness (857/2013).

2.2 EU regulations

These regulations and guidelines relate to the following EU regulations: (Issued on 23 September 2019, valid from 1 January 2020)

- Commission Delegated Regulation (EU) No 231/2013 (32013L0231) of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council with regard to exemptions, general operating conditions, depositaries, leverage, transparency and supervision; OJ L 83, 22.3.2013, p. 1–95 (below the delegated regulation)
- Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systematically important payment systems (ECB/2014/28); OJ L 217, 23.7.2014, p. 16–30.
- Regulation (EU) 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 (General Data Protection Regulation)
- Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to

regulatory technical standards for strong customer authentication and common and secure open standards of communication (hereinafter SCA delegated regulation)

2.3 EU directives

These regulations and guidelines relate to the following EU directives: (Issued on 23 September 2019, valid from 1 January 2020)

- Directive 2013/36/EU (32013L0036) of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EU and repealing Directives 2006/48/EU and 2006/49/EU; OJ L 176, 27.6.2013, p. 338
- Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU; OJ L 173, 12.6.2014, p. 349.
- Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC; OJ L 337, 23.12.2015.
- Directive 2002/87/EC (32002L0087) of the European parliament and of the Council of 16 December 2002 on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate and amending Council Directives 73/239/EEC, 79/267/EEC, 92/49/EEC, 92/96/EEC, 93/6/EEC and 93/22/EEC, and Directives 98/78/EC and 2000/12/EC of the European Parliament and of the Council; OJ L 35, 11.2.2003, p. 1–27
- Commission Directive 2006/73/EC (32006L0073) of 10 August 2006 implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive; OJ L 241, 2.9.2006, p. 26–58
- Directive 2009/65/EC (32009L0065) of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS); OJ L 302, 17.11.2009, p. 32–96
- Directive 2011/61/EU (32011L0061) of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010; OJ L 174, 1.7.2011, p. 1–73.
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

2.4 FIN-FSA's regulatory powers

The FIN-FSA's powers to issue regulations are based on the following provisions:

- section 18, subsection 2 of the Act on the Financial Supervisory Authority (878/2008), according to which FIN-FSA may issue regulations on the regular submission to FIN-FSA of information on a supervised entity's internal control and risk management
- chapter 9, section 24 of the CIA, according to which the FIN-FSA may issue detailed regulations on operational risk as referred to in chapter 9, section 16
- section 19, subsection 6 of the Act on the Amalgamation of Deposit Banks, according to which FIN-FSA may issue detailed regulations on the risk management of member companies of the amalgamation
- chapter 6, section 2, subsection 1 of the ISA and section 6, subsection 5 of the MFA, which provide that the regulations issued by the FIN-FSA by virtue of chapter 9, section 24 of the CIA also apply to investment firms and fund management companies as referred to in the above- mentioned legal provisions
- According to chapter 6, section 2, subsection 6 of the AIFMA, an alternative investment fund manager providing the services referred to in chapter 3, section 2, subsection 2 and chapter 3, section 3 of the AIFMA must always meet the requirements prescribed in chapter 6, section 2 subsection 1 of the ISA. It follows from chapter 6, section 2 subsection 1 of the ISA that regulations issued by the FIN-FSA under chapter 9, section 24 of the CIA also apply to alternative investment fund managers, as referred to in the above-mentioned legal provisions. (Issued on 29 January 2018, valid from 1 March 2018)
- section 30 a, subsection 3 of the MFA, by virtue of which the FIN-FSA may issue detailed regulations on the requirements pertaining to fund management companies' risk management systems and other internal control
- section 19, subsection 3 of the PIA, by virtue of which the FIN-FSA may issue detailed regulations on the organisation of operations so as to implement the Payment Services Directive (PSD) as well as sections 19 a and 19 b of the PIA, by virtue of which the FIN-FSA may issue detailed regulations on the management of operational and security risks and on the reporting of anomalies and fraud. Regulations issued by the FIN-FSA by virtue of sections 19 a and 19 b of the PIA also apply to persons providing payment services without authorisation as well as to credit institutions providing payment services on the basis of chapter 9 section 16 of the CIA. (Issued 29.1.2018, valid from 1.3.2018)
- section 16, subsection 3 of the Act on the Supervision of Financial and Insurance Conglomerates, by virtue of which the FIN-FSA may issue detailed regulations on the arrangement of internal control and risk management for the parent company and holding company of a conglomerate
- chapter 3, section 36, subsection 1, paragraph 1 of the Act on Trading in Financial Instruments, by virtue of which the FIN-FSA may issue detailed regulations on the organisation of operations of the stock exchange, as referred to in chapter 3, section 1 of the said Act.

2.5 International recommendations

The following international recommendations have been taken into account in preparing these regulations and guidelines:

- Basel Committee on Banking Supervision (Basel Committee) recommendation Principles for the Sound Management of Operational Risk (Bank for International Settlements, BIS, June 2011)
- European Banking Authority (EBA) Guidelines on the Management of Operational Risks in Market-related Activities (Committee of European Banking Supervisors, CEBS, October 2010)
- EBA Guidelines on Internal Governance (EBA/GL/2017/11) (Issued on 29 January 2018, valid from 1 March 2018)
- Basel Committee recommendation High level principles for business continuity (BIS, August 2006)
- Basel Committee recommendation Risk Management Principles for Electronic Banking (BIS, July 2003)
- European Securities and Markets Authority Guidelines on systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities (ESMA February 2012)
- Principles for financial market infrastructures (BIS/IOSCO, April 2012), issued by the Basel Committee on Payment and Settlement Systems (CPSS) and the Technical Committee of the International Organization of Securities Commissions (IOSCO)
- EBA Guidelines on the Security of Internet Payments (EBA/GL/2014/12_Rev1)
- EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP) (EBA/GL/2017/05) (Issued on 6 November 2017, valid from 1 March 2018)
- EBA Guidelines on Major Incident Reporting under Directive (EU) 2015/2366 (PSD2) (EBA/GL/2017/10) (Issued on 29 January 2018, valid from 1 March 2018)
- EBA Guidelines on the Security Measures for Operational and Security Risks of Payment Services under Directive (EU) 2015/2366 (PSD2) (EBA/GL2017/17) (Issued on 29 January 2018, valid from 1 March 2018)
- Joint Committee of the three European Supervisory Authorities (ESAs) Joint Position on Manufacturers' Product Oversight and Governance Processes (November 2013)
- EBA Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2) (EBA/GL/2018/05) (Issued on 23 September 2019, valid from 1 January 2020)
- EBA Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)) (Issued on 23 September 2019, valid from 1 January 2020)

3 Objectives

(1) These regulations and guidelines concern the principles and organisation of operational risk management. Subjects such as process management, staff, information and payment systems, information security, continuity planning and legal risk are covered in greater detail.

(2) Technological advances, product and service developments, new risk management procedures, outsourcing arrangements, corporate restructuring and the internationalisation of activities have added to the complexity of the operating environment and increased the operational risk in the production of financial services.

(3) Smoothly running payment and clearing systems are important, since most of the transferring and clearing of payments in our economy is done through these systems. Downtime and disruptions make it difficult for customers to handle their payments, which may cause far- reaching financial problems.

(4) The objective of these regulations and guidelines is to ensure that the following steps are taken:

- The supervised entity organises its operational risk management so as to fulfil the requirements determined by the scope and character of its operations.
- If necessary, the risk management tasks may be outsourced in compliance with FIN-FSA's regulations and guidelines 1/2012 on outsourcing.
- The supervised entity ensures an appropriate level of information management, information security and continuity of operations.
- The FIN-FSA is informed of significant disruptions and faults in the entity's operations and other impairments as well as losses due to realisations of operational risk.

4 General principles of operational risk management

4.1 Operational risk management

(1) Losses resulting from an operational risk event cannot always be measured. The risk may materialise after a time lag or indirectly for example through damage caused to the reputation or goodwill of the supervised entity.

(2) In operational risk management, an important role is played by measures taken to correct observed shortcomings and faults in processes and risk management and by other risk-limiting measures, such as staff-related and IT backup arrangements and acquisition of insurance cover.

(3) The Credit Institutions Act contains detailed provisions on operational risk management. In accordance with chapter 9, section 16, subsection 1 of the CIA, a credit institution shall have procedures for identification, assessment and management of operational risk. It shall prepare for modelling risk and for rarely materialising severe risk events. A credit institution must clearly describe what it considers to be operational risks. It shall have written policies and procedures for operational risk management.

4.2 Establishment and maintenance of operational risk management

(4) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulation on the establishment and maintenance of risk management.

Regulation (paragraphs 5-6)

(5) The Board of the supervised entity shall confirm the principles for operational risk management, which cover the procedures and processes for identification, assessment, control and mitigation of risk. The principles shall regularly be reviewed, taking into account any changes in the operating environment and in the supervised entity's own business.

(6) The supervised entity shall define operational risk on the basis of its own business activities, considering the typical characteristics of its business.

Guideline (paragraphs 7-8)

(7) The FIN-FSA recommends that the supervised entity's executive management ensure practical compliance with the principles adopted for operational risk management in all operations of the entity and companies in the group. It should also ensure that the employees identify the operational risks inherent in their own activities and are familiar with the procedures involved in managing these risks.

(8) The FIN-FSA recommends that the Board of the supervised entity ensure that the entity's internal audit regularly assesses the efficiency and coverage of the operational risk management.

4.3 Identification and assessment of operational risk

(9) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulations on the establishment and maintenance of risk management.

(10) More detailed provisions on investment firms' product governance procedures are provided in chapter 7, section 7 and 18 of the Act on Investment Firms. (Issued on 23 September 2019, valid from 1 January 2020)

Regulation (paragraphs 11-15)

(11) The supervised entity must identify all the operational risks attached to its major products, services, functions, processes and systems that may have significant effects on the achievement of objectives set for the operations.

(12) The supervised entity shall assess the risks of a new product and service prior to their introduction. Such assessment shall also be performed at the introduction of a new service package, when products and services are combined in a new way, if the supervised entity does not consider that the assessments performed cover the risks related to the introduction of the new service package.

(13) In the ongoing risk assessment, the probability of risk realisation and the effects of a damage shall be considered. In planning its risk management, the supervised entity shall confirm the necessary risk mitigation methods and other necessary corrective measures.

(14) As regards key activities, the supervised entity shall decide on an acceptable risk-taking level and set limits and other restrictions for the risks.

(15) The supervised entity shall create alternative scenarios in order to take into account at least the malfunctioning of key processes and systems, incapacity of staff as well as the effects of external factors.

Guideline (paragraphs 16-22)

(16) As to identified, material operational risks, the FIN-FSA recommends that the supervised entity decide how it will control the risks or whether it will bear the risks as they are or limit them or withdraw from the business activity causing them.

(17) The FIN-FSA recommends that risk assessment include analyses of adverse internal and external factors. A supervised entity's legal structure, changes in organisation, complexity of products and services, quality of human resources and turnover of employees, and the state of its IT systems are typical internal factors and technological advances and internationalisation of activities are typical external factors.

(18) The FIN-FSA recommends that the supervised entity aim to put in place proactive procedures and indicators for recognising operational risks. Applicable procedures may be standard self-analyses of the bank organisation, compilation of statistics on risk-related damages, use of critical variables describing operations, and the review of damages suffered by the supervised entity and its peer group.

(19) The FIN-FSA recommends that the supervised entity acquire insurance against economic effects due to operational risk. The executive management should ensure that the adequacy and costs of the insurance cover are regularly assessed, bearing in mind changes in the supervised entity's business activities. In addition, the counterparty risks inherent in the insurance contracts should be assessed as well as the capital adequacy of the contract company.

(20) The FIN-FSA recommends that the supervised entity prepare instructions on the procedure for approval of new products or services.

(21) The FIN-FSA recommends that the procedure for approval of new products or services comprise, for example, the following:

- description of products or services
- assessment of the compliance of products or services with the operational strategy
- geographical market area and target group
- risk surveys (assessments of risks related to the product or service)
- description of organisation of internal control and risk management as regards a new product or service
- review of the processes related to products or services (marketing, customer identification, sale, production, clearing and payments)
- legal issues and capacity to enter into contracts
- description of IT systems, information security and service continuity
- external and internal accounting requirements
- description of pricing, possible valuations, and use of pricing models
- assessment of impact on profitability and capital adequacy
- assessment of impact on taxation
- description of required training and instructions.

(22) The FIN-FSA recommends that the supervised entity inform The FIN-FSA of any significant new product or service well before its introduction.

4.4 Monitoring and damage reporting for operational risk

(23) Chapter 9 provides guidance on reporting to the FIN-FSA of disruptions and faults in operations and annual reporting of significant operational risk loss events.

(24) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulations on the establishment and maintenance of risk management.

Regulation (paragraphs 25-26)

(25) The supervised entity shall regularly assess the nature of recognised operational risks and the probability of risk realisations and monitor realised losses and loss amounts. The supervised entity shall examine the factors and cause-and-effect relations behind the realisation of damage events.

(26) The Board and the executive management of the supervised entity shall obtain information on the most significant operational risks of the different business areas. As part of the establishment and maintenance of internal control, the Board shall regularly receive reports on the supervised entity's most significant risks and damage events.

Guideline (paragraphs 27-30)

(27) The FIN-FSA recommends that the information to be reported include, for example, descriptions of events, reasons for events, estimates of direct and indirect costs, and measures for damage prevention. It is also recommended that the measures taken in response to the damage and the contact persons and schedule for the corrective actions be reported.

(28) The FIN-FSA recommends that the executive management of the supervised entity regularly assess the up-to-dateness, precision and appropriateness of the risk management procedures and reporting systems. The contents and level of detail of reports as well as their dissemination and reporting frequency should also be assessed on a regular basis.

(29) Bearing in mind the significance of monitoring and reporting, the FIN-FSA recommends the setting of a threshold amount, above which the events should be reported. Even small damages and close calls should be reported, if they are fundamentally important to the functioning of the risk management.

(30) The FIN-FSA recommends that the monitoring of losses due to operational risk be carried out according to the below table.

Loss type	Examples
Internal irregularities	embezzlement, fraud, bribe-taking, securities markets offence or violation, malicious damage, absence of (or acting beyond) powers, misuse of customer information, intentional misreporting of positions, breach of business confidentiality, extortion
External malicious damage	theft, robbery, fraud (eg in use of payment means), forgery, money laundering, intrusion into IT systems, spreading of malicious software, denial-of-service attacks on IT systems, bomb threats, threats to staff, extortion
Working conditions, occupational safety	violations of the Contracts of Employment Act (working hours, occupational safety), discrimination claims, disputes over wages, compensation or dismissal, labour market disputes

Losses due to questionable business practices	unlawful and objectionable or misleading marketing and provision of services; misuse of confidential customer information (eg in marketing); neglect of obligation to disclose information to customers, of secrecy requirements or of duty to investigate; improper execution of assignments or handling of customer assets; securities markets offence or violation; money laundering
Damage to physical assets	fire, water damage, floods
Damage from IT system disruptions and outages	software failure, data communication failure, computer downtime, hardware failure, power failure, disruption caused by external service provider
Process-related problems	misreporting, faulty customer information, data entry errors, pricing errors, contract invalidity, incomplete legal documentation, document disappearance, collateral management failures, unsuccessful execution of customer assignment, disruption in outsourced service, dispute with external service provider, accounting error

5 Key components of operational risk management

5.1 Processes

(1) In this chapter a process refers to the sum of activities and resources required to create a service or product. Process management comprises the aspects of customer satisfaction, efficiency, profitability and reliability and quality of operations. A survey of the operational risk related to the different phases of the processes will help the supervised entity to identify and mitigate operational risk.

(2) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulation on the establishment and maintenance of risk management.

Regulation (paragraph 3)

(3) Supervised entities must identify the key processes of their business. Controls shall be built into the different phases of the processes. The adequacy of the controls shall be assessed especially whenever the scope or contents of the business or processes change.

Guideline (paragraphs 4-6)

(4) The FIN-FSA recommends that the supervised entity pay special attention to the interfaces between different organisational units and companies in the processes, to possible points of discontinuity in the processes, cross-border operations and payment transactions.

(5) The FIN-FSA recommends that the key processes for the conduct of business should be documented in writing as uniformly as possible, including descriptions of the tasks involved in the process, the different phases of the process and their interdependencies and vulnerabilities. The documentation should also cover flows of information and materials, reporting, and interested parties and IT systems of the process. In particular, the supervised entity should see to it that instructions are in place for the handling of large transaction volumes and that they are well-documented. The process descriptions should be updated on a regular basis.

(6) The FIN-FSA recommends that the principles applied in the implementation of different projects should be as uniform as possible. Risk assessments of major projects should be made in advance.

5.2 Legal risk

(7) Legal risk may be caused by external factors, such as changes in the operating environment, and effects of the supervised entity's own activities. All business activities can be exposed to legal risk. The interpretation, scope and validity of the legal framework governing the supervised entity's operations entail uncertainties that may give rise to significant losses and have a bearing on the entity's legal responsibility and possible liability for indemnification.

(8) Disputes concerning the validity and contents of contracts may have an adverse effect on supervised entities' business activities. Disengagement from disadvantageous contracts and entry into compensating contracts may involve risk of loss. This applies to the use of standardised contracts in particular. Documents issued by supervised entities, such as prospectuses and

advertisements, may also give rise to indemnification liability or risk of damaged reputation or reduced goodwill.

(9) By virtue of its regulatory powers as referred to in section 2.4, the FIN-FSA issues the following regulation on the establishment and maintenance of risk management.

Regulation (paragraph 10)

(10) The Board of the supervised entity must identify the key legal risks in the entity's business activities and ensure that the legal risks are appropriately managed.

Guideline (paragraphs 11-15)

(11) The FIN-FSA recommends that the executive management organise the legal risk management and ensure that adequate resources are allocated so that legal risks can be identified, monitored and mitigated in different business areas.

(12) The FIN-FSA recommends that the supervised entity ensure adequate expertise for managing legal risks for the purpose of entering into contracts and other legal commitments. The supervised entity should ensure that representatives of contract parties are entitled to sign the contract.

(13) The FIN-FSA recommends that the supervised entity keep files of contract-related documentation in an appropriate manner and that validity of contracts and possible differences of interpretation and disputes be monitored.

(14) The FIN-FSA recommends that the supervised entity keep track of changes in both legislation and international regulations so as to be well prepared in advance for new legal and regulatory requirements. The supervised entity should know the legal praxis of its own business area.

(15) The FIN-FSA recommends that the parent company of financial and insurance conglomerates see to it that all companies included in the conglomerate have adequate knowledge of the provisions and regulations of both business sectors. Supervised entities that operate across borders must take into account that key legal principles and practices may vary significantly from one country to another.

5.3 Staff

(16) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulation on the establishment and maintenance of risk management.

Regulation (paragraphs 17-20)

(17) The supervised entity shall ensure that the professional skills of the entity's employees and new recruits are adequate for the tasks involved, the size of the entity and the scope and nature of its activities.

(18) The supervised entity shall have procedures in place to ensure that the requirements on staff skills, such as formal qualification and sufficient education and experience, are met at all times. When recruiting new members of staff, special attention shall be paid to their reputation and background.

(19) The executive management shall ensure that there are sufficient human resources to handle all the tasks involved. In order to ensure business continuity, particularly employees performing key duties shall have deputies who can act in their stead in case of sudden termination or interruption of employment.

(20) The supervised entity shall use all necessary procedures to ensure that employees do not reveal financial or private details, or business or professional secrets, concerning customers or other parties associated with the entity. Such information may only be divulged if the conditions stated in law are fulfilled.

6 IT systems and information security

6.1 IT systems

(1) In accordance with chapter 9, section 16, subsection 2 of the CIA, a credit institution shall have adequate, secure and reliable payment, security and other IT systems.

(2) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulations on the establishment and maintenance of risk management.

Regulation (paragraphs 3-6)

(3) The Board of the supervised entity shall ensure that the entity has IT systems in place that are adequate and appropriate vis-à-vis the nature and scope of its business. The adequacy and appropriateness of the IT systems shall be assessed in relation to the supervised entity's business activities, the requirements of the Board and the fact that the systems must support business activities according to policies set by the Board.

(4) The supervised entity shall have the expertise, organisation and internal control required to record, transfer, process and file information. If these functions are outsourced, the supervised entity shall ensure that the company providing IT services comply with the principles laid down in this chapter.

(5) The Board shall adopt an IT strategy in accordance with the entity's current and projected future needs and review it regularly. In addition, the Board shall monitor the IT costs.

(6) There must also be standard procedures in place for launching systems, managing changes and testing. The systems must be thoroughly tested before introduction. If necessary, load and capacity tests of the systems must be performed.

Guideline (paragraphs 7-10)

(7) The FIN-FSA recommends that the supervised entity put in place policies to ensure cooperation between business units and IT service units. However, supervised entities should separate systems development and production from each other.

(8) The FIN-FSA recommends that the supervised entity introduce methods for system development and quality control, in order to ensure that the systems function as planned. In addition, there should be documentation on the systems to ensure that they can be used and developed despite, for example, turnover of key persons.

(9) The FIN-FSA recommends that the supervised entity describe the procedures applied, when key software and hardware are purchased or contracts entered into with service providers.

The supervised entity should ensure that procurements and contracts meet the entity's needs and the quality levels set for the operations, and that they guarantee continuity of service.

(10) The FIN-FSA recommends that the supervised entity take into account in the management of their IT system risks the EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP). (Issued on 6 November 2017, valid from 1 March 2018)

6.2 Information security

6.2.1 Definition and basic requirements of information security

(11) Information security refers to administrative, technical and other measures by which a company's data, services, systems and data communications are protected and secured under normal as well as emergency conditions.

(12) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulations on the establishment and maintenance of information security.

Regulation (paragraphs 13-17)

(13) The supervised entity's general information security level and the basic safety levels of the different data systems shall be adequate vis-à-vis the nature and scope of the entity's activities, the severity of threats to the information systems, and the general level of technological development.

(14) The Board of the supervised entity is responsible for adequate information security within the entity. The general information security level shall be defined and approved by the Board. The supervised entity shall allocate necessary resources and delegate responsibilities for maintaining an adequate level of information security. The supervised entity shall regularly review the information security level. Detected insufficiencies in security must be addressed promptly.

(15) Supervised entities shall specify the owners of the data that they store and process, and the owners of the systems that they use. The owners are responsible for utilisation policies, access rights and security relating to information and systems. The supervised entities shall categorise all stored and processed data by their security requirements, and draw up handling rules for the different security categories.

(16) Supervised entities shall grant authorisations to access data, programs and systems and ensure that systems are used according to uniform principles adopted by the management. Authorisations shall be granted on the basis of staff duties. Technical authentication methods shall be used to restrict access to data, programs and systems to authorised users only. Access violations shall be investigated and reported to the organisational entity responsible for the systems.

(17) Access to the information systems shall be monitored. Non-repudiation of electronic events and identification and authentication of intercommunicating parties must be handled appropriately. The information systems must also provide a full audit trail of all events.

Guideline (paragraphs 18-19)

(18) The FIN-FSA recommends that supervised entities, as applicable, follow the instructions of the Government Information Security Management Board.[1]

[1] *Instructions on Implementing the Decree on Information Security in Central Government, VAHTI 2/2010.*

(19) The FIN-FSA recommends the keeping of an appropriate log of events pertaining to the development of services. In addition, the monitoring of access to services and the identification and authentication of users should be taken into account.

6.2.2 Management of information security risks and handling of information security events

(20) An information security incident is an event or act of non-compliance with the information security principles (for example a virus attack), an IT system intrusion, or a data leakage.

(21) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulation on the establishment and maintenance of information security risk management.

Regulation (paragraphs 22-24)

(22) Information security risk assessment shall be built into the supervised entity's risk management to ensure that the Board and executive management comprehend the total impact of all major risks associated with the business activities.

(23) The assessment of a supervised entity's information security level shall be based on regular assessment of information security risks. In the risk assessments, the supervised entity's key activities and resources and the threats thereto, the vulnerability of the entity's activities and resources to these threats, and the threats[1] potential impacts on the entity's activities shall be noted. Built-in controls for managing recognised risks shall be established. The risks of launching new systems, technology and services shall also be assessed prior to introduction.

(24) Information security incidents shall be identified, analysed, filed and reported to designated persons within the organisation.

6.2.3 Information security rules and training

(25) Information security rules are, for example, rules on access control management, prevention of malicious software, and use of Internet and email.

(26) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulations.

Regulation (paragraphs 27-28)

(27) The supervised entity shall have up-to-date information security principles adopted by the Board and information security rules supporting those principles. The rules shall be communicated to the staff.

(28) Supervised entities shall clearly define the information security duties for each staff member and supply regular information security training to all staff. Information security development shall be an ongoing process, and the related managerial responsibilities shall be clearly defined.

6.2.4 Ensuring information security in online services

(29) Information security of online services comprises, among other things, the security of policies and applications used and of technical systems and data communications.

(30) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulations.

Regulation (paragraphs 31-32)

(31) Supervised entities shall assess the online suitability of services before existing services are made available online or new online services are launched. The major risks involved in such services and the risk management methods shall be documented, and the necessary controls for managing risks shall be built into the system. Internal control and risk management of online operations, IT systems and internal processes shall be designed and set up taking into account the nature and scope of the supervised entity's activities and the potential threats thereto.

(32) Supervised entities shall, on an ongoing basis, assess and upgrade their IT systems and the information security of them, and adequately protect themselves against the different kinds of disruptions and possible misuse.

6.2.5 Development of services with comprehensive information security

(33) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulations.

Regulation (paragraph 34)

(34) In its development of new services, the supervised entity shall analyse the information security risks. On the basis of the risk analysis, the necessary measures must be taken to manage the risks.

Guideline (paragraph 35)

(35) The FIN-FSA recommends that the supervised entity check at least the following items to ensure adequate information security before launching and offering a service:

- System-based information security tests and reviews have been made and ongoing monitoring and reporting of security levels and possible disruptions of systems have been carried out. A system review means a systematic examination of the security level of a system, service or activity to ensure that the targeted security level is achieved.
- In order to ensure the availability and continuity of a service, standby facilities have been described in advance and recovery plans have been prepared for the systems.
- Systems have been equipped with necessary anti-virus programs and other mechanisms to avert malicious software.
- Systems and their necessary data connections have been protected against, for example, denial-of-service attacks. Systems have been equipped with access control mechanisms,

and the supervised entity has ensured that appropriate management of authorisations is in place.

- The external network has been separated from the supervised entity's internal network by means of security features.
- Systems are tested on a regular basis and particularly after system changes. Detected security shortcomings are remedied immediately.
- Before roll-out, online services are subject to information security audits, which shall also be conducted on a regular basis during the ongoing provision of online services.
- Supervised entities have ensured that, in online services, data communications and data processing in service provider systems fulfil confidentiality, integrity and non-repudiation requirements. The procedures for identification and authentication of communicating parties should also be reliable.
- Supervised entities have equipped their IT systems with verification mechanisms and audit trails, which ensure the accuracy and integrity of input and output data. It should be possible to follow an end-to-end audit trail of all events processed in the systems.
- Systems have been equipped with built-in controls allowing reconciliation of transactions processed in different subsystems.
- Services have been developed with cognisance of standby facilities to prepare for disruptions and outages in activities and systems by setting up alternative modes of operation or systems. Standby facilities typically involve the use of duplex components in data processing and data communications as well as backup copying.
- Any customer-specific passwords have been encrypted within the system and for transfers between systems.
- Special care has been taken and hazardous combinations of duties avoided in creating, handling and delivering customer-specific ID data (user IDs and passwords).
- The systems have created logs on logins, login attempts and service usage. Logs and log reports are checked regularly.
- Customers are provided with sufficient information on the service provider, services offered, division of responsibilities between service provider and user, and secure use of the services.

7 Payment systems and money transmission

(1) In accordance with chapter 9, section 16, subsection 2 of the CIA, a credit institution shall have adequate, secure and reliable payment, security and other IT systems.

(2) Based on section 19 a and 19 b of the PIA, supervised entities providing payment services and persons providing payment services without authorisation must have adequate risk management procedures for managing the operational and security risks of payment services and for monitoring and reporting anomalies and fraud. (Issued on 29 January 2018, valid from 1 March 2018)

(3) Payment systems are generally characterised by the following features:

- use of agreed means of payments
- participants include credit institutions, payment institutions and clearing corporations
- participants agree on certain money transmission and risk management practices
- mediation of fund transfers between payer and payee

(4) Clearing systems provide intermediation of transactions in interbank fund transfers and may also provide transaction settlement services.

(5) Means of payment comprise payment cards, other tailor-made instruments or procedures, or combinations thereof, which may be used for execution of payment orders as agreed between the user and provider of payment services.

(6) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulations.

Regulation (paragraphs 7-11)

(7) The supervised entity's Board shall approve the money transmission principles for the payment and clearing systems that the entity participates in and for the payment services that the entity provides to its customers. The principles shall apply to present activities, but expected developments over the next few years shall also be taken into account. The Board shall set objectives for the activity to ensure and monitor efficient, high-quality and reliable money transmission. Theclearing systems used by the supervised entity shall also be in line with the objectives.

(8) The executive management is responsible for ensuring that the supervised entity has the necessary expertise, resources and internal control for the maintenance of efficient and secure money transmission. Supervised entities shall survey the risks related to the money transmission systems and payment services they use and regularly update these risk surveys.

(9) Supervised entities' money transmission systems shall be reliable and secure. The entities shall ensure that disruptions and delays in the money transmission are kept to a minimum. There shall be adequate standby facilities for handling the interbank transactions.

(10) Supervised entities providing payment services and persons providing payment services without authorisation shall have adequate risk management procedures to manage the operational and security risks related to payment services. (Issued on 29 January 2018, valid from 1 March 2018)

(11) Supervised entities providing payment services and persons providing payment services without authorisation shall prepare an assessment of the operational and security risks of payment services, including an assessment of the adequacy of risk management and control mechanisms. The assessment shall be submitted to the FIN- FSA annually in accordance with chapter 9.3. (Issued on 29 January 2018, valid from 1 March 2018)

Guideline (paragraphs 12-16)

(12) The FIN-FSA recommends that supervised entities submit risk assessments of new payment services, systems and techniques to FIN-FSA before their introduction. Risk assessments should also be submitted to the FIN-FSA before the introduction of significant changes in payments and clearing systems.

(13) The FIN-FSA recommends that supervised entities inform the FIN-FSA of new payment services and significant changes in existing services well in advance and prior to their introduction.

(14) The FIN-FSA recommends that supervised entities take account of EBA's Guidelines on the Security of Internet Payments in the provision and development of payment services.[2] (Issued on 21 April 2014, valid from 1 July 2015)

(15) The FIN-FSA recommends that supervised entities providing payment services and persons providing payment services without authorisation adhere to the EBA's Guidelines on Security Measures for Operational and Security Risks in the provision of payment services. (Issued on 29 January 2018, valid from 1 March 2018)

(16) The FIN-FSA recommends that supervised entities participating in the activities of a systematically important payment and clearing system comply, as applicable, with the ECB regulation ECB/2014/28, by which the CPSS and IOSCO recommendation Principles for financial market infrastructures is implemented.

[2] *The recommendations of the EBA's Guidelines on the Security of Internet Payments will gradually be replaced by EBA Guidelines on the management of payment service providers' operational and security risks and the European Commission's Regulation on regulatory technical standards on strong customer authentication and secure communication.*

8 Continuity and emergency planning

8.1 Legal framework

(1) In accordance with chapter 9, section 16, subsection 3 of the CIA, credit institutions shall have contingency and continuity plans to prepare for serious disruptions, ensure continued operations and mitigate damages due to disruptions.

(2) In accordance with chapter 5, section 16 of the CIA, credit institutions shall as far as possible ensure undisrupted operations regardless of contingencies by participating in financial market emergency planning, preparing in advance for operations in emergency conditions, and by taking other measures.

(3) In accordance with chapter 18, section 5 of the CIA, the provisions in chapter 5, section 17 on contingency planning correspondingly also apply to branches of foreign credit institutions. They do not apply to branches of foreign European Economic Area (EEA) credit institutions in so far as a branch, by virtue of the credit institution's home state legislation, has ensured its operations in emergency conditions in a way corresponding to chapter 18, section 5 of the CIA and has submitted an appropriate report thereon to FIN- FSA.

(4) In accordance with section 41 a of the PIA, payment institutions shall as far as possible ensure undisrupted operations regardless of contingencies by participating in financial market emergency planning, preparing in advance for operations in emergency conditions, and by taking other measures. A corresponding contingency planning obligation is required of branches of foreign payment institutions.

(5) In accordance with chapter 7, section 8 of the ISA, investment firms providing custody of financial instruments as an ancillary service shall as far as possible ensure undisrupted operations regardless of contingencies by participating in financial market emergency planning, preparing in advance for operations in emergency conditions, and by taking other measures. In accordance with chapter 1, section 4, subsection 2 of the ISA, the provisions on emergency planning apply to AIF managers providing investment services. (Issued on 29 January 2018, valid from 1 March 2018)

(6) In accordance with chapter 7, section 15 of the ISA, the provisions in section 8 on continuity planning also apply to branches of foreign EEA investment firms. In accordance with chapter 1, section 7 of the ISA, the provisions in chapter 7, section 15 of the ISA apply in respect of these services to third country companies providing investment services or pursuing investment activities in Finland via a branch. (Issued on 29 January 2018, valid from 1 March 2018)

(7) In accordance with section 4 a of the MFA, mutual funds shall as far as possible ensure undisrupted operations regardless of contingencies by participating in financial market emergency planning, preparing in advance for operations in emergency conditions, and by taking other measures. In accordance with chapter 1, section 6, subsection 2 of the AIFMA, the contingency planning obligation referred to in chapter 7, section 8 of the ISA applies to AIF managers providing investment services as referred to in chapter 3, section 2 of the AIFMA. (Issued on 29 January 2018, valid from 1 March 2018)

(8) In accordance with chapter 2, section 12 of the Act on the Book-Entry System and Settlement Systems, the Finnish Central Securities Depository (APK) shall as far as possible ensure

undisrupted storage of the data in the book-entry system regardless of contingencies by using data systems available in Finland or other appropriate facilities providing undisrupted operations as well as by participating in financial market emergency planning, preparing in advance for operations in emergency conditions, and by taking other corresponding measures. (Issued on 29 January 2018, valid from 1 March 2018)

8.2 Continuity planning

(9) Continuity planning refers to preparations that enable supervised entities to carry on their operations despite disruptions in business activities and to mitigate losses from different events that disturb business activities. Disturbing events may be caused by damages or intentional acts affecting, for example, the supervised entity's staff, business premises, IT systems or data communications, or by water damage, fire or power failure, or breakdowns in heating or water supply. As part of their continuity planning, supervised entities shall draw up separate plans for each key business area in order to enable continued business despite disruptions.

(10) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulations on continuity planning.

Regulation (paragraphs 11-18)

(11) The Board of the supervised entity is responsible for ensuring that the entity's key business areas are covered by continuity plans that are up-to-date and adequate. The executive management shall allocate the responsibilities for the supervised entity's continuity planning. The supervised entity shall have a clear model for preparing, maintaining and testing its continuity plans, and for monitoring continuity planning.

(12) The supervised entity shall map and prioritise its key business processes. Minimum recovery times, i.e. maximum acceptable disruptions, that would not disturb business activities, shall be defined for the processes. Alternative modes of operation and recovery procedures shall be set up for prioritised processes in case of disruptions. Special attention shall be paid to the restoration of information that is crucial for the resumption of business activities.

(13) IT systems and programs shall be ranked according to how quickly they must be recovered after different types of disruptions. There must be recovery plans for IT systems describing how each IT system can be reactivated in the event of a serious disruption or catastrophe.

(14) Backup copies and possible standby computer facilities shall be located so far from the ordinary IT centre that data and backup copies cannot be destroyed at the same time.

(15) Supervised entities' continuity plans must be based on threat and vulnerability analyses of the entity's business activities, i.e. on analyses of threats, vulnerabilities and risks affecting data, systems, activities and services.

(16) In business continuity plans, attention shall be paid to various threat scenarios and vulnerabilities in different functions. Continuity plans shall be gauged according to the nature, scope and complexity of the supervised entity's activities. The continuity plans shall guide the supervised entity's activities and information in case of any kind of disruption.

(17) Supervised entities shall prepare for disruptions in the activities of external service providers. The continuity plans shall describe the manner of preventing external service provider activity

disruptions from affecting the supervised entity's business activities and the entity's monitoring of external service providers' continuity planning. Contracts with external service providers must require that the providers analyse, update and test their own systems against disruptions of activities.

(18) Continuity plans shall be updated on a regular basis and adjusted to changes in the supervised entity's business activities, services and strategies. Continuity plans shall be tested and the planned measures practised on a regular basis. Responsibilities for seeing that continuity plans are up-to-date and tested shall be specifically assigned.

8.3 Contingency planning

(19) The requirements to plan for contingencies is based on the Emergency Powers Act and contingency planning guidelines issued by the authorities. Contingencies are situations as defined in section 3 of the Emergency Powers Act. Normal continuity arrangements form the basis for contingency planning for emergency conditions.

(20) As a rule, disruptions last longer in emergency conditions than those accounted for in normal continuity plans. In addition, the risks associated with emergency conditions are generally more serious than those prepared for in continuity plans.

(21) The guidelines for contingency planning included here may also be applied to severe disruptions and crises other than the emergency conditions referred to in the Emergency Powers Act. Serious disruptions and crises may, for example, be caused by serious threats to functioning of staff or destruction of a supervised entity's premises or IT environment.

(22) In its decision of 5 December 2013, the Government set general objectives for maintenance readiness. The guidelines for contingency planning issued by the Financial Maintenance Pool in 2009 provide more specific contingency planning objectives and more detailed guidelines for contingency planning.

Guideline (paragraphs 23-30)

(23) The FIN-FSA recommends that supervised entities, based on a risk analysis, consider whether central and significant production systems used for creating services and the know-how for guiding, maintaining, handling and technically supporting them should be exclusively or substantially maintained in Finland or whether it is sufficient that they can be returned to Finland according to pre-planned arrangements.

(24) The FIN-FSA recommends that supervised entities provide standby facilities for ensuring interbank payments, clearing, settlement and custody of securities, and payment of pensions and other regular transactions also in situations where critical systems for these functions are not available in or outside of Finland. In addition, supervised entities should ensure the card payment infrastructure and the functioning of card certification in Finland.

(25) The FIN-FSA recommends that supervised entities ensure that the paralysis or damage of a single function in the IT and data communication systems required for creating central services do not paralyse the whole system. Supervised entities should prepare for disruptions in international and national data communications by establishing standby facilities.

(26) The FIN-FSA recommends that IT systems and data warehouses required for creating central services be geographically separated into at least two places with different risk profiles. Key data and central functions may be moved within the EU area provided that their lawfulness, security and availability for achieving the service objectives defined in this guideline are ensured.

(27) The FIN-FSA recommends that supervised entities secure the key data required for creating services so that the data essential to the continuity of operations can be recovered, if the actual data processing centres or data therein are destroyed. This type of key data includes at least basic data on customers and customer contracts, for example personal data, and data on customers' asset and liability positions. Recovery of data from separate security backup to generally readable electronic format should be tested.

(28) The FIN-FSA recommends that supervised entities' contingency planning also cover outsourced activities in as far as core functions and services must be maintained during emergency conditions. Contingency planning requirements should be taken into account already when outsourcing contracts are drawn up. Supervised entities subject to contingency planning requirements should evaluate contingency plans drawn up by external suppliers and ensure that they meet prevailing requirements. A supervised entity subject to contingency planning requirements should, for example, test an external supplier's contingency plan in joint trial runs with the supplier.

(29) The FIN-FSA recommends that supervised entities subject to contingency planning requirements ensure that they have adequate resources and capacity to maintain their activities in emergency situations and during severe disruptions. Plans for accessing substitute staff and premises should also be made in advance. Availability of substitute resources should be ensured in advance for situations in which a large part of the supervised entity's staff is absent or part of the entity's main premises, hardware and software have been destroyed, or is not otherwise available, or the entity is prevented from carrying out business over a large geographic area.

(30) The FIN-FSA recommends that supervised entities subject to contingency planning requirements should continue their reporting to the authorities also in emergency conditions.

8.4 Emergency plan

(31) An emergency plan is a description of measures, drawn up in advance, by means of which a supervised entity subject to contingency planning requirements ensures that it can continue its operations during severe disruptions in normal conditions as well as in emergency conditions. The emergency plan may be part of the continuity plan, provided that it adequately covers emergency requirements.

Guideline (paragraphs 32-33)

(32) The FIN-FSA recommends that supervised entities maintain an up-to-date emergency plan. Supervised entities subject to contingency planning requirements should regularly test and practice the functioning of the emergency plan. This should be done both separately and together with the other market participants.

(33) The FIN-FSA recommends that supervised entities subject to contingency planning requirements should appoint one or several persons to be responsible for updating and disseminating information on the emergency plan.

9 Reporting to FIN-FSA

9.1 Reporting of disruptions and faults in operations

(1) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulations on regular submission to the FIN-FSA of information on internal control, risk management and disruptions. (Issued on 23 September 2019, valid from 1 January 2020)

Regulation (paragraphs 2-7)

(2) Supervised entities shall without delay submit an initial report to the FIN-FSA of any substantial faults or disruptions in services provided to customers and in payment and IT systems. Substantial disruptions in money transmission and card payments may be, for example, disruptions and delays affecting a large number of customers. Substantial disruptions also include disruptions and deviations related to network and information security or disruptions where customer information has come into the possession of external parties. Disruptions and faults damaging or jeopardising the supervised entity's capacity to continue its business activities or fulfil its obligations shall also be reported to the FIN-FSA without delay. (Issued on 23 September 2019, valid from 1 January 2020).

(3) The report must be identified by “information security” if it concerns an information security deviation and “data protection” if it involves a violation of data protection (Issued on 23 September 2019, valid from 1 January 2020).

(4) Soon after the first report, the supervised entity shall submit a supplementary report to the FIN-FSA with more detailed information on the disruption, and a final report once the root cause of the disruption has been identified. (Issued on 23 September 2019, valid from 1 January 2020).

(5) A report shall be submitted at least for the following disruption types: (Issued on 23 September 2019, valid from 1 January 2020)

- IT system intrusions
- exposure of information to unauthorized parties
- information security breach
- spreading of malicious software to IT systems
- denial-of-service attacks.

A report shall be submitted only on such occasions of exposure of information to unauthorized parties, which also shall be reported to the Data Ombudsman. The supervised entity may, if so decides, to use the same report for both authorities. For denial-of-service attacks only those shall be reported which affect the availability or reachability of the services.

(6) The following disruptions shall also be reported, if they affect the quality of the services provided to the customers:

- software failures
- disruptions in telecommunication

- system downtime
- hardware failures
- delays in money transmission.

(7) Supervised entities providing payment services and persons providing payment services without authorisation shall report significant operational and security disruptions concerning payment services to the FIN-FSA, adhering to EBA Guidelines.[3] Reporting shall cover the information referred to in the Guidelines, and major incident classifications and reporting deadlines according to the Guidelines shall be adhered to in reporting. (Issued on 29 January 2018, valid from 1 March 2018)

Guideline (paragraphs 8-10)

(8) The supplementary report may be submitted using a form available on the FIN-FSA website, disruption form. The form should be sent to the email address hairio@finanssivalvonta.fi. Supervised entities may also use their own internal reporting models, provided they include the information required on the FIN-FSA's reporting form.

(9) Significant operational and security disruptions concerning payment services are reported in accordance with EBA Guidelines. A reporting form is available on the FIN-FSA website. The form should be sent to the email address hairio@finanssivalvonta.fi. A FIN-FSA disruption form, as referred to in paragraph (7), need not be sent separately for these disruptions. (Issued on 29 January 2018, valid from 1 March 2018)

(10) The report submitted to the FIN-FSA does not remove the obligation of the supervised entity to report the exposure of information to unauthorized parties also in accordance with the reporting obligations of the General Data Protection regulation. (Issued on 23 September 2019, valid from 1 January 2020).

9.2 Annual report on losses from operational risk

(11) The report on losses from operational risk that is to be submitted to the FIN-FSA should be prepared on the basis of the supervised entity's internal loss reporting. Guidelines on the reporting of damages due to operational risk are provided in section 4.4.

(12) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulation on regular submission to FIN-FSA of information on internal control and risk management. (Issued on 29 January 2018, valid from 1 March 2018)

Regulation (paragraphs 13-16)

(13) Supervised entities shall, by 28 February, submit an annual report to the FIN-FSA on losses from operational risk detected in the previous year.

---

[3] *EBA Guidelines on Major Incident Reporting under Directive (EU)2015/2366 (PSD2).*

(14) The annual report shall be prepared on the five largest loss events in euro amounts due to operational risk during the course of the calendar year. However, no report need be prepared on damages of less than EUR 10,000.

(15) The report shall include at least the following information:

- event description and damage type according to the classifications defined in section 4.4
- information on measures taken in response to the event
- information on loss amount as well as on insurance indemnity or other compensations.

(16) The annual report shall be prepared using a form available on the FIN-FSA website, damage report. The form shall be sent to the email address opriskivahinko@finanssivalvonta.fi.

Guideline (paragraphs 17-18)

(17) The FIN-FSA recommends that the central body of the amalgamation of deposit banks submit the report on losses from supervised entities within the amalgamation, and that the Local Cooperative Bank Association submit the report on losses from cooperative banks within the association, to the FIN-FSA.

(18) The FIN-FSA recommends that an annual report be also submitted in case there have been no losses. (Issued on 23 September 2019, valid from 1 January 2020).

9.3 Annual assessment of operational and security risks of payment services (Issued on 29 January 2018, valid from 1 March 2018)

(19) By virtue of its regulatory powers referred to in section 2.4, the FIN-FSA issues the following regulation.

Regulation (paragraph 20)

(20) Supervised entities providing payment services and persons providing payment services without authorisation shall submit annually to the FIN-FSA their assessment of operational and security risks as well as risk management measures. A free-form risk assessment shall be submitted by 28 February to the email address operatiivinenriski@finanssivalvonta.fi. The first assessment shall be submitted for 2018 by 28 February 2019.

9.4 Reporting of fraud data related to payment services (Issued on 23 September 2019, valid from 1 January 2020)

(21) In accordance with chapter 3, section 19b(4) of the Act on Payment Institutions, payment institutions and persons providing payment services without an authorisation shall provide statistical data on fraud relating to different means of payment to the Financial Supervisory Authority. By virtue of chapter 3, section 19b(4) of the Act on Payment Institutions, the Financial Supervisory Authority may issue further regulations on this reporting obligation. The provision

also applies, in accordance with chapter 9, section 16(4) of the Credit Institutions Act, to credit institutions providing payment services.

(22) By virtue of Article 16 of Regulation EU) N:o 1093/2010 of the European Parliament and of the Council, the European Banking Authority issued “Guidelines on fraud reporting under Article 96(6) PSD2”. (EBA/GL/2018/05)

Regulation (paragraphs 23-26)

(23) Supervised entities providing payment services and persons providing payment services without authorisation as well as domestic credit institutions providing payment services and foreign credit institutions’ branches providing payment services in Finland must report data on fraud related to payment instruments on an MF form available at the FIN-FSA's Jakelu distribution service. (Issued on 23 September 2019, valid from 1 January 2020).

(24) Payment institutions and credit institutions providing payment services must submit the data to the FIN-FSA semi-annually by 28 February and 31 August. (Issued on 23 September 2019, valid from 1 January 2020).

(25) Persons providing payment service without authorisation must report the data annually by 28 February. (Issued on 23 September 2019, valid from 1 January 2020).

(26) Foreign payment or credit institutions’ branch operating in Finland must submit the data to the FIN-FSA semi-annually by 28 February and 31 August. (Issued on 23 September 2019, valid from 1 January 2020).

Guideline (paragraph 27)

(27) The FIN-FSA recommends that to the extent there are no binding regulations above in this chapter 9.4 on the EBA Guidelines referred to above in paragraph (20), parties falling within the scope of application of this chapter comply with said Guidelines. (Issued on 23 September 2019, valid from 1 January 2020).

9.5 Applying for an exemption from maintaining a contingency mechanism for a PSD2 dedicated interface (Issued on 23 September 2019, valid from 1 January 2020)

(28) By virtue of Article 16 of Regulation (EU) No 1093/2016 of the European Parliament and of the Council, the European Banking Authority (EBA) has issued “Guidelines of the European Banking Authority on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389” (regulatory technical standard on strong customer authentication and common and secure open standards of communication) (EBA/GL/2018/07).

Guideline (paragraph 29)

(29) The FIN-FSA recommends that entities and persons falling within the scope of application of these guidelines comply with the ESA Guideline referred in paragraph (26), which is available at finanssivalvonta.fi. (Issued on 23 September 2019, valid from 1 January 2020).

10 Repealed regulations and guidelines

Upon their entry into force, these new regulations and guidelines repeal the following FIN- FSA standards:

- The FIN-FSA standard 4.4b on management of operational risk
- The FIN-FSA standard RA4.2 on reporting of operational risk events
- Section 9.7 on operational risk management in the FIN-FSA standard 6.1 on the operations of payment institutions and persons providing payment services without authorisation
- Section 4.3.4 on reporting of operational risk events in the FIN-FSA standard RA 6.1 on the operations of payment institutions and persons providing payment services without authorisation

11 Revision history

Since their introduction, these regulations and guidelines have been revised as follows:

Issued on 21 April 2015, valid from 1 July 2015

- the reference to the European Central Bank's Recommendations for the security of internet payments in sections 2.5 and 7 has been replaced by a reference to the Guidelines on the Security of Internet Payments, issued by the European Banking Authority (EBA) on 19 December 2014.

Issued on 6 November 2017, valid from 1 March 2018

- a reference to the Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP), issued by the EBA on 11 May 2017, has been added to section 6.1, thereby changing the numbering of chapter 6.

Issued on 29 January 2018, valid from 1 March 2018

- sections 1.1 and 8.1 have been revised to correspond with provisions of the new Act on the Book-Entry System and Settlement Systems.
- sections 2.1, 2.3, 2.4 and 8.1 have been revised to correspond with the provisions of the new Act on Trading in Financial Instruments.
- section 8.1 has been revised to correspond with the provisions of the amended Investment Services Act (ISA).
- the reference to chapter 7, section 23, subsection 1, paragraph 3 of the ISA has been deleted from section 2.4, because the regulatory power of FIN-FSA included in chapter 7, section 23, subsection 1, paragraph 3 of the ISA has been repealed in connection with the national implementation of the Markets in Financial Instruments Directive ((EU) 65/2014, MiFID II).
- sections 7 and 9.1 have been revised to correspond with the provisions of the revised Payment Institutions Act, thereby changing the numbering of the sections.
- references have been added to the EBA's Guidelines on Major Incident Reporting under PSD2 and Guidelines on the Security Measures for Operational and Security Risks of Payment Services under PSD2, thereby changing the numbering of the sections and adding a new section 9.3

Issued on 23 September 2019, valid from 1 January 2020

- Journal number has been changed (FIVA 22/01.00/2019 instead of FIVA 8/01.00/2014)
- chapter 1.1 has been revised
- chapters 2.1, 2.3, 2.4 and 9.1 have been revised to correspond with the Network and Information Security Directive ((EU) 2016/1148) and national Acts related to its implementation

- chapter 2.2 has been revised to correspond with the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
- chapter 2.5 has been revised by including a reference to European Banking Authority Guideline ((EBA/GL/2018/05) on fraud reporting under Article 96(6) of the PSD2)
- chapter 4.3 has been revised by including a reference to the provisions of chapter 7, section 7 of the Act on Investment Firms on product governance procedures
- chapter 6.2 has been revised by including a guideline on information security audits for online services in paragraph (35)
- numbering in sections 8.3 and 8.4 has been corrected
- chapter 9.1 has been revised concerning the reporting to the FIN-FSA in terms of reporting obligations under the GDPR and guidelines concerning the reporting of disruptions clarified
- chapter 9.2 has been clarified regarding the reporting of losses caused by operational risks
- chapter 9.4 on the reporting of fraud data related to payment instruments has been added
    - regulations related to the collection of fraud data and reporting deadlines have been added
    - reference to Guidelines issued by the European Banking Authority on 18 July 2018 on the reporting of data on fraud related to payment instruments has been added
- chapter 9.5 on applying for an exemption from maintaining a contingency mechanism for a PSD2 dedicated interface has been added
    - reference to Guidelines issued by the European Banking Authority on 4 December 2018 on the conditions to benefit from an exemption from the contingency mechanism has been added