Methodological Instruction of the Banking Supervision Division of the National Bank of Slovakia No. 7/2004

on the audit of information systems security of banks and branch offices of foreign banks

Purpose

The purpose of the Instruction, in accordance with Article 40 paragraphs 8 and 9 of Act No. 483/2001 Z. z. on banks and on amendments to certain other laws as amended, shall be to determine for banks and branch offices of foreign banks (hereinafter "banks"):

a. he subject-matter of the audit of the security situation of bank information systems, which process and store banking data, particularly in terms of ensuring the protection of electronically processed and stored data against misuse, destruction, damage, theft, or loss;
b. the scope of information, to be presented by banks to the National Bank of Slovakia, about the provision of the audit of bank information systems security.

This Methodological Instruction shall be classified as the "**Risk Management Process**".

Contents

A. Definition of the audit of information systems security

1. The audit of bank information systems security shall be an independent, impartial, objective, and professional assessment of security features of the bank information system in terms of ensuring the overall security of the information system: particularly its efficiency, high quality and level of security-risk management, confidentiality, integrity, authenticity, and availability of information and processed data.

Definition of terms

2. For the purposes of this Methodological Instruction:

a. asset of information security (hereinafter "information asset") shall mean tangible or intangible entity, which participates in the functioning and formation of the information system of the bank, in particular:
   - data and documentary assets, mainly - databases and data files, data and information, system documentation, user manuals, training materials, operational or support procedures, continuity plans, agreements on contingency procedures used in the event of failure of the provided services or system, and archived information,
   - software assets, mainly - application software, system software, development tools and support programmes, open-source software libraries, and executable software libraries,
   - physical assets, mainly - computer equipment (processors, screens, laptops, modems),

communication equipment (routers, faxes, answering machines), magnetic media (tapes, diskettes, hard disks, compact disks), other technical equipment (power supply units, air-conditioning units), and furniture;

b. information system shall mean tangible and intangible entities, which are purposely selected and developed, and purposely interconnected, with the aim of the collection, exchange, processing, storage, generation and distribution of information and data within a pre-defined structure and time, in order to take decisions, support a decision-making process and disclose information.

B. Purpose of the audit of information systems security

3. The purpose of the audit of bank information systems security shall be to adequately ensure that

- data processed and stored by the bank are adequately protected against misuse, destruction, damage, theft, unauthorised access, change, or loss;
- the overall level of information systems protection and of data integrity, accessibility, confidentiality, and authenticity is provided by domestic legislation and internationally accepted standards;
- the information system of the bank complies with provisions of this Instruction, and assess the extent of compliance;
- the bank understands the information system protection as a continuous daily process, in which each employee of the bank participates.

C. Frequency of the audit of information systems security

4. In accordance with Article 40 paragraphs 8 and 9 the bank shall be obliged to provide an annual audit of information systems security and inform thereof the National Bank of Slovakia.

D. Eligibility to conduct the audit of the information-system security-situation

5. The audit of information systems security may be conducted by competent legal person or physical person, who has not participated in the development of the security project of the given information system and whose independence, impartiality and objectivity are not disputed.

6. The person conducting the audit of information systems security should be, as concerns their position and statements as to the audit of information systems security, objective and independent of the companies which have any related interest in the information system of the bank.

E. Subject of the audit

7. In accordance with the audit plan for information-system security-situation prepared by the bank, the subject of the audit shall be the whole information system of the bank, or its part, including relevant documentation and internal rules on information systems security.

F. Audited areas

8. In the process of developing, operating and administering its information system the bank may also use any internationally accepted standard providing information systems security if it contains minimally the following areas, which are subject to the information systems security audit.

I. Security policy

9. The bank should have security policy approved by its Board of Directors, which policy should determine objectives to be achieved in terms of the bank's information system security, and core principles and instruments to achieve these objectives.

The security policy should involve in particular:

- objectives at which the bank aims in the area of information security,
- core principles, instruments and procedures through which the bank wants to achieve the set objectives,
- powers and responsibilities for achieving the set objectives and for information security management,
- person responsible for the security policy as a whole,
- plan of security policy updating.

II. Organization and management of information security in the bank

10. The target shall be to ensure adequate protection of information assets - particularly those which can be accessible by third parties - and protection of information, particularly if it is processed by an external organization. Organization of information security should include:

- development of information-security infrastructure,
- provision of access of third parties,
- ensuring security of information assets and information if outsourcing is used.

11. Information-security infrastructure

The information-security infrastructure shall represent purposely designed managing bodies and working groups, the task of which shall be to manage and ensure required efficient level of information systems security (hereinafter "infrastructure"). The bank should have the infrastructure, approved by the Board of Directors of the bank, for information security management involving clearly determined tasks, powers and responsibilities of each managing body, working group and each of their members. The infrastructure of the bank should primarily manage the conduct of the following activities:

- design and updating of security policy,
- overall management and coordination of the development, implementation and maintenance of information security in the bank, including the allocation of powers and responsibilities,
- monitoring and assessment of security incidents and changes in information assets' exposure to risks, and subsequently adopting relevant decisions,
- provision of specialized consulting in information security in the bank.

12. Provision of access of third parties

In order to ensure information assets protection against risks ensuing from the access of third parties, the bank should:

- prepare procedures for risk management of third party access to the bank's information processing equipment and to information itself,

- allow access of a third party only on the basis of a valid contract with the third party for their access to the bank's information processing equipment and to information itself,
- specify those information assets (technical equipment, documents, information, etc.) which should, by no means, be accessible to third parties, and adopt adequate measures for their protection,
- allow, in a contract with a third party, sufficient latitude for operative measures necessary for contingency resolution and coordination of parallel access of more third parties.

13. Ensuring of the security of information assets and information if outsourcing is used

If outsourcing is used, beside the application of provisions on ensuring access of third parties, the bank should particularly:

- provide each supply on a contractual basis,
- apply such methods and procedures for assessment and selection of a supplier of delivered equipment, which involve the obligation to ensure protection of information assets,
- apply procedures for testing, and its assessment, of delivered equipment before it is accepted and introduced into the production process,
- apply procedures for the application and implementation of delivered equipment.

III. Security classification and security management of information assets

14. The purpose of the security classification of information assets and their security management shall be to determine and maintain efficient protection of information assets of the bank. The security classification of information assets and their security management involve:

- classification of information assets,
- responsibility for information assets.

15. Security classification of information assets

In order to determine the method of information assets handling, and provide their efficient protection, the bank should:

- prepare the methodology and procedures for security classification (selection, classification, labelling) of information assets,
- determine and register security classification of selected information assets in accordance with the methodology, arrange their placement and clear labelling,
- familiarize employees, in an appropriate manner, with the methodology of security classification of information assets, and with their duties and responsibilities following from this classification,

16. Responsibility for information assets

In order to ensure efficient protection of information assets the bank should:

- designate an organizational unit responsible for keeping the updated list of important information assets,
- designate owners of every single information asset and determine their responsibilities,
- designate an organizational unit responsible for the audit of maintaining the information asset security on the basis of the security classification of the given assets.

IV. Personal security

17. The purpose of personal security shall be to reduce the human factor risk (errors, thefts, frauds, misuse), provide adequate information to employees about information security risks and support their preparedness for security incidents and software malfunction. Personal security shall involve:

- security in the job description and employees recruitment,
- user training,
- reaction to security incidents and failure.

18. Security in the job description and employees recruitment

In order to minimize human factor risk of errors, thefts, frauds, and misuse of equipment and information the bank should:

- prepare a system of personal security of the bank covering all periods and activities related to the life cycle of an employee (start of employment, change in job description, change of position, termination of employment),
- bind the classification of information assets to the system of personal security,
- involve security requirements related to particular positions into the job descriptions of these positions and into the work contracts,
- conclude, in justified cases, confidentiality agreements.

19. User training

In order to familiarize users of the information system (employees and relevant third-party persons) with the information security risks the bank should:

- inform the information system users of current procedures for information systems security, of their responsibilities and of the legal consequences for them if they do not fulfil their tasks,
- train the information system users in the work with relevant equipment and application software, and review their knowledge.

20. Reaction to security incidents and failure

In order to minimize damage caused by the security incidents or failure of the whole information system, or of its parts, the bank should prepare procedures for its employees and managerial staff in the event of:

- security incident,
- software error,
- software failure,
- suspicion of disorder,
- situation when disciplinary proceedings have to be commenced against those persons who are suspected of compromising security and being responsible for this compromising.

V. Physical security and environmental security

21. The target shall be to prevent unauthorised access, damage and danger to the bank premises, damage to

information assets, interruption of bank activities, information misuse, and theft of information processing equipment. Physical security and environmental security shall involve:

- establishment of secured areas,
- equipment security.

22. Establishment of secured areas

In order to prevent unauthorised access as well as damage and danger to bank premises and information the bank should:

- identify and assess risks related to information, information processing equipment and to the built environment where information processing equipment is placed and where information is processed and stored,
- prepare procedures for the placement of data and information processing equipment,
- prepare procedures for ensuring protection of premises and built environment, where information and information processing equipment are placed, against unauthorized access, damage and danger.

23. Equipment security

In order to protect data and information, and maintain continuous business activities, the bank should:

- prepare procedures for complex protection of equipment for data and information processing, storing and archiving against loss, damage, misuse, environmental risks, and other security risks,
- prepare procedures for complex protection of transmission routes, through which data and information are transmitted (protection against unauthorised physical access, remote wiretapping, etc.),
- prepare procedures for stand-by power supply (UPS, stand-by motor generator),
- prepare procedures for the event of absolute failure of all types of stand-by power supply,
- prepare formal procedures for the management of the use of portable information processing equipment, as well as for the information and data processing outside the bank.

VI. Communication and operation management

24. The target shall be to ensure safe, reliable and smooth operation of information processing equipment; minimize the risk of information system failure, or its part failure; protect software, data and information integrity; provide accessible information processing and communication services; ensure security of networks and information transmitted via these networks; prevent interruption of business activities of the bank; and establish safe information-exchange among organizations. Communication and operation management shall involve:

- operational procedures and responsibilities,
- information-system planning and acceptance,
- protection against harmful software,
- operation management,
- network administration,
- safe handling of media,
- information and software exchange.

25. Operational procedures and responsibilities

In order to establish the safe and reliable operation of information processing equipment the bank should:

- prepare procedures for enabling information system operation (in particular procedures for administration, starting/shutting down the system, changes to the system, back-up filing and archiving),
- prepare procedures for the operation of application software,
- prepare procedures for the monitoring, administration and management of security incidents (in particular their identification and notification, recording, time series, analyses and conclusions, and the assessment of security system efficiency and responsibilities allocation),
- prepare procedures for the monitoring of third party activities,
- prepare procedures for the monitoring of the exploitation of the system's capacity and monitoring of the tasks running within the system,
- prepare procedures for implementing changes to the production information system,
- separate the production system from the development system, and establish separate back-up processing.

26. Information system capacity planning and information system acceptance

In order to provide reliable and smooth operation of the bank's information system, without its overload and consequent failure, the bank should:

- prepare procedures for the regular monitoring and assessment both of individual parameters of the information system and of the capacity of the information system as a whole,
- provide, well in advance, necessary extension of the information system capacity,
- prepare procedures for the complex steps and methodology of measuring, monitoring, assessing, planning, and the acceptance of, the information system, including the allocation of responsibilities and the assessment of its efficiency.

27. Harmful software

The bank should prepare and implement formal procedures to protect the integrity of its information system, software, information, and data against the impact (influence, effect) of harmful software. The procedures should include software implementation and maintenance in order to ensure protection against harmful software.

28. Operation management

In order to ensure bank's activities continuity and preserve integrity of, and accessibility to, information processing and communication services after the failure of the information system the bank should prepare procedures for:

- information system recovery,
- information system back-up,
- notification of errors in the information system as a whole or in its parts, and for the treatment of these notifications,
- keeping and assessing records of acts of employees carrying out operations, and records of the performance of, and important incidents within, the information system.

29. Network administration

In order to ensure the protection of data within networks and of network support infrastructure against unauthorised access the bank should:

- prepare procedures for the management of remote equipment,
- prepare analysis of risks connected with networks, and procedures for their management,
- separate, if necessary, responsibilities for network management from those for the operation of other information technologies and services.

30. Safe handling of transfer media

In order to protect against damage to information assets and interruption of business activities, and ensure the safe handling of transfer media (diskettes, magnetic disks, CDs, tapes, cassettes, and printed documents), the bank should prepare procedures for handling transfer media and for their liquidation.

31. Information and software exchange

In order to prevent misuse, loss or modification of information, software and data exchanged between the bank and any external person, the bank should:

- conduct the exchange exclusively on a contractual basis,
- prepare procedures for the exchange of information and physical data media,
- prepare procedures and measures (in the hardware, software, personal, and legislative areas) to ameliorate and eliminate risks connected with the operation of electronic-banking services operated using the public networks (Internet),
- prepare procedures for the implementation and use of electronic communication channels (e.g., electronic mail, electronic office systems and website),
- prepare procedures to provide information to the users of electronic communication channels about their responsibility for the data, information and software security in the process of their exchange.

VII. Access management

32. The target shall be to manage access of persons to the bank's data and information, to the equipment for their processing and to network services, as well as identify unauthorized activities and ensure information security when mobile processing and distance employment are used. Access management shall involve:

- preparation of principles of information access management,
- user access management,
- responsibilities of users,
- network access management,
- access to the operations systems and their services,
- access to applications,
- monitoring of access to information systems and of their use,
- mobile processing and distance employment.

33. Principles of information access management

In order to manage access to information the bank should prepare principles of information access management, which shall involve in particular:

- access management requirements in terms of the conduct of banking activities and the security requirements of the bank,
- access management rules,
- rules setting access rights and responsibilities of individual users and groups of users of the information system.

34. Management of user access to information shall include:

- procedures for the management and distribution of access rights and privileges to application software and services, taking account of all events within the user's working process,
- procedures for the management of user names and passwords (assignment, change, method of their storage on the memory media, etc.),
- process of user registration and recording.

35. Responsibilities of users

The bank should prevent the unauthorized access of users to information and information processing equipment. In this regard, the bank should inform users about their responsibilities for maintaining the efficient management of access to data, information, services, and information processing equipment.

36. Network access management shall include:

- procedure for the management, establishment, development, maintenance, and use of networks,
- procedure for access and connection of equipment to the connection ports of hardware equipment,
- procedure for risk management related to the connection of external user.

37. Management of access to operations systems shall include:

- log-in procedure,
- procedures for determining methods of user identification (e.g., password, biometric methods, tokens, encrypting tools, chip cards, combinations),
- standard management of selected methods of user authorisation,
- management of access to system software and of its use,
- protection of inactive equipment and users against their misuse (automatic log-out of a user, disconnection of equipment, task or application locking, equipment locking, etc.).

38. Application access management shall include:

- provision of access to applications on the basis of individual requirements in accordance with the defined access management policy and information access policy,
- distribution of access rights and privileges to the users of application software systems in accordance with the

security policy,

- procedures for, and methods of, distribution and approval of access rights and privileges.

39. Monitoring of access to information systems and of their use

In order to identify unauthorized activities the bank should:

- monitor departure from the principles of information access management in accordance with formal procedures for monitoring,
- automatically record information on important events in the system (audit log) for the purposes of obtaining evidence,
- archive audit logs in accordance with the archiving rules and security policy,
- regularly analyze and review audit logs in order to detect possible security incidents or unsuccessful attacks,
- protect software for creating audit logs,
- separate the roles of those who monitor from the roles of those who are monitored.

40. Mobile processing and distance employment

In order to ensure information security the bank should:

- prepare policy and procedures for the mobile processing and distance employment management,
- allow mobile processing and distance employment on a contractual basis only and after obligatory user training and practical training,
- identify risks specific for distance processing and employment, and implement appropriate measures for their elimination or reduction,
- ensure security if mobile equipment is connected to the bank's network, particularly through the user identification and authorisation.

VIII. Development and maintenance of the system

41. The target shall be to build-in information security directly to the information system; protect confidentiality, integrity, accessibility, and authenticity of data and information; manage that information system designing is made in a safe manner; and maintain security of application software. Development and maintenance of the system shall include:

- security requirements for information systems,
- security within application software systems,
- encrypting measures,
- security of system files,
- secure development and support processes.

42. Security requirements for the information system

In order to build-in security to information systems the bank should define security requirements as early as in the stage of information-system functionality specification.

43. Security within application software systems

The bank should prevent the loss, modification or misuse of data and information in the application software systems. In this regard the bank should involve in the application software systems the function of automated generation of audit logs.

44. Encrypting measures

In order to protect information (confidentiality, integrity, authenticity, and accessibility) the bank should establish its own policy and procedures particularly for:

- use of encrypting techniques,
- manipulation and administration of keys.

45. Security of system files

In order to ensure security of the information systems development and support activities, and to minimize the risk of damage to operations systems, the bank should prepare procedures for:

- operational software implementation,
- management of access to system files,
- ensuring security during the stage of information system development,
- handling of, and access to, old and current software libraries and test data,
- changes to files within the operational (production) system.

46. Secure development and support processes

In order to ensure the security of application software and involved data and information the bank should prepare procedures for:

- management of the security of the development and other support environments and systems,
- change management in the operational (production) system.

IX. Continuity management of bank's activities

47. The target shall be to prevent interruption in business activities of the bank. In order to ensure continuity of business activities and protection of its key business processes against large-scale failure and breakdown the bank should:

- prepare continuity plans for maintaining ongoing operation of its information system, which involve allocation of responsibilities and comply with continuity plans for maintaining business activities of the bank,
- regularly test and update its continuity plans for maintaining ongoing operation of its information system,
- define, for each continuity plan for maintaining operation of its information system, conditions for, and processes of, its activating, and allocate responsibilities.

X. Compliance with security rules

48. The target shall be to eliminate any breach of bank obligations in the area of information systems, harmonize information systems with security rules and standards of the bank. In the course of the development, operation and

administration of information systems the bank should comply with requirements following from:

- generally binding legal regulations,
- internal regulations,
- contracts,
- generally accepted standards and security requirements.

G. Scope of information about the security audit to be provided to the National Bank of Slovakia

49. The bank shall arrange that the person, who conducts the audit of information system security, prepare a written report on the conducted audit. This report shall provide sufficient information to the Board of Directors of the bank and to the National Bank of Slovakia about the security situation of the bank's information system.

50. The report on the audit of the bank's information system security prepared in order to inform the National Bank of Slovakia shall minimally involve the following items:

- scope of the security audit,
- applied standards,
- person conducting the audit,
- list of detected shortcomings, including reasons for the assessment of particular facts as shortcomings (reference to binding documents, internationally accepted standards; stressing risks, possible impacts and damage; mechanism and likelihood of their occurrence),
- recommendations to recover detected shortcomings,
- opinion on the bank's information-system security-situation, including constraints and reservations that adversely affected the conduct of audit and its result,
- bank's position on the report.

Done at Bratislava, on 1 October 2004

Ing. Milan Horvath
Chief Executive Director
Banking Supervision Division