Advisory Guidelines of Financial Supervision Authority

Requirements for the organisation of the field of information technology

Advisory guidelines have been laid down by decision No. 44-4 of the management board of the Financial Supervision Authority of 22.9.2004 pursuant to subsection 57 (1) of the Financial Supervision Authority Act, advisory guidelines' changes have been laid down by decision No. 1.1-7/51 of the management board of the Financial Supervision Authority of 04.11.2009.

Part I General provisions and definitions

1. Objective and application of advisory guidelines

1.1. The activity of entities in the financial sector depends, to a great extent, on information technology ("**IT**"). The objective of these guidelines is to lay down minimum requirements for the organisation of work in the field of information technology in entities in the financial sector, in order to increase the efficiency of the financial sector and to decrease systemic and operational risks.

1.2. These guidelines regulate the organisation of work in the field of information technology in the subjects of financial supervision listed in subsection 2 (1) of the Financial Supervision Authority Act.

The instructions provided in the guidelines shall be followed in compliance with the requirements provided in legislation.

1.3. The management objectives stated in the internationally recognised information technology auditing and management standard COBIT (*Control Objectives for Information and Related Technology*), and its short version COBIT *Quickstart*, served as the basis for compiling these guidelines. The management objectives of COBIT have been supplemented and specified with the requirements and definitions included in standards concerning information technology (BS:7799, EVS- ISO/IEC 2382).

1.4. The information technology management system or framework of a financial sector entity shall be created in such a manner that it provides a suitable level of support for business processes. The information systems of an entity shall correspond to the requirements of availability, integrity and confidentiality deriving from business activities. The implementation of these guidelines in an entity depends, first and foremost, on the size of the entity, complexity of processes, number of employees or the technology used.

2. Definitions used in the guidelines

2.1. Data – presentation of re-interpretable information in a formalised form that is suitable for transmission, interpretation or processing.

2.2. Data element – a data unit that in certain contexts is regarded as indivisible.

2.3. Data model – description of the organisation of data in a manner that reflects the information structure of an entity.

2.4. Information – knowledge that concerns objects, e.g., facts, events, things, processes or ideas, including definitions, and that has a specific meaning in a certain context.

2.5. Information system – information processing system providing and distributing information together with accompanying legal solutions and organisational resources, including human, technical and financial resources.

2.6. IT security – protection of information in order to ensure:

- confidentiality – protection of information against unauthorised public disclosure;
- integrity – protection of information against counterfeiting and unauthorised alteration;
- availability – timely and regular availability of information and services for authorised persons.

2.7. Information assets – information, data and the applications necessary for their processing.

2.8. Owner of information assets – an employee of an entity who is liable for the security and maintenance of information assets, and whose tasks, among others, include classification of data and determination of user’s rights.

2.9. Sensitive information – information that, according to the decision of a competent authority, shall be protected as its public disclosure, alteration, destruction or loss would cause significant damage to somebody or something.

2.10. Security incident – an event, the result of which is (or may be) violation of information security.

Part II Planning and organisation

3. Strategy

3.1. The basis of the information technology activities of an entity shall be the strategy deriving from business objectives and strategy of the entity approved by the management of the entity (IT strategy). In developing IT strategy it shall be assessed which information technology support is necessary for achieving the business objectives of the entity and support for financial supervision, and whether the existing IT solutions enable the achieving of the desired business result. Development plans shall be compiled and the priorities and investments of IT projects shall be determined on the basis of the IT strategy.
Amended by decision No. 1.1-7/51 of the management board of the Financial Supervision Authority of 04.11.2009.

3.2. The IT strategy shall be updated and supplemented regularly according to the changes in the business strategy of an entity or the development trends of information technology. The IT strategic planning process shall include the heads of both business as well as the IT spheres of responsibility of an entity.

4. Information architecture

4.1. An entity shall have general rules for determining the owners of information assets and classifying information assets into security classes, and owners shall be appointed for all information assets. Depending on the security class of data, relevant access restrictions shall be imposed on the data.

4.2. Security levels shall be established, introduced and implemented for each security class of information assets of an entity. Security levels shall provide minimum requirements for security and control measures that are to be regularly inspected and supplemented, if necessary.

4.3. Management shall lay down the procedures for determining the security classes of information assets. The owner of a relevant information asset shall be liable for the classification of information assets and imposition of access restrictions.

5. IT organization

5.1. In order to provide the information technology support necessary for business processes, an entity shall have an IT organisation suitable in terms of size and competence. If the information technology know-how is outsourced, it is necessary to determine the areas where and by whom such outsourcing can be used and by whom and how the services ordered from outside are administered.

5.2. An entity shall establish relevant procedures for recruiting IT personnel that enable the assessment of the suitability of a person for a position. In addition to professional competence, the field of operation of the entity and the need to work with sensitive information shall be taken into account.

5.3. The IT organisation of an entity shall have a clearly defined structure and tasks. It is necessary to ensure the existence of necessary resources for the performance of these obligations. Employees shall possess clearly defined and required skills, rights, liability and obligations, and these shall be reviewed regularly.

5.4. An entity shall implement the separation of the functions of information technology development, maintenance, use and control. If the introduction of the separation of duties of employment proves to be impossible, additional controls shall be implemented for risk management.

6. Management of IT investments

6.1. For the optimal management of information technology related expenditures corresponding to business objectives, the management of IT investments shall be carried out through a periodical budgeting process.

6.2. Management shall analyse the IT situation of the entity at least once a year. It is recommended to regularly review the prudent use of IT resources for the support of business strategies and to approve the budget for the following period.

7. Compliance with external requirements

7.1. The management of an entity shall ensure the regular assessment of the compliance of the IT organisation of an entity with external requirements (laws, regulations, etc.) and consideration of their effects. Measures shall be taken for bringing the IT organisation into compliance with external requirements, if necessary.

8. Risk management

8.1. The management of an entity shall ensure the functioning of the risk management process connected to information technology that would determine risk management methodology, reporting requirements and control mechanisms. It is necessary to ensure regular risk assessment updates and the continuity of the risk management process.

8.2. Expenditures on IT security and IT services should be justified with risk assessments and cost-effectiveness assessments. In the course of risk analysis, it is necessary to determine any possible threats or weaknesses, to assess the likelihood of the realisation of threats and the damage accompanying them, to choose suitable measures for reducing the effect of realisation of threats, to assess their cost-effectiveness and determine the size of acceptable residual risk.

8.3. Risk assessment shall accompany any major changes in information systems or processes. In planning any changes to an information technology system it shall be determined whether and how the change influences the security of the system and the process and to reduce in every way the effect of risks that accompany the change.

9. Project management

9.1. Each important development project in the field of information technology shall have a specified and measurable objective, and a specific commencement date and end date. The development of an information system shall derive from the needs of the entity, and the decision regarding the initiation of projects shall be made by the management on the basis of the approved IT strategy.

9.2. A project organisation shall be established for the implementation of each project. The course, budget and time-scheme of the project shall be constantly monitored.

Part III Acquisition and implementation

10. System development

10.1. In order to create suitable solutions for meeting business requirements it is necessary to determine user requirements and assess alternative solutions beforehand. The decision of management regarding the initiation of the development project and the choice of an alternative solution shall be based on the cost-benefit analysis that indicates the technical, operational and economic justification of the project.

10.2. The separation of the development, testing and production environment shall be guaranteed when developing application software.

10.3. In developing a solution it is necessary to specify the functional and operational requirements of the solution, including maintenance, performance, reliability, monitoring, security and compatibility with existing systems. Testing standards and acceptance criteria of the system shall be defined clearly. System requirements, standards, acceptance criteria and intellectual property rights shall also be fixed upon ordering development from external service providers.

11. Management of procedures

11.1. Documented work instructions and procedures shall be laid down for the management and use of the information system. Upon making changes in the information system, relevant procedures shall also be reviewed and the users shall be notified of the changes made.

12. Change management

12.1. The correctness, compliance with legal acts and controllability of the execution of changes shall be guaranteed for the reduction of the likelihood of any disruptions and errors and reduction of likelihood of conflict with legal acts that may arise from the changes to the information system. An action plan shall be compiled for the execution of changes. An audit trail shall remain from the execution of changes that would enable the identification of the time of the execution of the change, the executer and content of the change.
Amended by decision No. 1.1-7/51 of the management board of the Financial Supervision Authority of 04.11.2009.

12.2. Upon executing and planning changes to an information technology system, it shall be determined if and how the changes affect the security of the system. A prior analysis for determining new security requirements is necessary, in case of major changes regarding the acquisition of new hardware, software or service. Any planned changes in the hardware and software of the system shall be tested beforehand. The execution of emergency and planned changes shall be approved.

12.3. In case the integrity or availability of information, in comparison with that of the entity for the period prior to the performance of the action, is violated as a consequence or possible consequence of a change to the information system by an administrative act or proceeding of an agency performing financial supervision or an investigating agency, then the entity shall present to the corresponding performer of financial supervision or the investigating agency a motivated explanation regarding the changes and the legal protection measures or other actions implemented regarding the information asset owner.

Changed by decision No. 1.1-7/51 of the management board of the Financial Supervision Authority of 04.11.2009.

Part IV Delivery and support

13. Use of external service providers

13.1. Selection procedures for external service providers shall be implemented in the entity that would ensure the use of a functioning and efficient service for the entity.

13.2. The procedures of an entity shall ensure that contracts are concluded with all external service providers and that regular review of the compliance of provided services with the terms and conditions of the contract and the needs of the entity is carried out.

13.3. All external service providers shall be identified and any organisational relationships and technical interfaces with them shall be documented.

13.4. No access shall be granted to external service providers to the means of the organisation until the necessary security measures have been taken and a contract specifying access conditions has been signed.

14. Volume and performance management

14.1. An entity shall have an operating process for the monitoring of the performance of the information system and for reporting. Requirements of users on the availability and performance of the information system shall be determined and reviewed regularly. Timely meeting of performance needs of the information system shall be guaranteed on the basis of the results of monitoring of the performance of the existing system and the forecast of future performance needs.

15. Operation continuity

15.1. Codes of practice and guidelines for the supervised entity’s business continuity process and business continuity planning are covered by the advisory guidelines of the Financial Supervision Authority “Requirements for Organising the Business Continuity Process of Supervised Entities”, established 06.12.2006 with management decision no 96.
Amended by decision No. 1.1-7/51 of the management board of the Financial Supervision Authority of 04.11.2009.

16. Systems security

16.1. Codes of practice and guidelines for the information security process are covered by the advisory guidelines of the Financial Supervision Authority "Requirements for the organization of the field of information security", established 04.11.2009 with management decision no 1.1-7/52.
Amended by decision No. 1.1-7/51 of the management board of the Financial Supervision Authority of 04.11.2009.

17. Configuration management

17.1. An entity shall have a complete and regularly updated list of inventory of the information technology hardware and software configuration used. The hardware and software platform used shall be standardised, if possible.

17.2. An entity shall lay down requirements that would preclude the use of unauthorised and unlicensed software. An entity shall perform routine checks for the discovery of unauthorized software and for the control of conformity with licence agreements.

18. Problem and incident management

18.1. Official procedures and duties shall be laid down for the reduction of damages resulting from security attacks, emergencies and system failures, for the registration of security incidents, response to those incidents and the drawing of conclusions from them.

18.2. Notification procedure in regard to different types of security incidents (violation of security, threat, defect or failure) that may affect the security of the assets of an organisation shall be communicated to all relevant employees and contract partners. Relevant security points shall be notified of any discovered or suspected security incidents as soon as possible.

19. Facility management

19.1. Codes of practice and guidelines for the information security process are covered by the advisory guidelines of the Financial Supervision Authority "Requirements for the organization of the field of information security", established 04.11.2009 with management decision no 1.1-7/52.
Amended by decision No. 1.1-7/51 of the management board of the Financial Supervision Authority of 04.11.2009.

20. Operations management

20.1. Main standard IT operations shall be documented and reviewed regularly in order to ensure systematic processing (in terms of timing, order, quality, etc.). Operations logs shall be checked in order to ensure the correctness and integrity of processing.

Part V Monitoring

21. Monitoring and assessment

21.1. Requirements for the control and assessment of information technology activities shall be provided for in an entity. It is necessary to assess whether internal requirements of the entity, efficiency of IT services and correspondence of IT activities to business objectives have been followed in information technology activities. Independence of the assessment shall be ensured in providing the assessment.

21.2. An external audit shall be used, if necessary, for the assessment of compliance of information technology controls, laws and regulations concerning information technology and the performance of contractual obligations in the field of information technology. Assessment results shall be presented to the management of the entity.

Part VI Final provisions

22. Entry into force of guidelines

22.1. The guidelines shall enter into force on 1.1.2005.

22.2. The changes shall enter into force on 01.12.2009.