Advisory Guidelines of the Financial Supervision Authority

Requirements for Organising the Business Continuity Process of Supervised Entities

These advisory guidelines were established by Resolution No 96 of the Management Board of the Financial Supervision Authority of 6 December 2006.

1. Competence

According to § 3 of the Financial Supervision Authority Act (hereinafter FIS), the Financial Supervision Authority conducts state financial supervision 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.

According to FIS § 57 (1), the Financial Supervision Authority has the right to issue advisory guidelines to explain legislation regulating the activities of the financial sector and to provide guidance to subjects of financial supervision.

2. Purpose and scope

The financial system operates as a network of closely interrelated markets, infrastructures and market participants. The activity of each link of the network can influence others and is capable of interrupting the entire financial system, thus impacting on the whole economy.

Business continuity planning is a process through which supervised entities ensure the administration or recovery of their business, including services for customers, upon the occurrence of extraordinary disruptions. A functioning business continuity process shows that an undertaking is prepared for business disruptions that may occur for reasons beyond the undertaking's control, and has plans in place for continuing its operations and reducing potential losses. Business disruptions may be caused by e.g. loss of staff, problems with the physical location or infrastructure of the business, malfunctioning of the undertaking's information systems, various environment-related disasters (e.g. a fire).

The goals of business continuity plans are to save human lives and reduce potential injuries, to minimise the financial losses of supervised entities, to continue servicing customers and financial market participants, to reduce the negative impact of disruptions on the entity's strategic plans, reputation, principal business, liquidity, credit quality, market position, and the ability to comply with the requirements of law.

The purpose of these guidelines is to:

- contribute to the supervised entities' process of preparation and administration of business continuity plans;
- facilitate among supervised entities a uniform understanding of the process of preparation and administration of business continuity plans and the requirements for those plans.

These guidelines establish advisory and general codes of practice, and guidelines for supervised entities for organising their business continuity processes and plans, taking into account international practice in the area and the recommendations of international organisations.

The "High-level principles for business continuity" issued by the Joint Forum[1] in August 2006 were used for developing the recommendations contained herein.

These guidelines contain what the Financial Supervision Authority believes to be the minimum requirements for ensuring business continuity. The scope of application of the guidelines depends on every undertaking's organisational structure, scope and risk level of its business, the quantity and complicacy of the financial services and products offered, and the entity's overall impact on the financial system.

Application of these guidelines should take into account the requirements of law, as well as the other advisory guidelines of the Financial Supervision Authority and the characteristics of the particular supervised entity, as well as the internal organisation of business continuity of the entity. Where the legislation provides for special requirements, these shall be followed.

The "comply or explain" principle should be taken into account in the application of these guidelines: if necessary, a supervised entity shall be able to explain why it is not applying or is only partly applying any of the paragraphs of these guidelines.

The guidelines should be applied, and any interpretation problems should be solved, following the principle of reasonability, taking into account the purpose of these guidelines, and acting in good faith with the diligence expected of a supervised entity.

3. Definitions

Business continuity – a supervised entity's ability to conduct business without disruptions;

Business continuity plan – an integral written activity plan, which is a component of business continuity management, for recovering and continuing business in the event of an unforeseeable business disruption.

[1] The Joint Forum — Basel Committee On Banking Supervision, International Organization Of Securities Commissions, International Association Of Insurance Supervisors, C/O Bank For International Settlements.

Risk analysis – a process, which is a component of business continuity management, of assessing potential risks and their impact on the supervised entity's processes and systems and identifying the major risks.

Business impact analysis – a process, which is a component of business continuity management, of systematically identifying and assessing (qualitatively and quantitatively) the impact of business disruptions on the supervised entity's business processes and other processes. Business impact analysis is used to identify recovery priorities and the resources required for recovery (including staff) and to develop business continuity plans.

Major business disruption – a disruption of a supervised entity's business that exceeds the acceptability level established by the entity (the maximum failure time) and influences the functioning of the business processes that have been defined as critical by supervised entities.

Recovery plan – a document, which is a part of the business continuity plan, that describes the roles, responsibilities and other activities for the recovery of business and other processes after an unforeseeable business disruption.

Supervised entity – a person treated as a subject of financial supervision under FIS § 2 (1) (except for insurance brokers as referred to in § 130 (2) 1) of the Insurance Activities Act).

4. Role of the continuity process in corporate risk management and the role of management

4.1. Business continuity management should be treated as an integral part of a supervised entity's risk management programme, while the management policies, standards and processes should be implemented throughout the organisation.

4.2. The management board ensures that the entity's business continuity process is functioning and has the role of ensuring that the supervised entity has updated and adequate business continuity plans for its critical business processes.

4.3. The management board of a supervised entity is to allocate sufficient resources and appoint competent staff for the development of business continuity plans. The person appointed to manage the business continuity process is to be supplied with sufficient powers to perform his or her obligations. It is advisable that the management board set up a relevant committee, which is led by the person responsible for business continuity and which organises all the activities pertaining to business continuity.

4.4. A clear framework (policies, procedures, etc.) shall be created for the preparation of business continuity plans, their later administration, testing, and staff training, which supplies the management board and supervisory board of the supervised

entity with regular reporting on the business continuity process, covering amongst other things the implementation status, incident reports, test results, and activity plans prepared on their basis.

4.5. The management board of a supervised entity shall review and approve the business continuity plans and their testing results regularly, at least once a year.

4.6. The management board of a supervised entity is responsible for training the staff and ensuring that they are aware of their roles in the business continuity process and plans.

5. Preparation of business continuity plans

5.1. The process of business continuity planning is to cover the entire entity. The supervised entities' goal of business continuity planning is to ensure business continuity in the event of extraordinary disruptions and to recover business and IT systems after such disruptions.

5.2. A major disruption of the business of one participant in the financial system may influence the ability of its customers and other participants in the financial market – possibly also of the financial system – to continue normal business operations. This is why supervised entities shall assess, in the course of risk analysis, the scope of the potential risk they can cause to the entire financial system. The scope of business continuity plans shall correspond to the nature, scope, and complicacy of the entity's business.

5.3. An effective business continuity plan is based on thorough business impact and risk analyses. Business continuity planning begins with defining a supervised entity's critical business processes. Since the availability of the resources needed for complete recovery of the business may be limited, a supervised entity is to use business impact analysis to identify the business functions and activities to be recovered in the first order. Both business and IT staff shall be involved in the process of a successful business impact analysis.

5.4. To recover its critical business functions, a supervised entity shall set appropriate recovery goals (e.g. scope, time) for major business disruptions, which would be proportional to the entity's impact on its customers' activities and the functioning of the entire financial system.

5.5. The management board of a supervised entity should approve the critical business processes and their priorities, which have been identified as a result of the business impact analysis, as well as the recovery goals.

5.6. Supervised entities should conduct a risk analysis to assess the potential risks and their impact on processes and systems. Potential event scenarios may be classified as follows:

- information system problems;
- physical breakdowns (buildings, equipment, etc.);
- loss of human resources;
- the above scenarios in conjunction.

A risk analysis should be conducted periodically at least once per year and upon major changes in the supervised entity's business (major organisational changes, launch of new products, emergence of new customer segments, introduction of new information technology solutions, etc.).

5.7. In order to handle business disruptions, alternative operating models and recovery procedures shall be prepared for the prioritised business processes, and it should be ensured that the critical information required for business recovery can be restored and renewed.

5.8. Based on the priorities set in the business impact analysis and the required recovery times, priorities shall be identified for IT systems and applications, and their mutual dependencies and resource needs defined. Appropriate IT solutions shall be used which ensure compliance with the time criteria defined in the business impact and risk analyses. IT system recovery plans shall be prepared to describe how the various IT systems can be re-launched after a disruption.

5.9. The larger the scope of business and risk level of the supervised entity and the entity's impact on the financial system as a whole, the greater the amount of attention the supervised entity needs to pay to a potential alternative location. The alternative location shall be far enough from the main location and shall not depend on the same infrastructure components (e.g. power supply, communication channels) as the main location. An entity shall keep in mind that the alternative location should have sufficient updated data and the necessary equipment, systems and alternative workstations in order to recover and administer critical processes and services during sufficient time in case the main location is damaged or access to it is limited.

5.10. Since the staff of the main location may be unavailable, the business continuity plan is to define how the entity intends to supply (substitute) staff, which is adequate in terms of numbers and experience/knowledge to ensure the recovery of critical processes and services during the time specified in the recovery goals. Where necessary, the logistical movement of the existing staff from the main to the alternative location shall be covered.

5.11. Security requirements (physical and data security) shall not be overlooked when planning recovery operations.

6. Requirements for the content of business continuity plans

6.1. The business continuity plan of a supervised entity shall contain at least the following components:

- Emergency procedures to ensure the safety of all employees;
- An information services function, the roles and responsibilities of recovery service suppliers, service users, and administrative support staff;
- A list of system resources that require alternatives (hardware, peripheral equipment, software, etc.);
- A list of applications, beginning with the higher priorities, required recovery times and expected performance standards;
- Sufficiently detailed recovery scenarios for step-by-step implementation, beginning with minor and ending with greater losses, and the corresponding responses;
- delimitation of special equipment and supplies (e.g. communication equipment, telephone, etc.) with the defined source and alternative source;
- the existence and announcement of and training in individual and collective roles;
- schedule for testing, last test results, and additional measures taken based on previous test results;
- a list of contractual service provides, services, and expected responses;
- logistical information on the location of important resources, including the alternative location of necessary contracts, customer files, operating systems, applications, data files, operating instructions, and programme, system and user documentation;
- logistical information for transporting important resources, including employees, from the main to the alternative location;
- updated information on key employees – names, addresses, and all telephone numbers;
- alternatives for re-launching business operations (e.g. if the system has been restored at the alternative location, but the user workstations have been completely destroyed).

6.2. The regular backup copies of the electronic data of a supervised entity shall be stored at a sufficient distance from the main IT centre so as to ensure that the data and the backup copies are not destroyed simultaneously.

6.3. Where the supervised entity requires non-electronic data (e.g. hardcopy contracts, etc.) to conduct critical business processes, such backup copies shall be stored at a sufficient distance from the main location of data and they shall be available at the alternative location.

6.4. If the supervised entities outsource recovery services to a third party (e.g. an external service provider), the service provider and extent to which the services cover the entity's needs shall be thoroughly assessed using objective sources of information. Where the supervised entities are too superficial in assessing the recovery service and rely mainly on the supplier's information, this may lead to solutions that might not adequately cover the entity's needs as they arise.

Detailed requirements for outsourcing are covered by the **advisory guidelines of the Financial Supervision Authority "Outsourcing Requirements for Supervised Entities"** (see www.fi.ee).

6.5. The business continuity plans of supervised entities shall clearly specify liabilities and powers of action.

7. Communication

7.1. Supervised entities shall include in their business continuity plans the communication procedures for internal communication and external communication with key parties. Communication plans shall cover informing the various interest groups (employees, suppliers, business partners, customers) of the crisis situation (in the business continuity context) and the recovery status. The Financial Supervision Authority has to be informed, as one of the parties, using the general contact details.

7.2. A supervised entity's communication procedures (crisis communication) should:

- identify the person responsible for communication with the staff and external parties;
- identify the potential problems that may arise during major disruptions, e.g. how to behave if the primary communication systems break down;
- be regularly updated and periodically tested.

7.3. To avoid any potential risk to their reputation, a supervised entity shall give timely and sufficient information to the public. Standard press releases may be prepared to simplify the dissemination of primary information.

7.4. Considering the scope of these guidelines as provided in paragraph 2 hereof, § 3 of the financial Supervision Authority Act which defines the objective of financial supervision, and based on § 99 (1) 1) of the Credit Institutions Act, § 170 (1) 1) of the Insurance Activities Act, § 286 (1) 1) and 4) of the Investment Funds Act, and § 230 (1) of the Securities Market Act, under which the Financial Supervision Authority may request information, documents and explanations for performing supervision, supervised entities are required to inform the Financial Supervision Authority of major business disruptions at the earliest opportunity.

Not later than within three working days after solving the problem, a description of the event shall be submitted to the Financial Supervision Authority using the general contact details and specifying:

- the time of the disruption;
- the scope and impact of the disruption;
- a description of how the disruption was treated;
- the reason for the disruption;
- measures to be taken to avoid similar events in the future.

8. Testing and administration of business continuity plans

8.1. The relevance and adequacy of supervised entities' business continuity plans can be determined only by way of testing or actual implementation. Supervised entities shall test their business continuity plans to be certain of their ability to restore the business processes during the specified time, while identifying any shortcomings in the plans.

8.2. Business continuity plans shall be tested regularly. The scope and frequency of testing shall be determined depending on the criticality of the business functions, the entity's role on the wider market, and significant changes in the entity's business or external environment.

8.3. The staff's awareness and understanding of their roles and responsibilities is important for ensuring the business's continuity and recovering the business processes of a supervised entity. Business continuity plans shall be tested with the involvement of the staff whose duty it is to act in the event of major disruptions.

8.4. By virtue of paragraph 4 of these guidelines, according to which business continuity management is an integral part of a supervised entity's risk management programme, a document on the time schedule of the planned tests shall be submitted to the Financial Supervision Authority once per year and the Authority shall be informed of the main results of the test after the test results have been analysed. The testing schedule shall be submitted at least one month before the tests and test results shall be submitted not later than one month after the test. The document shall contain at least the following information:

- the name of the supervised entity to conduct the test;
- the time of testing;
- the reason for testing (scheduled or non-scheduled, with reasoning);
- scope of testing (organisation covered, processes covered, etc.);
- expected/achieved results along with conclusions.

8.5. The results of completed tests shall be duly documented and contain at least the following information: the purpose, scope, and time of the test, resources involved, the performer and results of the tests.

8.6. The test results shall be analysed and, based on the analysis results, changes shall be made in the supervised entity's business continuity and recovery plans.

8.7. Any changes in a supervised entity's processes, staff, and resources, shall be reflected in the business continuity plan. Reflecting changes in the business continuity plan shall be a mandatory part of the entity's change administration process. Changes are reflected in the business continuity plan together with the conduct of the risk analysis (see paragraph 5.6 above).

8.8. Internal or external audit of a supervised entity's business continuity plan shall be conducted regularly.

8.9. A supervised entity's business continuity plan shall be reviewed and, as necessary, supplemented or amended at least once a year or more frequently if needed (e.g. after the launch of a new critical business process, infrastructure component, software application; upon changes in key employees, etc.); see also paragraph 4.5 above.

9. Implementation

9.1. These guidelines shall enter into force from 1 March 2007.

9.2. Clause 12 of the Financial Supervision Authority's advisory guidelines "Requirements regarding the arrangement of operational risk management" and clause 15 of the advisory guidelines "Requirements for the organisation of the field of information technology" are repealed by the adoption and entry into force of these guidelines.