Finantsinspektsioon

Optional Guideline of the Financial Supervisory Authority

Tallinn

REQUIREMENTS FOR ORGANISATION OF BUSINESS CONTINUITY PROCESS OF SUBJECT OF FINANCIAL SUPERVISION

This optional guideline has been established with Resolution No. 1.1-7/96 of the management board of the Financial Supervision Authority of 06.12.2006 and amended with Resolution No. 1.1-7/53 of the management board of the Financial Supervision Authority of 04.11.2009 and Resolution No. 1.1-7/41 of the management board of the Financial Supervision Authority of 12.02.2018 pursuant to subsections 57 (1) and (3) of the Financial Supervision Authority Act.

1. Competence

Pursuant to § 3 of the Financial Supervision Authority Act (hereinafter the FSAA), financial supervision is conducted in order to enhance the stability, reliability, transparency and efficiency of the financial sector, to reduce systemic risks and to promote prevention of the abuse of the financial sector for criminal purposes, with a view to protecting the interests of clients and investors by safeguarding their financial resources, and thereby supporting the stability of the Estonian monetary system.

Pursuant to subsection 57 (1) of the FSAA, the Financial Supervision Authority has the right to issue advisory guidelines to explain legislation regulating the activities of the financial sector or to provide guidance to subjects of financial supervision.

2. Purpose and scope of application

The financial system functions as a closely connected network of markets, infrastructures and market participants. The functioning of each link in this network can affect the others and lead to the interruption of the entire financial system, which would affect the entire economy of Estonia.

Business continuity planning is a process used by supervised entities to guarantee the continuity or recovery of their operations, including the provision of services to clients, in the case of extraordinary events. A functional business continuity planning process guarantees that the entrepreneur has prepared for extraordinary interruptions in their business activities that may occur due to reasons independent of themselves and has plans for continuing their operations and reducing potential losses.

Extraordinary interruptions in business operations may be caused by the non-functioning of information systems, problems with the physical location or infrastructures of the subject of supervision, loss of staff or different accidents related to the environment (e.g. a fire).

The objectives of business continuity plans are to save lives and reduce possible injuries, minimise the financial losses of the supervised entities, continue serving clients and financial market participants, reduce the negative impact of the interruption on the strategic plans, reputation, principal activities, liquidity, credit quality and market position of the supervised entities as well as their ability to comply with the requirements arising from legislation.

The purpose of this guideline is to support the planning of a business continuity process that meets the needs of the supervised entities and complies with the requirements set for them.

This guideline establishes the optional and general action guidelines and instructions for the organisation of the business continuity of a supervised entity and the development of business continuity plans, considering the international practice in the relevant area of activity and the recommendations of international organisations.

The recommendations made in this guideline were developed on the basis of international standard ISO 22301 and the document "High-level principles for business continuity" issued by the Basel Committee on Banking Supervision in 2006[1].

The guideline regulates the organisation of the business continuity process of companies regarded as subjects of financial supervision on the basis of subsection 2 (1) of the FSAA. A supervised entity for the purposes of this guideline is an entity regarded as a subject of supervision on the basis of subsection 2 (1) of the FSAA. An insurance specified in subsection 174 (2) of the Insurance Activities Act (hereinafter the IAA), a small fund manager specified in subsection 3 (6) of the Investment Funds Act (hereinafter the IFA), an investment agent specified in subsection 119[1] (1) of the Securities Market Act (hereinafter the SMA) and the paying agent specified in subsection 59 (1) of the Payment Institutions and E-money Institutions Act (hereinafter the PIEIA).

This guideline provides the general requirements for guaranteeing business continuity. The scope of application of the guideline depends on the organisational structure, business volume and risk level of the subject of supervision, as well as the quantity and complexity of the financial services provided and its impact on the financial system as a whole.

Application of these guidelines should take into account the requirements arising from legislation, the instructions arising from the other optional guidelines of the Financial Supervision Authority and the specific characteristics of the supervised entity that implements the guideline alongside the internal organisation of business continuity of the specific subject. In the case of special requirements arising from legislation, the provisions of legislation must be adhered to.

The 'comply or explain' principle must be considered upon the implementation of the guideline, pursuant to which the supervised entities must be able to justify where necessary why they do not implement some points of the guideline or implement them partially.

The principle of reasonability must be proceeded from in the case of interpretation problems, considering the purpose of this guideline, and the supervised entity must act in good faith with the due diligence expected from them.

3. Definitions

Significant business interruption means a disruption or interruption in a system, operation, outsourced service, use of premises, staff, etc., which has exceeded the acceptable level established by the supervised entity and may lead to the interruption of the business processes defined as critical by the subject of supervision.

Recovery plan means a document regarded as a part of the business continuity plan that describes the roles, responsibilities and actions in the recovery of business and other processes after a significant business interruption.

Business continuity means the capability of the supervised entity to continue providing services at the predetermined acceptable levels after a significant business interruption.

Business continuity plan means documented procedures that help supervised entity's to react, continue and recover its operations at the predetermined level after a significant business interruption.

Business impact analysis means the process of analysing operations and the impact that an interruption of business operations could have on them.

4. Place of the business continuity process in the management of risks in the subject of supervision and the role of management

4.1. Business continuity process

4.1.1 Business continuity management must be treated as an inseparable part of the supervised entity's risk management programme, while business continuity management policies, standards and processes must be implemented throughout the organisation.

[1] The Basel Committee on Banking Supervision, the International Organisation of Securities Commissions and the International Association of Insurance Supervisors participated in the development of the document.

4.1.2 Upon the implementation and management of the business continuity process, the supervised entity must guarantee the consideration of the applicable legislation and other relevant requirements in relation to the functioning of the services.

4.1.3 In the development of its business continuity process, the supervised entity must:

4.1.3.1 outline its goals, including the goals related to business continuity;

4.1.3.2 define the external and internal risk factors that increase the risk level;

4.1.3.3 define any risks that must be approached and a suitable approach considering the objectives of business continuity and recovery.

4.1.4 The supervised entity must determine the relevant interested parties in the context of business continuity and their requirements and expectations for the organisation of business continuity.

4.2. Role of management in the business continuity process

4.2.1. The functionality of the business continuity process of a supervised entity is guaranteed by the management board, whose task is to ensure that the entity has up-to-date and adequate business continuity plans for its critical business processes.

4.2.2. The management board must guarantee that principles and objectives, which correspond to the strategy and business model of the supervised entity, have been set for the business continuity process. Business continuity objectives must be measurable, consider the minimal level acceptable to the subject of supervision and the applicable requirements, and be up to date.

4.2.3. The management board of the supervised entity must allocate sufficient resources and appoint competent staff for business continuity planning.

4.2.4. The person appointed to manage the business continuity must be given adequate authorities for the performance of their duties. The management board is advised to form the relevant committee, which is managed by the person responsible for business continuity and organises all of the activities related to business continuity.

4.2.5. A clear framework (policies, rules of procedure, etc.) must be established for the preparation, management and testing of business continuity plans and for training staff.

4.2.6. The management board of the supervised entity must approve the critical business processes determined as a result of business impact analysis and risk assessment (point 5.2 of this guideline) and their priorities, as well as the established recovery objectives. The schedule and results of business continuity tests (point 5.5 of this guideline) must be regularly submitted to the management board and approved by the management board.

4.2.7. The management board of the supervised entity must obtain an overview of the functionality of the business continuity process regularly and not less frequently than once a year. The management board of the supervised entity must be guaranteed regular, at least annual, reporting related to the business continuity process, including the status of implementation and improvement, significant incident reports, testing results and the action plans prepared on the basis of these.

4.2.8. The management board of the supervised entity must guarantee staff training in and awareness of the business continuity process in general and its objectives, as well as the roles of staff in the business continuity process and business continuity plans.

5. Organisation of the business continuity process

5.1. Planning

5.1.1. When planning the business continuity process, the supervised entity must consider the requirements applicable to them and determine the risks and opportunities that must be dealt with for the achievement of the planned objectives and prevention or reduction of undesirable impacts.

5.1.2. The business continuity planning process must be carried out in such a manner that it covers the entire entity. The objective of planning the business continuity of the supervised entity must be to guarantee

the continuity of business activities during significant business interruptions as well as to manage significant business risks via various preventive actions.

5.1.3. A major interruption in the services of a financial market participant may influence the capability of clients and other financial market participants – possibly the whole financial system – to continue with normal business operations. Thus, the scope of the business continuity plans must correspond to the nature, scope and complexity of the operations of the supervised entity.

5.1.4. When planning the achievement of business continuity objectives, the supervised entity must determine responsibilities, activities, the necessary resources, the principles for assessing the effectiveness of recovery activities and the criteria for ending the activity used as a temporary alternative in order to guarantee business continuity.

5.1.5. An efficient business continuity plan is based on the functioning of the business impact and risk assessment processes.

5.2. Business impact analysis and risk assessment

5.2.1. The supervised entity must have functioning process(es) that include systematic assessment of the impact of significant business interruptions on business and other processes as well as possible threats, and ascertaining the most significant risks.

5.2.2. The supervised entity must guarantee that the results of the business impact analysis and risk assessment are up to date. The assessment must be carried out regularly at least once a year and upon significant changes in the business operations of the supervised entity (major organisational changes, launch of new products, introduction of new IT solutions or similar).

5.2.3. The business impact analysis and risk assessment should include, in particular, the following potential event scenarios: problems with information systems; physical faults (buildings, equipment, etc.); loss of human resources; confluence of aforementioned scenarios.

5.2.4. Business and IT employees must be involved in the process in order to carry out the business impact analysis and risk assessment successfully.

5.2.5. The supervised entity must ascertain the following via business impact analysis and risk assessment:

5.2.5.1. critical business processes and the activities that support them;

5.2.5.2. suitable recovery objectives (e.g. scope, time), which would be proportionate to the impact the supervised entity has on the operations of clients and the work of the entire financial system;

5.2.5.3. a prioritised plan for continuing with the aforementioned activities at the determined minimal acceptable level;

5.2.5.4. dependencies and supporting resources for the activities that support the provision of services, including processes, systems, information, staff, assets, suppliers, partners and other stakeholders. The supervised entity must have a detailed overview of the recourses related to the functioning of critical business processes, possible threats and the probability of their materialisation;

5.2.5.5. the risks related to interruptions in services that must be approached and the approach that would correspond to business continuity and recovery objectives.

5.2.6. In respect of outsourcing, the supervised entity must assess the consequences of the possible interruption of the operations of the service provider or other factors that obstruct operations. If necessary, the subject of supervision must receive the relevant input from the service provider, which would allow it to take into account the risks arising from the service provider when preparing its business continuity and recovery plans. The relevant contract must establish requirements for the functioning of services and the capability of recovering services. Detailed requirements for outsourcing are given in the optional guideline of the Financial Supervision Authority “Outsourcing requirements for supervised entities” (see www.fi.ee).

5.3. Establishment and content of business continuity plans

5.3.1. According to the results of business impact analysis and risk assessment, the supervised entity must choose a suitable business continuity strategy for protecting priority operations, stabilising supporting processing and resources, continuation and recovery, mitigating, reacting to and managing impacts.

5.3.2. The supervised entity must determine the requirements for the resources necessary for the implementation of the selected strategies, incl. for people, information and data, buildings and the working environment, information and communications technology (ICT) systems, transport, partners and suppliers.

5.3.3. In the case of identified risks that must be approached, the supervised entity must implement preventive measures that reduce the probability of service interruptions, reduce their length and decrease their impact on services.

5.3.4. The supervised entity must implement and maintain documented business continuity plans based on recovery objectives identified on the basis of business impact analysis in order to manage significant business interruptions and continue with its activities.

5.3.5. The business continuity plan of a supervised entity must be accessible to the people concerned where necessary, have a logical structure and be understandable.

5.3.6. The business continuity plan of a supervised entity must define at least the following:

5.3.6.1. the purpose, scope and objectives of the plan;

5.3.6.2. the conditions of implementation of the plan;

5.3.6.3. implementation procedures;

5.3.6.4. roles, obligations and authorities;

5.3.6.5. communication procedures for internal communication and external communication with significant parties;

5.3.6.6. internal and external dependencies;

5.3.6.7. resource requirements;

5.3.6.8. document management.

5.3.7. Security requirements (physical and data security) must not be left without the necessary attention when business continuity is planned.

5.3.8. The higher the business volume and risk level of the supervised entity and its impact on the financial system as a whole, the more attention the supervised entity must pay to a possible alternative location. The alternative location must be far enough from the main location and may not depend on the same infrastructure components (e.g. power supply, communication channels) as the main location. It must be guaranteed that the alternative location has sufficiently up to date data and the necessary equipment, systems and, where necessary, alternative workplaces to recover and manage critical processes and service during a sufficient time in a situation where the main location is damaged to access to it is restricted.

5.3.9. The business continuity plan must define the staff suitable in terms of the necessary experience and knowledge to guarantee that critical processes and services are recovered during the time set for recovery objectives.

5.3.10. Proceeding from the priorities determined in the business impact analysis and the required recovery times, priorities must be determined for IT systems and applications, and interdependencies and resource requirements must be defined.

5.3.11. The subject of supervision must use suitable IT solutions, whereby adherence with the time criteria defined in the business impact analysis would be guaranteed.

5.3.12. System (incl. IT) recovery plans must be prepared within the scope of business continuity planning, which would describe how various systems can start operating again in the case of a significant business interruptions. The information security policy of the supervised entity and, where necessary, the recovery plans of service providers and partners must be taken into account when IT recovery plans are prepared.

5.3.13. The regulation preservation of backup copies of the electronic data of the supervised entity must be done far enough from the principal IT centre, which guarantees that the data and backup copies do not perish at the same time.

5.3.14. If the supervised entity procures the recovery service from a third party (e.g. an external service provider), the service provider and the correspondence of the provided services and the entity's needs must be thoroughly assessed using unbiased sources of information. If the supervised entity assesses the recovery service too superficially and relies mainly on the information provided by the supplier, this may lead to solutions that may not adequately satisfy the entity's needs when they arise.

5.4. Communication

5.4.1. The supervised entity must develop communication procedures for internal communication and external communication with significant parties. Communication plans must include informing various stakeholders (employees, suppliers, partners, clients, media, supervision) of significant business interruptions (in the context of business continuity) and the status of recovery.

5.4.2. The communication procedures of the supervised entity must:

5.4.2.1. define the person responsible for communication with the staff and external parties;

5.4.2.2. define the possible problems that may emerge during a significant business interruption, e.g. how to behave in the case of primary faults in communication systems;

5.4.2.3. be regularly updated and tested.

5.4.3. In order to avoid a possible reputation risk, the information communicated by the supervised entity to the general public must be timely and sufficient. Standard press releases may be prepared for various situations in order to facilitate the issue of primary information.

5.4.4. The legislation that regulates the operations of subjects of financial supervision stipulates the right of the Financial Supervision Authority to receive information from subjects of financial supervision for exercising supervision.

Based on the above, a supervised entity must notify the Financial Supervision Authority as soon as possible about the identification of an incident related to a significant business interruption, including all of the information about the incidents that is known by the time of notification.

A description of what happened must be submitted to the Financial Supervision Authority not later than three days after the solution of the incident, using general contact details. The forwarded information must include the time, scope and impact of the interruption, the description of its elimination, the reasons and a description of the measures planned to be taken for the prevention of similar incidents in the future and/or for minimising the impact of incidents.

5.4.5. If a subject of supervision sends the information described in point 5.4.4 to the Financial Supervision Authority within the scope of reporting carried out on the basis of legislation, the notification obligation described in point 5.4.4. will be deemed to have been performed.

5.5. Testing of business continuity plans

5.5.1. The relevance and adequacy of the business continuity plans of the supervised entity can be determined only by testing or actual implementation. The supervised entity must test its business continuity plans to be certain of its capability of recovering critical business processes during the determined time and also identify any possible deficiencies in such plans.

5.5.2. Testing of business continuity plans must be carried out regularly. The scope and frequency of testing are defined according to the criticality of the business functions, the role of the supervised entity on the broader market and significant changes in the business or external environment of the supervised entity.

Testing must give the reassurance that the supervised entity is capable of achieving the goals set with business continuity.

5.5.3. The awareness and understanding of the staff of their roles and responsibilities is important in guaranteeing the business continuity and recovering the business processing of the supervised entity. The staff obliged to act in the event of significant business interruptions must be included in the testing of business continuity plans.

5.5.4. The tests of business continuity and recovery plans must be based on scenarios with well-planned and clearly defined targets and objectives.

5.5.5. If the critical business processes or operations of a supervised entity depend on external partners, then significant partners should also be included in business continuity tests.

5.5.6. The results of a performed tests must be properly documented and at least the following information must be recorded: the objective and scope of the test, the time of the test, the resources included in the test, the person who performed the test, the success/failure of the test and the conclusions made from the test.

5.5.7. The results of the test must be analysed and changes must be made in the business continuity plans of the supervised entity on the basis of the analysis results where necessary.

5.6. Updating of business continuity plans

5.6.1. Any changes in the processes, staff and resources of a supervised entity must be recorded in business continuity plans. Recording changes in business continuity plans must be a mandatory part of the change management process of the supervised entity.

5.6.2. The business continuity plans of the supervised entity must be reviewed and updated, where necessary, at least once a year or more frequently where necessary (e.g. after the launch of a new critical business process, infrastructure component, software application, changes in key staff, etc.).

6. Performance assessment

6.1. Regular assessment and improvement

6.1.1. The supervised entity must regularly review its business continuity plans, their relevance and functioning and update them in a timely manner, considering the results of practices, testing and post-incident analysis reports.

6.1.2. A supervised entity must regularly assess the compliance of the implemented business continuity process with the effective legal and regulative requirements and best practices, and its own business continuity objectives.

6.1.3. If a non-compliance is found, the supervised entity must identify it, take measures to manage it and ensure compliance, deal with the consequences and take measures to prevent its reoccurrence.

6.2. Audit

6.2.1. The organisation, compliance and functioning of the business continuity process and the business continuity plans of a supervised entity must be regularly assessed by an internal or external audit.

6.2.2. The importance of the reviewed processes and the results of risk assessment and previous audits must be considered when the frequency of audits is planned.

6.2.3. The scope of internal audit activities must be sufficient to obtain reassurance about the adequacy and efficiency of the organisation of the business continuity process.

7. Implementation

This version of the guidelines enters into force on 01.05.2018.