Regulations and guidelines 8/2014

Management of operational risk in supervised entities of the financial sector

Journal Number
FIVA/2024/1666

Issued
4.11.14

Valid from
1.2.15

Further information from:
Digitalisation and Analysis/Payment services and IT supervision

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.

Recommendations and other operating guidelines that are not binding are also 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 Scope of application

These regulations and guidelines apply to the following supervised entities as referred to in section 4 of the Act on the Financial Supervisory Authority (878/2008, FIN-FSA Act):

- credit institutions
- 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
- payment institutions
- the stock exchange
- fund management companies
- investment firms (excluding small and non-interconnected investment firms as referred to in Article 12(1) of the EU Regulation on the prudential requirements of investment firms
- central bodies of amalgamations of deposit banks
- As regards Alternative Investment Fund Managers (AIFM), the regulations provided in the chapter are provided as recommendations.
- These regulations and guidelines apply to the following other financial market participants referred to in section 5 of the FIN-FSA Act, as separately specified in the relevant chapter.
- persons providing payment service without authorisation in accordance with sections 7, 7a and 7b of the Act on Payment Institutions

These regulations and guidelines apply to the Finnish branches of the following foreign EEA supervised entities as referred to in section 6 of the FIN-FSA Act, as separately specified in the relevant chapter:

- foreign credit institutions
- foreign payment institutions
- foreign fund management companies
- foreign investment firms
- foreign Alternative Investment Fund Managers

1.2 Principle of proportionality

These regulations and guidelines are applicable to different kinds of supervised entities, other financial market participants and various governance models. In applying these regulations and guidelines, supervised entities and other financial market participants may take into account the nature, scale, complexity and risks of their activities and other similar factors in considering how to implement the regulations and guidelines appropriately and effectively.

1.3 Definitions

Supervised entity refers to all supervised entities falling within the scope of application of these regulations and guidelines as set out above in chapter 1.1 and as referred to in the FIN-FSA Act.

EEA branch refers to all foreign EEA supervised entities' branches located in Finland and falling within the scope of application of these regulations and guidelines as set out above in chapter 1.1. (*Issued on 1.2.2026, valid from 1.6.2026*).

Operational risk refers to the risk of loss associated with:

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

Operational risk includes legal risk. Strategic risks are here excluded from operational risk. Information and Communication Technology (ICT) risks are included in operational risks: ICT risk management is governed by DORA (Regulation 2022/2554/EU), and these matters are not included in these regulations and guidelines. (*Issued on 1.2.2026, valid from 1.6.2026*).

Controls mean procedures for ensuring that operational objectives are achieved. Controls include all measures taken to prevent, detect and mitigate disruptions, omissions, errors and misuse.

Examples of controls include reconciliations, 'the four eyes principle', comparison of counterparties' confirmations against own contract documentation, as well as various testing and exercises.

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

2 Legal framework and international recommendations

2.1 Legislation

The following legal provisions are related to the matters addressed in these regulations and guidelines:

- Act on the Book-Entry System and Settlement Activities (348/2017)
- Act on Trading in Financial Instruments (1070/2017)
- Act on the Supervision of Financial and Insurance Conglomerates (699/2004)
- Act on the Amalgamation of Deposit Banks (599/2010)
- Act on Alternative Investment Fund Managers (162/2014)
- Act on Credit Institutions (610/2014)
- Act on Payment Institutions (297/2010)
- Act on Payment Services (290/2010)
- Act on Investment Services (747/2012)
- Act on Common Funds (213/2019)
- Emergency Powers Act (1552/2011)
- Ministry of Finance Decree on the Basis for Preparedness Planning by Credit Institutions (71/2025) 6.3.2025/71 (*Issued on1.2.2026, valid from 1.6.2026)*
- Government Decree on the Objectives of Security of Supply (568/2024).

2.2 European Union Regulations

The following European Union regulations are related to the matters addressed in these regulations and guidelines:

- Regulation of the European Central Bank (EU) 795/2014 on oversight requirements for systemically important payment systems (ECB/2014/28)
- 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, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) (*Issued on 23.9.2019, valid from 1.2.2020*)
- Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (hereinafter *DORA*) (*Issued on 1.2.2026, valid from 1.6.2026*)
- Regulation (EU) No 2019/2033 of the European Parliament and of the Council of 27 November 2019 on the prudential requirements of investment firms and amending Regulations (EU) No 1093/2010, (EU) No 575/2013, (EU) No 600/2014 and (EU) No 806/2014 (hereinafter *IFR*) (*Issued on 1.2.2026, valid from 1.6.2026*)

- Commission Delegated Regulation 231/2013/EU supplementing Directive 2011/61/EU of the European Parliament and of the Council with regard to exemptions, general operating conditions, depositories, leverage, transparency and supervision
- Commission Delegated Regulation 2017/584/EU supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying organisational requirements of trading venues (*Issued on 1.2.2026, valid from 1.6.2026*)
- Commission Delegated Regulation (EU) 2018/389 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 (*Issued on 23.9.2019, valid from 1.1.2020*)

2.3 EU Directives

The following European Union Directives are related to the matters addressed in these regulations and guidelines: (*Issued on 23.9.2019, valid from 1.1.2020*).

- Directive 2002/87/EC of the European Parliament and of the Council 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
- Directive 2009/65/EC of the European Parliament and of the Council on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS)
- Directive 2011/61/EU of the European Parliament and of the Council 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
- Directive 2013/36/EU of the European Parliament and of the Council on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC
- Directive 2014/65/EU of the European Parliament and of the Council on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU
- Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market amending Directives 2002/65/EC, 2009/110/EC, 2013/36/EC and 2006/1093/EC and repealing Directive 2007/64/EC
- Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union

2.4 FIN-FSA's regulatory powers

The FIN-FSA's power to issue binding regulations is based on the following legal provisions: (*Issued on 1.2.2026, valid from 1.6.2026*).

- Section 18, subsection 2 of the Act on the Financial Supervisory Authority (878/2008), according to which the FIN-FSA may issue regulations on the regular submission to the FIN-FSA of information on a supervised entity's internal control and risk management.

- Chapter 9, section 24 of the Act on Credit Institutions, according to which the FIN-FSA may issue detailed regulations on operational risk as referred to in chapter 9, section 16.
- In accordance with section 18 of the Act on the Amalgamation of Deposit Banks, the central institution shall meet the requirements set for the parent company of the consolidation group in chapters 7–9 of the Act on Credit Institutions. In accordance with chapter 9, section 1, subsection 3 of the Act on Credit Institutions, the provisions of chapter 9, including section 24, on a credit institution and its risk management shall also apply to the parent company of the credit institution's consolidation group, other undertaking belonging to its consolidation group as well as to risk management of the credit institution's consolidation group.
- In accordance with chapter 5, section 1, subsection 3 of the Act on Common Funds, the FIN-FSA shall issue further regulations on the requirements to be imposed on the risk management systems and other internal control referred to in subsection 1 as well as on sound governance. In accordance with subsection 1 of the section, the management company shall have adequate internal control and risk management systems in proportion to its activities.
- In accordance with chapter 6b, section 2b, subsection 8 of the Act on Investment Services, the FIN-FSA may issue further regulations on the management of the risks referred to in subsection 1. The FIN-FSA may therefore issue regulations on procedures, processes and systems whereby risks to clients and the investment firm, among other things, are identified, measured, managed and monitored. In accordance with section 19, subsection 1 of the Act on Payment Institutions, a payment institution shall have internal governance enabling effective risk management and adequate internal control and risk management systems in proportion to its activities. In accordance with subsection 3 of said section, the FIN-FSA shall issue further provisions required to implement the Payment Services Directive on the organisation of activities.
- In accordance with section 19a, subsection 1 of the Act on Payment Institutions, a payment institution shall establish a sufficient risk management system for managing operational and security risks. In accordance with subsection 3 of said section, the FIN-FSA may issue regulations on the abovementioned risk management systems.
- In accordance with section 19a, subsection 2 of the Act on Payment Institutions, a payment institution shall provide at least annually the FIN-FSA with an assessment of the operational and security risks related to payment services and of the sufficiency of its risk management measures and control mechanisms. In accordance with subsection 3 of said section, the FIN-FSA may issue regulations on the content if the assessment.
- In accordance with section 16, subsection 3 of the Act on the Supervision of Financial and Insurance Conglomerates, the FIN-FSA may issue further regulations to the parent undertaking and holding company of a conglomerate on the organisation of internal control and risk management.
- In accordance with chapter 3, section 36, subsection 1, paragraph 1 of the Act on Trading in Financial Instruments, the FIN-FSA may issue further regulations on risk management referred to in chapter 3, section 1 of the Act in regard to the operational risks of a stock exchange.

2.5 International recommendations

The following guidelines issued by the European Banking Authority (EBA) are related to the matters addressed in these regulations and guidelines:

- EBA Guidelines on internal governance (EBA/GL/2021/05) (*Issued on 16.2.2022, valid from 1.3.2022*)

- EBA Guidelines on ICT risk assessment under the supervisory review and evaluation process (SREP) (EBA/GL/2017/05) (*Issued on 6.11.2017, valid from 1.3.2018*)
- EBA Guidelines on ICT and security risk management (EBA/GL/2025/02) (*Issued on 1.2.2026, valid from 1.6.2026*)
- EBA Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2) (EBA/GL/2018/05) (*Issued on 23.9.2019, valid from 1.1.2020*)
- 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 23.9.2019, valid from 1.1.2020*)

The EBA Guidelines are available on the FIN-FSA website at Finanssivalvonta.fi, and the EBA website at www.eba.europa.eu. (*Issued on 1.2.2026, valid from 1.6.2026*).

Interpretations of regulation (Q&A) published by the EBA are available at www.eba.europa.eu.

3 Objectives

(1) These regulations and guidelines address 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 create a complex operating environment involving operational risk.

(3) Smoothly running payment and clearing systems are important, since most of the payments moving in our economy are transferred and cleared in 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 the following outcomes:

- Supervised entities organise their operational risk management in line with the requirements posed by the scale and nature of their operations.
- If necessary, the risk management tasks may be outsourced in compliance with FIN- FSA regulations and guidelines 1/2012 on outsourcing in supervised entities belonging to the financial sector. (*Issued on 23.2.2012, valid from 1.4.2012*).
- Supervised entities ensure an appropriate level of information management, information security and continuity of operations.
- The FIN-FSA is informed of significant disruptions and errors in supervised entities' operations and of other realised damages and loss events caused by operational risk.

4 General principles of operational risk management

4.1 Scope of application and regulatory powers (*Issued on 1.2.2026, valid from 1.6.2026)*

(1) This chapter 4 applies to supervised entities.

(2) The FIN-FSA's power to issue binding regulations is based on the following legal provisions:

- Section 18, subsection 2 of the Act on the Financial Supervisory Authority (878/2008), according to which the FIN-FSA may issue regulations on the regular submission to the FIN-FSA of information on a supervised entity's internal control and risk management.
- Chapter 9, section 24 of the Act on Credit Institutions, according to which the FIN-FSA may issue further regulations on operational risk as referred to in chapter 9, section 16.
- In accordance with section 18 of the Act on the Amalgamation of Deposit Banks, the central institution shall meet the requirements set for the parent company of the consolidation group in chapters 7–9 of the Act on Credit Institutions. In accordance with chapter 9, section 1, subsection 3 of the Act on Credit Institutions, the provisions of chapter 9, including section 24, on a credit institution and its risk management shall also apply to the parent company of the credit institution's consolidation group, other undertaking belonging to its consolidation group as well as to risk management of the credit institution's consolidation group.
- In accordance with chapter 5, section 1, subsection 3 of the Act on Common Funds, the FIN-FSA shall issue further regulations on the requirements to be imposed on the risk management systems and other internal control referred to in subsection 1 as well as on sound governance. In accordance with subsection 1 of the section, the management company shall have sufficient internal control and sufficient risk management systems in proportion to its activities.
- In accordance with chapter 6b, section 2b, subsection 8 of the Act on Investment Services, the FIN-FSA may issue further regulations on the management of the risks referred to in subsection 1. The FIN-FSA may therefore issue regulations on procedures, processes and systems whereby risks to clients and the investment firm, among other things, are identified, measured, managed and monitored. In accordance with section 19, subsection 1 of the Act on Payment Institutions, a payment institution shall have internal governance enabling effective risk management and adequate internal control and risk management systems in proportion to its activities. In accordance with subsection 3 of said section, the FIN-FSA may issue further regulations on the organisation of activities to implement the Payment Services Directive.
- In accordance with section 19a, subsection 1 of the Act on Payment Institutions, a payment institution shall establish a sufficient risk management system for managing operational and security risks. In accordance with subsection 3 of said section, the FIN-FSA may issue regulations on the abovementioned risk management systems.
- In accordance with section 19a, subsection 2 of the Act on Payment Institutions, a payment institution shall provide at least annually the FIN-FSA with an assessment of the operational and security risks related to payment services and of the sufficiency of its risk management measures and control mechanisms. In accordance with subsection 3 of the section, the FIN-FSA may issue regulations on the contents of the assessment.

- In accordance with section 16, subsection 3 of the Act on the Supervision of Financial and Insurance Conglomerates, the FIN-FSA may issue further regulations to the parent undertaking and holding company of a conglomerate on the organisation of internal control and risk management.
- In accordance with chapter 3, section 36, subsection 1, paragraph 1 of the Act on Trading in Financial Instruments, the FIN-FSA may issue further regulations on risk management referred to in chapter 3, section 1 of the Act in regard to the operational risks of a stock exchange.

4.2 Management of operational risk

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

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

4.3 Organisation of operational risk management

(5) By virtue of its regulatory powers referred to in chapter 4.1 paragraph (2), the FIN-FSA issues the following regulations on the organisation of risk management.

REGULATION (paragraphs 6–7)

(6) The board of directors of a supervised entity shall adopt the policies and procedures for operational risk management, which cover the methodologies and processes for the identification, assessment, control and mitigation of risk. The policies and procedures shall be reviewed on a regular basis, taking into account any changes in the operating environment and in the supervised entity's own business.

(7) The supervised entity shall define operational risk on the basis of its own business activities, considering any special characteristics of its operations. It shall prepare for the materialisation of low-frequency high-severity risk events and describe clearly what it regards as operational risks. (*Issued on 1.2.2026, valid from 1.6.2026*).

GUIDELINE (paragraphs 8–9)

(8) The FIN-FSA recommends that the supervised entity's senior 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.

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

4.4 Identification and assessment of operational risk

(10) By virtue of its regulatory powers referred to in chapter 4.1, paragraph (2), the FIN-FSA issues the following regulations on the organisation of risk management.

REGULATION (paragraphs 11–15)

(11) Supervised entities shall identify operational risks related to all their significant products, services, functions, processes and systems that may have a material impact 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 model where products and services are combined in a new way, unless the supervised entity considers that the previous assessments cover the risks related to the introduction of the new service model.

(13) In the continuous assessment of risks, the probability of the materialisation of the risks, and the impacts in the event of their occurrence, shall be taken into account. In planning its risk management, the supervised entity shall establish 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 which aim to take into account at least the failure of key processes, systems and persons, and the impact of external factors.

GUIDELINE (paragraphs 16–22)

(16) As regards the most important identified operational risks, the FIN-FSA recommends that the supervised entity decide how it will control the risks, whether to 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 an analysis of adverse internal and external factors. Internal factors include, for example, the supervised entity's legal structures, organisational changes, the complexity of the products and services offered, the professional competence and turnover of its staff, and the state of IT systems. External factors include, for example, technological advances and internationalisation of activities.

(18) The FIN-FSA recommends that the supervised entity aim to put in place proactive procedures and indicators for recognising operational risks. The applicable procedures may include standard self-analyses by the supervised organisation, compilation of statistics on risk-related losses, the use of key risk indicators (KRI), and the review of losses incurred by the supervised entity and its peer group.

(19) The FIN-FSA recommends that the supervised entity obtains insurance coverage against financial impacts arising from operational risk. Senior management should ensure that the sufficiency and costs of the insurance coverage are assessed regularly, bearing in mind changes in the supervised entity's business activities. In addition, the assessment should cover counterparty risks arising from the insurance contracts and solvency of the contracting company.

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

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

- a description of products or services
- an assessment of the suitability of products or services for the business strategy
- the geographical market area and target group
- risk mappings (assessments of risks related to the product or service)
- a description of organisation of internal control and risk management for the new product or service
- a review of the processes related to the product or service (for example, offer phase, customer identification, sale, production, settlement and payments)
- legal issues and capacity to enter into contracts
- a description of IT systems, information security and service continuity
- external and internal accounting requirements
- a description of pricing, any valuations, and the use of pricing models
- an assessment of impacts on profitability and capital adequacy
- an assessment of impacts on taxation
- a description of required training and instructions.

(22) The FIN-FSA recommends that supervised entities present significant new products or services to the FIN-FSA well in advance of their roll-out.

4.5 Monitoring of operational risk and loss reporting

(23) Chapter 8 provides guidance on notifying the FIN-FSA of incidents and errors in operations, as well as on the annual reporting of significant operational risk loss events.

(24) By virtue of its regulatory powers referred to in chapter 4.1, paragraph (2), the FIN-FSA issues the following regulations on the organisation of risk management.

REGULATION (paragraphs 25–26)

(25) Supervised entities shall regularly assess the nature of operational risks identified by it and the probability of materialisation of these risks, and monitor realised losses and their amount. Supervised entities shall examine the factors and causalities behind the materialisation of loss events.

(26) The board of directors and senior management of a supervised entity shall receive information on the most significant operational risks across its different business areas. As part of the organisation of internal control, the board of directors shall regularly receive reports on the supervised entity's most significant risks and loss events.

GUIDELINE (paragraphs 27–30)

(27) The FIN-FSA recommends that the information reported includes, for example, a description of the events, underlying reasons, an estimate of direct and indirect costs, and measures for loss prevention. In addition, it is recommended to report the measures taken as a result of the loss, as well as the persons responsible for corrective actions and the implementation schedule.

(28) The FIN-FSA recommends that the senior management of a supervised entity regularly assesses the up-to-datedness, accuracy and appropriateness of the risk management methods and reporting systems. The contents and level of detail of reports as well as their dissemination and reporting frequency should be assessed on a regular basis.

(29) The FIN-FSA recommends that a monetary threshold is defined for materiality in monitoring and reporting, above which events are reported. Even small losses and so-called near misses should be reported if they have fundamental importance for the functioning of risk management.

(30) The FIN-FSA recommends that the monitoring of losses caused by operational risk is organised in accordance with the following table, unless otherwise provided by EU supervisory authorities.

Loss type	Examples
Internal fraud	embezzlement, fraud, receipt of a bribe, securities markets offence or violation, damage, absence of (or acting beyond) powers, misuse of customer information, intentional misreporting of positions, breach of business confidentiality, extortion
External fraud	theft, robbery, fraud (e.g. in use of payment means), forgery, money laundering, intrusion into IT systems, spreading of malicious software, denial-of-service attack on IT systems, bomb threat, threat to staff, extortion
Employment practices and workplace safety	violations of the Employment Contracts Act (working hours, occupational safety), discrimination claims, disputes over wages, compensation or dismissal and labour market disputes
Clients, products and business practices	unlawful and objectionable or misleading marketing and provision of services, misuse of confidential customer information (for example in marketing), neglect of the obligation to disclose information to clients, neglect of secrecy requirements or neglect of the obligation to obtain information, improper execution of orders or handling of client assets, securities markets offence or violation, money laundering
Damage to physical assets	fire, water damage, flood
Business disruption and system failures	software failure, data communication failure, computer downtime, hardware failure, power outage, disruption caused by external service provider
Execution, delivery and process management	reporting error, faulty customer information, data entry errors, pricing errors, contract invalidity, incomplete documentation, document disappearance, collateral management failures, unsuccessful execution of customer assignment, disruption in outsourced service, dispute with external service provider, accounting error

5 Sub-areas of operational risk management

5.1 Scope of application and regulatory powers (*Issued on 1.2.2026, valid from 1.6.2026)*

(1) This chapter 5 applies to supervised entities. The FIN-FSA's power to issue binding regulations is based on the following legal provisions:

- Section 18, subsection 2 of the Act on the Financial Supervisory Authority (878/2008), according to which the FIN-FSA may issue regulations on the regular submission to the FIN-FSA of information on a supervised entity's internal control and risk management.
- Chapter 9, section 24 of the Act on Credit Institutions, according to which the FIN-FSA may issue further regulations on operational risk as referred to in chapter 9, section 16.
- In accordance with section 18 of the Act on the Amalgamation of Deposit Banks, the central institution shall meet the requirements set for the parent company of the consolidation group in chapters 7–9 of the Act on Credit Institutions. In accordance with chapter 9, section 1, subsection 3 of the Act on Credit Institutions, the provisions of chapter 9, including section 24, on a credit institution and its risk management shall also apply to the parent company of the credit institution's consolidation group, other undertaking belonging to its consolidation group as well as to risk management of the credit institution's consolidation group.
- In accordance with chapter 5, section 1, subsection 3 of the Act on Common Funds, the Financial Supervisory Authority shall issue further regulations on the requirements to be imposed on the risk management systems and other internal control referred to in subsection 1 as well as on sound governance. In accordance with subsection 1 of the section, the management company shall have adequate internal control and risk management systems in proportion to its activities.
- In accordance with chapter 6b, section 2b, subsection 8 of the Act on Investment Services, the Financial Supervisory Authority may issue further regulations on the management of the risks referred to in subsection 1. The FIN-FSA may therefore issue regulations on procedures, processes and systems whereby risks to clients and the investment firm, among other things, are identified, measured, managed and monitored. In accordance with section 19, subsection 1 of the Act on Payment Institutions, a payment institution shall have internal governance enabling effective risk management, and adequate internal control and risk management systems in proportion to its activities. In accordance with subsection 3 of said section, the FIN-FSA may issue further regulations on the organisation of activities to implement the Payment Services Directive.
- In accordance with section 19a, subsection 1 of the Act on Payment Institutions, a payment institution shall establish an adequate risk management system for managing operational and security risks. In accordance with subsection 3 of said section, the Financial Supervisory Authority may issue regulations on the abovementioned risk management systems.
- In accordance with section 19a, subsection 2 of the Act on Payment Institutions, a payment institution shall provide the FIN-FSA at least annually with an assessment of the operational and security risks related to payment services and of the sufficiency of its risk management measures and control mechanisms. In accordance with subsection 3 of the section, the Financial Supervisory Authority may issue regulations on the contents of the assessment.
- In accordance with section 16, subsection 3 of the Act on the Supervision of Financial and Insurance Conglomerates, the FIN-FSA may issue further regulations to the parent undertaking and holding company of a conglomerate on the organisation of internal control and risk management.

- In accordance with chapter 3, section 36, subsection 1, paragraph 1 of the Act on Trading in Financial Instruments, the FIN-FSA may issue further regulations on risk management referred to in chapter 3, section 1 of the Act in regard to the operational risks of a stock exchange.

5.2 Processes

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

(3) By virtue of its regulatory powers referred to in chapter 5.1, paragraph (2), the FIN-FSA issues the following regulation on the organisation of risk management.

REGULATION (paragraph 4)

(4) Supervised entities shall identify the most important processes for their business operations. Controls shall be built into the different phases of the processes. The sufficiency of the controls shall be assessed especially whenever the scope or contents of the business or processes change.

GUIDELINE (paragraphs 5–7)

(5) The FIN-FSA recommends that supervised entities 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 traffic.

(6) The FIN-FSA recommends that the key processes for the conduct of business are documented in writing as uniformly as possible, including descriptions of the tasks and phases involved in the process, and their interdependencies and vulnerabilities. The documentation should also cover the flows of information and materials, reporting, and the stakeholders and IT systems related to 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.

(7) The FIN-FSA recommends that the principles applied in the implementation of different projects are as uniform as possible. Risk assessments should be prepared in advance for important projects and initiatives.

5.3 Legal risk

(8) Legal risk may arise from by external factors, such as changes in the operating environment, and from 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 a supervised entity's operations are subject to uncertainties that may result in significant losses and have a bearing on the entity's legal responsibility and liability.

(9) Disputes concerning the validity and contents of contracts may have an adverse impact on a supervised entity's business activities. Exiting from unfavorable contracts and entering into replacement contracts

may involve a risk of loss. This applies in particular to the use of contracts with standard terms. Documents issued by the supervised entity, such as prospectuses and advertisements, may also give rise to liability for damages or the risk of damage to its reputation and goodwill.

(10) By virtue of its regulatory powers referred to in chapter 5.1, paragraph (2), the FIN-FSA issues the following regulation on the organisation of risk management.

REGULATION (paragraph 11)

(11) The board of directors of a supervised entity shall identify the key legal risks related to the activities and ensure that the management of legal risks is organised appropriately.

GUIDELINE (paragraphs 12–16)

(12) The FIN-FSA recommends that supervised entities' senior management organise the management of legal risks and allocates adequate resources the identification, monitoring and mitigation in different business areas.

(13) The FIN-FSA recommends that supervised entities ensure sufficient expertise to manage legal risk in entering into contracts and other legal commitments. Supervised entities should ensure that representatives of the contracting party are entitled to sign the contract.

(14) The FIN-FSA recommends that supervised entities archive contract-related materials in an appropriate manner and monitor the validity of contracts as well as any interpretation disputes or disputes that may arise from them.

(15) The FIN-FSA recommends that supervised entities keep track of changes in both legislation and international regulation so as to be prepared in advance for new legal and regulatory requirements. Supervised entities should know the case law related to their field.

(16) The FIN-FSA recommends that the parent company of a financial and insurance conglomerate ensures that all companies belonging to the conglomerate have adequate knowledge of the provisions and regulations of both sectors. Supervised entities that operate across borders should take into account that key legal principles and case law may vary significantly from one country to another.

5.4 Personnel

(17) By virtue of its regulatory powers referred to in chapter 5.1, paragraph (2), the FIN-FSA issues the following regulations on the organisation of risk management.

REGULATION (paragraphs 18–21)

(18) Supervised entities shall ensure that the professional competence of the persons employed and recruited by them is sufficient and proportionate to their tasks and to the size, scale and nature of their operations.

(19) Supervised entities shall establish procedures to ensure that their staff continuously meet the requirements set for professional competence, such as formal qualifications and sufficient training and

experience. When recruiting new members of staff, special attention shall be paid to reputation and background.

(20) The senior management of a supervised entity shall ensure that sufficient staff is allocated to the performance of the tasks involved. To ensure business continuity, particularly staff in key positions should have deputies in case of sudden termination or interruption of their employment.

(21) Supervised entities shall ensure through appropriate procedures that their employees do not disclose information concerning the financial position or personal circumstances of a client or another person related to the supervised entity's activities, or any business or professional secrets. Such information may only be disclosed if the conditions laid down by law are met.

6 Payment systems and services

6.1 Scope of application and regulatory powers (*Issued on 1.2.2026, valid from 1.6.2026)*

(1) This chapter 6 applies to the following entities and persons:

- Credit institutions providing payment services
- Payment institutions
- Persons providing payment service without authorisation:
- Credit institutions
- Holding companies of credit institutions and investment firms
- Central institutions of amalgamations of deposit banks

(2) The FIN-FSA's power to issue binding regulations is based on the following legal provisions:

- Section 18, subsection 2 of the Act on the Financial Supervisory Authority (878/2008), according to which the FIN-FSA may issue regulations on the regular submission to the FIN-FSA of information on a supervised entity's internal control and risk management.
- Chapter 9, section 24 of the Act on Credit Institutions, according to which the FIN-FSA may issue further regulations on operational risk as referred to in chapter 9, section 16.
- In accordance with section 18 of the Act on the Amalgamation of Deposit Banks, the central institution shall meet the requirements set for the parent company of the consolidation group in chapters 7–9 of the Act on Credit Institutions. In accordance with chapter 9, section 1, subsection 3 of the Act on Credit Institutions, the provisions of chapter 9, including section 24, on a credit institution and its risk management shall also apply to the parent company of the credit institution's consolidation group, other undertaking belonging to its consolidation group as well as to risk management of the credit institution's consolidation group.
- In accordance with chapter 5, section 1, subsection 3 of the Act on Common Funds, the Financial Supervisory Authority shall issue further regulations on the requirements to be imposed on the risk management systems and other internal control referred to in subsection 1 as well as on sound governance. In accordance with subsection 1 of the section, the management company shall have adequate internal control and risk management systems in proportion to its activities.
- In accordance with chapter 6b, section 2b, subsection 8 of the Act on Investment Services, the Financial Supervisory Authority may issue further regulations on the management of the risks referred to in subsection 1. The FIN-FSA may therefore issue regulations on procedures, processes and systems whereby risks to clients and the investment firm, among other things, are identified, measured, managed and monitored. In accordance with section 19, subsection 1 of the Act on Payment Institutions, a payment institution shall have internal governance enabling effective risk management and adequate internal control and risk management systems in proportion to its activities. In accordance with subsection 3 of said section, the FIN-FSA may issue further regulations on the organisation of activities to implement the Payment Services Directive.
- In accordance with section 19a, subsection 1 of the Act on Payment Institutions, a payment institution shall establish a sufficient risk management system for managing operational and security risks. In accordance with subsection 3 of said section, the Financial Supervisory Authority may issue regulations on the abovementioned risk management systems.

- In accordance with section 19a, subsection 2 of the Act on Payment Institutions, a payment institution shall provide the FIN-FSA at least annually with an assessment of the operational and security risks related to payment services and of the sufficiency of its risk management measures and control mechanisms. In accordance with subsection 3 of the section, the Financial Supervisory Authority may issue regulations on the contents of the assessment.
- In accordance with section 16, subsection 3 of the Act on the Supervision of Financial and Insurance Conglomerates, the FIN-FSA may issue further regulations to the parent undertaking and holding company of a conglomerate on the organisation of internal control and risk management.
- In accordance with chapter 3, section 36, subsection 1, paragraph 1 of the Act on Trading in Financial Instruments, the FIN-FSA may issue further regulations on risk management referred to in chapter 3, section 1 of the Act in regard to the operational risks of a stock exchange.

6.2 Payment systems and payment intermediation

(3) In accordance with chapter 9, section 16, subsection 2 of the Act on Credit Institutions, a credit institution shall have adequate, secure and reliable payment, securities and other information systems.

(4) Based on section 19a and 19b of the Act on Payment Institutions, supervised entities providing payment services and persons providing payment services without authorisation shall have adequate risk management procedures for managing operational and security risks in payment services and for monitoring and reporting anomalies and fraud. *(Issued on 29.1.2018, valid from 1.3.2018).*

(5) A payment system in general refers to a system where:

- agreed payment instruments are used
- the participants include credit institutions, payment institutions and clearing houses
- the participants agree on various practices for payment intermediation and risk management
- the transfer of funds from the payer to the payee is made possible.

(6) A clearing system acts as an intermediary for payment transactions in interbank fund transfers and can also provide services related to the settlement of payment transactions.

(7) Payment instrument means a payment card or any other personalised device or procedure, or a combination thereof, which the payment service user and the payment service provider have agreed to use for payment orders.

(8) By virtue of its regulatory powers referred to in chapter 6.1, paragraph (2), the FIN-FSA issues the following regulations.

REGULATION (paragraphs 9–13)

(9) The board of directors of a supervised entity shall approve the payment intermediation 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 cover present activities but also take into account expected developments over the next few years. The board of directors shall set objectives for the activity to ensure and monitor efficient, high-quality and reliable payment intermediation. The clearing systems used by the supervised entity shall also be in line with the objectives.

(10) Senior management is responsible for ensuring sufficient competence, resources and internal control so that payment intermediation can be carried out efficiently and securely. The supervised entity shall map the risks related to the payment intermediation systems and payment services used by it, and update these risk mappings on a regular basis.

(11) The supervised entity's payment intermediation systems shall be reliable and secure. The supervised entity shall ensure that disruptions and delays in the payment intermediation are kept to a minimum. There shall be adequate contingency solutions for handling interbank payment traffic.

(12) 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 the payment services offered. (*Issued on 29.1.2018, valid from 1.3.2018*).

(13) 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 8.5. (*Issued on 29.1.2018, valid from 1.3.2018*)

GUIDELINE (paragraphs 14–15)

(14) The FIN-FSA recommends that supervised entities submit to the FIN-FSA risk assessments concerning new payment services, systems and techniques before they are introduced. Risk assessments should be submitted to the FIN-FSA also before the introduction of significant changes in payment traffic and clearing systems.

(15) The FIN-FSA recommends that supervised entities inform the FIN-FSA well in advance of new payment services, and before introducing significant changes to existing services.

7 Continuity and contingency planning

7.1 Scope of application and regulatory powers (*Issued on 1.2.2026, valid from 1.6.2026)*

(1) Chapter 7.2 applies to supervised entities. The FIN-FSA's power to issue binding regulations is based on the following legal provisions:

- Section 18, subsection 2 of the Act on the Financial Supervisory Authority (878/2008), according to which the FIN-FSA may issue regulations on the regular submission to the FIN-FSA of information on a supervised entity's internal control and risk management.
- Chapter 9, section 24 of the Act on Credit Institutions, according to which the FIN-FSA may issue further regulations on operational risk as referred to in chapter 9, section 16.
- In accordance with section 18 of the Act on the Amalgamation of Deposit Banks, the central institution shall meet the requirements set for the parent company of the consolidation group in chapters 7–9 of the Act on Credit Institutions. In accordance with chapter 9, section 1, subsection 3 of the Act on Credit Institutions, the provisions of chapter 9, including section 24, on a credit institution and its risk management shall also apply to the parent company of the credit institution's consolidation group, other undertaking belonging to its consolidation group as well as to risk management of the credit institution's consolidation group.
- In accordance with chapter 5, section 1, subsection 3 of the Act on Common Funds, the Financial Supervisory Authority shall issue further regulations on the requirements to be imposed on the risk management systems and other internal control referred to in subsection 1 as well as on sound governance. In accordance with subsection 1 of the section, the management company shall have adequate internal control and risk management systems in proportion to its activities.
- In accordance with chapter 6b, section 2b, subsection 8 of the Act on Investment Services, the Financial Supervisory Authority may issue further regulations on the management of the risks referred to in subsection 1. The FIN-FSA may therefore issue regulations on procedures, processes and systems whereby risks to clients and the investment firm, among other things, are identified, measured, managed and monitored. In accordance with section 19, subsection 1 of the Act on Payment Institutions, a payment institution shall have internal governance enabling effective risk management and adequate internal control and risk management systems in proportion to its activities. In accordance with subsection 3 of said section, the FIN-FSA may issue further regulations on the organisation of activities to implement the Payment Services Directive.
- In accordance with section 19a, subsection 1 of the Act on Payment Institutions, a payment institution shall establish a sufficient risk management system for managing operational and security risks. In accordance with subsection 3 of said section, the Financial Supervisory Authority may issue regulations on the abovementioned risk management systems.
- In accordance with section 19a, subsection 2 of the Act on Payment Institutions, a payment institution shall provide the FIN-FSA at least annually with an assessment of the operational and security risks related to payment services and of the sufficiency of its risk management measures and control mechanisms. In accordance with subsection 3 of the section, the FIN-FSA may issue regulations on the contents of the assessment.
- In accordance with section 16, subsection 3 of the Act on the Supervision of Financial and Insurance Conglomerates, the FIN-FSA may issue further regulations to the parent undertaking and holding company of a conglomerate on the organisation of internal control and risk management.

- In accordance with chapter 3, section 36, subsection 1, paragraph 1 of the Act on Trading in Financial Instruments, the FIN-FSA may issue further regulations on risk management referred to in chapter 3, section 1 of the Act in regard to the operational risks of a stock exchange.

(2) Chapters 7.3 and 7.4 of these regulations and guidelines apply to the following supervised entities EEA branches under the obligation to prepare for emergency conditions referred to in the Emergency Powers Act (1552/2011):

- credit institutions
- payment institutions
- investment firms (*Issued on 29.1.2018, valid from 1.3.2018*), providing custody of financial instruments as an ancillary service (*Issued on XX, valid from YY*)
- fund management companies
- alternative investment fund managers (AIFM) providing investment services
- Finnish branches of foreign credit institutions
- Finnish branches of foreign payment institutions
- Finnish branches of foreign investment firms
- Finnish branches of foreign fund management companies.
- the central securities depository
- the stock exchange

7.2 Continuity planning

(3) Continuity planning refers to preparations that enable supervised entities to carry on their operations despite disruptions in business activities and to mitigate losses from various disruptions affecting business activities. Disruptions include damage or intentional acts affecting the supervised entity's staff, premises, IT systems or data communications; water damage, fire or power failure; or outages for example in the supply of electricity, heat or water. In continuity planning, continuity plans are prepared for the most important business areas, on the basis of which operations are continued in the event of a disruption.

(4) By virtue of its regulatory powers referred to in chapter 7.1, paragraph (2), the FIN-FSA issues the following regulations on continuity planning.

REGULATION (paragraphs 5–10)

(5) The board of directors of a supervised entity is responsible for ensuring that the entity’s key businesses are covered by up-to-date and sufficient continuity plans. Senior management shall define the responsibilities for the supervised entity’s business continuity planning. Supervised entities shall have a clear operating model for preparing, maintaining and testing their continuity plans, and for monitoring the state of continuity planning.

(6) Supervised entities shall identify and prioritise their most important business processes. For these processes, recovery times shall be defined, meaning the maximum tolerable downtime before business

operations are affected. For prioritised processes, alternative operating models and recovery procedures shall be planned in the event of operational disruptions. In particular, it shall be ensured that data critical for business recovery can be restored to an up-to-date state.

(7) Supervised entities' continuity plans shall be based on threat and vulnerability analyses of their businesses, that is, assessments of threats, vulnerabilities and risks to data, systems, operations and services.

(8) The business continuity plans shall take into account the various threats and vulnerabilities affecting the operations. The extent of the business continuity plans shall be proportionate to the nature, scale and complexity of the supervised entity's operations. Continuity plans shall guide activities and communications in various disruptions.

(9) A supervised entity shall prepare for disruptions in the operations of external service providers. The continuity plans shall describe the efforts made to prevent external service providers' operational disruptions from affecting the supervised entity's operations and how the supervised entity monitors external service providers' continuity planning. Contracts with external service providers shall require that the providers assess, update and test their systems against operational disruptions.

(10) Continuity plans shall be updated on a regular basis and adapted to changes in the supervised entity's business activities, services and strategies. Continuity plans shall be tested and the activities under them shall be exercised regularly. Responsible persons shall be appointed to monitor the up-to-datedness and testing of the continuity plans.

7.3 Preparation for emergency conditions

(11) The requirement to prepare for emergency conditions is based on the Emergency Powers Act and guidance issued by authorities on preparedness for emergency conditions. Emergency conditions refer to circumstances defined in section 3 of the Emergency Powers Act. Preparation for emergency conditions is based on continuity arrangements for normal conditions.

(12) As a rule, disruptions in emergency conditions last longer than the situations anticipated in continuity plans for normal conditions. In addition, the risks associated with emergency conditions are usually more serious than those for which continuity plans are prepared.

(13) The guidelines for preparedness planning included here may also be applied to severe disruptions and crises other than the emergency conditions defined in the Emergency Powers Act. Severe disruptions and crises may include, for example, a threat that seriously endangers the operational capacity of the supervised entity's staff, or the destruction of its premises or data processing environment.

(14) The Government Decision on the Objectives of Security of Supply currently in force sets out the general objectives of the security of supply. The Finance Sector Pool has drawn up a voluntary preparedness guideline that sector operators can use to support their preparedness.

GUIDELINE (paragraphs 15–22)

(15) The FIN-FSA recommends that supervised entities or EEA branches assess, based on a risk analysis, whether the production systems used for the provision of central and important services, as well as the expertise for their steering, maintenance, system administration and technical support, should be kept

in Finland entirely or in material respects, or whether it is sufficient that they can be restored to Finland through pre-planned arrangements.

(16) The FIN-FSA recommends that supervised entities ensure backup arrangements to secure interbank payment traffic, securities clearing, settlement and custody activities, and the payment of pensions and other recurring payments, even if critical systems for these operations in Finland or abroad are unavailable. In addition, supervised entities should ensure the functioning of card payment infrastructure and card authorisations in Finland.

(17) The FIN-FSA recommends that supervised entities ensure that the failure or damage of any single component in the information and communication systems required to provide critical services does not disable the entire system. Supervised entities should prepare for disruptions in international and national data communication connections through backup arrangements.

(18) The FIN-FSA recommends that the information systems and data repositories required for critical services are geographically distributed to at least two locations with different risk profiles. Key data and central functions may be relocated within the EU area provided that their lawfulness, security and availability are ensured to achieve the service objectives defined in this guideline.

(19) The FIN-FSA recommends that supervised entities ensure that key data required for the provision of services is secured so that data essential to operational continuity can be recovered, even if the actual data processing centres or the data stored in them are destroyed. Such fundamental data includes at least basic customer and customer contract data (including personal data) and data on customers' asset and liability positions. The recovery of data from separate backups into a generally readable electronic format should be tested.

(20) The FIN-FSA recommends that supervised entities' preparedness also cover outsourced activities to the extent required to secure the core functions and services maintained during emergency conditions. Preparedness requirements should be taken into account already when drawing up outsourcing contracts. Entities subject to the preparedness obligation under the Emergency Powers Act should evaluate their service providers' preparedness and ensure that it is consistent with applicable requirements. Entities under the preparedness obligation should test the service provider's preparedness for example in joint trial runs.

(21) The FIN-FSA recommends that entities under the preparedness obligation ensure that they have the resources and capacity needed to maintain their operations in emergency conditions and during severe disruptions. The availability of human resources and backup premises should also be planned in advance. The availability of resources should be secured in advance through preparatory measures for situations where a significant part of staff is unavailable, some of its key premises, equipment and systems have been destroyed or are otherwise unavailable, or operations over a wide area are prevented.

(22) The FIN-FSA recommends that entities under the preparedness obligation maintain regulatory reporting also during emergency conditions.

7.4 Contingency plan

(23) A contingency plan means a pre-established description of the measures by which an entity under the preparedness obligation ensures the continuation of its operations in serious disruptions during normal

times and in emergency conditions. The contingency plan may be part of a continuity plan, provided that the preparedness needs for emergency conditions are sufficiently taken into account.

GUIDELINE (paragraphs 24–26)

(24) The FIN-FSA recommends that supervised entities maintain an up-to-date contingency plan. Supervised entities under to the preparedness obligation should regularly test and exercise the functioning of the contingency plan, both independently and together with other market participants.

(25) The FIN-FSA recommends that supervised entities appoint a person or persons responsible for maintaining the contingency plan and for communicating about it.

(26) The minimum requirements for credit institutions are laid down in Ministry of Finance Decree 2025/71. The FIN-FSA recommends that the other supervised entities listed in chapter 7.1, paragraph (3) should also comply with the following parts of the Decree: (*Issued on 1.2.2026, valid from 1.6.2026*).

- Preparedness planning is based on a risk assessment that addresses at least the threats listed in the Decree.
- A contingency plan describes how the supervised entity prepares in advance for the risks identified in the risk assessment.
- A contingency plan includes an assessment of how the supervised entity has planned its operations located in Finland, at least to the extent required by the Decree.
- The supervised entity describes which capabilities and services it ensures will continue to function in the situations identified in the risk assessment.

8 Reporting to the FIN-FSA

8.1 Scope of application (*Issued on 1.2.2026, valid from 1.6.2026*)

(1) Chapter 8.2 applies to supervised entities as well as to persons providing payment services without authorisation. Chapter 8.3 applies to the following entities and persons:

- credit institutions providing payment services
- payment institutions
- persons providing payment services without authorisation

8.2 Operational disruptions, errors and losses (*Issued on 1.2.2026, valid from 1.6.2026*)

8.2.1 Reporting of operational disruptions and errors

GUIDELINE (paragraphs 2–5)

(2) Supervised entities shall submit ICT incident notifications in accordance with DORA. In addition, the FIN-FSA recommends that all entities referred to in chapter 1.1 notify the FIN-FSA without delay of any disruptions and errors that hinder or endanger their ability to continue business operations or meet their obligations.

(3) The FIN-FSA also recommends that entities forwards to the FIN-FSA any notifications they have submitted to the Office of the Data Protection Ombudsman under the GDPR.

(4) A notification to the FIN-FSA does not remove the entities' obligation to report the disclosure of data to unauthorised parties in accordance with the GDPR reporting obligations. (*Issued on 23.9.2019, valid from 1.1.2020*).

(5) Instructions for submitting the incident and data protection notifications are available on the FIN-FSA website.

8.2.2 Annual report on operational risk losses

(6) In accordance with section 18, subsection 2 of the Act on the Financial Supervisory Authority (878/2008), the FIN-FSA may issue regulations on the regular submission to FIN-FSA of information on a supervised entity's internal control and risk management.

(7) The report on operational risk losses for the FIN-FSA should be prepared on the basis of the supervised entity's internal loss data reporting. Guidelines on the reporting of operational risk loss events are provided in chapter 4.5.

REGULATION (paragraphs 8–12)

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

(9) The annual report shall be prepared on the five largest loss events in euro amount due to operational risk incurred during the calendar year. However, there is no need to report losses below ten thousand euro (€10,000).

(10) The report shall include information at least on the following loss events:

- description of the event and loss type according to the classification in chapter 4.5
- report of measures taken due to the incident
- report of the amount of loss and insurance or other compensations.

(11) The annual report shall be made with the form available on the FIN-FSA's website and submitted according to the instructions available on the FIN-FSA's website. *(Issued on 1.12.2022, valid from 1.1.2023).*

(12) Supervised entities shall submit the annual report even if they had no loss events exceeding the reporting threshold. *(Issued on 23.9.2019, valid from 1.1.2020).*

GUIDELINE (paragraph 13)

(13) The FIN-FSA recommends that the central body of the amalgamation of deposit banks submit the report on losses for supervised entities within the amalgamation to the FIN-FSA. This recommendation means submitting multiple reports at once rather than one combined report. It does not replace the entity-specific reporting obligations.

8.3 Payment services

8.3.1 Annual assessment of operational and security risks of payment services (*Issued on 29.1.2018, valid from 1.3.2018*)

(14) In accordance with section 19a, subsection 2 of the Payment Institutions Act, payment institutions, persons providing payment services under the exemption referred to in section 7 of the Act, and account information service providers referred to in section 7b shall provide the Financial Supervisory Authority annually with an assessment of the operational and security risks relating to the payment services provided and on the adequacy of their mitigation measures and control mechanisms.

(15) What is stated in paragraph (14) also applies, under chapter 9, section 16, subsection 4 of the Act on Credit Institutions, to credit institutions providing payment services.

(16) Pursuant to section 19a, subsection 3 of the Payment Institutions Act, the FIN-FSA may issue further regulations on the content of the assessment referred to in subsection 2.

REGULATION (paragraph 17)

(17) Supervised entities providing payment services and persons providing payment services without authorisation shall submit their assessment of operational and security risks as well as risk management measures annually to the FIN-FSA. A free-form risk assessment shall be submitted by 28 February according to the instructions available on the FIN-FSA's website. *(Issued on 1.12.2022, valid from 1.1.2023).*

GUIDELINE (paragraph 18)

(18) The assessment should specify the operational and security risks of each payment service offered. The FIN-FSA recommends including in the assessment a risk mapping for each payment service, information on identified risk events, and a review of the development work, current status and objectives for the relevant services and systems, from both a systems and risk management perspective. (*Issued on 1.2.2026, valid from 1.6.2026*)

8.3.2 Statistical data to be submitted to the FIN-FSA on fraud relating to payment instruments

(19) Under section 19b, subsection 2 of the Payment Institutions Act, a payment institution, a person providing payment services under the exemption referred to in section 7, and an account information service provider referred to in section 7b shall submit to the FIN-FSA at least annually statistical data on fraud relating to payment instruments..

(20) This obligation also applies, pursuant to chapter 9, section 16, subsection 4 of the Act on Credit Institutions, to credit institutions providing payment services.

GUIDELINE (paragraph 21)

(21) The entities referred to in this chapter shall report statistical data on fraud relating to payment instruments to the Bank of Finland as specified by it. The FIN-FSA receives the statistical data needed for supervisory purpose on fraud relating to payment instruments from the Bank of Finland.

9 Repealed regulations and guidelines

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

- FIN-FSA standard 4.4b Management of operational risk
- Standard RA4.2 on the reporting of operational risk events to the Financial Supervision Authority, issued by the former Financial Supervision Authority (Rahoitustarkastus)
- Chapter 9.7 on operational risk management of FIN-FSA standard 6.1 Operations of payment institutions and persons providing payment services without authorisation
- Chapter 4.3.4 on reporting of operational risk events in FIN-FSA standard RA 6.1 on the operations of payment institutions and persons providing payment services without authorisation

10 Revision history

These regulations and guidelines have been amended after their entry into force as follows:

Issued on 21.4.2015, valid from 1.7.2015

- Reference to the European Central Bank's Recommendations for the security of internet payments in chapters 2.5 and 7 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 6.11.2017, valid from 1.3.2018

- In chapter 6.1 a reference to the EBA Guidelines on ICT Risk Assessment published on 11 May 2017 added, as a result of which the numbering in chapter 6 changed.

Issued on 29.1.2018, valid from 1.3.2018

- Revised chapters 1.1 and 8.1 to correspond with provisions of the new Act on the Book-Entry System and Settlement Systems.
- Revised chapters 2.1, 2.3, 2.4 and 8.1 to correspond with the provisions of the new Act on Trading in Financial Instruments.
- Revised chapter 8.1 to correspond with the provisions of the amended Act on Investment Services
- Removed from section 2.4 a reference to chapter 7, section 23, subsection 1, paragraph 3 of the Act on Investment Services, because the FIN-FSA's regulatory powers included in chapter 7, section 23, subsection 1, paragraph 3 of the Act were repealed in connection with the national implementation of the Markets in Financial Instruments Directive ((EU) 65/2014, MiFID II).
- Revised chapters 7 and 9.1 to correspond with the provisions of the revised Act on Payment Institutions, as a result of which the chapter numbering changed.
- Added to chapters 7 and 9.1 references to EBA Guidelines on Major Incident Reporting under PSD2 and Guidelines on the Security Measures for Operational and Security Risks of Payment Services under PSD2, as a result of which the numbering of the chapters changed.
- Added new chapter 9.3.

Issued on 23.9.2019, valid from 1.1.2020

- Revised chapter 1.1.
- Revised chapters 2.1, 2.3, 2.4 and 9.1 to correspond with the Network and Information Security Directive ((EU) 2016/1148) and national Acts related to its implementation.
- Revised chapter 2.2 to correspond with 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.
- Revised chapter 2.5 by adding a reference to European Banking Authority Guideline ((EBA/GL/2018/05) on fraud reporting under Article 96(6) of the PSD2); revised chapter 4.3 by adding a reference to the requirements on the product governance procedure in chapter 7, section 7 of the Act on Investment Services.

- Revised chapter 6.2 by adding in paragraph (35) a guideline on information security audits for online services.
- Corrected numbering in chapters 8.3 and 8.4.
- Revised chapter 9.1 with respect to reporting to the FIN-FSA concerning GDPR reporting obligations; specified guidelines concerning the incident notification.
- Specified chapter 9.2 regarding the reporting of operational risk losses.
- Added chapter 9.4 on the reporting of fraud data related to payment instruments
    - Added regulations related to the collection of fraud data and reporting deadlines.
    - Added reference to Guidelines issued by the EBA on 18 July 2018 on the reporting of data on fraud related to payment instruments.
- Added chapter 9.5 on applying for an exemption from maintaining a contingency mechanism for a PSD2 dedicated interface.
- Added reference to Guidelines issued by the EBA on 4 December 2018 on the conditions to be met to benefit from an exemption from contingency measures.

Issued on 16.2.2022, valid from 1.3.2022

- Updated the reference in chapter 2.5 to the Basel Committee on Banking Supervision document 'Revisions to the Principles for the Sound Management of Operational Risk'.
- Updated the reference in chapter 2.5 to the EBA's Guidelines on Internal Governance
- Removed from chapter 2.5 the reference to obsolete EBA Guidelines on the security of internet payments.
- Updated the reference in chapter 2.5 to the EBA's Guidelines on Major Incident Reporting
- Removed the reference in chapter 2.5 to obsolete EBA Guidelines to the Security Measures for Operational and Security Risks of Payment Services
- Added to chapter 2.5 a reference to EBA Guidelines on ICT and security risk management.
- Updated the reference in chapter 7, paragraph (14), to EBA Guidelines on ICT and security risk management.
- Updated the reference in chapter 7, paragraph (15), to EBA Guidelines on ICT and security risk management.
- Updated the reference in chapter 9, regulation (7), to EBA Guidelines on Major Incident Reporting.
- Updated in chapter 9 the new guideline on fraud data reporting.

Issued on 1.12.2022, valid from 1.1.2023

- Updated in chapter 9.1 guideline (8) on the submission of an incident notification to the FIN-FSA.
- Updated in chapter 9.1 guideline (9) on the submission of an incident notification concerning payment services to the FIN-FSA.
- Updated in chapter 9.2 guideline (16) on the submission of an annual report to the FIN-FSA.
- Updated in chapter 9.3 regulation (20) on the submission of an annual assessment to the FIN-FSA.

Issued on 1.2.2026, valid from 1.6.2026

- Merged chapters 1.1 and 1.2 into a single 'Scope of application' chapter.
- Supplemented in chapter 1.3 'Definitions' paragraph (6) on legal risks. Paragraph (8) also supplemented.
- Updated references in chapter 2.1 'Legislation'.
    - Act on Common Funds: '48/1999' -> '213/2019'
    - Government Decision: '857/2013' -> '568/2024'
    - Added Ministry of Finance Decree on the Basis for Preparedness Planning by Credit Institutions
- Updated references in chapter 2.2 'European Union Regulations':
    - '2016/1148' -> '2022/2555'
    - Added a reference to DORA.
    - Added a reference to the Regulation on the prudential requirements of investment firms.
    - Added a reference to the Delegated Regulation on the organisational requirements of trading venues.
- Updated references in chapter 2.2 'European Union Directives'
    - Removed 2006/73.
    - Removed 2016/1148.
    - Added 2022/2555 on measures for cybersecurity.
- Updated chapter 2.4 'FIN-FSA's regulatory powers'.
    - Reference to the FIN-FSA Act supplemented with a comment on the submission method.
    - Reference to the powers concerning the amalgamation of deposit banks updated.
    - Reference to the powers concerning Act on Investment Services updated.
    - Reference to the powers concerning the Act on Common Funds updated.
    - Reference to the powers concerning the Act on Alternative Investment Fund Managers removed.
    - Reference to the powers concerning the Act on Payment Institutions updated.
- Reference to a repealed Guideline removed from chapter 2.5.
    - Principles for financial market infrastructures of the Basel Committee on Payment and Settlement Systems and the Technical Committee of the IOSCO (BIS/IOSCO, April 2012)
    - Removed CEBS October 2010
    - Removed BIS August 2006
    - Removed BIS July 2003
    - Removed BIS March 2021

- Removed ESMA February 2012
- Removed EBA/GL/2021/03
- Removed 'Joint position on Manufacturers…'

- Added to chapter 2.5 references used in other regulations and guidelines to the websites of the European Supervisory Authorities.
- Added to chapter 4 a new subchapter 4.1 on the scope of application and regulatory powers.
- Removed from chapter 4.2 (formerly chapter 4.1 on the management of operational risk) paragraph (3). Updated references to regulatory powers in paragraphs (3), (8) and (22) of this document. Removed paragraph (9) of the previous version of the document regarding product governance procedures as unnecessary.
- Added to chapter 5 a new subchapter 5.1 on the scope of application and regulatory powers. Updated references to regulatory powers in paragraphs (4), (11) and (18) of this document.
- Repealed chapter 6 'IT systems and information security', as these matters are regulated by DORA. Updated the chapter numbering accordingly.
- Added to chapter 6 'Payment systems and payment intermediation' of this document a new subchapter 6.1 on the scope of application and regulatory powers. Updated references to regulatory powers in paragraph (8) of this document.
- In addition, references in chapter 6 of this document to paragraphs (14) and (15) of chapter 7 of the previous version regarding EBA guidelines removed, as they do not need to be presented in these regulations and guidelines.
- Added to chapter 7 'Business continuity and contingency planning' a new subchapter 7.1 on the scope of application and regulatory powers. Updated references to regulatory powers in paragraph (6) of this document. In addition, the subchapter 'Legal framework' entirely removed, as legal text does not need to be repeated in these regulations and guidelines.
- Removed the original subchapter 8.1 'Legal framework' in 'Continuity and contingency planning'.
- Removed overlaps with DORA from chapters 7 and 8.
- Added to chapter 8 'Reporting to the FIN-FSA' a new subchapter 8.1 on the scope of application and regulatory powers. Added a new subchapter 8.2 on reports required by DORA. Regulations in chapter 8.3 changed into guidelines and updated to correspond to the reporting of incidents other than those under DORA.
- Added to chapter 8.5 a new guideline in paragraph (23) on the annual assessment of operational and security risks of payment services.
- Added chapter 8.6, which notes that the FIN-FSA needs the aforementioned statistical data on fraud for its supervisory work. The Bank of Finland collects this data and submits it to the FIN-FSA.
- Repealed chapter 9.4 'Reporting of fraud data related to payment services' as obsolete
- Removed chapter 9.5 'Applying for an exemption from maintaining a contingency mechanism for a PSD2 dedicated interface', which contained references to EBA guidelines, as they do not need to be presented in these regulations and guidelines.