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.

Part I General provisions and definitions

1. Objective and application of advisory guidelines

1.1. The activities of companies of the financial sector depend 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 the companies of 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 are to be followed in compliance with the requirements provided in legislation.

1.3. The control objectives stated in COBIT (*Control Objectives for Information and Related Technology*) and its short version COBIT *Quickstart* served as the basis for compiling these guidelines. The control 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 control system or framework of a company of the financial sector must be created so that it would provide a suitable support for business processes. The information systems of a company must correspond to the requirements of availability, integrity and confidentiality deriving from business activities. The implementation of these guidelines in a company depends first and foremost on the size of the company, complexity of processes, number of employees or the technology used.

2. Definitions used in guidelines

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

2.2. Data element – a data item 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 a company.

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 publication;
- integrity – protection of information against counterfeiting and unauthorised alteration;
- availability – timely 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 a company 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, must be protected as its publication, 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 information technology activities of a company must be the strategy deriving from business objectives and strategy of the company approved by the management of the company (IT strategy). In developing IT strategy it must be assessed which information technology support is necessary for achieving the business objectives of the company and whether the existing IT solutions enable to achieve the desired business result. Development plans must be compiled and the priorities and investments of IT projects must be determined on the basis of the IT strategy.

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

4. Information architecture

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

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

4.3. The management must 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 organisation

5.1. For providing information technology support necessary for business processes, a company must 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. A company must establish relevant procedures for recruiting IT personnel that enable to assess the suitability of a person for a position. In addition to professional competence, the field of operation of the company and the need to work with sensitive information must be taken into account.

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

5.4. A company must 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 must be implemented for risk management.

6. Management of IT investments

6.1. For the optimal management of information technology expenses that would correspond to business objectives, the management of IT investments must be carried out through a periodical budgeting process.

6.2. Management must analyse the IT situation of the company 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 a company must ensure the regular assessment of the compliance of IT organisation of a company with external requirements (laws, regulations, etc.) and consideration of their effects. Measures must be taken for bringing IT organisation into compliance with external requirements, if necessary.

8. Risk management

8.1. The management of a company must 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. Expenses of 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, weaknesses, to assess the likelihood of realisation of threats and damages resulting from 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 must accompany any major changes in information systems or processes. In planning any changes to an information technology system it must 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 must have a specified and measurable objective and a specific commencement date and end date. The development of an information system must derive from the needs of the company and the decision regarding the initiation of projects must be made by the management on the basis of the approved IT strategy.

9.2. A project organisation must be established for the implementation of each project. The course, budget and time-scheme of the project must 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 the management regarding the initiation of the development project and the choice of an alternative solution must be based on the cost-benefit analysis that indicates the technical, operational and economic justification of the project.

10.2. The separation of development, testing and production environment must be guaranteed in 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 must be defined clearly. System requirements, standards, acceptance criteria and intellectual property rights must also be fixed upon ordering development from external service providers.

11. Management of procedures

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

12. Change management

12.1. The correctness and controllability of the execution of changes shall be guaranteed for the reduction of the likelihood of any disruptions and errors that may arise from the changes in the information system. An action plan must be compiled for the execution of changes. An audit trail must remain from the execution of changes that would enable to identify the time of the execution of the change, the executer and content of the change.

12.2. Upon executing and planning the changes in an information technology system it must 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 must be tested beforehand. The execution of emergency and planned changes must be approved.

Part IV Delivery and support

13. Use of external service providers

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

13.2. The procedures of a company must 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 company is carried out.

13.3. All external service providers must be identified and any organisational relationships and technical interfaces with them must 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. A company must 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 must be determined and reviewed regularly. Timely meeting of performance needs of the information system must 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. A company must have a working operation continuity planning process that takes into account the critical nature of business processes and ensures the development of continuity plans.

15.2. Planning of operation continuity must cover the measures for identifying and decreasing risks, reduce possible consequences of an accident and ensure fast continuation of important operations.

15.3. In order to ensure their efficiency and relevance, operation continuity plans must be tested regularly and updated, if necessary.

15.4. A company must have documented and introduced procedures for making back-ups and guaranteed regular making of back-ups. Back-ups must be made regularly and they must be stored in a separately located storage room that prevents unauthorised access and guarantees physical protection of back-ups. One back-up copy must regularly and securely be stored in a location geographically separate from the building where back-ups are made. The fitness for use and integrity of back-ups must be checked periodically.

16. Systems security

16.1. General principles of IT security of a company must be fixed in IT security policy. The management must give the policy a certain direction, show support and provide help to ensuring IT security in the organisation. IT security policy must state the definition of IT security, indicate the measures with which IT security is ensured, who is responsible for IT security and also a reference to the action plans and procedures laid down in the company that support the implementation of IT security. It is advisable to delegate liability for the coordination of IT security to one member of the management.

16.2. The confidentiality requirements, security roles and liability stated in the IT security policy of an organisation must be fixed for every employee.

16.3. For the regulation of access privileges a company must implement official procedures that cover access to all phases of the life cycle from initial registration of new users to the final log-off of the users that no longer need information services. Access to data and information must be limited to persons who need this for the performance of their official duties. Granting of access privileges must be coordinated with the owner of information assets. Granted access privileges must be documented and based on the will of the owner of information assets. Correspondence of documented access privileges with actually granted ones must be checked regularly.

16.4. Prior to granting access to information services for users, they must receive relevant training in the field of both organisation policies and procedures (including security requirements and other operating mechanisms) as well as correct use of the information technology. For increasing security awareness it is advisable to organise regular trainings in the company for all employees (including the management) and introduce first and foremost the company's IT security policy, reasons of importance of IT security, obligations and procedures related to this, security requirements, notification of security incidents and their effect.

16.5. Protection of sensitive data must be ensured in a company in the event of their transmission via a public network. Upon transmission of sensitive data through public network, the possibility of their disclosure to third parties must be precluded.

16.6. A suitable system access rights and use monitoring must be implemented for the assessment of efficiency of the implemented access control measures and for the timely discovery of unauthorised activities. An audit trail of activities carried out in the information system is necessary for the organisation of monitoring. The necessary monitoring level of information system parts must be determined on the basis of risk assessments. Upon violation of security it is necessary to ensure immediate notification thereof and application of measures.

16.7. Necessary measures must be applied and liability determined for the timely discovery and prevention of malicious software and viruses.

17. Configuration management

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

17.2. A company must lay down requirements that would preclude the use of unauthorised and unlicensed software. A company must perform routine checks for the discovery of unauthorised software and for the control of conformity with licence agreements.

18. Problem and incident management

18.1. Official procedures and duties must be laid down for the reduction of damages resulting from security attacks, emergencies and system failures, for registration of security incidents, responding to them and drawing 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 must be communicated to all relevant employees and contract partners. Relevant security points must be notified of any discovered or suspected security incidents as soon as possible.

19. Facility management

19.1. Information technology means supporting critical or sensitive operation functions must be installed in security areas with restricted access and they must be physically protected from unauthorised inquires, damage, security threats (e.g. fire) and environmental risks.

20. Operations management

20.1. Main standard IT operations must be documented and reviewed regularly in order to ensure the systematic processing (in terms of timing, order, quality, etc.). Operations logs must 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 must be provided for in a company. It is necessary to assess whether internal requirements of the company, efficiency of IT services and correspondence of IT activities to business objectives have been followed in information technology activities. Independence of the assessment must be ensured in providing the assessment.

21.2. External audit must 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 must be presented to the management of the company.

Part VI Final provisions

22. Entry into force of guidelines

22.1. The guidelines shall enter into force on 1.1.2005.