Polish Financial Supervision Authority

Recommendation D

On the Management of Information Technology and ICT Environment Security at Banks

Warsaw, January 2013

Table of Contents

I. Introduction

This Recommendation is issued on the grounds of Article 137 of the Banking Law Act of 29 August 1997 (Journal of Laws of 2012, item 1376, as amended). It replaces „Recommendation D on the management of risks associated with ICT systems used by banks", prepared and issued in 2002. Issuance of the Recommendation's revision is necessary due to a significant technological development and systematic increase in importance of the information technology for the operation of banks and because of new threats in this area. This revision also include the conclusions drawn from supervisory activities of the Polish Financial Supervision Authority (hereinafter referred to as PFSA)

The purpose of this Recommendation is to notify banks of expectations of the PFSA regarding prudent and stable information technology and ICT environment security management, in particular regarding management of risk associated with these areas. The risk may be defined as an uncertainty related to the proper, effective and secure support of the operation of a bank by its ICT environment. It is primarily associated with operational risk (therefore this Recommendation should be regarded as a supplement of „Recommendation M on the management of operational risk at banks" in the areas of information technology and ICT environment security), but includes also, among others, reputation risk and strategic risk. This Recommendation is intended for banks operating as domestic banks pursuant to the Banking Law Act of 29 August 1997 (Journal of Laws of 2012, item 1376, as amended). This Recommendation is also intended for branches of foreign banks.

This document contains 22 recommendations which have been divided into the following areas:

- Information Technology and ICT Environment Security Strategy and Organisation,
- ICT environment Development,
- Maintenance and Exploitation of ICT Environment,
- ICT Environment Security Management,

This Recommendation is intended for all banks. However, taking into account the characteristics of issues related to the information technology and ICT environment security and differences in the conditions, scale of operation and risk profiles of the banks, the manner of implementation of the goals that arise from this Recommendation will be different. Therefore, the descriptions and comments under individual recommendations should be regarded as a set of good practices, which should be applied in accordance with the principle of proportionality. This means that application of the good practices should depend on the degree to which they comply with the specific risk profile of a given bank and the characteristics of its ICT environment, as well as the ratio of cost of their introduction to the resulting benefits (also from the perspective of security of bank clients). The PFSA expects that decisions concerning the scope and manner of implementation of the solutions specified in this Recommendation are preceded by an in-depth analysis and supported by an appropriate line of reasoning.

In case of cooperative banks the PFSA expects that affiliating banks will support the implementation of this Recommendation, taking into account the scale and business characteristics of a given cooperative bank, in accordance with the principle of proportionality. The scale of operation and the used information technologies should decide about the scope and level of the adopted solutions. However, the process of implementation these solutions at cooperative banks, despite the active role of an affiliating bank, cannot go against the scope of obligations and responsibility of statutory organs (authorities) of affiliated cooperative banks, defined in particular recommendations.

The PFSA expects that appropriate actions aimed at the implementation of „Recommendation D on the Management of Information Technology and ICT Environment Security at Banks", issues as an attachment to the Act 7/2013 of PFSA of 8 January 2013 (Journal of PFSA of 2013, item 5) are taken by the banks not later than by 31 December 2014.

II. Glossary

Access account - an individual space within the service that provides the client with a free access (via an electronic device) to the services provided by the bank with the use of electronic access channels and the possibility to perform via the space passive operations (e.g. a preview of personal data) and active operations (e.g. submission of offers and requests, data modification).

Business area - area regarding bank operations whose functioning is supported by the ICT environment, including e.g. operational activity, risk management, accounting, finance etc.

Business continuity plan (BCP) [1] – documented procedures that after occurrence of a disturbance support the organization in responding, achieving efficiency and recovery of activities at a predefined operational level (based on ISO 22301: 2012).

Cloud Computing - model of service provision that ensures convenient, "on demand" independent of location network access to a shared pool of configurable computing assets (mass storage servers, applications or services) which may be dynamically delivered or released with a minimum management and involvement of the service provider (based on NIST Special Publication 800-145 "The NIST Definition of Cloud Computing", National Institute of Standards and Technology)

Data availability - characteristic feature of data whereby they are available and may be used on demand of an authorised entity (based on ISO/IEC 27000:2012).

Data confidentiality - characteristic feature of data whereby data remain unavailable or undisclosed to unauthorised persons, processes or other entities (based on ISO/IEC 27000:2012)

Data integrity- characteristic feature of data that determines data accuracy and completeness (based on ISO/IEC 27000:2012).

Data processing - any operations conducted on data, such as collection, recording, storage, organisation, alteration, disclosure and erasure.

ICT environment - ICT infrastructure of bank with information systems utilising it and information systems used at bank supporting its activity, which are based on the ICT infrastructure delivered by external entities.

ICT environment security area- area regarding bank's operations designed to ensure proper management of the ICT environment security risk at these banks.

ICT environment security breach - single unwanted or unexpected ICT environment incident (i.e. occurrence of an ICT environment component condition that indicates potential security breach or of the control mechanism error or an unknown situation which may be relevant from the security perspective) or a series of such incidents, in the case of which a significant probability of disruption or information security breach occurs (based on ISO/IEC 27000:2012)

[1] BCP – *Business Continuity Plan*

ICT environment security management system - set of rules and mechanisms referring to processes designed to ensure proper level of ICT environment security

ICT infrastructure - a set of devices and transmission connections, including in particular hardware platforms (including servers, matrices, workstations), telecommunication network (including routers, switches, firewalls and other network devices), system software (including operating systems and database management systems) and other elements for failure-free and safe operation of the above resources (including UPS , generators, air conditioning devices), also those used in the backup centres.

Information security- information confidentiality, integrity and availability; information security may also include other characteristics, such as authenticity, accountability, non-repudiation and reliability (based on ISO/IEC 27000:2012).

Information technology area- area regarding bank' operations designed to ensure proper support by the ICT environment of the bank'.

IT system - computer application or a set of related computer applications for data processing.

Management Board of Bank- Management Board and directors, managers of organisational units and key processes managers at bank.

Operational risk – the risk of loss resulting from inadequate or incorrect internal processes, actions of staff members or system operation, or from external incidents (based on "Methodology of study and supervisory evaluation (BION) of banks").

Risk profile - scale and structure of exposure to risk taking into account the characteristics of business activity of the bank.

Susceptibility – equivalent to Vulnerability.

Threat- potential cause of an unwanted incident which may cause damage to the system or the organisation (based on ISO/IEC 27000:2012).

Vulnerability - resource weakness or control mechanism weakness which may be exploited by a threat (based on ISO/IEC 27000:2012).

III. List of Recommendations

Information Technology and ICT Environment Security Strategy and Organisation

Recommendation 1

Supervisory Board of the bank should supervise operation of the information technology and ICT environment area security, and the Management Boards of the bank should ensure correct and efficient management of these areas.

Recommendation 2

As part of information technology and ICT environment security areas, the bank should have a formal management information system that would provide each information recipient with a proper knowledge on these areas.

Recommendation 3

Bank should develop and implement information technology and ICT environment security strategy in line with the operational strategy of the bank.

Recommendation 4

Bank should determine principles of cooperation and the responsibility limits in the business area, information technology and ICT environment security area that allows to utilise the ICT environment potential in an effective and safe manner, in the business activity of the bank.

Recommendation 5

Organisational solutions and human resources in the information technology and ICT environment security areas at the bank should be adequate to its risk profile, the scale and characteristics of operation and to allow effective performance of activities in these areas.

ICT Environment Development

Recommendation 6

Bank should have formal principles of implementation of the ICT environment projects, which are adequate to the scale and characteristics of the projects implemented.

Recommendation 7

IT systems at the bank should be developed in such manner that supports its operation and complies with the ICT environment security requirements.

Maintenance and Operations of ICT Environment

Recommendation 8

Bank should have formal principles of the management of data used in its operation that include, in particular, data architecture and quality management and that properly support business activity of the bank.

Recommendation 9

Bank should have formal principles of ICT infrastructure management, including management of its architecture, its components, efficiency, capacity and documentation that properly support business activity of the bank.

Recommendation 10

Bank should have formal principles of cooperation with external service providers that ensure security of data and correct operation of the ICT environment, taking into account the ICT services provided by entities included in the bank's capital group.

Recommendation 11

Bank should have formal principles and technical systems that ensure adequate level of control over the logical access to data and information and physical access to key elements of the ICT infrastructure.

Recommendation 12

Bank should ensure proper protection of the ICT environment against malware.

Recommendation 13

Bank should provide internal users of information systems with support regarding resolution of problems related to their operations, including those arising from failures and other non-standard incidents affecting their use.

Recommendation 14

Bank should undertake effective measures aimed at achievement and maintenance of an appropriate level of employee competencies in the area of ICT environment and security of data processed in that environment.

Recommendation 15

Continuity Management should take into account special conditions related to the ICT environment and data processed in that environment.

Recommendation 16

Bank providing services with the use of electronic access channels should have effective technical and organisational solutions that ensure security of clients' identity, data and funds, and should educate clients on the principles of safe use of these channels.

Recommendation 17

Bank should have formal principles of management of the so called End-User Computing that effectively mitigate the risk related to usage of such tools.[2]

[2] End-User Computing, EUC – tools developed and operating based on applications such as MS Excel or MS Access installed on personal computers, which allow users who are not programmers to create business applications.

ICT Environment Security Management

Recommendation 18

Bank should have a formalised and effective ICT environment security management system, including activities related to the identification, assessment, control, mitigation, monitoring and reporting of risk in that area, integrated with a risk management and information security system at the bank.

Recommendation 19

Bank should classify information systems and information processed in those systems in accordance with the principles that take under consideration, in particular, security level required for such systems and information.

Recommendation 20

Bank should have formal principles of the management of ICT environment security breach incidents including identification, registration, analysis, prioritisation, link search, taking corrective measures and removing their causes.

Recommendation 21

Bank should ensure compliance of information technology and ICT environment security operation with the legal requirements, external and internal regulations, agreements concluded and standards adopted at the bank.

Recommendation 22

Information technology and ICT environment security areas at the bank should undergo systematic audits.

IV. Information Technology and ICT Environment Security Strategy and Organisation

Role of the Management Board and Supervisory Board

1. **Recommendation** 1

Supervisory Board of the bank should supervise operation of the information technology and ICT environment area security, and the Management Boards of the bank should ensure correct and efficient management of these areas.

1.1. The bank's Supervisory Board and Management Board should give special attention to:

- ICT environment security and continuity management[3][4],
- the process of development and update of the information technology and ICT environment security strategies[5],
- Electronic access channels management[6].
- cooperation with external providers of services regarding the ICT environment and its security[7],
- ensuring adequate organisational structure and human resources in the information technology and IT environment security areas[8],
- management of the quality of data that are key for the bank[9].

1.2. In order to increase the effectiveness of supervision and control over the ICT environment security and to ensure efficient communication in that area as well as compliance of its actions with the goals and needs of the organisation, the bank should consider (taking into account, in particular, complexity of the ICT environment, risk exposure regarding the ICT environment security and specificity of the business activity) and make appropriate decisions whether appointment or designation[10] of a committee competent for the ICT environment safety is necessary. Work of the committee should be governed by an adequately qualified member of the bank's Management Board or a representative appointed by the bank's Management Board.

Management Information System

2. **Recommendation** 2

[3] See section "ICT Environment Security Management".
[4] See section "ICT Environment Continuity
[5] See section "Strategic Planning".
[6] See section "Electronic Access Channels Management".
[7] See section "Cooperation with External Providers of Services".
[8] See section "Information Technology and ICT Environment Security Organisation"
[9] See sub-section "Data Quality Management".
[10] It is not necessary that it is a separate, dedicated committee - in particular, it is permissible e.g. to take into account the tasks of the Committee for the ICT environmental security in the works of units responsible for operational risk. Bank should, however, ensure that the adopted solution allowed effective execution of tasks in the area

As part of information technology and ICT environment security areas, the bank should have a formal management information system that would provide each information recipient with a proper knowledge on these areas.

2.1. While developing the information technology and ICT environment security management information system, the bank should:

- identify issues within the information technology and ICT environment security areas which should be covered by the management information system taking into account the risk and other specific conditions related to them,
- determine the manner and principles of making available and obtaining information on these issues (including to define the source from which it is possible to obtain information in an automatic manner) and define responsibility in that respect,
- determine the adequate scope and frequency of reporting,
- identify the persons and functions being recipients of the information,
- ensure that information provided to each of the recipients is clear, reliable, exact and valid, has an adequate scope and is delivered on time and with adequate frequency.

Strategic Planning

3. Recommendation 3

Bank should develop and implement information technology and ICT environment security strategy in line with the operational strategy of the bank.

3.1. Main function of the information technology area in bank is to ensure support for the operations of the institution by its ICT environment, whereas main responsibility of the ICT environment security area is to ensure that the risk associated to this environment's security is properly managed. Therefore, a starting point for the development of a strategy[11] in information technology and ICT environment security areas should be the bank's business strategy.

3.2. In order to ensure that the strategy in information technology and ICT environment security is realistic and at the same time complies with current and future (expected) conditions and business expectations, the bank should have the necessary knowledge of the ICT environment, allowing for the identification of interdependence between its individual components and the data, circumstances, goals and business needs processed in that environment.

3.3. As part of implementation of the strategy mentioned above, the bank should determine, in particular, specific and measurable goals and programs/projects with defined priorities and time frame (in accordance with the identified needs). These should include:

- development of the software used,

[11] The singular used in the term "strategy in information technology and ICT environment security areas" does not mean that it should be necessarily developed as a single document. The bank should however ensure that the strategies in both areas are consistent.

- changes in respect of data processed as part of the operation of the bank,
- ICT Infrastructure development,
- Organisational and process changes in the management of information technology and ICT environment area,

taking into account requirements referring to ICT environment security, risk associated with implementation of the strategy and funds necessary to implement it.

3.4. Bank should ensure that implementation of the strategy mentioned above undergoes effective monitoring, in particular through monitoring of its goals and programs/projects defined in it.

3.5. Bank should ensure that the strategy mentioned above undergoes systematic[12] review and corresponds to changes in the bank and its environment, such as changes in the operation strategy of the bank, changes to its risk profile, legal and regulatory changes or technological development.

3.6. The scope and level of specificity of the strategy documentation should be adequate to its complexity and scale and operation profile of the bank.

Business and Technical Areas Cooperation Principles

4. **Recommendation** 4

Bank should determine principles of cooperation and the responsibility limits in the business area, information technology and ICT environment security area that allows to utilise the ICT environment potential in an effective and safe manner, in the business activity of the bank.

4.1. Principles that govern cooperation between business areas, information technology and ICT environment security as well as the manner of communication between these areas should be defined and formalised in a manner that is adequate to the scale and operation profile of the bank.

4.2. These principles should ensure that:

- decision making procedure and the scope of tasks and responsibility in information technology and ICT environment security are precisely defined and adequate to the role of information technology at the bank.
- business area specifies its expectations (including their priorities) towards information technology and ICT environment security in the most precise manner possible, in particular through co-participation in the creation of information technology and ICT environment security strategies,
- information technology and ICT environment security areas inform the business area, in a possibly most precise manner, of the estimated funds that are necessary to meet the needs of that area,

[12] i.e. in an orderly and methodological manner.

- information technology and ICT environment security areas participate in the development of information systems and in the development and acknowledgement of standards and mechanisms that affect the ICT environment security level,
- information technology and ICT environment security areas take part in giving opinions on operational strategies of the bank, including as regards defining limitations and threats associated with such strategies that are identifies from the perspective of these areas,
- business area is informed on a regular basis of the implementation of programs/projects that are important from the business area perspective and that are associated with the ICT environment.

4.3. In order to increase efficiency of supervision and control over the information technology area (including control over projects implemented in that area) and to ensure efficient communication in that area as well as compliance of its operation with the goals and needs of the institution, bank should consider (taking into account, in particular the scale and specificity of operation, complexity of the ICT environment and strategic assumptions regarding development of that area) and make appropriate decisions whether appointment or designation[13] of a committee competent for cooperation between the business and information technology area is necessary. Work of the committee should be governed by an adequately qualified member of the bank's Management Board or a representative appointed by the bank's Management Board.

4.4. Simultaneously, in order to ensure the closest integration possible of the information technology and ICT environment security management with the management of the entire bank, the bank should ensure adequate cooperation between the units responsible for the information technology area, bank's business strategy, ICT environment security, continuity, operational risk management, process management, project management and internal audit (allowing for an appropriate degree of independence of each of these areas).

[13] It is not necessary that it is a separate, dedicated committee. Bank should, however, ensure that the adopted solution allowed effective execution of tasks in the area.

Information Technology and ICT Environment Security Organisation

5. Recommendation 5

Organisational solutions and human resources in the information technology and ICT environment security areas at the bank should be adequate to its risk profile, the scale and characteristics of operation and to allow effective performance of activities in these areas.

Organisational Structure

5.1. Bank should ensure that the organisational structure of information technology and ICT environment security allows effective implementation of the bank's goals in these areas in proportion to the scale and profile of the bank's operation and complexity of the ICT environment. Adequacy of such structure should undergo systematic verification and should be adjusted to modifications in the internal environment of the bank and its area, if such need arises.

Distribution of Duties

5.2. Bank should precisely define the duties and rights of individual employees regarding information technology and information security. Duties and rights should be defined in writing and the distribution of duties should minimise the risk of errors and irregularities in the processes and systems. Therefore, attention should be given to appropriate separation of employees' duties, in particular to the separation of:

- the creation function or modification function of information systems from their testing (except for tests performed by programmers while creating software) administration and use,
- the ICT environment component administration function from designing security control mechanisms associated with it,
- the information system administration function from the monitoring of its administrators' operations,
- the audit function from other functions in the information technology and ICT environment security.

5.3. Bank should appoint people or define functions responsible for making decisions regarding individual systems utilised at the bank (often referred to as system owners based on the bank's ICT infrastructure as well as on the ICT infrastructure delivered by external entities. Duties of these persons or functions should include, in particular:

- ensuring correct operation and safety of the system in terms of business (e.g. through proper definition of the procedures for using the system, participation in continuity management, participation in authorisation management),
- supervision over the activities of system users,
- participation in decision-making regarding development of these systems.

In the event that for a given system more than one owner has been specified, the bank should give special attention to the precise determination of distribution of competencies and duties.

5.4. Ensuring security of the information processed in the ICT environment is not the exclusive competency of the units responsible for the information technology and ICT environment security, but it depends to a large extent on proper actions of direct users of information systems and data. Therefore, every employee of the bank should be aware that its duty is to ensure security of the information processed in the ICT environment. To that end, the bank should take measures to create the so called information security culture, to educate employees in the ICT environment security and obtain written declarations of compliance with the internal regulations regarding this area.[14]

5.5. To supplement the above, employees of the ICT environment security area should independently and in an active manner, monitor the implementation of activities in the area assigned to business units and to persons responsible for the information technology area (e.g. in terms of periodic reviews of system authorisations, current safety control of the ICT environment conducted by organisational units, testing the correctness of the ICT environment components recovery based on emergency backup copies, etc.).

5.6. With regard to transaction systems, it is advisable to implement a mechanism for the manual confirmation by a second person of transactions involving significant amounts (co called “four-eyes control”). The abovementioned significant amount should be determined by the bank on the basis of an analysis of the nature of the transactions it processes.

Human Resources

5.7. Taking into account the scale of implemented operations, the bank should ensure that both the number and level of knowledge and qualifications of the information technology and ICT environment security employees or people to whom responsibility for these areas has been entrusted allow safe and correct operation of the entire ICT environment. Therefore, the bank should

– ensure that employee work load allows effective implementation of their duties,

– provide employees with regular training (adequate to their position) promote the acquisition of knowledge and enable employees to exchange experiences (e.g. through access to the so-called knowledge bases, participation in sector conferences and forums).[15]

5.8. Bank should not introduce new information technologies without having the knowledge and competencies that enable proper management of the related risk. Therefore, the bank should assess adequacy of each of the competencies, and if they are found to be insufficient, take measures to ensure their supplementation (e.g. employee training, hiring new employees, cooperation with external service providers, etc.).

5.9. Bank should give special attention to the selection of employees working in positions that give access to the information with a high degree of confidentiality[16].

[14] See also: “Employee Education”

[15] See also: “Employee Education”.

[16] See section: “Information and IT Systems Classification”

5.10. Bank should take measures to minimise the risk associated with possible resignation of key employees within the information technology and ICT environment security or persons responsible for the information technology and ICT environment security ceasing their activities. In particular, the bank should:

- identify key employees whose resignation is associated with a significant risk for the operation of the bank,
- ensure availability of an updated and precise documentation of the ICT environment[17],
- ensure that duties assigned to key employees are periodically performed by other persons (e.g. when key employees go on a sufficiently long vacation),
- have succession programs for key employees,
- promote sharing of knowledge among employees,
- cover significant events associated with key employees with management information (especially information on resignation or long absence of the employees resignation)[18].

[17] See section: "IT Infrastructure Documentation".

[18] See also: "Management Information System".

V. ICT Environment Development

ICT Environment Projects

6. Recommendation 6

Bank should have formal principles of implementation of the ICT environment projects, which are adequate to the scale and characteristics of the projects implemented.

6.1. The principles of implementation of the ICT environment projects should, in particular:

– introduce definition of the project,[19]

– cover all project stages, from its initiation and the decision about its initiation until formal closing.

– determine the manner of selecting project stakeholders,

– determine the manner of selecting project participants, determine their role, rights and responsibilities,

– take into account the manner of project documentation,

– define the principles of cooperation and communication between the parties involved in the project,

– define the principles of management of the project schedule, budget, scope and quality,

– define the principles of project risk management,

– define the principles of project modification management,

– define the principles, roles and responsibilities for acceptance and introduction to use of products of the project works,

– define the principles of decision making to abandon the project.

6.2. Projects should be carried out with or in relation to the recognised standards and best practices in the area of project management, such as standards related to project management proposed by the PMI (Project Management Institute), in particular the PMBoK standard (Project Management Body of Knowledge), or the PRINCE2 methodology (PRojects IN Controlled Environments.

6.3. Taking into account, in particular, the level of complexity of the ICT environment, level of risk exposure in respect of the ICT environment security and specificity of the business activity, the bank should make decisions on whether it is necessary to include in the project implementation principles, the participation of the ICT environment security representatives in the entire project life cycle.

Development of IT Systems

7. Recommendation 7

[19] Definition of the project may be specified e.g. in relation to the size of the estimated project budget or the number of business days required for its implementation.

IT systems at the bank should be developed in such manner that supports its operation and complies with the ICT environment security requirements.

7.1. Development of IT systems should correspond to the plans arising from the strategy of the bank in relation to information technology and ICT environment security.

7.2. Bank should identify specific requirements for the development of IT systems, taking into account current and anticipated needs and the future opportunities for ICT environment development. Each requirement should be formulated in such manner that enables clear assessment of its fulfilment. In particular, analysis of the requirements should include the following: [20]

– requirements in terms of functionality of the system,

– requirements regarding the scope, quantity and form of the data processed in the system, including assessment of the possibility of data migration from the currently used systems,

– requirements regarding the ability to communicate with other information systems used by the bank, in particular regarding the principles and scope of data exchange,

– requirements regarding expected performance and availability of the system, including its heavy load,

– requirements regarding system resistance to failure, including requirements regarding recovery time after failure and acceptable data loss,

– requirements regarding operation of the system environment,

– requirements regarding security of the system and data processed in the system, including cryptography, access control and registration of incidents occurring in the system,

– requirements under the law, internal regulations and standards applicable at the bank[21].

7.3. While designing the IT system, the bank should take into account the possibility to modify it in the future, resulting in particular from amendments to legal provisions, operating strategy or standards applicable at the bank. This means that by developing IT systems, bank should identify changes in the internal and external conditions that are possible to predict, and consider the necessity of ensuring flexibility of a given system to an appropriate extent that enables effective implementation of necessary modifications in the future.

7.4. Introduction of a new IT system, as well as significant modifications to the existing system should be preceded by analysis of the risk arising from the information technologies applied and by assessment of the impact of the modifications introduced on the ICT

[20] In case of any modifications to the existing IT systems, the elements to be taken into account in the analysis of requirements should be adequate to the scope of these modifications

[21] See also: “Formal and Legal Security”.

environment and business processes at the bank with particular emphasis on security aspects[22].

7.5. In the case of in-house software development, the bank should have a defined approach in that regard. A good practice is to determine, at least:

– software development methodology used, specifying e.g. software development process,

– standards used in software development, including:

  ▪ architectural standards, including used platforms, technologies, integration mechanisms etc.,

  ▪ programming tools and code repositories used,

  ▪ source code standards, including the preferred programming languages and queries, notation used and manner of making comments,

  ▪ principles of the use of current tests and code reviews that ensure an adequate degree of independence of these reviews,

  ▪ software quality criteria (e.g. regarding easy maintenance, portability, etc.),

  ▪ standards for technical documentation being created,

  ▪ principles of software versioning.

7.6. In the case of software development carried out with the participation of external entities, the bank should use services of reliable suppliers with appropriate experience (documented with completed projects), and reputation in the market that ensure an adequate level of service quality and security. Bank should also consider and make appropriate decisions whether it is necessary to include software development standards and methodologies adopted at the bank in the agreements on software development concluded with external suppliers.[23] In particular, the bank should ensure that before the deliverables are implemented, they undergo internal tests conducted by the supplier, however performance of such tests should not in any way limit the scope of tests performed at the bank.

7.7. Both new software and modifications introduced to the already existing IT solutions should be tested adequately to their complexity and the impact on other elements of the ICT environment at the bank. Bank should have software testing methodology that includes, in particular, the following best practices:

– organisation of tests should ensure a possibly high degree of independence while verifying fulfilment of the adopted assumptions,

– tests should be conducted with the participation of representatives of the widest possible range of the bank’s organisational units that use the implemented solution (or

[22] See sub-section “IT Environment Security Risk Identification”

[23] See also: “Cooperation with External Providers of Services”.

in the case of modifications, the modified part), as well as information technology and ICT environment security areas,

- test scenarios and the scope and volume of data used in the tests should be as close as possible to the procedures and data processed under the actual system utilisation, and the bank should ensure an appropriate level of confidentiality of the real data used for testing,
- the manner of reporting and correcting software errors should be clearly specified and should ensure registration of all reported errors,
- tests should be carried out in a dedicated test environment,
- the scope of testing should include verification whether all requirements have been fulfilled, in particular the following areas:[24]
  - compliance with the functional requirements established,
  - performance and availability of the system, including heavy load conditions,
  - compliance of the new solution with safety requirements, including in terms of authorisations,
  - correct operation of the mechanisms that ensure the required availability and recovery after failure, including system recovery from emergency backup copies,
  - compliance with the adopted software quality measurements,
  - correct integration (data exchange) of a given system with other systems,
  - proper operation of systems integrated with a given system, as well as, in the case of modifications, the remaining (unmodified) part of the system functionality.

7.8. Bank should ensure that the procedures for transferring of a new system or modification of the already existing system to a production environment minimise the risk of standstill in the bank’s operation. In particular, after moving of the system into the production environment, the bank should verify its proper operation and compliance with requirements, and then monitor the system in this respect for a suitable period in order to identify potential problems that require intervention. Therefore, taking into account technical capacity and the costs to risk ratio, the bank should consider and make appropriate decisions whether it is necessary to ensure mechanisms that enable returning to the state before the implementation in the event of emergency (such as making emergency backup copies of an appropriate ICT environment).

7.9. Development, testing and production environments operating at the bank should be sufficiently separated. The chosen method of separation (e.g. logical separation using

[24] In case of modifications to the existing information systems, the areas taken into consideration during testing should be adequate to the scope of these modifications.

virtualisation, physical separation, etc.) should correspond to the level of risk and technical conditions related to a given environment and the systems operating within that environment.

7.10. Bank should ensure that development of information systems is accompanied by development or update of appropriate functional, technical, operational[25] and in-use documentation (with its versioning ensured), and that appropriate training[26] is provided to users of the systems under development.

7.11. Bank should establish a formalised process of change management in IT systems, which defines the principles and procedures in respect of:

- submitting proposals of modifications,
- acceptance of modifications,
- defining modification priorities,
- implementation of modifications,
- monitoring of the implementation of modifications,
- testing of the implementation of modifications,
- closing the modifications being implemented,
- management of emergency modifications.

7.12. While making decision whether to approve a given modification, the bank should analyse its compliance with the requirements previously set out for the modified IT system, in particular those related to its security. If there is a discrepancy in that respect, the decision to accept the modification should be taken with extreme caution.

7.13. Introduction of modifications to the IT systems should be properly documented, in particular, the bank should keep a record of modifications introduced to individual systems and conduct periodic verification whether entries in that register comply with the facts.

7.14. Bank should give special attention to modifications in the ICT environment resulting from mergers or acquisitions. In such cases, the bank should ensure that the resources dedicated to the target design, combined environment, integration and replacement of IT systems, planning and execution of data migration, and verification of results of these works are adequate to the scale and specificity of the modifications being introduced.

7.15. Bank should have formalised regulations for taking the ICT solutions used out of service. These regulations should specify, in particular, the following principles:

- decision making on taking systems out of service taking into consideration importance of a given system,[27]
- notifying interested parties (including users) on taking a given system out of service,
- conducting data migration and control of its correctness,

[25] See also: “IT Infrastructure Documentation”.

[26] See also: “Employee Education”.

[27] See section: “Information and IT Systems Classification”.

- archiving the solutions taken out of service, in particular ensuring access to data and their proper protection required under the law and conditions at the bank.
- update of the ICT infrastructure configuration in connection with taking a given solution out of service (e.g. in terms of disabling system accounts, reconfiguring firewalls, etc.),
- safe elimination of the ICT infrastructure components taken out of service,
- update of the bank's ICT environment documentation.

VI. Maintenance and Exploitation of ICT Environment

Data Management

8. Recommendation 8

Bank should have formal principles of the management of data used in its operation that include, in particular, data architecture and quality management and that properly support business activity of the bank.[28].

Data Architecture Management

8.1. Bank should have knowledge about what data are processed as part of its business activity, what their sources are (including whether these are the internal or external sources) and in what units, processes and systems the processing is performed. To that end, the bank should conduct inventory of the processed data and systematically review the results of such inventory for compliance with the facts. Taking into account the scale and characteristics of the business activity conducted and complexity of the ICT environment, the bank should also consider and make appropriate decisions whether the use of an electronic repository in order to perform the inventory referred to above and to collect its results is necessary.

8.2. The scope and level of detail of the inventory referred to above should depend on the scale of the bank's business activity, and validity of individual groups of data determined by the bank (i.e. data referring to an area of activity specified by the bank). In the case of significant data groups, the bank should develop their detailed documentation, including models of these data, which would describe, e.g. dependencies between the individual elements and flow between information systems, and should define appropriate data processing principles (policies, standards, procedures, etc.).

8.3. For each data group under inventory (or its subset) it is necessary to assign an entity (organisational unit, role, person, etc.) that is ultimately responsible for the quality of data and supervision over them, in particular, as regards the management of related rights and participation in the development of IT systems in which they are processed.

Data Quality Management

8.4. Bank should have formal rules of data quality management whose scope and level of detail should depend on the scale and specificity of the bank, and validity of individual groups of data determined by the bank. Regardless of the methodology and nomenclature in that respect adopted by the bank, these principles should include:

- periodic assessment of data quality,
- data cleansing,
- identifying the causes of errors in the data,
- ongoing monitoring of data quality.

[28] Data management, which may be defined as all activities related to the control, protection and improvement of data and information, also includes other elements, such as data development management, data security management and database management.These elements have been discussed in other parts of this document.

8.5. While performing periodic data quality assessment, the bank should, in particular, identify errors in the data and examine their impact on its business activity. Bank should also make sure that the data processed are adequate from the perspective of management (including measurement) of different types of risk, as well as meeting the reporting and analysis of the needs of their key recipients, i.e., whether and to what extent wrong decisions may result from a poor quality of the underlying data. To this end, the bank should in particular:

- specify the attributes used to assess data quality (e.g. accuracy, consistency, completeness, timeliness, etc.), and the frequency and methods of the attribute measurement (e.g. automatic comparison of data referring to the same operations stored in different sources, verification with source documentation based on a sample, data user satisfaction survey); with regard to individual data, it is possible to use different attributes and measurement methods,
- determine threshold values for these attributes, which are deemed by the bank to be acceptable with regard to individual data,
- perform regular measurement of data quality in accordance with the principles specified as part of the above activities.

8.6. While performing data cleansing (i.e. transformation of data assessed as erroneous into data that is fit for purpose of its use), as long as these activities are carried out in an automatic manner, the bank should give special attention to proper construction of cleansing algorithms. While improving some of the data, an invalid algorithm may in fact cause deterioration of other data (through side effects).

8.7. While identifying the causes of errors in the data, the bank should take into account, e.g. causes related to inadequate data processing procedures and a low efficiency of control mechanisms operating in the field of data quality, and implement new mechanisms and improve mechanisms that already operate (both at the stage of entering data to the system, and their subsequent processing), in particular through:

- modification of data collection and processing (including means of data exchange between information systems),
- introduction or modification of the ongoing control mechanisms (such as automatic validation rules, monitoring of data exchange interfaces, inserting data quality measurement points in business processes, reconciliation of data between systems, etc.),
- introduction or modification of periodic control mechanisms and other elements of data quality management,
- implementation of automated solutions that support data quality management.

These control mechanisms should also be reviewed and adjusted in the event of material modifications in business processes, organisational structure, information systems, etc.

8.8. Ongoing monitoring of data quality should include information obtained with the use of introduced control mechanisms. Aggregated information on monitoring results and results of periodic data quality assessments should be delivered at appropriate organisational hierarchy levels within the management information system[29].

8.9. While designing the approach to data quality management, especially in the absence of a separate organisational unit responsible for this area, the bank should ensure that the scope of responsibilities and distribution of tasks in this area is clearly and precisely defined. Bank should also provide an appropriate degree of confidentiality of the data used in the process of data quality management.

8.10. While designing and implementing data quality management process, the bank should in particular take into account typical factors that may lead to a poor data quality, which may include:

– manual entry of data into the system, which in the absence of sufficient input data validation makes them susceptible to human error, whereas – if the control is too strict – to entering data that are inconsistent with reality (e.g. inputting zeroes in required numeric fields which real values are unknown),

– data exchange between systems, which involves:

  ▪ threats arising from the lack of updates of data exchange principles when performing source or target system modifications,

  ▪ threats arising from the difficulty in making adjustments in the data identified as erroneous in a situation in which data exchange interfaces have already transferred the erroneous data to other systems,

– migration of data (including those related to the consolidation of systems), in which data structures in the source and target systems are often different, and data quality itself in the source systems is sometimes insufficient.

8.11. Bank should create an organisational culture in which ensuring adequate quality of data entered by employees to information systems is emphasised.

8.12. Bank’s approach to data quality management should take into account specific conditions related to the limited control of the bank over the quality of data from external sources (such as interbank information exchange systems BIK, AMRON or ZORO). Bank should take measures to enable assessment of data quality and its improvement, in particular by requiring external data providers to submit confirmation of data quality (in the form of independent audit results). Bank should also give particular attention to the quality of the data entered by the companies to external databases.

8.13. In view of the fact that the quality of data processed in the ICT environment has an important impact on the quality of bank’s management, and recipients of such data do not have a direct influence on the quality of such data, taking into account the particular characteristics of its organisational structures and data processing processes implemented, the

[29] See also: “Management Information System”.

bank should consider and make appropriate decisions whether appointment or designation of a committee responsible for data quality management is necessary.[30]

ICT Infrastructure Management

9. Recommendation 9

Bank should have formal principles of ICT infrastructure management, including management of its architecture, its components, efficiency, capacity and documentation that properly support business activity of the bank.

ICT Infrastructure Architecture

9.1. ICT network at the bank should ensure security of data being transferred. In particular, the network connecting the ICT infrastructure components whose disabling makes it impossible for the entire bank or its significant part to operate, should be able to function relying on backup connections.

9.2. Taking into account, in particular, the level of complexity and distribution of the ICT environment and level of risk exposure in respect of the ICT environment security, the bank should consider and make appropriate decision whether application of the solutions allowing network load monitoring and automatic launch of the backup connections is necessary.

9.3. Bank providing services via electronic distribution channels should have alternative access to telecommunication connections used for the purpose of these services in case of failure at the basic provider.

9.4. Connections of the internal network at the bank with external networks (especially with the Internet) should be secured with a firewall system[31].

9.5. Bank should consider and make appropriate decision whether it is necessary to divide the ICT network into sub-networks (logical or physical), separated by firewalls that ensure adequate access control, and to use other mechanisms (e.g. network traffic encryption) that take into account the required security level of data processed through:

- separation of the sub-networks for the internal systems at the bank from the sub-networks for data exchange systems with the external environment,
- separation of the back-office from front-office sub-networks,
- separation of sub-networks for the purpose of infrastructure administration,
- separation of sub-networks for the purpose of information system development.

9.6. Network traffic management principles and principles for the registering of events by the ICT infrastructure security monitoring tools and for reporting of these events should be formalised. These events should be subject to a systematic analysis. Taking into account

[30] It does not have to be a separate, dedicated committee. However, undertakings should ensure that the adopted solution allows effective implementation of tasks in that area.

[31] Firewall - physical or logical protection that controls the flow of data to and from a given infrastructure component and between sub-networks and networks (including between internal and external networks).

complexity of the ICT environment and exposure to risk in the area of the ICT environment security, the bank should consider and make appropriate decisions whether application of the IDS / IPS (*Intrusion Detection System* / *Intrusion Prevention System*) class solutions that improve the ICT infrastructure security through detection (IDS) and detection and blocking (IPS) of attacks in real time is necessary.

9.7. Bank should have formal principles of connecting the terminal equipment (computers, mobile devices) to the ICT infrastructure. Development of these principles should be preceded by a risk analysis in this area. In addition, if the bank allows employees to use personal devices for business purposes, it should develop formalised principles in this regard, specifying in particular:

– permissible scope of the use of such devices, with an indication of the type of information that may be processed using such devices[32],

– acceptable types of devices,

– acceptable applications which may be used by employees for business purposes,

as well as support enforcement and control of these principles through the IT solutions and systematically educate employees on the safe use of personal devices for business purposes[33].

9.8. The use by the bank of wireless network should involve analysis of the associated risks. In particular, the bank should determine what data may be accessed with the use of these networks and what authentication and encryption mechanisms will be used.

ICT Infrastructure Components

9.9. The type and configuration of each of the components of ICT infrastructure should result from the analysis of the role that a given element has in the ICT environment and the level of security required by information systems making use of a given component or data sent through the information system[34]. In particular:

– component type should be selected taking into account advantages and disadvantages of a given solution from the perspective of a point in the infrastructure where it is to be located (e.g. choice between hardware and software firewalls),

– while determining how to configure a component, the bank should be guided by the principle of minimising services provided by a given component (including e.g. open ports, supported protocols, etc.), simultaneously ensuring the planned functionality.

9.10. Bank should verify predefined settings made by the manufacturer of a device or a system, leaving a default configuration (and therefore a well-known one, i.e. in respect of standard accounts and passwords) significantly increases the level of ICT environment security risk.

[32] See sub-section: “Information and IT Systems Classification”.

[33] See also: “Employee Education”.

[34] See section: “Information and IT Systems Classification”

9.11. Bank should consider (taking into account in particular the level of complexity of the ICT environment, level of risk exposure in respect of the ICT environment security and specificity of the business activity) and make appropriate decisions whether to:

- develop configuration standards,
- maintain the register of infrastructure components, along with basic information on their type and configuration,
- maintain electronic repository of the configuration copy used.

9.12. Bank should have formalised principles for the introduction of modifications to the configuration of ICT infrastructure components that take into account the significance of individual components and that ensure:

- implementation of modifications in a planned and controlled manner, including the impact of a given modification on other components,
- protection of components against the introduction of unauthorised modifications,
- the ability to withdraw modifications, including availability of emergency backup copies of component configuration,
- the ability to identify people who introduce and approve individual configuration modifications.

9.13. In case of the transfer of the equipment for repair or maintenance to an external entity, the bank should ensure that the entity does not have access to the data of high confidentiality stored in these devices or that responsibility for maintaining confidentiality[35] of such information during provision of services and upon termination of cooperation is governed in the agreement with the external entity.

9.14. Bank should have formal principles of taking ICT infrastructure components out of service, in particular those that ensure mitigation of risk associated with the possibility that the information stored on the components taken out of service leaks.

9.15. Configuration of the firewall system should ensure that non-standard activities are registered in order to allow their analysis for detection of internal and external attacks. The firewall system should also provide outbound traffic control in order to block attempts to establish session from inside of the network by malware.

9.16. Bank using server virtualisation[36] technology should analyse the risks associated with that technology in relation to its own conditions. Based on the results of the above analysis, the bank should ensure proper operation of the relevant control mechanisms. Good practice in this area may include e.g.:

- cover with close supervision the availability of physical machine resources (processors, operational memory, disk space, etc.)

[35] See section: “Information and IT Systems Classification”

[36] Server virtualisation - technique that allows simultaneous operation of multiple logical servers on a given hardware platform

– placement of the service console and all the tools for managing resources virtualisation platform in the form of sub-network dedicated to the management of that platform

– limiting the potential for abuse of resources by each virtual machines and sharing the clipboard between the physical and the virtual machines,

– specific protection of physical machines on which virtual machines are located, against unauthorised access to the files of virtual machines (due to the small number of files that make up the virtual machine, it is particularly susceptible to being stolen) and other threats such as *"Denial-of-Service"* attacks[37] (in the case of server virtualisation, consequences of such attacks on the physical machine may be much more serious, as they affect multiple virtual machines).

9.17. Bank should monitor ICT networks, ICT infrastructure components, network services and information systems in respect of security and correct operation in accordance with the associated level of risk. The degree of automation of the monitoring referred to above should be appropriate to the complexity of ICT environment at the bank.

9.18. Bank should consider (taking into account in particular the level of complexity of the ICT environment, level of risk exposure in respect of the ICT environment security and specificity of the business activity) and make appropriate decisions whether introduction of additional protection in the e-mail system used which would facilitate control of information with high degree of confidentiality[38] contained in electronic mail sent outside of the bank, should be introduced.

9.19. Printers used at the bank for printing documents containing highly confidential information should be protected against the possibility of information leakage (for network printers, e.g. through encrypting the data sent to them and printing tasks stored in them and appropriate user identity verification mechanisms). The bank should also ensure an appropriate level of protection with regard to sensible paper forms which are stored in the printers' feeders.

9.20. Network scanners used at the bank for scanning documents containing personal data or whose unauthorised disclosure could expose the bank to significant losses, should be protected from the possibility of information leakage (e.g. through transmission of data in encrypted form, or by other mechanisms). Solutions in this area at the bank should also ensure that scanned documents are available only to authorised persons.

9.21. Configuration of the ICT infrastructure components should undergo periodic verification for other changes in the environment, as well as security gaps disclosed. Bank should consider (taking into account in particular the level of complexity of the ICT environment, level of risk exposure in respect of the ICT environment security) and make appropriate decisions whether support of the process by control activities that automate tools is necessary. One of the tools that should be systematically used to assess the effectiveness of control mechanisms in highly significant ICT environment, are penetration tests.

[37] *Denial-of-Service-type attack*- attack consisting in an attempt to prevent the use of a given ICT environment component by other components of the environment or by authorised users.

[38] See sub-section: "Information Classification".

Update of the ICT Infrastructure Components Software

9.22. Bank should have formalised principles for carrying out software updates, both in reference to computers and mobile devices, and other elements of the ICT environment (including updates of operating systems, database management systems, utility software, network equipment software etc.), taking into account the importance of such software and the level of criticality of each update

9.23. Principles concerning update of the ICT infrastructure components software should indicate, in particular, people responsible for making decisions with regard to changes in the production environment.

9.24. Before updating the ICT infrastructure components software in the production environment affecting the IT systems that are highly significant from the perspective of the bank[39], the bank should consider and make appropriate decisions whether verification of the impact of update on the test environment is necessary.

9.25. Timeliness and correctness of updates installation should be subject to periodic control. Bank should consider (taking into account in particular the level of complexity of the ICT environment, level of risk exposure in respect of the ICT environment security) and make appropriate decisions whether application of automatic software update installation mechanisms on personal computers and mobile devices, as well as automated tools for the analysis of the ICT environment for software validity is necessary.

9.26. Bank should aim at reducing of the number of ICT environment components without adequate vendor support, in particular as regards the elements significant from the perspective of the bank's activities. In this regard, the bank should in particular:

– identify and record cases of components in the ICT environment without adequate vendor support and assess the associated risk,

– analyse the possibility of exchange of such components to components covered by an adequate support or taking other measures to control the associated risk.

This should be done in a timely manner, i.e. taking into account the period required to implement measures to ensure the control of risk arising from the use of components that are not covered by vendor support.

Management of the ICT Infrastructure Components Capacity and Efficiency

9.27. ICT infrastructure at the bank should be characterised by:

– scalability, defined as a timely increase in efficiency and capacity,

– redundancy, defined as the ability to handle an increased number of transactions on the basis of resources currently used (temporary increases in the load may result e.g. from handling a higher number of transactions during a month's end, instalment payments, payroll accounting, servicing promotional activities, period near holidays, unavailability of a part of the ICT infrastructure's components, etc.).

[39] See: section "IT Systems Classification"

9.28. Bank should have documented principles for the management of ICT infrastructure components' performance and capacity taking into account the significance of individual components for the business activity of the bank and the relationship between these components, including in particular:

– defining performance parameters (e.g. system response time, processing time) and capacity (e.g. ICT network load, utilisation of mass storage devices, processor utilisation, the number of open connection sessions), together with an indication of the warning and borderline values in this regard,

– monitoring of the above parameters,

– trend analysis and forecasting of the performance and capacity demand, taking into account the strategic objectives of the bank, in particular with regard to the planned number of customers being served as well as changes in the business activity profile and the associated expected volume of data processed,

– taking actions in the cases of exceeding the warning and borderline values of the above parameters, and when the analyses of the performance and capacity demand show that current resources are not sufficient to meet the demand,

– reporting in respect of the performance and capacity of ICT infrastructure components, in particular, to information system owners.

9.29. In order to increase the efficiency of performance and capacity management, the bank should consider (including in particular the level of complexity of the ICT environment and the exposure to risk in respect of the ICT environment security), and make appropriate decisions concerning:

– the use of tools that allow automated monitoring of resource load,

– formalisation of parameters of the quality of services provided by the ICT environment for internal and external users, and inclusion of reporting in this regard to the management information system[40].

9.30. Bank should periodically verify the ability of ICT environment in the reserve centre to maintain the required performance and capacity parameters.

ICT Infrastructure Documentation

9.31. Bank should ensure that documentation of individual ICT environment components (including their configuration) and the relationship between them:

– is valid,

– its level of detail is adequate to the level of significance of each of these elements,

– enables reliable analyses of the environment in terms of its security and optimisation,

– allows localisation and removal of the causes of failure,

[40] See also: "Management Information System".

– enables recovery of operations should such need arise,

– allows effective execution of internal control tasks.

9.32. Documentation of the ICT infrastructure should be subject to protection adequate to its sensitivity. The scope of documentation (in particular documents describing details of the configuration and operation of security systems) available for individual employees should not go beyond the minimum arising from the scope of duties entrusted to them.

9.33. Future versions of the documentation should be marked and should be accompanied with the list of modifications in the document (date of introduction, persons responsible for development and approval).

9.34. Bank should consider (including in particular the level of complexity of the ICT environment, the frequency of technical modifications and the number of administrators and technicians), and make appropriate decisions whether implementation of electronic ICT infrastructure documentation repository is necessary.

9.35. Bank should have procedures for the operation and administration of each of the elements of ICT environment. Completeness and validity of these procedures should be subject to periodic review, especially in the case of ICT environment components in which frequent modifications are introduced.

Cooperation with External Providers of Services

10. Recommendation 10

Bank should have formal principles of cooperation with external service providers that ensure security of data and correct operation of the ICT environment, taking into account the ICT services provided by entities included in the bank's capital group..

10.1. Taking into account specificity of the banking sector, out of services offered by external service providers, information technology activities are characteristic due to their direct impact on the quality and security of services provided to clients and reputation of the bank. Simultaneously, depending on the specific conditions at the bank, the impact of the quality of cooperation with external service providers on the quality of services provided by the bank to clients varies greatly. Therefore, management of relationships with external service suppliers should be adapted to these conditions.

10.2. The bank should not treat outsourcing of any services to any external service providers as an exemption from the liability for the quality and security of services provided to clients and security of client data.

10.3. Procedures for the selection of external service providers, especially in the case of services of special importance to the bank, should include the risks associated with given services and cover, in particular, assessment of the economic and financial condition of external service providers, security and quality of services provided by the external providers (possibly also based on the experience of other entities).

10.4. Bank should analyse the risk associated with bankruptcy of external service providers or sudden termination of cooperation and have effective contingency plans related to the occurrence of such situations. Where possible, the bank should reduce the number of cases in which an external service provider has monopolist position in relation to the bank.

10.5. Bank should monitor the quality of services provided by external service providers, and important findings resulting from such monitoring should be periodically presented to the Management Board of the bank under the management information system.[41] The scope, frequency and methods of monitoring and reporting should take into account specificity of the services provided and their significance from the perspective of continuity and security of activities performed of the bank.

10.6. If the services provided by external entities include processing of data with a high degree of confidentiality or significance to the bank outside the ICT infrastructure of the bank (e.g. in the C*loud Computing* model or other *Application Service Provision* models in external data processing centres, etc.), the bank should in particular:[42]

– introduce the necessary control mechanisms to ensure confidentiality of data (e.g. through their encryption),

[41] See also: "Management Information System".

[42] See sub-section: "Information and IT Systems Classification".

- ensure that the information on any incidents that threaten security of the data is reported by suppliers,
- have information about the geographic locations in which such data are processed, about the law that is applicable in that location in this respect, and ensure that the services provided are in compliance with the law applicable in Poland,
- ensure effective mechanisms that allow safe completion of cooperation (in particular in terms of return of data and their deletion along with all copies, by service providers),
- consider and make appropriate decisions whether introduction of an obligation for the supplier to produce certificates of compliance with internationally recognised information security standards (especially in the case of data processing outside the European Economic Area) is necessary.

10.7. Bank should exercise control over the activities of service providers in terms of services provided by them. Depending on the nature and level of significance of these services from the perspective of bank and the classification of information processed by service providers[43] (in particular resulting from legal requirements relating to the processing of personal data of the bank's clients), such control may, in particular, consist in:

- verification of the control mechanisms used by suppliers, including measures to protect and control access to the premises of service providers, in which provision of services for the bank is taking place,
- review of results of control mechanisms verification conducted through internal audit of service providers or through independent internal audits.

The possibility to exercise control over the activities of external service providers should be regulated in agreements concluded with them.

10.8. In addition, agreements concluded with service providers should, if possible, determine:

- responsibility of the parties to the agreements,
- the scope of information and documentation transferred by service providers in connection with the services provided,
- principles of the exchange and protection of information, including the terms of awarding to employees of external entities of access authorisations to bank's information and ICT environment resources, which take into account the specificity of the applicable law and regulations of the bank in this regard; in the case of service providers who have access to information with a high degree of confidentiality, the issue of responsibility for maintaining the confidentiality of such information during performance of these services and upon termination of the agreement should also be regulated,

[43] See: subsection "Information Classification"

- principles relating to the rights to software (including its source codes) during cooperation and after its termination, in particular access to the source codes if provision of software development support services by the supplier (e.g. using source code deposit services) is terminated,
- parameters related to the quality of the services provided and the manner of monitoring and enforcement of the parameters,
- principles and procedures of handling reports of problems in terms of the services provided,
- principles and procedures of the updating of the software infrastructure components under control of the supplier,
- principles of cooperation in the event of an ICT environment security breach incident,
- principles of further outsourcing of activities to subcontractors of external service providers,
- contractual penalties associated with failure to comply with contractual conditions, in particular as regards the security of information processed by service providers.

10.9. Agreements concluded by the bank with external service providers should ensure that the provision of services is compliant with legal requirements, internal and external regulations and standards adopted at the bank[44].

10.10. Contract templates or contracts made by the bank with external service providers should be verified to an appropriate extent by the units of the bank which are responsible for the legal area and ICT environment security area.

10.11. Bank should make arrangements for cooperation with employees of external service providers, taking into account in particular:

- conditions for granting access to information with a high degree of confidentiality[45],
- principles of supervision over the activities of external employees,
- the necessity to ensure that every external employee with access to information with a high degree of confidentiality is covered by at least the same security restrictions, as employees of the bank with access to such information.

10.12. Principles of cooperation between the bank and external service providers should take into account the principles of communication and coordination in terms of activities performed by the external service providers (e.g. in terms of data migration, maintenance, ICT infrastructure scanning, etc.), that minimise their negative impact on the quality and security of services provided to clients of the bank.

10.13. Bank should give special attention to the risk associated with granting the rights of access administration to the bank's information systems to external service providers (in particular to those who are not members of the capital group).

[44] See also: “Formal and Legal Security”.

[45] See sub-section: “Information and IT Systems Classification

Access Control

11. Recommendation 11

Bank should have formal principles and technical systems that ensure adequate level of control over the logical access to data and information and physical access to key elements of the ICT infrastructure.

Logical Access Control Mechanisms

11.1. IT systems operated by the bank should have access control mechanisms that allow to clearly identify and authenticate user identity and to authorise users.

11.2. Parameters of the access passwords (including password length and complexity, frequency of modifications, the ability to reuse a historic password) and the principle of blocking user accounts should be established in the internal regulations, including classification of the system and other associated conditions, including legal conditions and those related to standards adopted by the bank[46] [47] Functionality of the information systems used should, whenever possible, enforce application of principles adopted at the bank regarding access passwords and blocking a user account if a wrong password is used.

11.3. Authorisation management should be formalised in internal procedures defining the principles of applying for, granting, modification and withdrawing access to the systems or their functionality, and access monitoring. The scope of access granted should not go beyond user material responsibilities and authorisations (including external users, e.g. banking agencies) and should be reviewed periodically.

11.4. Bank should carry out regular reviews of the authorisations granted, including compliance of the actually granted authorisations in the computer systems with both authorisations in the authorisation registry, and with the material scope of duties and authorisations of individual users. Frequency of these reviews should result from the analysis of the level of risk associated with individual employees and IT systems, but it should not be less frequent than annual one. Reviews of authorisations should be made to the extent applicable also in the case of modifications in the functionality of IT systems and modification of employee responsibilities. Substantial irregularities revealed as a result of these reviews and measures taken in connection with them should be reported under the management information system.[48]

11.5. In order to increase the efficiency of management and supervision and to limit the risk of awarding inadequate access, the bank should consider (including in particular the level of complexity of the ICT environment and the exposure to risk in respect of the ICT environment security), and make appropriate decisions concerning:

– development of standard access profiles for specific groups of employees or positions,

[46] See section: "Information and IT Systems Classification".
[47] See also: "Formal and Legal Security".
[48] See also: "Management Information System"

– application of tools that make management of user authorisations automatic (in particular historical authorisations registration).

11.6. If possible, the bank should limit users' access to functions allowing to them to independently increase their own authorisations. In situations where the above principle cannot be followed (e.g. in the case of IT system administrators) other control mechanisms in this area should be provided.

11.7. In the case of systems whose unauthorised use may result in particularly high losses, the bank should consider and make appropriate decisions whether merging passwords with other user identity verification mechanisms (e.g. tokens, electronic identification cards, etc.) is necessary.

11.8. All users of IT systems at the bank should be informed about the responsibility for ensuring confidentiality of passwords and for the consequences of actions performed with the use of their accounts.

11.9. Authorisation management principles applicable at the bank should in particular take into account the threats associated with the misuse of privileged user authorisations. Taking into account, in particular, the level of complexity of the ICT environment and level of risk exposure in respect of the ICT environment security) the bank should consider and make appropriate decisions whether introduction of mechanisms that ensure registration each time and the possibility to monitor access to the most sensitive components of the ICT environment at the level of privileged authorisations is necessary.

11.10. Data processing systems of high significance for the bank should have mechanisms for automatic registration of incidents taking place in them in such manner that records of such registers could - provide credible evidence of the use of these systems that is improper or inconsistent with the scope of user tasks, if such necessity arises.[49] Incident registration mechanisms should also prevent unauthorised deletion or modification of records.

11.11. Bank should have formal cryptographic key management principles, including in particular, creation, storage, distribution, destruction and archiving of such cryptographic keys that ensure protection of such keys against unauthorised modification or disclosure.

Physical Access Control Mechanisms

11.12. An important element of the ICT environment security is to control physical access to the premises where servers, other key elements of the ICT infrastructure and equipment that supports its operation are located (including UPS, generators, air conditioning and electrical switchboards). Physical access control mechanisms should provide access only to authorised persons (i.e. to those who need to have access due to the scope of their duties) and initiate an alarm in the event of access attempts by unauthorised persons. These mechanisms should also include registration of user traffic. The solutions applied should be adequate to the level of risk associated with components located throughout the premises, specific conditions (including conditions related to the premises) the bank and the scale and nature of its operations.

[49] See section: "Information and IT Systems Classification"

11.13. At the premises where key elements of the ICT infrastructure are located, if no exceptional circumstances arise, persons residing at the premises should not be allowed to take photographs, make audio / video recordings etc. Permits providing for exceptions in this regard should be issued by duly authorised persons and registered.

Malware Protection

12. Recommendation 12

Bank should ensure proper protection of the ICT environment against malware.

12.1. Bank should provide automatic protection against malware (such as viruses, Trojan horses, worms, rootkit[50] software etc.), both in the case of central ICT infrastructure elements requiring such protection (servers, domain controllers, etc.) as well as personal computers and mobile devices. Such protection should be implemented on a continuous basis, and the users should not be able to disable it. The scope of protection should correspond to the exposure of each infrastructure component to threats, as well as potential severity of the impact of such threats on the bank.

12.2. Applications that protect against malware, and malware signatures must be updated on a regular basis. If possible, the bank should ensure that the above is verified each time when an attempt to connect a device to the internal network at the bank is made.

12.3. Bank should have formalised principles for protection against malware, including in particular:

– the manner of dealing with different kinds of malware detected,

– decision-making procedures to discontinue the use of the ICT environment components at risk or their isolation from the remaining part of the environment,

– procedures for notifying relevant units of the bank about a threat.[51]

12.4. Regardless of the level of automatic protection used against malware, awareness of the end users of security rules is also key from this perspective Therefore, the bank should ensure appropriate level of user education in that respect[52].

User Support

13. Recommendation 13

Bank should provide internal system users with support regarding resolution of problems related to their operations, including those arising from failures and other non-standard incidents affecting their use.

13.1. Operation of the area providing support to the internal users of the information systems should be adapted to the scale of business activity, ICT environment complexity and

[50] Rootkit software - tool that modifies system files in such manner as to hide its presence on the computer from the user, anti-virus software, etc., and allows to perform actions specified by its developer (such as capturing passwords or preventing update of the anti-virus software) without user's knowledge.

[51] See also: "IT Environment Security Breach Management".

[52] See section "Employee education"

the number of its internal users, and should take into account possible dependence on the external service providers.

13.2. Functioning of support provided to the internal users of the IT systems should be formalised in proportion to the complexity of the ICT environment at the bank and the number of internal users of its IT systems. Reports should be registered and analysed in order to take preventive measures in relation to the identified problems. Persons responsible for providing support to users should also be trained in the identification and escalation of ICT environment security incidents.[53]

13.3. Bank should consider (including in particular the level of complexity of the ICT environment and the number and characteristics of its users), and make appropriate decisions whether support of user reports handling by the IT system allowing in particular collection and reporting of the data on occurring problems and monitoring the quality of support provided is necessary.

Employee Education

14. Recommendation 14

Bank should undertake effective measures aimed at achievement and maintenance of an appropriate level of employee competencies in the area of ICT environment and security of data processed in that environment.

14.1. Bank should maintain the qualifications of all employees at a level appropriate to ensure security of the information processed in the ICT environment and to enable the use of the hardware and IT systems. This level should be varied depending on, e.g. risks associated with the level of authorisations and competency of individual employees and their role in the ICT environment security management system.

14.2. In order to ensure an appropriate level of qualifications of the employees in this regard, the bank should use appropriate forms of training, provide proper materials, as well as carry out a variety of educational campaigns aimed at increasing information security culture (e.g. with the use of posters or screansavers). Bank should also consider and make appropriate decisions whether rewarding behaviour that supports information security culture is necessary.

14.3. As part of employee education, the bank should take into account, e.g. the risk associated with the use of mobile devices, the use of personal IT equipment for business purposes and the use of business equipment for personal purposes, publishing of information on the bank on the Internet by employees (especially on social network sites) and sociotechnical attacks, and to inform employees about the process of disciplinary proceedings against persons who fail to comply with safety procedures

[53] See section: "ICT Environment Security Breach Management".

IT Environment Continuity

15. Recommendation 15

Continuity Management should take into account special conditions related to the ICT environment and data processed in that environment.

Continuity Plans and Contingency Plans

15.1. Business continuity plans and contingency plans of the bank should fulfill conditions defined in „Recommendation M on the management of operational risk at banks".

15.2. Bank should consider (taking into account in particular the level of risk exposure in respect of the ICT environment security and scale and specificity of the business activity) and make appropriate decisions on the appointment or designation of a committee competent for supervision over availability of necessary resources that allow continuity or recovery of business activity.[54]

15.3. Since recovery of the ICT environment is usually necessary to resume business processes, the bank should pay special attention to business continuity management in terms of the units responsible for the operation of the information technology area.

15.4. Documentation of business continuity management at the bank as regards the ICT environment (in particular procedures for data replication, creation of backup copies and recovery procedures) should take into account classification of IT systems and the information processed in them , as well as the relationship between these systems.[55] Validity of such documentation should be verified on a regular basis.

15.5. Bank should have formalised system of business continuity management documents distribution in the ICT environment that would ensure both its confidentiality and availability to appropriate persons.

15.6. As part of the business continuity management approach, the bank should take into account dependency on external service providers who are of key importance from the business continuity from the bank's perspective. To this end, the bank should:

– determine the procedure for communication and cooperation with external service providers in emergency situation,

– take into account participation of external service providers in the process of testing business continuity management[56],

– develop principles associated with a need to change the external service provider during emergency situation.

Technical Resources and Physical and Environmental Conditions

15.7. Bank should have technical resources adequate to the scale and specificity of the business activity which allow ongoing functioning of key processes and their recovery in

[54] It does not have to be a separate, dedicated committee. However, the undertaking should ensure that the adopted solution allows effective implementation of tasks in that area.

[55] See section: "Information and IT Systems Classification"

[56] See sub-section: "Efficiency Verification of the Contingency Management Approach".

emergency situation, in particular, with regard the following elements defined for these processes:

– parameters that determine the maximum time for the recovery of these processes[57],

– parameters that determine the maximum amount of the data stored in the IT systems may be lost[58] (e.g. for which period data may be lost)

15.8. In the event of a serious failure or unavailability of the primary data processing centre, the bank should be able to reproduce the ICT environment (adequate to the assumptions of the contingency plan) in the backup location. This location should be sufficiently distant from the primary centre, in order to minimise the risks associated with the unavailability of the two centres as a result of a single cause (e.g. flood). Recovery of the environment should be formalised in detailed internal regulations defining the responsibilities, necessary resources, order and manner of recovery of the ICT environment components.

15.9. Characteristics of the backup centre operation should be adapted to the scale and specificity of the operations conducted and take into account the maximum period of service unavailability acceptable to the bank.

15.10. Uninterrupted and secure operations of the ICT environment depend on physical and environmental security in the locations where key elements of the ICT infrastructure are located, in particular as regards the conditions associated with the continuity of electrical power and stability of the parameters, temperature, humidity and dust levels, as well as key elements of the protection against flood, fire, burglary and theft or intentional damage. Therefore, the bank should identify threats in this respect and analyse their potential impact on the security of ICT environment and business continuity (especially when the backup centre resources do not allow immediate resumption of operation). Such analysis should allow to determine whether the location the premises where key elements of the ICT infrastructure are located is adequate and whether they are adequately protected.

15.11. While carrying out the above analysis, the bank should consider the risk associated, in particular, with:

– location and vicinity of the building (including airports, military objects in the area, etc.),

– location and vicinity of the premises where key elements of the ICT infrastructure are located (in particular the risk associated with location of the premises in the cellar or at the loft),

– construction conditions (e.g. durability of the ceilings, tightness of the premises, quality of the lightning protection system).

[57] RTO - Recovery Time Objective

[58] RPO –Recovery Point Objective

15.12. In order to ensure proper physical and environmental conditions at the location where key elements of the ICT infrastructure are located, the bank should comply with the following principles:

- doors, windows, walls and ceilings at the premises where key elements of the ICT infrastructure are located should ensure proper mechanical, fire and burglary protection,
- flammable materials should not be placed at the premises where key elements of the ICT infrastructure are located or, should such need arise, such materials should be properly secured (in cabinets that ensure fire protection),
- extinguishing agents used should minimise the risk of damage to electronic devices and data stored in them,
- burglary and fire protection systems should immediately notify the persons responsible for such protection and the initiation of fire-fighting and rescue. Bank should also consider and make appropriate decisions whether supplementation of the fire protection system with automatic fire extinguishing equipment is necessary,
- in areas where ICT infrastructure components are located must be environmental parameters (e.g. temperature, humidity, dust levels, etc.) should be maintained at the level specified by the manufacturers of these components. The devices used by the bank to control these parameters should be characterised by a proper efficiency and redundancy (in case of failure) bank should consider and make appropriate decision whether application of solutions for automatic monitoring and regulation of environmental parameters is necessary,
- selection of mechanisms ensuring continuity of electrical power should be done based on the specificity of a given bank. Emergency power supply based solely on battery power supply (UPS) makes it possible to maintain operation of resources for a short period and usually to a limited extent, therefore, the bank should consider and make appropriate decisions whether an independent power supply based on a generator, launched automatically to the greatest extent possible in the event of failure of the primary power supply, as well as the use of multiple electric lines is necessary.

15.13. In the event of a temporary transfer of the ICT equipment to another room (e.g. in connection with a renovation) the bank should provide adequate physical and environmental conditions, and an appropriate level of access control in that room.[59]

15.14. Effectiveness of the mechanisms for ensuring proper physical and environmental conditions in locations where key elements of the ICT infrastructure are located, should be subject to periodic verification.

Backup Copies

15.15. One of the measures aimed at ensuring business continuity in the event failure or disaster are emergency copies of data, IT systems instances and key ICT infrastructure

[59] See section: “Physical Access Control Mechanisms”.

components configurations. Bank should have formal principles for the management of data carriers that hold emergency copies. These principles should cover in particular:

- scope, method and frequency of making data copies,
- methods of data carrier identification,
- place, time and manner of secure storage of the data carriers,
- manner and form of authorisation of modifications of data carriers and deletion of data,
- roles and responsibilities in data carrier management,
- methods of proper and permanent deletion of unnecessary data (in terms of both the liquidation of data stored on data carriers being still in use and utilisation of data carriers taken out of use).

15.16. Correct manner of making emergency copies and the possibility of reproducing the data stored on them should undergo periodic control. Such control may be automatic, however, in such case competent persons should be notified of the control results

15.17. Bank should have detailed regulations and instructions on the manner of recovery of the ICT environment components based on emergency copies. These documents should be written in such manner that the process may be carried out by third parties having appropriate qualifications and licenses to (i.e. those who do not deal with the administration of a given environment component). The recovery process of the ICT environment components should undergo regular tests.

15.18. Bank should provide integrity of emergency copies from their creation to disposal. This means that throughout this period, the copies should reflect the actual resources at the time when the copies were created, which excludes the possibility of removing any information recorded on them. Regulations and instructions for the recovery of data from emergency copies should include principles of introduction to the data recovered of modifications arising between the creation of an emergency copy (or their sequence) and its use to restore the ICT environment before failure.

15.19. Copies, especially those transported or transmitted outside the bank, should be secured (e.g. with cryptography) against unauthorised access, at a level corresponding to the classification of data stored on them[60]. Data carriers containing copies should be stored in a manner that minimises the risk of damage (e.g. in a fire, flood, by magnetic field), or unauthorised modification. They should also be stored separately from the environment components to which they relate.

15.20. Damaged data carriers or data carriers taken out of use should be destroyed in a manner that prevents recovery of data.

[60] See section: “Information and IT Systems Classification”

Efficiency Verification of the Contingency Management Approach

15.21. Bank should verify the effectiveness of adopted approach to business continuity management as regards the ICT environment, including the ability to restore operations based on the backup environment.

15.22. Frequency, scope and method of testing (such as simulations, overall operational tests, etc.) should take into account the scale and characteristics of business activity of the bank and the risk associated with individual components of the ICT environment.

15.23. Test plans, especially in the case where they may affect the current business activity of the bank should undergo consultation in the organisation and should be approved by the Management Board of the bank.

15.24. Test results and plans for corrective measures to be taken to remove the identified irregularities should be documented. The Supervisory Board and Management Board of the bank should be informed of the test results and the timeliness and effectiveness of corrective measures taken.

Electronic Access Channels Management

16. Recommendation 16

Bank providing services with the use of electronic access channels should have effective technical and organisational solutions that ensure security of clients' identity, data and funds, and should educate clients on the principles of safe use of these channels.

Client Identity Verification

16.1. Confirmation whether or not the attempt to contact, access, or perform a transaction is authorised is essential for the banking services provided through electronic access channels. Therefore, the bank should define and use possibly reliable methods and means of:

- verification of a customer's identity when opening a bank account, also where such agreements are concluded remotely (without a customer being physically present in a bank's branch), taking into account the respective legal requirements[61],
- confirmation of the identity and authorisation of clients using electronic access channels that minimises the risk of granting access to unauthorised persons.

16.2. Bank should choose methods to authenticate the identity of clients using electronic access channels on the basis of an analysis of risks associated with these channels. Such analysis should be carried out on a systematic basis and should reflect transactional capacity of a given access channel, data processed by the channel, identified attack techniques, and simultaneously the ease of use by a client of different identity authentication methods. Typical methods used for identity confirmation in electronic access channels include, among others, the PIN codes, static passwords, electronic signatures, smart cards, one-time passwords, tokens, biometric data or digital certificates, while the methods of identity verification may be based on single or multiple factors (e.g. using both static and one-time passwords). Bank

[61] See section: "Formal and Legal Security".

should also consider whether and to what extent the use of multifactorial identity verification would increase the level of client security.

16.3. Bank should consider and make appropriate decisions whether application of other security mechanisms, such as verification of the place and time of logging in to the electronic access channels is necessary in the case of electronic banking services provided to companies.

Security of Client Data and Funds

16.4. In addition to these measures, in order to prevent unauthorised access to the client's account by means of electronic access channels, and to prevent clients from repudiation of performed transactions, IT systems used in the area of these channels should be designed and configured in such manner as to ensure a sufficiently high level of integrity, confidentiality and availability of data associated with transactions (as well as other data processed using these channels) throughout their processing (both at the bank and by external service providers). In addition, the bank should ensure that:

- it has principles of granting authorisation to electronic access channels and detection of manipulation with transaction or electronic banking data to minimise the risk of internal fraud,
- electronic banking connection sessions are encrypted and additional mechanisms are introduced that make these sessions resistant to the greatest extent possible to manipulations (e.g. by closing the session if no user activity for a specified period or after closing of the client application without logging off is detected),
- IT systems used in electronic access channels allow identification and preservation of evidence that may be used in any legal proceedings (in particular, the risk of such evidence being lost or rejected because of inadequate protection of data is minimised),
- IT systems used in electronic access channels are designed in a way that minimises the probability of accidental initiation of a transaction by authorised users,
- solutions used in electronic access channels provide the bank with access to audit trails, including in particular:
    - transactions,
    - opening and closing of client's account,
    - modification of client data,
    - any limits granted to a client and permissions to exceed them,
    - successful and unsuccessful attempts to log in to the systems,
    - all cases to grant, modify or revoke access authorisation to such systems.

16.5. If in the provision of services through electronic access channels is effected with the participation of external service providers, the bank should ensure that it has appropriate programs for security management of the information processed for the bank, in accordance with the standards adopted at the bank[62].

16.6. Agreements concluded with clients concerning the use of electronic access channels should specify information protection principles and specific access conditions (in particular identity verification methods), if the applicable law requires conclusion of an agreement with a client in a given case.

16.7. Bank should provide its clients with communication channel (e.g. e-mail inbox, telephone number) for notifying the bank about security incidents in the electronic access channels identified by clients (e.g. attacks based on the *phishing* technique).

Client Education

16.8. Bank should aim at providing clients using electronic access channels with appropriate level of knowledge necessary to understand the threats associated with the use of these channels and the use of effective methods for protection against these threats. This may be achieved e.g. through clearly visible message published on the internet banking websites, through leaflets, e-mails, etc.

16.9. Due to the fact that a major part of the channel used to render electronic banking services is out of scope of the bank's direct control, the bank should inform clients about the risk related to in particular:

– inadequate protection of the data used to log in to the electronic access channels,

– inadequate protection of the equipment used for the implementation of services provided through electronic access channels (mobile phones, computers), including the significance of using anti-virus software and firewalls, physical access control, regular software updates, etc.,

– other techniques designed to intercept information that allows access to the account (e.g. through attacks based on the *phishing* technique), together with an indication of the ways to protect oneself against such techniques.

End-User Computing[63] Management

17. Recommendation 17

Bank should have formal principles of management of the so called End-User Computing that effectively mitigate the risk related to usage of such tools.

17.1. Due to the risk associated with the use of End-User Computing (such as high susceptibility to programming errors, probability of data loss is usually higher than in the case of conventional IT systems, high susceptibility to interference in the data processing

[62] See also: "Cooperation with External Providers of Services".

[63] End-User Computing, EUC – tools developed and operating based on applications such as MS Excel or MS Access installed on personal computers, which allow users who are not programmers to create business applications.

algorithms contained in these tools, etc.), in the management of such software the bank should in particular:

- identify important end-user computing, i.e. such that processes data with high relevance to the bank or such that is important from the perspective of processes implemented at the bank,
- document important end-user computing, including its role in the business processes, scope of data processed, data processing algorithms, etc.,
- keep a register of the important end-user computing operating within the bank,
- ensure an adequate level of security of important end-user computing (e.g. by protecting folders where it is stored, or blocking the possibility to edit forms) in order to prevent unauthorised modifications, both in the tool itself, as well as data stored in it,
- have formalised rules for creating, testing and making changes to the significant important end-user software,
- identify the threats and problems associated with the use of end-user computing in specific business areas and, if significant risks or problems in this area are revealed, consider and make appropriate decisions whether replacing it by the functionalities of the existing or new systems is necessary.

VII. ICT Environment Security Management

ICT Environment Security Management

18. Recommendation 18

Bank should have a formalised and effective ICT environment security management system, including activities related to the identification, assessment, control, mitigation, monitoring and reporting of risk in that area, integrated with a risk management and information security system at the bank.

18.1. ICT environment security management system should be based on the strategy of the bank in the ICT environment security and be based on formalised internal regulations. Information security policy should be a basic document in this regard.

18.2. ICT environment security management system should be the subject of systematic reviews aimed at introduction of possible improvements and accounting for changes in both the environment of the bank and its internal environment.

18.3. Bank should examine the benefits of international standards (or their Polish equivalents) in the field of information security (such as ISO / IEC 27000 standards) and make a decision on whether to adapt the ICT environment security management system functioning at the bank to the requirements of these standards.

18.4. Bank should ensure the closest possible integration of the ICT environment security management system with the operational risk management process. For this purpose, the bank should, e.g. use appropriate operational risk management tools in the ICT environment security management system, such as tools based on the economic environment and internal control factors self-assessment of operational risk, scenario analysis or risk maps.[64]

ICT Environment Security Risk Identification

18.5. Identification of the ICT environment security risk is aimed at determining the related risk that may cause losses (including financial losses) to a given institution and determining where, how and why these threats may occur.

18.6. Identification of the ICT environment security risk should be carried out systematically and be based on:

- identification of the risk associated with potential ICT environment security breach prior to the occurrence of given threats,
- identification of the risk associated with potential ICT environment security breach after the occurrence of threats.

18.7. While identifying risks associated with the potential ICT environment security breach prior to the occurrence of given threats, the bank should give special attention to identification of the existing ICT environment vulnerabilities (including ICT infrastructure

[64] Eg. the number of ICT environment security breach incidents during a given reporting period, the number of significant recommendations in the environment security issued by the internal audit unit, the number of unprotected vulnerabilities in vital components of the ICT environment.

components) and threats that may take advantage of these vulnerabilities. Bank should consider (including in particular the level of complexity of the ICT environment and the exposure to risk within the ICT environment security), and make appropriate decisions whether the use of automated tools to identify existing vulnerabilities is necessary. Regardless of a periodic evaluation, identification of risk within ICT environment security should be carried out every time when significant modifications are planned, both as regards the IT systems alone and their application, and when implementation of new technologies (e.g. payments using near-field communication, mobile banking, technologies based on social networks for the purpose of communicating with a bank's customers, etc.).[65]

18.8. While identifying the risk associated with the ICT environment security breach, after the occurrence of threats, the bank should collect information on the incidents that occurred in its business activity and that affect security of the information processed at the bank, and in the case of compliance with the definition of an operational incident adopted by the bank, it should include them in the operational incidents database.

18.9. It is recommended to establish permanent cooperation with other bank (in particular by using interbank information exchange systems) for the exchange of information on the identified threats as well as conclusions and experiences arising from the analysis of ICT environment security breach incidents identified. The manner and scope of the information exchanged should ensure its confidentiality, in particular banking secrecy.

ICT Environment Security Risk Assessment

18.10. Assessment of the ICT environment security risk is aimed at determining the probability and potential impact of the occurrence of threats associated with the risk on the institution and - assessing this risk on that basis.

18.11. Risk assessment measures taken should have regard to the classification of information and the information systems .[66] Studying the impact of identified threats should also include elements associated with the component for which a given threat has been identified. As a result of the risk assessment, the bank should obtain knowledge about the threats occurring in its business activity associated with the ICT environment security, the likelihood that the identified threats may occur and the possible consequences of occurrence, including potential loss of reputation which may lead to a decline in client confidence and termination of their cooperation with the bank, and which may have a particular impact on liquidity of the bank. Such knowledge should allow to make appropriate decisions as regards control and mitigation of risk.

ICT Environment Security Risk Control and Mitigation

18.12. Taking into account the results of the ICT environment security risk assessment, the bank should make appropriate decisions regarding the approach to specific threats, such as:

– risk mitigation, i.e. introduction and modification of the existing organisational and technical ICT environment security control mechanisms,

[65] See also: "Development of IT Systems".

[66] See section: "Information and IT Systems Classification"

- risk transfer, i.e. transfer of part of or the entire risk associated with a threat onto an external entity[67], in particular through commissioning external service providers[68] to perform tasks, or through insurance,
- risk avoidance, i.e. avoidance of actions which involve a given threat,
- risk acceptance, i.e. conscious avoidance of actions to reduce the likelihood or impact of the occurrence of a given threat, along with possible provision of funds to cover potential losses associated with it.

18.13. Control mechanisms used should be adequate in particular to:

- identified threats, assessed risk arising from these threats and significance of associated ICT environment components, and in particular of IT systems[69],
- the scale and characteristics of the business activity of the bank,
- complexity of the ICT environment.

18.14. Bank should ensure that all exceptions from the regulations and control mechanisms applicable at the bank are recorded and subject to control in accordance with the formal procedure that specifies e.g. situations in which consent is allowed to be given to exceptions, principles of the submission and approval of a request for such consent (ensuring that the application contains justification of the need for the exception), persons authorised to give consent, acceptable duration of the exceptions and reporting principles in this regard. Bank should also analyse the risk associated with the exceptions referred to above on a regular basis.

18.15. Bank should verify on a regular basis whether the adopted control mechanisms are adequate to its risk profile and whether operation of these mechanisms is correct. In the event of such necessity (e.g. if it is established that the internal resources of the bank are insufficient in this respect), for this purpose, the bank should use external experts, keeping in mind the need to preserve the confidentiality of information they acquired in connection with the control conducted.

18.16. Control of the ICT environment security risk should be conducted in proportion to the level of risk, regardless of whether the risk is associated with the processing of data of the bank's clients (or conducting other operations as part of the banking or trading business activities) or with data processing for external entities (e.g. in case of custodian banks).

ICT Environment Security Risk Monitoring and Reporting

18.17. The results of identification and assessment of the ICT environment risk and the results of testing of the effectiveness of implemented control mechanisms should undergo monitoring (including for the existing trends), and should be presented to the Management Board and Supervisory Board of the bank as part of the management information system

[67] However, risk transfer should not be regarded to be alternative to proper risk management by the undertakings.
[68] See section "Cooperation with External Providers of Services".
[69] See section: "Information and IT Systems Classification"

operating at the bank.[70] Such information should be transferred on a regular basis and the frequency and scope should take into account the bank's risk profile, and enable for taking appropriate reaction.

[70] See also: "Management Information System".

Information and IT System Classification

19. Recommendation 19

Bank should classify information systems and information processed in those systems in accordance with the principles that take under consideration, in particular, security level required for such systems and information..

Information Classification

19.1. Bank should develop principles for the classification of information to ensure that any information processed in the ICT environment of the bank is subject to an appropriate level of protection. For this purpose, it is necessary to establish a system of information classification which would include all the data processed in the IT systems of the bank, as well as to ensure that the classification of each piece of information is appropriate to the current internal and external conditions at the bank.

19.2. Information should be classified for the level of security required, taking into account in particular:

– significance of the information for the bank and the processes implemented at the bank,

– significance of the information from the perspective of management of the types of risk that have been identified to be significant in the business activity of the bank,

– results of loss or unauthorised modification of a given piece of information,

– results of an unauthorised disclosure of a given piece of information,

– detailed regulatory and legal requirements related to information of a given type.[71]

19.3. Classification of each piece of information should be taken into account when defining security mechanisms that protect the information throughout its processing, from acquisition, through utilisation, possible transfer outside an bank to archiving and deletion.

19.4. Access to information with a high degree of confidentiality, including information constituting professional secret and confidential information, should be granted only to persons whom the bank finds eligible to receive access to such information in the light of the applicable law. In addition, any person to whom an bank provides access to information with a high degree of confidentiality, including information constituting professional secret and confidential information, should be obliged to sign a commitment to maintain confidentiality (also for an appropriate time after termination of access, subject to applicable law). The principle does not apply in cases where applicable law requires granting such access.

19.5. Storing information of high significance to the bank on desktop computers, laptops or mobile devices should be limited to the necessary minimum and protected in proportion to the classification of the information (e.g. through encryption, access control mechanisms, mechanisms that allow recovery of data).

[71] See also: “Formal and Legal Security”.

19.6. Bank should consider (including in particular the level of complexity of the ICT environment, the degree of exposure to risk within the ICT environment security and the scale and characteristics of its business activity), and make appropriate decisions whether the use of solutions that automate the measures taken as regards control of the risk associated with security of the information processed in the ICT environment, such as solutions that limit the ability of the IT system users to save information on portable data carriers, prevent control over the information sent via e-mail, and restrict access to other e-mail systems than those adopted at the bank. However, it should be kept in mind that utilisation of such automatic solutions does not exempt the bank from the obligation to exercise supervision over that area by the employees.

IT System Classification

19.7. Bank should develop principles of classification of the IT systems that would take into account, in particular:

- classification of the information processed within a given system,
- significance of a given system to the business activity of the bank,
- significance of other IT systems whose operation depends on a given system.

ICT Environment Security Breach Management

20. Recommendation 20

Bank should have formal principles of the management of ICT environment security breach incidents including identification, registration, analysis, prioritisation, link search, taking corrective measures and removing their causes.

20.1. Bank should have internal regulations describing procedures in the event of ICT environment security breach incidents, i.e. failure and overload of the IT systems, loss of devices or data, human errors resulting in a threat to the ICT environment security, violations or attempted violations of protection, uncontrolled modifications of the systems etc. The scope and level of detail of these regulations should correspond to the scale and specificity of the business activity of the bank and the level of complexity of its ICT environment.

20.2. Principles of managing ICT environment security breach incidents should specify in particular:

- methods and scope of incident information collection,
- scope of responsibility regarding incident management,
- the manner of conducting analyses of the impact of incidents on the ICT environment, including its security,
- principles of categorisation and prioritisation of incidents, taking into account classification of information and IT systems connected to a given incident[72],

[72] See section: “Information and IT Systems Classification”

- principles of detection of dependencies between incidents (example of such dependency in a Denial-of-Service-type attack that prevents immediate identification of another incident and removal of its causes,
- principles of communication, including both the bank's employees and external service providers, and - in the case of significant exposure to the effects of an incident - also other third parties (clients, counterparties, etc.), ensuring adequately prompt notification of the interested parties and taking measures in proportion to significance of the incident,
- principles of collecting and preserving evidence relating to incidents that could be used in legal proceedings (in particular those that minimise the risk of such evidence being lost or rejected because of an inadequate protection of data),
- principles concerning taking corrective and preventive measures, including in particular assignment of persons responsible for taking these measures and monitoring their implementation status,

20.3. In order to, e.g. allow preventive measures as regards the identified problems, the bank should keep a register of the ICT environment security breach incidents, which should include detailed information on:

- date of occurrence and identification of the incident,
- causes of the incident,
- course of the incident,
- results of the incident,
- corrective measures taken.

20.4. Bank should ensure that all employees and other persons providing services to the bank that have access to the ICT environment, are aware of the principles of management of the ICT environment security breach incidents within the scope that is appropriate to the duties performed and authorisations held. In particular, these persons should be obliged to report ICT environment security breach incidents (including suspected incidents) as soon as possible. To this end, the bank should establish an appropriate contact centre (e.g. as part of units responsible for IT systems user support) dedicated to the management of reports within the scope referred to above, which should be known in the institution, constantly available and should allow proper reaction time. Persons responsible for the management of reports should have qualifications and knowledge that allow proper classification of each report and taking measures in connection with their management or escalation, i.e. assigning persons with a higher level of competencies in a given area (in particular based on the classification of information or IT systems with which a given incident is associated) to manage reports.[73]

20.5. It is recommended that in reference to incidents that have a significant impact on the security of data processed, including, in particular, security of clients' funds (also in

[73] See section: "Information and IT Systems Classification"

reference to the incidents about which the bank is notified by external service providers[74]), the bank has a fast reporting route of their occurrence (including defining possible causes and effects) to the Management Board of the bank. Rapid flow of information in respect of the occurrence of a significant security breach should allow appropriate involvement of the Management Board of an bank in the process of taking corrective measures. Management Board of an bank should be also notified on the implementation of these measures on a regular basis.

20.6. Bank should consider (including in particular the level of complexity of the ICT environment and the exposure to risk within the ICT environment security and the scale and specificity of the business activity), and make appropriate decisions on defining composition of the teams that will be responsible for taking appropriate measures when incidents that have a significant impact on the security of data processed (in particular on the security of clients' funds), who have appropriate qualifications and knowledge in this respect and hold authorisations that enable them to take effective measures in an emergency.

20.7. Bank should consider (taking into account in particular the level of complexity of the ICT environment, the degree of exposure to risk the safety of the environment and the scale and characteristics of its business activity), and make appropriate decisions whether the use of SIEM class solutions (*Security Information and Event Management*) that facilitate incident management including security violation by centralizing the collection, analysis and storage of logs generated by the information systems and other components of the ICT environment is necessary.

[74] See section: Cooperation with External Providers of Services

Formal and Legal Security

21. Recommendation 21

Bank should ensure compliance of information technology and ICT environment security operation with the legal requirements, external and internal regulations, agreements concluded and standards adopted at the bank.

21.1. Bank should systematically identify, document and monitor compliance with the requirements referring to the information technology and ICT environment security (also in respect of the activity entrusted to external service providers[75]) arising from the applicable law, internal and external regulations, agreements concluded and standards adopted at the bank, including in particular:

- the Banking Law Act of 29 August 1997 (Journal of Laws of 2012, item 1376, as amended),
- the Accounting Act of 29 September 1994 (Journal of Laws of 2009 no. 152, item 1223, as amended),
- the Act of 16 November 2000 on counteracting money laundering and terrorist financing (Journal of Laws of 2010 no. 46, item 276, as amended),
- the Bank Guarantee Fund Act of 14 December 1994 (Journal of Laws of 2009 no. 84, item 711, as amended),
- the Personal Data Protection Act of 29 August 1997 (Journal of Laws of 2002 no. 101, item 926, as amended),
- the Classified Information Protection Act of 5 August 2010 (Journal of Laws of 2010 no. 182, item 1228, as amended),
- the Copyright and Neighbouring Rights Act of 4 February 1994 (Journal of Laws of 2006 no. 90, item 631, as amended), as well as agreements and licences within the scope of the software used,
- the Electronic Payment Instruments Act of 12 September 2002 (Journal of Laws of 2012, item 1232, as amended),
- administrative acts with regard to the above-mentioned acts,
- supervisory regulations.

21.2. Fulfilment of these requirements should be reported under the management information system[76].

[75] See also: Cooperation with External Providers of Services

[76] See also: “Management Information System”

Role of the Internal and External Audit

22. Recommendation 22

Information technology and ICT environment security areas at the bank should undergo systematic audits..

22.1. Bank should consider (including in particular the level of complexity of the ICT environment and the exposure to risk within the ICT environment security), and make appropriate decisions on establishing, as part of internal audit, the unit responsible for information technology and ICT environment security audit. In the case of cooperative banks it is admissible that these functions are performed by the auditors from the affiliating bank.

22.2. Persons responsible for information technology and ICT environment security audit should have appropriate qualifications. Audit should be conducted with the observance of acknowledged international standards and good practices in information technology and ICT environment security, such as:

- standards related to audits of ISACA IT systems (Information Systems Audit and Control Association),
- COBIT (Control Objectives for Information and related Technology),
- GTAG (Global Technology Audit Guide) and GAIT (Guide to the Assessment for IT Risk),
- ISO standards (International Organisation for Standardisation).

22.3. Audit of information technology and ICT environment security should be conducted on a regular basis and each time after introduction of modifications that may significantly influence the level of ICT environment security. Frequency and scope of audits should arise from the level of risk associated with individual audit areas and results of previous review

22.4. Entrusting additional audits to professional external institutions that specialise in information technology and ICT environment audits is a factor that may significantly strengthen control over the risk associated with this area. Bank should consider and make appropriate decision whether supplementing of the actions of internal audit by external audits conducted by such entities, in particular in respect of areas with a high level of risk.