Guidelines

on the Management of Information Technology and ICT Environment Security in capital market infrastructure entities

Table of contents

1 Introduction.

Having regard to the objectives of supervision of the financial market, specified in art. 2 of the act of July 21st, on supervision of the financial market (that is: Dz. U. of 2012, item 1149 as amended, hereinafter referred to as the act), such as: ensuring of the proper functioning of the market, its stability, security and trust in the market, as well as safeguarding of interests of its participants and the task of the Polish Financial Supervision Authority, specified in art. 4 item 1 clause 2 of the act, consisting of performance of activities contributing to the proper functioning of the financial market, these "Guidelines for management of the fields of ICT technology and security of the ICT environment in capital market infrastructure entities" have been published (hereinafter referred to as the Guidelines).

The obligations in this regard, imposed upon various categories of capital market infrastructure entities, are rooted mainly in the following legal provisions:

1) Entities, which run the regulated market:

- Art. 18 item 1 clause 2 of the act of July 29th, 2005 on trade in financial instruments (Journal of Laws of 2014, item 94 as amended; hereinafter referred to as the act on trade), specifying the obligation to ensure the safe and efficient course of all transactions,
- § 2, § 4 item 2, § 5 of the Regulation of the Minister of Finance of October 23rd, 2009 on the detailed prerequisites to be met by a regulated market (Dz. U. no. 187, item 1447), which indicates that an entity running a regulated market is to ensure the proper conditions for effective and safe trade on this market, including effective and immediate completion of orders made on this market, and indicates that for the purpose of proper management of the risk, the entity running the regulated market is to establish and implement written procedures pertaining to: management of technical functioning of the IT systems of the regulated market, safe access for members of the regulated market to the IT systems of this market and the system of management of continuity of operation and the principles of maintenance of continuity of operation in the case of extraordinary situations, and which specifies the minimum scope of information made available to the general public, pertaining to offers, transactions and turnover on the regulated market.

2) Entities engaged in an alternative trading system:

- Art. 78 item 1 clause 2 of the act on trade, which specifies the obligation of ensuring safe and effective course of transactions,
- § 2-3 and § 11 item 2 of the Regulation of the Minister of Finance of October 23rd, 2009 on the detailed prerequisites to be met by an alternative trading system organized by an investment company (Dz. U. no. 187, item 1448), which are applied on the basis of art. 16 item 3 of the act on trade, accordingly, to the company running the regulated market, which, at the same time, organizes the alternative trading system; according to these provisions, the organizer of the alternative trading system is to ensure concentration of supply and demand for financial instruments, in particular, through specification and implementation of the principles, which ensure the effective completion of orders in this system; the legal provisions specify the minimum scope of information on trade and turnover in the alternative trading system, made available to the general public by the investment company; moreover, these provisions demand that the investment company manages the technical functioning of software and hardware of the alternative trading system, the continuity of their operation and safe access of participants to such hardware and software.

3) Entities, which run a clearing house:

- Art. 68c item 1 of the act on trade, which identifies the obligation of the clearing house to define the scope of duties of parties to a transaction for the purpose of provision by the parties of pecuniary or non-pecuniary benefits.

4) Entities, which run a settlement house:

- Art. 68a item 2 of the act on trade, which indicates that a settlement house is understood as the persons, devices and technical measures established for the purpose of organization and maintenance of settlement of transactions.

5) The Central Securities Depository of Poland:

- Art. 48 item 1 of the act on trade, which indicates that the tasks of the Central Securities Depository of Poland include: maintenance of the deposit of securities, supervision of compliance of the issue volume with the number of securities, traded securities registered in the depository; management of performance of obligations of the issuers towards persons entitled under the securities and settlement of financial instruments and funds in association with transactions executed on the regulated market and transactions executed in the alternative trading system, as well as art. 48 item 2 and 7, stating that the Central Securities Depository in Poland or its subsidiary may also, among other things, settle transactions and maintain a system that warrants security of clearing of transactions.
- Art. 18 item 1 of the act of October 26th, 2000 on commodities exchanges (Journal of Laws of 2014 item 197; hereinafter referred to as the act on commodities exchanges), which indicates that the functions of the exchange settlement house can be performed by the Central Depository or a company, which has been entrusted by the Central Depository with performance of tasks, referred to ion art. 48 item 2 of the act on trade.

6) Entities running commodities exchanges:

- Art. 4 clause 2 of the act on commodities exchanges, indicating, among other things, that the purpose of operation of a company running the exchange is to ensure the safe and efficient course of exchange transactions and settlements.

7) Entities running the exchange settlement house:

- Art. 15 item 6 of the act on commodities exchanges, indicating that an exchange settlement house ensures settlement of members due to exchange transactions, in particular, by providing a warranty for their liabilities and claims, resulting directly from these transactions.

The necessity to issue these Guidelines is due to the substantial technological development and a systematic increase in the significance of the area of ICT technology for the operation of capital market infrastructure entities, as well as emergence of new threats in this regard.

These Guidelines are aimed at presenting to the capital market infrastructure entities of the expectations of the competent authorities with regard to careful and stable management of the ICT technology and security of the ICT environment, in particular, with regard to the risks associated with these fields. This risk can be defined as the uncertainty, associated with the proper, effective and safe supporting of activity of capital market infrastructure entities by their ICT environment. It is associated mainly with operational and legal risk, as well as the risk of loss of reputation.

The document contains 22 guidelines, divided into the following areas:

- Strategy and organization of the ICT technology fields and security of the ICT environment,
- Development of the ICT environment,
- Maintenance and use of the ICT environment,
- Management of security of the ICT environment.

In their business activity, capital market infrastructure entities should take into account the Guidelines, specified in this document. However, taking into account the specific nature of issues related to technology and security of the ICT environment, as well as the differences with regard to the conditions, profile of activity of capital market infrastructure entities, the mode of implementation of these Guidelines and the objectives defined herein may be different. Therefore, the descriptions and comments attached to individual Guidelines should be treated as a set of tools, recognized by the Commission as being useful for performance of the obligations with regard to securing of the ICT environment at the capital market infrastructure entities, pertaining to the mode of implementation of the legal provisions, mentioned above, which should, however, be implemented in accordance with the principle of proportionality. This means that the mode of application of the Guidelines should depend, among other things, on the extent, in which they match the specific character and profile of activity and characteristics of the ICT environment of the capital market infrastructure entity, as well as the correlation between the costs of introduction of these Guidelines and the resulting benefits (also from the perspective of security of the customers of capital market infrastructure entities). The competent authority expects that the capital market infrastructure entities will apply all Guidelines, and proportionality will refer exclusively to the mode of implementation of individual Guidelines. At the same time, the competent authorityexpects that decisions with regard to the range and mode of implementation of solutions, specified in the Guidelines, will be preceded by in-depth analysis and supported by adequate arguments, documenting the process of management of the ICT technology and environment, adapted to the applicable risk level.

Moreover, in relation to companies running the regulated market, which organize an alternative trading system, it is recommended that in the case of entrusting third persons with performance of some of the tasks associated with running of the alternative trading system, the company should make its best efforts to make sure that such persons perform these tasks in accordance with the scope of these Guidelines. At the same time, it is recommended that in their agreements with third parties, entities running regulated markets and organizing alternative trading systems should include the appropriate clause warranting compliance of such parties with the Guidelines.

The competent authorityexpects that the standards, referred to in the Guidelines, will be implemented by capital market infrastructure entities no later than by December 31st, 2016. The Guidelines should be applied in accordance with the „comply or explain" principle in relation to the mode of application of individual Guidelines in accordance with the precautionary approach, the acceptable risk level and the necessity to comply with the legal provisions in force.

Information concerning application of the Guidelines should be communicated on the form, which should be filled out by capital market infrastructure entities for the purpose of internal assessment of their compliance with the Guidelines. The document is to consist one of the methods of verification by the competent authority of compliance with the requirements, specified in the Guidelines.

The Guidelines do not violate any rights and obligations, specified in legal provisions.

Glossary **Information security –** preservation of confidentiality, integrity and availability of information; In addition, other properties, such as authenticity, accountability, non-repudiation , and reliability can also be involved (based on ISO/IEC 27000:2009).

Cloud Computing – a model of rendering of services, ensuring convenient network access – regardless of location - „on demand" to the contended pool of configurable computing assets (such as servers, mass storage devices, applications or services), which can be dynamically

provided or released with minimum labor input and minimum participation of the supplier of services (based on NIST Special Publication 800-145 „The NIST Definition of Cloud Computing", National Institute of Standards and Technology).

Data availability – data property of being accessible and usable upon demand by an authorized entity (based on ISO/IEC 27000:2009).

ICT environment security breach - single or a series of unwanted or unexpected information security events (identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls or a previously unknown situation, which may be of significance for security) that have a significant probability of compromising business operations and threatening information security (based on ISO/IEC 27000:2009).

ICT infrastructure – a set of transmission connections „ encompassing, in particular, the hardware platforms (including: servers, array, workstations), the ICT network (including: routers, switches, firewalls and other network equipment), the system software (including operating systems and database management systems) and other components that allow for faultless and safe operation of these assets (including UPS devices, power generators, air-conditioning equipment), as well as those used in disaster recovery centers of a capital market infrastructure entity.

Data Integrity - property of protecting the accuracy and completeness of assets (based on ISO/IEC 27000:2009).

Management of the capital market infrastructure entity – the management board of the capital market infrastructure entity, managers of organizational units and managers for key processes at the capital market infrastructure entity.

ICT environment security area - area of investment fund companies' operations designed to ensure proper management of the ICT environment security risk at investment fund companies.

Business area – the area of activity of the capital market infrastructure entity, which is supported by the ICT environment, including business operations, risk management, accounting, finances etc.

ICT area – the area of activity of a capital market infrastructure entity, aimed at ensuring the proper support by the ICT environment.

Outsourcing – entrusting (ordering) a third party with performance of tasks associated with activity of the capital market infrastructure entity.

Vulnerability - weakness of an asset or control that can be exploited by a threat (based on ISO/IEC 27000:2009).

A capital market infrastructure entity – a company, which has obtained a permit for running of a regulated market, a clearing house, a settlement house, an exchange settlement house, a commodities exchange, Warsaw Stock Exchange, the Central Securities Depository in Poland and the company, which has been entrusted with performance of task by the Central Securities Depository in Poland.

Data confidentiality - characteristic feature of data whereby data remain unavailable or undisclosed to unauthorized persons, processes or other entities (based on ISO/IEC 27000:2009)Risk profile - the scale and structure of exposure to risk.

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

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

ICT environment security management system - a set of principles and mechanisms, referring to processes aimed at ensuring the proper level of security of the ICT environment.

ICT environment – the ICT infrastructure of the capital market infrastructure entity with information systems utilising it and information systems used at investment fund company supporting its activity which are based on the ICT infrastructure provided by external entities.
Threat - potential cause of an unwanted incident which may cause damage to the system or the organisation (based on ISO/IEC 27000:2009). List of Guidelines.

Information Technology and ICT Environment Security Strategy and Organisation

Guideline 1

The board of supervisors of the capital market infrastructure entity should supervise the functioning of the information technology and ICT environment security areas, and the management board of the capital market infrastructure entity should make sure that the above areas are managed in the correct and effective manner.

Guideline 2

In the capital market infrastructure entity, there should be a formalized management information system in the information technology and ICT environment security areas, providing all of the information recipients with the proper level of knowledge on these areas.

Guideline 3

The capital market infrastructure entity should develop and implement a strategy in the information technology and ICT environment security areas, consistent with the strategy of operation of the capital market infrastructure entity.

Guideline 4

The capital market infrastructure entity should define the principles of cooperation and scope of responsibility of the business, information technology and ICT environment security areas, allowing for effective and safe use of the potential of the ICT environment in the activity of the capital market infrastructure entity.

Guideline 5

Organisational solutions and human resources in the information technology and ICT environment security areas 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

Guideline 6

The capital market infrastructure entity should develop formal principles of implementation of projects in the area of ICT environment, adequate to the scale and specific nature of the projects implemented.

Guideline 7

IT systems of the capital market infrastructure entity should be developed in a manner, which ensures support for its business activity and taking into account the ICT environment security requirements.

Maintenance and Exploitation of the ICT environment

Guideline 8

The capital market infrastructure entity should develop formal principles of management of

data used in its business operation, in particular, including data quality and architecture management and ensuring the proper support of activity of the capital market infrastructure entity.

Guideline 9

The capital market infrastructure entity should develop formal principles of management of the ICT infrastructure, including its architecture, individual components, performance, capacity and documentation, ensuring the proper support of activity of the capital market infrastructure entity and security of the data processed.

Guideline 10

The capital market infrastructure entity should develop formal principles of cooperation with external suppliers of IT services, warranting security of data and proper operation of the ICT environment, taking into account services rendered by entities belonging to the capital group of the capital market infrastructure entity.

Guideline 11

The capital market infrastructure entity should develop formal principles and technical mechanisms that ensure the proper level of control of logical access to data and information and physical access to the key components of the ICT infrastructure.

Guideline 12

The capital market infrastructure entity should ensure the proper protection of the ICT environment against malware.

Guideline 13

The capital market infrastructure entity should provide the internal users of IT systems with support in solving of problems associated with operation of these systems, including those resulting form failures and other non-standard events that interfere with use of these systems.

Guideline 14

The capital market infrastructure entity should engage in effective activities, aimed at achieving and maintaining the proper level of employee qualifications with regard to the ICT environment and security of information processed in this environment.

Guideline 15

The business continuity management system of the capital market infrastructure entity should take into account the specific conditions associated with its ICT environment and the data processed by it.

Guideline 16

Any capital market infrastructure entity that renders services using electronic access channels, should have in place the effective technical and organizational solutions to ensure verification of identity and security of data and funds of the customers, and it should educate the customers with regard to the principles of safe use of these channels.

Guideline 17

The capital market infrastructure entity should develop formal principles of management of the so-called end user computing[1], effectively limiting the risk associated with use of this software.

ICT Environment Security Management

[1] **End-User Computing**, **EUC** – the tools developed and functioning on the basis of applications installed on PC computers, such as MS Excel or MS Access, allowing users other than programmers to create business applications.

Guideline 18

The capital market infrastructure entity should use a formal, effective system for management of the ICT environment security, encompassing tasks associated with identification, estimation, control, counteracting, monitoring and reporting of risks in this regard, integrated with the overall risk management and information security system of the capital market infrastructure entity.

Guideline 19

The capital market infrastructure entity should classify IT systems and the information processed in accordance with the principles, which take into account, in particular, the security level required for these systems and information.

Guideline 20

The capital market infrastructure entity should have formal principles of managing information security incidents, including their identification, recording, analysis, prioritization, searching for links, undertaking corrective actions and elimination of causes.

Guideline 21

The capital market infrastructure entity should ensure compliance of functioning of the information technology and ICT environment security areas with the legal requirements, internal and external regulations, the contracts signed and the internal standards of the capital market infrastructure entity.

Guideline 22

The information technology and ICT environment security areas should be subject to systematic, independent audits.

2 The strategy and organization of the information technology and ICT environment security areas.

2.1 The role of the management board and the board of supervisors

Guideline 1

The board of supervisors of the capital market infrastructure entity should supervise the functioning of the information technology and ICT environment security areas, and the management board of the capital market infrastructure entity should make sure that the above areas are managed in the correct and effective manner.

1. The supervisory board and the management board should pay particular attention to:

- Management of security of the ICT environment[2] and business continuity[3],
- The process of development and updating of the strategy in the areas of information technology and the ICT environment[4],
- Management of the electronic access channels[5],
- Cooperation with external suppliers of services associated with the ICT environment and its security[6],
- Providing the adequate organizational structure and staffing in the areas of information technology and security of the ICT environment[7],

[2] See: section „ICT environment security management".
[3] See: section „Business continuity of ICT environment".
[4] See: section „Strategic planning".
[5] See: section „Management of electronic access channels".
[6] See: section „Cooperation with external suppliers of services".
[7] See: section „Organization of the information technology and ICT security areas"

- Management of the quality of data of key significance for the capital market infrastructure entity[8],
- Cyclical inspections of security status of the ICT environment.

2. In order to increase the effectiveness of supervision and control of the area of security of the ICT environment, as well as ensuring effective communication in this area and compliance of its activity with the purposes and needs of the institution, the capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment, the degree of exposure to risk with regard to security of this environment and the scale and specific nature of its business activity) and make the appropriate decision with regard to appointment or designation[9] (according to the principle of proportionality) of a representative of management of the capital market infrastructure entity or the team appropriate for the issues of the ICT environment security. The works of such team should be managed by a member of the management board having the appropriate qualifications or a representative of the company management, designated by the management board of the capital market infrastructure entity.

2.2 The management information system

Guideline 2

In the capital market infrastructure entity, there should be a formalized management information system in the information technology and ICT environment security areas, providing all of the information recipients with the proper level of knowledge on these areas.

1. Developing the management information system in terms of the information technology and the ICT environment security, the capital market infrastructure entity should:

- Identify the issues in the areas of information technology and security of the ICT environment, which should be subject to the management information system, taking into account the associated risk and other specific conditions,
- Specify the mode and principles of granting access and obtaining information on the above issues (including specification of sources, allowing for automatic collection of such information) and specify the scopes of responsibility in this regard,
- Specify the adequate scope and frequency of reporting,
- Specify the persons or roles to receive such information,
- Make sure that the information delivered to each of the recipients is clear, reliable, accurate, updated, within the appropriate scope and delivered timely at the appropriate frequency.

2.3 Strategic planning

Guideline 3

The capital market infrastructure entity should develop and implement a strategy in the information technology and ICT environment security areas, consistent with the strategy of operation of the capital market infrastructure entity.

1. The basic function of the information technology area in a capital market infrastructure entity is to make sure that the ICT environment of a given institution supports its activity, and the basic function of the ICT security area is to make sure that the risk associated with

[8] See: section „Data quality management".

[9] It is not demanded that a separate, dedicated committee is established – in particular, it is acceptable, for instance, to include the scope of tasks of the committee for security of the ICT environment in the tasks of the committee for the affairs of operational risk. The capital market infrastructure entity should, however, make sure that the solution applied allows for effective performance of the tasks under concern.

the environment security is appropriately managed. Therefore, the starting point for development of the strategy[10] for the information technology and ICT environment security areas should be the strategy of operation of the capital market infrastructure entity.

2. In order to make sure that the strategy for the information technology and ICT environment security areas is realistic and, at the same time, consistent with the present and future (expected) conditions and business expectations, the capital market infrastructure entity should have the necessary knowledge on the ICT environment, sufficient for grasping of correlations between its individual components and data processed and the business conditions, objectives and needs. Within the framework of implementation of the above strategy, the capital market infrastructure entity should, in particular, define the specific and measurable objectives and programmes/ projects with defined priority levels and time frames (in accordance with the scope of needs defined). These should include:
   - Development of the software used,
   - Changes in the scope of data processed within the framework of activity of the capital market infrastructure entity,
   - Development of the ICT infrastructure,
   - Organizational and process changes with regard to management of information technology and ICT environment security areas, taking into account the requirements for the ICT environment security, risk associated with implementation of this strategy and the funds necessary for this purpose.
3. The capital market infrastructure entity should make sure that the implementation of this strategy is effectively supervised, in particular, through monitoring of implementation of the objectives defined and the programmes/ projects to be performed.
4. The capital market infrastructure entity should make sure that the above strategy is systematically[11] reviewed and adapted to changes taking place in the capital market infrastructure entity and in its environment (changes in the strategy of operation of the capital market infrastructure entity, changes in the risk profile, legal and regulatory changes and technological development).
5. The scope and level of detail of the documentation for the above strategy should be adequate to its complexity and the scale and profile of operation of the capital market infrastructure entity.

2.4 The principles of cooperation between business and technical areas

Guideline 4

The capital market infrastructure entity should define the principles of cooperation and scope of responsibility of the business, information technology and ICT environment security areas, allowing for effective and safe use of the potential of the ICT environment in the activity of the capital market infrastructure entity.

1. The principles specifying the mode of cooperation between the area of business, information technology and ICT security and the mode of communication of these areas should be specified and formalized in the manner, which is adapted to the scale and profile of operation of the capital market infrastructure entity.
2. The above principles should warrant that:
   - The decision-making mode and the scope of tasks and responsibility with regard to

[10] Singular used in the expression „strategy in the information technology and ICT environment security areas" does not mean it should be developed as a single document. The capital market infrastructure entity should, however, ensure the consistency of strategy implemented in both of these areas.

[11] That is, in a systematic and orderly manner.

information technology and the ICT environment security have been precisely defined and adequate to the role of the information technology area, defined in the capital market infrastructure entity,

- The business area has defined with maximum precision its expectations (including priorities) towards the information technology and ICT environment security areas, in particular, through participation in the process of development of strategies for the information technology and ICT environment security areas,
- the information technology and ICT environment security areas inform the business area with maximum precision of the estimated funds necessary to satisfy the needs of this area,
- the ICT environment security area participates in the process of development of IT systems and in the process of development and approval of standards and control mechanisms, which exert impact on the level of security of the ICT environment,
- the information technology and ICT environment security areas participate in issuing of opinions concerning strategies of operation of the capital market infrastructure entity, in particular, with regard to specification of limitations and threats associated with this strategy, identified from the perspective of these areas,
- the business area is systematically informed of the status of implementation of programmes/projects that are of significance to the business area, associated with the ICT environment.

3. In order to increase the effectiveness of supervision and control of the area of information technology, and to ensure effective communication in this area and compliance of its activity with the objectives and needs, the capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment and the strategic assumptions for development of a management representative or a team appropriate for the issues of cooperation between the business area and the information technology area. The works of the team should be managed by a member of the management board of the capital market infrastructure entity, having the appropriate qualifications, or an employee of the capital market infrastructure entity, designated by the management board.

4. At the same time, in order to ensure maximum integration of management of information technology and ICT environment security areas and management of the entire institution, the capital market infrastructure entity should ensure the proper cooperation between entities responsible for the area of information technology, the strategy of operation of the capital market infrastructure entity, security, business continuity, operational risk management, the compliance and the internal audit (maintaining the appropriate level of independence of each of these).

2.5 Organization of the information technology and ICT environment security areas

Guideline 5

Organizational solutions and human resources in the areas of information technology and ICT environment security should be adequate to the risk profile and the specific nature of business activity and allow for successful completion of tasks in these areas.

The organizational structure

1. The capital market infrastructure entity should make sure that the organizational structure of the information technology and ICT environment security areas allows for effective achievement of the objectives of the capital market infrastructure entity in these areas, in accordance with the scale and profile of operation of the capital market infrastructure entity and the level of complexity of the ICT environment. The adequacy of this structure

should be verified systematically and – if necessary – adapted to changes in the internal and external environment of the capital market infrastructure entity.

The division of duties

1. The capital market infrastructure entity should precisely define the obligations and rights of individual employees with regard to information technology and information security. Specification of the scope of rights and obligation should be provided in writing, and the division of duties should minimize the risk of errors and abuse in the processes and systems. For this purpose, it is necessary to make sure that employee obligations are appropriately separated, in particular, by isolating the following:

- The function of creation or modification of IT systems - from testing (apart from tests performed by programmers during development of software), administration and use of these systems,
- The function of administration of a given component of the ICT environment - from development of the associated control mechanisms in terms of security,
- The function of administration of a given IT system – from monitoring of activity of the system administrators,
- The function of audit from the remaining functions in the areas of information technology and ICT environment security.

2. The capital market infrastructure entity should designate persons or functions responsible for decision-making in association with individual systems used at the capital market infrastructure entity (often referred to as the system owners), based both on the ICT infrastructure of the capital market infrastructure entity and on the infrastructure provided by external entities. The obligations of such persons or roles should include in particular:

- Ensuring the proper operation and security of the system in terms of business (e.g. through the proper defining of procedures of use of the system, participation in the system operation continuity management, participation in the authorizations management process),
- Supervision of activity of the system users,
- Participation in the decision-making process with regard to development of these systems.

If, for a given IT system, more than one owner has been defined, the capital market infrastructure entity should pay particular attention to precise definition of division of competences and obligations of the individual owners.

3. Ensuring of security of information processed in the ICT environment is not exclusively the domain of units responsible for the information technology and ICT environment security areas, but largely depends on the proper behavior of direct users of the IT systems and data. Therefore, all employees of the capital market infrastructure entity should be aware of the fact that it is their duty to care for security of the information processed in the ICT environment. For this purpose, the capital market infrastructure entity should engage in activities aimed at development of the so-called culture of information security, education of employees in the area of ICT environment security[12] and obtain written commitments for compliance with the internal regulations, applicable to this area.

4. As an addition to the above, the employees of the ICT environment security area should independently actively monitor implementation of the activities assigned in this area to business units and responsible for the area of information technology (e.g. with regard to periodic reviews of system access authorizations, day-to-day control of the ICT

[12] See also: section „Employee education".

environment security within organizational units, testing of correctness of the process of recovery of the ICT environment components on the basis of backup copies made etc.).

5. With regard to transaction systems, it is recommended that events are identified and a mechanism of confirmation of significant data entered is introduced, e.g. with regard to substantial amounts of money paid or withdrawn by the customers (e.g. above the average value for such operations on the bank account of the customer), cancelling or adjusting of the orders made and transactions entered.

The human resources

1. The capital market infrastructure entity should make sure that both the number and level of knowledge and qualifications of employees of the information technology and ICT environment security areas, are sufficient to allow for safe and proper operation of the entire ICT environment. In association with the above, the capital market infrastructure entity should:
   - Make sure that the burden of duties imposed on the employees allows for effective completion of tasks entrusted to them,
   - Provide employees with regular trainings (adequate to the specific nature of the position occupied)[13], promote knowledge development and offer opportunities for exchange of experience (e.g. through access to the so-called knowledge base, participation in trade conferences and forums).
2. The capital market infrastructure entity should not introduce new IT technologies without having the necessary knowledge and competences to manage the associated risk properly. Therefore, the capital market infrastructure entity should each time assess the adequacy of these competences, and in the case of finding them insufficient – engage in activity aimed at their development (e.g. employee trainings, hiring of new employees, engaging in cooperation with external suppliers of services etc.).
3. The capital market infrastructure entity should attach particular importance to selection of employees occupying positions associated with access to highly confidential information [14].
4. The capital market infrastructure entity should engage in activities aimed at minimizing the risk associated with the potential termination of employment of key employees of the information technology and ICT environment security areas. In particular, the capital market infrastructure entity should:
   - Identify the key employees, whose loss is associated with substantial risk for operation of the capital market infrastructure entity,
   - ensure access to updated and accurate documentation of the ICT environment[15],
   - make sure that the activities assigned to key employees are periodically performed by other persons (e.g. during the appropriately long vacation leaves of the key employees),
   - have the succession schemes for key employees,
   - promote sharing of knowledge between employees,
   - include in management information the significant events concerning key employees (in particular, information concerning termination of their employment or long-term absence periods)[16].

[13] See also: section „Employee education".
[14] See: section Classification of information and IT systems".
[15] See: section „The ICT infrastructure documentation".
[16] See also: section „The management information system".

3 Development of the ICT environment

3.1 Projects for the ICT environment

Guideline 6

The capital market infrastructure entity should develop formal principles of implementation of projects in the area of ICT environment, adequate to the scale and specific nature of the projects implemented.

1. The principles of implementation of projects in the area of ICT environment should in particular:

- Introduce the project definition[17],
- Encompass all stages of the project, from initiation and decision on commencement until formal closing,
- Specify the mode of indicating of the project stakeholders,
- Specify the mode of selection of the project participants and indicate their roles, authorizations and responsibilities,
- Take into account the mode of documenting of the project implementation,
- Specify the principles of cooperation and communication between the parties participating in the project implementation,
- Specify the principles of management of the schedule, budget, scope and quality in the project,
- Specify the principles of risk management in the project,
- Specify the principles of change management in the project,
- Specify the principles, roles and responsibility with regard to acceptance and commissioning of the project products,
- Specify the principles of decision-making with regard to withdrawal from project implementation.

2. Projects should be managed using or with reference to the recognized standards and best practices in the field of project management, such as the standards for project management proposed by PMI (Project Management Institute) – in particular, PMBoK (Project Management Body of Knowledge) – or the PRINCE2 (Projects IN Controlled Environments) methodology.

3. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment, the level of risk exposure with regard to security of this environment and the scale and specific nature of operation) and make the appropriate decision with regard to providing – within the framework of project management - for participation of representatives of the ICT environment security area throughout the entire lifecycle of the project.

3.2 Development of IT systems

Guideline 7

IT systems of the capital market infrastructure entity should be developed in a manner, which ensures support for its business activity and taking into account the ICT environment security requirements.

1. Development of IT systems should be consistent with the assumptions of the plans, based

[17] The definition of the project can be given, for instance, with reference to the estimated project budget size or the number of work hours necessary for the project implementation.

on the strategy of the capital market infrastructure entity with regard to the information technology and ICT environment security areas.

2. The capital market infrastructure entity should define the specific requirements with regard to development of IT systems, taking into account the current and expected needs and possibilities of future development of the ICT environment. Each requirement should be formulated in the manner allowing for unequivocal assessment of whether it has been fulfilled. Analysis of the requirements should include in particular[18]:

- The system functionality requirements,
- Requirements with regard to the scope, quantity and format of data processed in the system, taking into account assessment of the possibility of data migration from the currently used IT systems,
- Requirements with regard to possibility of communication with other IT systems used by the capital market infrastructure entity, in particular, the principles and scope of data exchange,
- Requirements with regard to the expected performance and availability of the system, taking into account the situations, in which it is substantially loaded,
- Requirements with regard to resistance of the system to emergency situations, including requirements with regard to the time of recovery after a failure and the acceptable scope of data loss,
- Requirements for the system operating environment,
- Requirements with regard to security of the system and data processed in it, including the cryptographic mechanisms, access control mechanisms and recording of events taking place within the system,
- Requirements based on legal provisions, internal regulations and standards applicable at the capital market infrastructure entity[19].

3. Within the framework of designing of the IT system, the capital market infrastructure entity should take into account the possibility of its modifications in the future, resulting, in the first place, from amendment of legal provisions, of the strategy of operation of the capital market infrastructure entity or the applicable internal standards. This means that developing its IT systems, the capital market infrastructure entity should identify the foreseeable changes in the internal and external conditions and consider reasonability of ensuring flexibility of a given system to the required extent, allowing for effective introduction of the necessary modifications in the future.

4. Introduction of a new IT system, as well as a substantial modification of an existing system, should be preceded by a risk analysis, based on the IT technologies applied and the conducted assessment of impact of the changes being introduced on the ICT environment and the business processes of the capital market infrastructure entity, taking into account, in particular, the aspects of security[20].

5. In the case of software produced using its own resources, the capital market infrastructure entity should have a defined policy in this regard. It is a good practice to specify:

- The software development methodology used, defining, among other things, the course of this process,
- The software development standards applied, including:

[18] In the case of modification of the existing IT systems, the components taken into account during analysis of the requirements should be adequate to the scope of such changes.

[19] See also: section „Formal and legal security"

[20] See: section „Identification of risk with regard to the ICT environment security".

- Architectural standards, such as the platforms, technologies, integration mechanisms used etc.,
- The programming tools and code repositories used,
- Standards with regard to source codes, including the preferred programming languages and queries, notations and commenting modes used,
- The principles of performance of the current code reviews and tests, ensuring the appropriate degree of independence of such reviews,
- The software quality criteria (e.g. easy maintenance, transferability etc.),
- Standards with regard to the technical documentation developed,
- The software versioning principles.

6. In the case of development of software in cooperation with external entities, the capital market infrastructure entity should take advantage of services rendered by reliable suppliers with adequate experience (documented in the projects implemented) and market reputation, warranting the proper level of quality of the services rendered. The capital market infrastructure entity should also analyze reasonability and make the appropriate decision as to whether include in the contracts concluded for software development with external suppliers any provisions concerning application of the software development methodologies and standards, applied by the capital market infrastructure entity[21]. In particular, the capital market infrastructure entity should make sure that prior to test implementation of the work products, they are tested internally by the supplier, provided that the fact that such tests have been conducted should not in any case limit the scope of tests conducted at the capital market infrastructure entity.

7. Both the new software and changes made in the already functioning IT solutions should be tested in accordance with their complexity and impact on the remaining components of the ICT environment of the capital market infrastructure entity. The capital market infrastructure entity should have a software testing methodology, taking into account, in particular, the following best practices:

- The mode of test organization should ensure the highest possible level of independence in verification of compliance with the assumptions made,
- The tests should be attended by representatives of as many organizational units of the capital market infrastructure entity, using the solution being implemented (or – in the case of modifications – its modified part) as possible, as well as by representatives of the information technology and ICT environment security areas,
- The test scenarios, as well as the scope and volume of data used in the tests should be as close as possible to the procedures and data processed within the framework of the actual use of the system, and the capital market infrastructure entity should ensure the appropriate level of confidentiality of real data used for test purposes,
- The mode of reporting and correcting of errors in the software should be stated precisely and warrant recording of all errors reported,
- Tests should be conducted in a dedicated test environment,
- The scope of the tests conducted should include verification of compliance with all requirements, in particular, in the following areas[22]:
  - Compliance with the established functional requirements,
  - System performance and availability, also under substantial loading,

[21] See also: section „Cooperation with external suppliers of services".

[22] In the case of modification of existing IT systems, the areas taken into account during tests should be adequate to the scope of these changes.

- Compliance of the new solution with the security requirements, including authorizations,
- Correct functioning of mechanisms that ensure the required availability and recovery after a failure, including recovery of the system from backup copies,
- Compliance with the approved quality measures for the software,
- Correctness of integration (data exchange) of a given system with other systems,
- Proper functioning of systems integrated with a given system, as well as – in the case of changes – the remaining (not modified) part of the system functionality.

8. The capital market infrastructure entity should make sure that the procedures of transfer of a new IT system or modification of the already functioning system minimize the risk of outage in the capital market infrastructure entity. In particular, after the transfer of the system to the production environment, the capital market infrastructure entity should verify its proper operation and compliance with the requirements, and then – for the appropriate amount of time – monitor the system in this regard. In association with the above, the capital market infrastructure entity should analyze the reasonability (taking into account, in particular, the technical capabilities and the risk-cost balance) and make the appropriate decision as to whether provide mechanisms warranting recovery to the status from before the implementation in the case of emergence of a critical situation (such as creation of backups of the appropriate part of the ICT environment).

9. The development, test and production environments, functioning within the capital market infrastructure entity, should be appropriately separated from one another. The separation method selected (e.g. logical separation using virtualization, physical separation etc.) should be adequate to the risk level and technical requirements, associated with a given environment and the associated systems.

10. The capital market infrastructure entity should make sure that along with development of IT systems, the appropriate functional, technical, operational[23] and utility documentation is created (and its versioning is provided), and the users of systems under development are provided with adequate trainings[24].

11. At the capital market infrastructure entity, there should be a formal system of change management in IT systems, specifying the principles and modes of action with regard to:

- Reporting of change proposals,
- Acceptance of changes,
- Specification of change priorities,
- Implementation of changes,
- Monitoring of change implementation,
- Testing of change implementation,
- Closing of changes implemented,
- Management of urgent/ emergency changes.

12. Making the decision as to whether accept a given change, the capital market infrastructure entity should conduct an analysis of compliance of such change with the requirements previously set for the modified IT system, in particular, associated with the system security. If there is a discrepancy in this regard, the change acceptance decision should be made with particular care.

13. The course of the process of making changes in the IT systems should be appropriately documented; in particular, the capital market infrastructure entity should maintain a register

[23] See also: section „ICT infrastructure documentation".
[24] See also: section „Employee education".

of changes made in the individual systems and perform a periodic verification of compliance of the provisions of this register with the actual conditions.

14. The capital market infrastructure entity should pay particular attention to changes in the ICT environment, resulting from a merger or takeover. In such cases, the capital market infrastructure entity should make sure that the resources dedicated to designing of the target, unified environment integration and replacement of IT systems, planning and implementation of data migration and verification of results of such works are adequate to the scale and nature of the changes made.

15. The capital market infrastructure entity should have formal regulations with regard to withdrawal of IT solutions from use. These regulations should, in particular, define the principles of:

- Decision-making with regard to withdrawal of systems, taking into account the system significance[25],
- Informing the interested parties (including the users) of withdrawal of the system,
- Conducting of data migration and control of its correctness,
- Archiving of the solutions withdrawn, in particular, in accordance with the legal provisions in force and conditions of operation of the capital market infrastructure entity, access to data and proper securing of data,
- Updating of the ICT infrastructure configuration in association with withdrawal of a solution (e.g. with regard to deactivation of system accounts, reconfiguration of firewalls etc.),
- Safe elimination of the ICT infrastructure components withdrawn from use,
- Updating of the ICT environment documentation of the capital market infrastructure entity.

4 Maintenance and operation of the ICT environment

4.1 Data management

Guideline 8

The capital market infrastructure entity should develop formal principles of management of data used in its business operation, in particular, including data quality and architecture management and ensuring the proper support of activity of the capital market infrastructure entity[26].

Data architecture management

1. The capital market infrastructure entity be familiar with the scope of data processed by it within the framework of its operation, the sources of such data (including recognition of internal and external sources), as well as the units, processes and systems, in which such processing takes place. For this purpose, the capital market infrastructure entity should conduct a stocktaking of the data being processed and systematically review the results of such stocktaking with regard to its compliance with the actual situation. The capital market infrastructure entity should also analyze the reasonability (taking into account, in particular, the scale and nature of its operation and the level of complexity of the ICT environment) and, on this basis, make the appropriate decision as to whether to use the electronic repository for such stocktaking and gathering of the stocktaking results.

[25] See: section "Classification of IT systems"

[26] A data management area – which can be defined as all activities associated with control, protection, delivery and correction of data and information – contains also other components, such as data development management, data safety management or database management. These components have been discussed in other sections of this document.

2. The scope and level of detail of such stocktaking process should depend on the scale of operation of the capital market infrastructure entity and the significance of individual groups of data, specified by the company (that is, data pertaining to a specific area of activity, defined by the capital market infrastructure entity). In the case of significant groups of data, the capital market infrastructure entity should developed a detailed documentation, containing the data models, describing, for instance, the correlations between individual components and flows between the IT systems, as well as have in place the appropriate principles (policies, standards, procedures etc.) for processing of such data.
3. An entity (organizational unit, role, person etc.) should be assigned to each data group recorded during the stocktaking process (or a subset of such data) as being responsible for the quality and supervision of such data, in particular, with regard to management of the associated authorizations and participation in development of the IT systems, in which such data is processed.

Data quality management

1. The capital market infrastructure entity should introduce formal principles of data quality management, and the scope and level of these should depend on the scale and nature of operation of the capital market infrastructure entity, as well as the defined level of significance of individual data groups. Regardless of the methodology and nomenclature applied by the capital market infrastructure entity in this regard, these principles should include:
   - Periodic assessment of data quality,
   - Data cleansing,
   - Identification of causes of errors in data,
   - Day-to-day monitoring of data quality.
2. When performing a periodic assessment of the data quality, the capital market infrastructure entity should, in particular, identify data errors and analyze their impact on its business activity. The capital market infrastructure entity should also make sure that the data being processed is adequate from the perspective of management (including measurement) of various types of risk, as well as satisfying of reporting and analytical needs of the key data recipients – that is, whether and to what extent wrong decisions may be caused by low quality of data, on the basis of which they are made. For this purpose, the capital market infrastructure entity should in particular:
   - Define the attributes used for assessment of data quality (e.g. accuracy, consistency, completeness, validity etc.), as well as the frequency and methods of measuring (e.g. automatic comparison of data pertaining to the same operations, stored in various sources, verification with the source documentation on a sample basis, data user satisfaction surveys); in relation to various data, different attributes or measurement modes can be applied,
   - Specify the threshold values for the above attributes, which the capital market infrastructure entity considers to be acceptable in relation to individual data sets,
   - Conduct regular measurements of the data quality, in accordance with the principles specified within the framework of the above activities.
3. During data cleansing (that is, correction of data assessed to be wrong in accordance with the needs and purpose of such data) – if these activities have been automated – capital market infrastructure entity should pay particular attention to the proper construction of the cleansing algorithms. A defective algorithm may correct some data while (due to side effects) lead to deterioration of quality of other sets of data.
4. When identifying the causes of errors in data, the capital market infrastructure entity

should take into account, for instance, the causes associated with improper data processing procedures and low effectiveness of the control mechanisms, functioning in the area of data quality assurance, and implement new and improve the existing mechanisms (both at the stage of data entry in the systems and further processing), in particular, through:

- Modification of the processes of data collection and processing (including the methods of exchange of data between IT systems)
- Introduction or modification of the current control mechanisms (such as automatic validation rules, monitoring of data exchange interfaces, placing of data quality measurement points in the business processes, reconciliation of data between systems etc.),
- Introduction or modification of the periodic control mechanisms and other components of the data quality management process,
- Implementation of automated solutions to support the data quality management process.

The above control mechanisms should also be reviewed and adapted in the case of significant changes in the business processes, the organizational structure, IT systems etc.

Day-to-day data quality monitoring should include information obtained using the control mechanisms introduced. Aggregated information on the results of monitoring, as well as the results of periodic data quality assessments, should be transferred to the appropriate levels of the organization hierarchy within the framework of the management information system[27].

5. When designing the data quality management approach – in particular, if there is no separate organizational unit responsible for this area – the capital market infrastructure entity should make sure that the scope of responsibilities and division of tasks in this regard are clear and precisely defined. The capital market infrastructure entity should also ensure preservation of the adequate level of confidentiality of data used in the data quality management process.

When designing and implementing the data quality management system, the capital market infrastructure entity should, in particular, take into account the typical factors, which may lead to low data quality, including:

- Manual data entry in the systems, which, in the case of lack of sufficient validation of input data, makes it susceptible to human error, and in the case of excessive control – to entry of untrue data (e.g. entry of zeros in the required fields, if their real value is unknown),
- Exchange of data between systems, which is associated, among other things, with:
  - Threats due to lack of updates of the rules of data exchange upon modification of the source or target system,
  - Threats due to difficulties in adjustments of data identified as erroneous in a situation, in which data exchange interfaces have already been transferred to other systems,
- Data migration (also in the case of system consolidation), within which the data structures in the source and target systems are often different, and the quality of data in the source systems is sometimes insufficient.

6. The capital market infrastructure entity should establish an organizational culture, in which emphasis is put on ensuring the proper quality of data entered by employees in the IT systems.

7. The approach of the capital market infrastructure entity to data quality management should take into account the special conditions, associated with limited control of the capital

[27] See also: section „The management information system".

market infrastructure entity over the quality of data from external sources (such as e.g. quotations of financial instruments by liquidity providers on the OTC market). The capital market infrastructure entity should engage in activities aimed at providing the possibility of assessment and improvement of the quality of such data, in particular, by demanding that the suppliers of external data provide confirmations of the adequate quality of the data (supported by the results of an independent external audit).The capital market infrastructure entity should also pay particular attention to the quality of data entered in its external databases.

8. As the quality of data processed in the ICT environment exerts significant impact on the quality of management of the capital market infrastructure entity, and, in many cases, the recipients of this data have no direct impact on its quality (e.g. in the case of data entered in the sales area and then used in the risk area), the capital market infrastructure entity should analyze the situation (taking into account, in particular, the nature of its organizational structure and the implemented data processing procedures) and make the appropriate decision as to whether a representative of the management or the team for data quality affairs should be designated.

4.2 Management of the ICT infrastructure

Guideline 9

The capital market infrastructure entity should develop formal principles of management of the ICT infrastructure, including its architecture, individual components, performance, capacity and documentation, ensuring the proper support of activity of the capital market infrastructure entity and security of the data processed.

The ICT infrastructure layout

1. The extensive ICT network of the capital market infrastructure entity should warrant security of the data transferred. In particular, the network connecting the ICT infrastructure components, which, upon shutdown, prevent operation of the entire capital market infrastructure entity or its significant part, should have the option of operation on the basis of a backup link.

2. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity and dispersion of the ICT environment and the degree of exposure to risk with regard to security of this environment) and make the appropriate decision as to whether apply the solutions allowing for monitoring of the network load and automatic activation of a backup link.

3. A capital market infrastructure entity, which renders services via electronic access channels, should provide an alternative mode of access to telecommunication connections used for these services to be used in case of a failure at the principal supplier.

4. The interconnection point between the internal network of the capital market infrastructure entity and the external networks (especially with the Internet) should be secured with a firewall system[28].

5. The capital market infrastructure entity should analyze the situation and make the decision on division of the ICT network into sub networks (logical or physical), separated by firewalls ensuring the proper level of access control, and using other mechanisms (e.g. encryption of network traffic), taking into account the required level of security of data processed in the system, e.g. through:

- Separation of a sub network for internal IT systems of the capital market infrastructure

[28] A firewall – physical or logical protection, controlling the flow of data to and from a given ICT infrastructure component and between the sub networks and networks (including between the internal and external networks).

entity from the sub network for systems exchanging data with the external environment,

- Separation of sub networks serving the back-office and those serving the front-office,
- Separation of a sub network for the purpose of administration of the infrastructure,
- Separation of a sub network for the purpose of development of the IT systems.

6. The principles of management of network traffic should be formalized, like the principles of recording of events by tools monitoring security of the ICT infrastructure and informing of these events. Such events should be subject to systematic analysis. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment and the degree of exposure to risk with regard to security of this environment) and make the appropriate decision with regard to application of IDS/IPS (*Intrusion Detection System*/ *Intrusion Prevention System)* class solutions, which improve security of the ICT infrastructure through real-time detection (IDS) or detection and prevention (IPS) of attacks.
7. The capital market infrastructure entity should develop formal principles of connecting of terminal devices (computers, mobile equipment) to the ICT infrastructure. Development of these principles should be preceded by an appropriate risk analysis. Moreover, in the case if the capital market infrastructure entity allows the employees to use private equipment for business purposes, it should develop formal principles in this regard, specifying in particular:
   - The acceptable scope of use of such equipment, indicating the type of information that can be processed by it[29],
   - The acceptable types of devices,
   - The acceptable applications, which the employees may use for business purposes,

   as well as provide support in enforcement and control of these principles by IT solutions and systematically educate employees in the area of safe use of private equipment for business purposes[30].

Use of wireless communication by the capital market infrastructure entity should be based on analysis of the associated risks. In particular, the capital market infrastructure entity should specify the type of data that can be made available using the wireless networks and the authentication and encryption mechanisms to be used.

The ICT infrastructure components

1. The type and configuration of each of the components of the ICT infrastructure should be based on analysis of the function performed by each component in the ICT environment and the level of safety required by IT systems using a given component, or data transmitted using this component[31]. In particular:
   - The component type should be selected taking into account the pros and cons of a given solution from the perspective of the infrastructure, in which it is to be located (e.g. when choosing between the hardware and software firewalls),
   - When defining the component configuration, the capital market infrastructure entity should aim at minimization of services made available by a given component (such as open ports, protocols managed etc.) while warranting the planned functionality.
2. The capital market infrastructure entity should verify the predefined settings entered by the manufacturer of the device or system – leaving of a default configuration (which is widely known, e.g. with regard to the standard accounts and passwords) increases greatly the level

[29] See: section „Classification of information".
[30] See also: section „Employee education".
[31] See: section „Classification of information and IT systems".

of risk in terms of the ICT environment security.

3. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment and the degree of risk exposure in terms of security of this environment) and make the appropriate decisions with regard to:
   - Development of configuration standards,
   - Maintaining of a register of components of the IT infrastructure along with basic information on their type and configuration,
   - Maintaining of an electronic repository of the configuration backup.
4. The capital market infrastructure entity should develop formal principles of modification of the ICT infrastructure component configuration, taking into account the significance of individual components and ensuring:
   - Implementation of changes in a planned and controlled manner, taking into account the impact of a given change on other components,
   - Securing of components against unauthorized changes,
   - The possibility of withdrawal of changes, including availability of a backup configuration of the components,
   - The possibility of identification of persons making and approving individual changes in the configuration.
5. If equipment is transferred to an external entity for maintenance or repair, the capital market infrastructure entity should make sure that such entity has no access to highly confidential data saved in such equipment[32], or that the responsibility for confidentiality of such information during the period of maintenance or repair and after termination of cooperation is defined in the agreement concluded with such external entity.
6. The capital market infrastructure entity should develop formal principles of withdrawal of the ICT infrastructure components from use, in particular, to ensure minimization of risk associated with the possibility of leakage of information stored on the computers being withdrawn.
7. Configuration of the firewall system should ensure recording of non-standard activity in order to allow for its analysis in terms of external and internal attacks. The firewall system should also ensure control of outgoing traffic in order to prevent any attempts of session initialization by malware within the network structure.
8. Any capital market infrastructure entity using the server virtualization technology[33] should conduct a risk analysis in association with this technology in the context of own conditions. On the basis of results of such analysis, the capital market infrastructure entity should ensure the correct functioning of the appropriate control mechanisms. The best practices in this regard include:
   - Strict supervision of availability of the physical machine resources (processors, internal memory, disk space etc.)
   - Locating the service console and all tools for management of the resource virtualization platform in a sub network dedicated to administration of this platform,
   - Limiting of the possibility of abuse of resources by individual virtual machines and sharing of the clipboard by the physical and the virtual machine,
   - Particularly careful securing of physical machines, in which virtual machines are

[32] See: section „Classification of information and IT systems".

[33] Server virtualization – a technology allowing for simultaneous functioning of many logic serves on a given hardware platform.

located, against unauthorized access to files of virtual machines (due to the small number of files that constitute a virtual machine, it is particularly vulnerable to theft) and other threats, such as „Denial-of-Service" attacks[34] (in the case of server virtualization, the consequences of such attacks on the physical machine may be much more serious as many virtual machines will suffer).

9. The capital market infrastructure entity should monitor the ICT networks, the ICT infrastructure components, network services and IT systems in terms of their security and proper functioning adequately to the associated risk level. The degree of automation of such monitoring should match the degree of complexity of the ICT environment of the capital market infrastructure entity.

10. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the degree of risk exposure in terms of security of the ICT environment and the number of its users) and make the appropriate decision with regard to introduction of additional means of security in the electronic mail system used, facilitating control of information, which is highly confidential [35], attached to electronic mail messages sent to external recipients.

11. Printers used at the capital market infrastructure entities to print documents containing business secrets or confidential information should be secured against leakage of information (in the case of network printers – e.g. by encryption of data sent and the stored printing tasks and the appropriate mechanisms for verification of user identity).

12. Network scanners, used by the capital market infrastructure entity for scanning of documents containing business secrets or confidential information, should be secured against leakage of information (e.g. through encryption of data transmitted). The solutions of the capital market infrastructure entity in this regard should warrant that the documents scanned are made available to authorized persons only.

13. The configuration of components of the ICT infrastructure should be subject to periodic verification in terms of other changes taking place in this environment, as well as the security gaps revealed. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment and the degree of risk exposure in terms of security of this environment) and make the appropriate decision with regard to supporting of this process with tools that allow for automation of control tasks. One of the tools, which should be used systematically for assessment of effectiveness of control mechanisms in the ICT infrastructure areas of high significance, are penetration tests.

Updating of software of the ICT infrastructure components

1. The capital market infrastructure entity should develop formal principles of software updates for computers and mobile devices, as well other components of the ICT environment (including updates of operating systems, database management systems, utility software, network devices software etc.), taking into account the significance of this software and the level of criticality of individual updates.

2. The principles of updating software of the ICT infrastructure components should, in particular, designate the persons responsible for making decisions concerning changes in the production environment.

3. Prior to updating of software of the production environment components, which exert impact on IT systems of high significance for the operation of the capital market

[34] A „*Denial-of-Service*" attack – an attack based on an attempt to prevent use of a given component of the ICT environment by other components or by authorized users.

[35] See: section „Classification of information".

infrastructure entity [36], the situation should be analyzed in the context of the decision on verification of the impact of such update using the test environment.

4. Timeliness and correctness of the update installation should be subject to periodic inspections. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment and the degree of risk exposure in terms of security of this environment) and make the appropriate decision with regard to application of automated mechanisms for installation of updates of PC and mobile device software components, as well as automatic tools to analyze the ICT environment with regard to software updates.
5. The capital market infrastructure entity should aim at limiting the number of the ICT environment components having no manufacturer support, in particular, with regard to those components, which are of significance for the operation of the capital market infrastructure entity. In this regard, the capital market infrastructure entity should in particular:
   - Identify and record the cases of ICT environment components receiving no manufacturer support and assess the associated risk,
   - Conduct analyses of the possibility of replacement of such components with components receiving such support or of undertaking other tasks aimed at control of the associated risk.

The above activities should be performed in advance, taking into account the period required to implement the tasks aimed at assuring control of risk associated with use of components, which are not receiving manufacturer support.

Management of capacity and performance of the ICT infrastructure components

1. The ICT infrastructure of a capital market infrastructure entity should be characterized by:
   - Scalability, understood as the possibility of increasing performance and capacity quickly,
   - Redundancy, understood as the possibility of managing an increased number of operations on the basis of the currently used resources (the temporary increase in load may be due e.g. to management of an increased number of orders and transactions conducted by the customers).
2. The capital market infrastructure entity should have in place the documented principles of management of performance and capacity of the ICT infrastructure components, taking into account the significance of individual components for operation of the capital market infrastructure entity and the correlations between these components, including in particular:
   - Specification of the performance parameters (e.g. system response time, processing time)
   - And capacity (e.g. loading of the ICT network, utilization rate for the mass storage devices, utilization rate for processors, number of open connection sessions), specifying the warning and threshold values in this regard,
   - Monitoring of the above parameters,
   - Analysis of trends and forecasting of demand for performance and capacity, taking into account the strategic objectives of the capital market infrastructure entity, in particular, with regard to the planned number of customers served and changes in the profile of operation and the associated expected volume of data processed,

[36] See: section „Classification of IT systems".

- Undertaking action in the case of exceeding of the warning and threshold values of the above parameters and in the case if analyses of demand for performance and capacity indicate that the present resources are insufficient to satisfy such demand,
- Reporting with regard to performance and capacity of the ICT infrastructure components, in particular, to the owners of IT systems.

3. In order to increase the effectiveness of the capacity and performance management process, the capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment and the degree of risk exposure in terms of security of this environment) and make the appropriate decision with regard to:
- Application of tools that allow for automation of monitoring of the degree of loading of resources,
- Formalization of quality parameters of services rendered by the ICT environment on behalf of internal and external users and commencement of reporting in this regard to the management information system[37].

4. The capital market infrastructure entity should conduct periodic verifications of the capability of the ICT environment in the disaster recovery center to maintain the required capacity and performance parameters.

The ICT infrastructure documentation

1. The capital market infrastructure entity should make sure that documentation of individual components of the ICT environment (including their configuration) and correlations between them:
- Is up-to-date,
- Is sufficiently detailed for the level of significance of each of these components,
- Enables conducting of reliable analyses of the environment in terms of its security and optimization,
- Allows for identification and elimination of causes of failures,
- Allows for recovery of activity if necessary,
- Allows for effective completion of internal control tasks.

2. The ICT infrastructure documentation should be subject to protection in accordance with its sensitivity level. The scope of documentation (in particular, documents that specify in detail the configuration and functioning of the security systems), made available to individual employees, should not exceed the necessary minimum associated with their scope of obligations.

3. The subsequent versions of the documentation should be marked and include the metrics of changes (date of introduction, persons preparing and approving the document),

4. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment, the frequency of introduction of technical changes and the number of administrators and service technicians) and make the appropriate decision with regard to implementation of the electronic repository of documentation for the ICT infrastructure.

5. The capital market infrastructure entity should develop the procedures of use and administration of individual components of the ICT environment. The completeness and validity of these procedures should be subject to periodic verification, particularly in the case of those components of the ICT environment, which are modified frequently.

[37] See also: section „The management information system".

4.3 Cooperation with external suppliers of services

Guideline 10

The capital market infrastructure entity should develop formal principles of cooperation with external suppliers of IT services, warranting security of data and proper operation of the ICT environment, taking into account services rendered by entities belonging to the capital group of the capital market infrastructure entity.

1. Taking into account the specific nature of operation of the capital market sector, among the services rendered by external entities, the tasks performed in the area of information technology are of particular significance due to their direct impact on the quality and security of services rendered on behalf of customers and the reputation of the capital market infrastructure entity. At the same time, depending on the specific conditions of operation of the capital market infrastructure entity, the impact of quality of cooperation with external entities on the quality of services rendered by the capital market infrastructure entity on behalf of its customers is highly diversified. Therefore, the process of management of relationships with external service providers should be adapted to these conditions. The capital market infrastructure entity should not treat ordering of any services to an external entity as a release from responsibility for the quality and security of these services, rendered on behalf of the customers, and the security of their data.

2. The agreements concluded by the capital market infrastructure entity with external service providers should warrant that these services will be rendered in accordance with the legal requirements, internal and external regulations[38].

3. The agreement templates or agreements concluded by the capital market infrastructure entity with external service providers should be verified in the appropriate extent by the capital market infrastructure entity units responsible for the legal issues and for security of the ICT environment.

4. The capital market infrastructure entity should develop the rules of cooperation with employees of external service providers, taking into account in particular:

- The conditions of granting access to business secrets and confidential information[39],
- The principles of supervision of activity of external employees,
- The necessity to make sure that every external employee having access to business secrets and confidential information is subject to at least the same restrictions with regard to security as the employees of the capital market infrastructure entity, having access to such information.

5. The principles of cooperation between the capital market infrastructure entity and the external service provider should take into account the principles of communication and coordination of activities performed by the service provider (e.g. data migration, maintenance tasks, scanning of the ICT infrastructure etc.), minimizing their negative impact on the quality and security of services rendered on behalf of the customers of the capital market infrastructure entity.

6. The capital market infrastructure entity should pay particular attention to the risk associated with granting to external service providers (particularly those not belonging to the capital group) of competences with regard to administration of access rights with regard to the IT systems.

---

[38] See also: section „Formal and legal security".
[39] See: section „Classification of information".

4.4 Access control

Guideline 11

The capital market infrastructure entity should develop formal principles and technical mechanisms that ensure the proper level of control of logical access to data and information and physical access to the key components of the ICT infrastructure.

Logic access control mechanisms

1. The IT systems used by the capital market infrastructure entity should have access control mechanisms, allow for unequivocal determination and authentication of identity and user authorization.
2. The access password parameters (including the length and complexity of the password, frequency of change, possibility of repeated use of a historic password) and the principles of blocking of user accounts should be established in the internal regulations, taking into account the system classification[40] and other associated conditions, including the legal aspects[41]. Functionality of the IT systems used should, as much as possible, enforce the application of rules of the capital market infrastructure entity with regard to access password and blocking of user accounts if a wrong password is used.
3. The process of management of authorizations should be formalized in the internal procedures, specifying the principles of applying for, granting, modification and withdrawal of access rights to systems or functionalities, as well as access monitoring. The scope of access rights granted should not go beyond the substantive scope of obligations and rights of the user (including external users, such as capital market infrastructure entity agents) and it should be subject to periodic inspections.
4. The capital market infrastructure entity should conduct regular reviews of the authorizations granted, including compliance of the authorizations actually granted in the IT systems with the authorizations assigned in the authorization registers, as well as with the substantive scope of rights and obligations of individual users. The frequency of such reviews should be based on analysis of the level of risk, associated with individual employees and IT systems, and it should not be less than once a year. The authorization reviews should be performed in accordance with the appropriate scope also in the case of modification of an IT system functionality and changes in the scope of duties of employees. The significant inconsistencies detected and the actions undertaken in association with these should be reported within the framework of the management information system[42].
5. In order to increase the effectiveness of management and supervision of rights and to limit the risk of granting of inadequate access rights, the capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment, the degree of exposure to risk with regard to security of this environment and the number of its users) and make the appropriate decision with regard to:
   - Development of the standard access profiles for specific employee groups or positions,
   - Use of tools for automation of the user authorization management process (in particular, for recording of historic authorizations).
6. To the extent possible, the capital market infrastructure entity should limit user access to functions allowing for independent increasing of own rights. In situations, in which the above principle cannot be followed (e.g. in the case of IT system administrators), other

[40] See: section „Classification of IT systems".
[41] See also: section „Formal and legal security".
[42] See also: section „The management information system".

control mechanisms should be provided.

7. In the case of systems, which can bring exceptionally high losses in the case of their unauthorized use, the capital market infrastructure entity should analyze the situation and make the appropriate decision with regard to combining of access passwords with other user identity verification mechanisms (e.g. tokens, electronic ID cards, biometric methods etc.).
8. All users of IT systems of the capital market infrastructure entity should be informed of their responsibility for their password confidentiality and for the consequences of activities performed using their accounts.
9. The authorization management principles, applicable at the capital market infrastructure entity should, in particular, take into account the threats associated with abuse of privileged user authorizations. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment and the degree of risk exposure in terms of security of this environment) and make the appropriate decision with regard to introduction of mechanisms that warrant registration every time and the possibility of monitoring of access at the privileged authorization level to the most sensitive components of the ICT environment.
10. IT systems, which process data of high importance for the capital market infrastructure entity[43] should have mechanisms in place, allowing for automatic recording of the events taking place so that the records can be used – if necessary – as reliable evidence of improper or inadequate use of these systems. The event recording mechanisms should also prevent unauthorized deletion or modification of entries.
11. The capital market infrastructure entity should develop formal principles of management of cryptographic keys, in particular, their development, storage, distribution, deletion and archiving, to ensure protection of these keys against unauthorized modification and disclosure.
12. A significant aspect of the ICT environment security is control of physical access to rooms, in which servers and other key components of the ICT infrastructure are located, as well as the supporting equipment (including standby power supply, power generators, air-conditioning and switching stations). The physical access control mechanisms should warrant access only for authorized persons (that is, those, who have been granted access in accordance with the scope of their duties) and activation of alarm signal in the case of access attempts made by unauthorized persons. Such mechanisms should also include recording of individual traffic. The solutions applied should be adequate to the level of risk associated with components located in a given room, the specific conditions (including the location) of the capital market infrastructure entity and the scale and nature of business operation.
13. In rooms, in which the key components of the ICT infrastructure are located, apart from exceptional situations, taking photos, audio and video recordings should be prohibited. Authorizations in exceptional cases should be granted by the appropriately authorized persons and recorded.

4.5 Malware protection

Guideline 12

The capital market infrastructure entity should ensure the proper protection of the ICT environment against malware.

1. The capital market infrastructure entity should provide automatic protection against

[43] See: section „Classification of information and IT systems".

malware (such as viruses, Trojan horses, worms, rootkit[44] software etc.), both for the central components of the ICT infrastructure, which require such protection (servers, domain controllers etc.) and for PC computers and mobile devices. Such protection should be provided on a continuous basis, and the users should not be able to turn it off. The scope of protection should be associated with the degree of exposure of each infrastructural component to a threat, as well as the potential severity of its consequences for the capital market infrastructure entity.

2. Applications ensuring protection against malware and malware signatures should be updated systematically. To the extent possible, the capital market infrastructure entity should make sure that the above validity is verified at every attempt of connecting a device to the internal network.
3. The capital market infrastructure entity should develop formal principles of malware protection, including in particular:
   - The mode of action in relation to various types of malware found,
   - The mode of decision-making with regard to withdrawal from use of the threatened components of the ICT environment or their separation from the remaining part of this environment,
   - The mode of notifying of the appropriate units of the capital market infrastructure entity of the threat[45].
4. Regardless of the level of automatic protection against malware, of key significance in this regard is also the awareness of the security issues among the end users. Therefore, the capital market infrastructure entity should ensure the proper level of user education in this regard[46].

4.6 User support

Guideline 13

The capital market infrastructure entity should provide the internal users of IT systems with support in solving of problems associated with operation of these systems, including those resulting form failures and other non-standard events that interfere with use of these systems.

1. The mode of operation of the area of support for internal users of IT systems should be adapted to the scale of operation, complexity of the ICT environment and the number of internal users, taking into account the potential dependence on the external service providers.
2. The functioning of the process of support of the internal users of IT systems should be formalized adequately to the complexity of the ICTS environment of the capital market infrastructure entity and the number of internal users of the IT systems. Notifications should be recorded and analyzed in order to enable preventive actions with regard to the problems identified. Persons responsible for providing user support should also be trained in identification and escalation of the information security incidents[47].
3. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment and the number and profiles of its users) and make the appropriate decision with regard to providing support for

[44] Rootkit software – a tool, which modifies system files to hide its presence from the user, anti-virus software etc., allowing for performance of tasks defined by the programmer (such as taking over of user passwords or preventing anti-virus updates) without the knowledge of the user.
[45] See also: section „Management of information security incidents".
[46] See: section „Employee education".
[47] See: section „Management of information security incidents".

management of user notifications by the IT system, allowing, in particular, for collecting and reporting of data on the existing problems and monitoring of quality of the support provided.

4.7 Employee education

Guideline 14

The capital market infrastructure entity should engage in effective activities, aimed at achieving and maintaining the proper level of employee qualifications with regard to the ICT environment and security of information processed in this environment.

1. The capital market infrastructure entity should maintain the proper level of qualifications of all employees in order to ensure security of information processed in the ICT environment and to enable the proper use of IT equipment and systems. This level should be diversified depending, among other things, on the risk associated with the authorization and competence levels of individual employees and their roles in management of the ICT environment security.
2. In order to ensure the proper level of employee qualifications in this regard, the capital market infrastructure entity should apply the adequate formats of training, provide the appropriate materials and engage in various education initiatives, aimed at development of the information security culture (e.g. using posters or screen savers). The capital market infrastructure entity should also analyze the situation and make the appropriate decisions with regard to awarding of positive behaviors that support the culture of information security.
3. Within the framework of employee education, the capital market infrastructure entity should take into account, among other things, the threats associated with use of mobile devices, use of own IT equipment for professional purposes and use of business equipment for private purposes, publication of information on the capital market infrastructure entity on the Internet (particularly in the social media) and socio-technical attacks, as well as inform the employees of the process of disciplinary sanctions against persons, who fail to comply with the security procedures.

4.8 Continuity of operation of the ICT environment

Guideline 15

The business continuity management system of the capital market infrastructure entity should take into account the specific conditions associated with its ICT environment and the data processed by it.

Business continuity plans and emergency plans

1. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the degree of risk exposure in terms of security of the ICT environment and the scale and nature of its operation) and make the appropriate decision with regard to designation of the person or team for the affairs of business continuity, in particular, to supervise the availability of the necessary resources, allowing for continuation or recovery of business activity.
2. Since recovery of operation of the ICT environment is usually necessary to recover the functioning of the business processes, the capital market infrastructure entity should pay particular attention to management of business continuity with regard to the units responsible for the functioning of this environment.
3. The business continuity management system documentation of the capital market infrastructure entity, concerning the ICT environment (in particular, the data replication,

backup creation and recovery procedures) should take into account the classification of IT systems and the information processed by these systems[48], as well as the correlations between these systems. The validity of this documentation should be verified on a regular basis.

4. The capital market infrastructure entity should have an effective system for distribution of documentation of the business continuity management system with regard to the ICT environment, warranting its confidentiality, as well as access by authorized persons.
5. Within the framework of its business continuity management strategy, the capital market infrastructure entity should take into account the issue of dependency upon the external service providers, being of key significance from the perspective of business continuity of the capital market infrastructure entity. In particular, the capital market infrastructure entity should:
   - Define the mode of communication and cooperation with the service provider in the case of an emergency situation,
   - Take into account the participation of external service providers in the process of testing of the business continuity management system[49],
   - Develop the principles associated with emergence of the necessity to replace a service provider during an emergency situation.

Technical resources and the physical and environmental conditions

1. The capital market infrastructure entity should have the technical resources, adequate to the scale and nature of its operation, allowing for day-to-day functioning of the key processes and their recovery in the case of an emergency situation, taking into account, in particular, the following parameters, defined for these processes:
   - Parameters defining the maximum duration of recovery of functioning of these processes [50],
   - Parameters defining the maximum quantity (that is, the maximum length of the period) of data stored in IT systems, which can be lost[51].
2. In the case of an extensive failure or inaccessibility of the basic data processing center, the capital market infrastructure entity should be able to recover the ICT environment (adequate to the assumptions of the emergency plans) at the disaster recovery location. This locations should be sufficiently distant from the basic center in order to minimize the risk of inaccessibility of both centers due to a single cause (such as a flood). The process of recovery of the environment should be formalized in the detailed internal regulations, defining the scope of competences, the necessary resources and the order and mode of recovery of the ICT environment components.
3. The mode of functioning of the disaster recovery center should be adapted to the scale and nature of business operation and take into account the maximum service unavailability time accepted by the capital market infrastructure entity.
4. A prerequisite for continuous and safe functioning of the ICT environment is to ensure the physical and environmental safety in the locations, in which the key components of the ICT infrastructure are stored, in particular, with regard to the conditions associated with continuity of power supply and stability of its parameters, temperature, humidity and dust level, as well as key components of the flood, fire, theft or intentional damage protection systems. Therefore, the capital market infrastructure entity should identify the threats in

[48] See: section „Classification of information and IT systems".
[49] See: section „Verification of effectiveness of approach to business continuity management".
[50] RTO - Recovery Time Objective.
[51] RPO –Recovery Point Objective.

this regard and analyze their potential impact on security of the ICT environment and business continuity (in particular, if the resources of the disaster recovery center are not sufficient to allow for a rapid resumption of activity). This analysis should allow for determining whether location of the rooms, in which the key components of the ICT infrastructure have been installed, is proper and whether they have been appropriately secured.

5. Conducting the above analysis, the capital market infrastructure entity should, in particular, take into account the threats associated with:

- Building location and the nearby facilities (including airports, military structures etc.)
- Location and surrounding area of the rooms, in which the key components of the ICT infrastructure are installed (in particular, the threats associated with these rooms being located at the basement or attic level),
- Structural conditions (such as the load capacity of the roof, air-tightness of the rooms, quality of the lightning protection system).

6. In order to warrant the proper physical and environmental conditions in the location of key components of the ICT infrastructure, the capital market infrastructure entity should, in particular, comply with the following principles:

- The doors, windows, walls and roofs in rooms, in which the key components of the ICT infrastructure are located, should be characterized by appropriate mechanical, fire and burglar resistance.
- No flammable materials should be placed in rooms, in which the key components of the ICT infrastructure are located, or – if necessary – such materials should be appropriately secured (e.g. placed in cabinets, which warrant fire protection).
- The fire extinguishing agents used should minimize the risk of damaging of the electronic devices and the data stored.
- The anti-burglar and fire protection measures should provide for immediate notification of persons responsible for protection and for initiation of a firefighting and rescue action. The capital market infrastructure entity should also analyze the situation and make the appropriate decision with regard to adding the automatic fire extinguishing equipment to the fire protection system.
- in rooms, in which the key components of the ICT infrastructure are located, it is necessary to maintain the environmental parameters (e.g. temperature, humidity, dust level etc.) specified by manufacturers of these components. The devices used by the capital market infrastructure entity to control these parameters should be characterized by appropriate performance and redundancy (in the case of an emergency). The capital market infrastructure entity should analyze the situation and make the appropriate decision with regard to application of solutions to ensure the automatic monitoring and adjustment of the environmental parameters.
- Selection of mechanisms to ensure continuity of power supply should take into account the size, scale and nature of operation of the capital market infrastructure entity. Emergency power supply in form of batteries (UPS) allows for maintenance of operation of the resources for a limited period of time, and, usually, within a limited scope – therefore, the capital market infrastructure entity should analyze the situation and make the appropriate decision with regard to providing an independent power supply, based on a power generator, if possible, activated automatically in the case of a failure of the main power supply, as well as application of multiple power supply lines.

7. In the case of temporary moving of the ICT equipment to another room (e.g. in association with a renovation), the capital market infrastructure entity should make sure that the

physical and environmental conditions in this room are proper and provide the appropriate access control level[52].

8. Effective functioning of mechanisms aimed at ensuring the proper physical and environmental conditions in locations, in which the key components of the ICT infrastructure are installed, should be subject to periodic reviewing.

Backup copies

1. One of the methods of ensuring continuity of operation in the case of a failure or a disaster are backup copies of data, IT system instances and configuration of the key components of the ICT infrastructure. The capital market infrastructure entity should develop formal principles of management of storage media, used to store the backup copies. These principles should, in particular, include the following:
   - The scope, mode and frequency of data copying,
   - The modes of identification of storage media,
   - The place, period and mode of safe storage of the media,
   - The mode and form of authorization of data modification and removal from the storage media,
   - The roles and responsibilities with regard to storage media management,
   - The modes of proper and permanent liquidation of unneeded data (with regard to liquidation of data saved on the storage media still in use and liquidation of storage media withdrawn from operation).
2. The correctness of backup and possibility of recovery of backup data should be subject to periodic inspections. Such inspections can be performed automatically; in such case, the appropriate persons should be informed of the inspection results.
3. The capital market infrastructure entity should have the detailed regulations and instructions for recovery of the ICT environment components on the basis of backup copies. The content of these documents should allow for implementation of the process by third persons, having the appropriate qualifications and authorizations (that is, persons, who are not involved in day-to-day administration of a given component of the environment). The process of recovery of the ICT environment components should be systematically tested.
4. The capital market infrastructure entity should ensure integrity of the backup copies from their creation until liquidation. This means that throughout the entire period, defined above, the copies are to reflect the actual status of resources at the time of creation of the backup copy, which excludes the possibility of removal of any data. The regulations and instructions with regard to recovery of data from backup copies should include the rules of modifying the data recovered to reflect the changes made in the period between creation of a given backup copy (or sequence) and its use to recover the state of the ICT environment as it was before the failure.
5. The backup copies, particularly those, which are transported or transmitted outside the capital market infrastructure entity, should be secured (e.g. with cryptographic protection) against unauthorized access at the level adequate for the classification of data stored[53]. Media containing backup copies should be stored in a manner that minimizes the risk of their damage (e.g. as a result of a fire, flood, electromagnetic field) or unauthorized modification. They should also be stored separately from the related environment components.

[52] See: section „Physical access control mechanisms".
[53] See: section „Classification of information and IT systems".

6. Media, which have been damaged or withdrawn from use, should be destroyed in the manner preventing data recovery.

Verification of effectiveness of approach to business continuity management

1. The capital market infrastructure entity should, on a regular basis, verify the approach to business continuity management with regard to the ICT environment, including the capability of recovery of operation on the basis of a backup copy. The frequency, scope and mode of tests to be conducted (such as simulations, overall operation tests etc.) should take into account the scale and nature of operation of the capital market infrastructure entity and the threats associated with individual components of the ICT environment. The test plans, particularly those, which may exert impact on day-to-day operation of the capital market infrastructure entity, should be consulted within the organization and approved by the management board of the capital market infrastructure entity. The test results and corrective action plans, which are to be implemented to eliminate the inconsistencies identified, should be documented. The board of supervisors and management of the company should be informed of the test results and timeliness and effectiveness of the corrective action undertaken.

4.9 Management of the electronic access channels

Guideline 16

Any capital market infrastructure entity that renders services using electronic access channels, should have in place the effective technical and organizational solutions to ensure verification of identity and security of data and funds of the customers, and it should educate the customers with regard to the principles of safe use of these channels.

Customer identity verification

1. An issue of key significance in the services of a capital market infrastructure entity, rendered through electronic access channels, is confirmation of whether a given attempt of contact or access is authorized or not.

Therefore, the capital market infrastructure entity should define and apply the best possible methods and means of:

- Verification of identity of the customer when opening the account, including the procedures of remote agreement conclusion[54],
- Confirmation of identity and authorization of customers using the electronic access channels, minimizing the risk of granting access to unauthorized persons.

2. Selection of the methods applied by the capital market infrastructure entity in order to confirm the identity of customers using the electronic access channels should be made on the basis of analysis of the risk associated with these channels. Such analysis should be conducted systematically, taking into account the transaction options offered by a given access channel, the data processed, recognized attack techniques, as well as the ease of use by the customer of individual methods of identity confirmation. The typical methods of identity confirmation in the electronic access channels include the personal identification number, passwords, electronic signatures, smart cards, single-use codes, tokens, biometric data and digital certificates; the identity verification methods can be based on one or many factors (e.g. use of passwords and one-time codes at the same time). The capital market infrastructure entity should also determine whether and to what extent application of a multi-factor identity verification system will contribute to enhancement of customer security.

[54] See also: section „Formal and legal security".

3. The capital market infrastructure entity should analyze the situation and make the appropriate decision with regard to application of other security mechanisms, such as verification of the logging time and place using an electronic access channel.

Security of customer data and funds

1. Apart from the above measures, in order to prevent unauthorized access to the account of the customer using electronic access channels, the IT systems used in these channels should be designed and configured in the manner, which ensures the sufficiently high level of integrity, confidentiality and availability of data processed using these channels throughout the entire process of data processing (both by the capital market infrastructure entity and by external service providers). In addition, the capital market infrastructure entity should make sure that:
   - It has developed the principles of granting authorizations to electronic access channels, minimizing the risk of internal fraud,
   - The connection sessions are encrypted and additional mechanisms have been introduced to make these sessions as much resistant to manipulations as possible (e.g. by closing the session in the case of user inactivity for a specified time period or upon closing of the client application without logging out),
   - The IT systems used in conjunction with the electronic access channels allow for identification and securing of evidence, which could be used in court (in particular, minimizing the risk of loss of such evidence or its rejection due to insufficient securing of data),
   - The IT systems used in conjunction with the electronic access channels have been designed to minimize the probability of accidental access by unauthorized users,
   - The solutions used in association with electronic access channels provide the capital market infrastructure entity with access to control and verification paths, in particular with regard to:
     - Opening and closing of customer accounts,
     - Change of customer information,
     - All limits granted to the customer and authorizations to exceed these limits,
     - Successful and unsuccessful log-in attempts,
     - All cases of granting, modification or withdrawal of system access authorizations.
2. In the case if external service providers participate in the process of rendering of services using the electronic access channels, the capital market infrastructure entity should make sure that they have the appropriate software for management of security of information processed on behalf of the capital market infrastructure entity.[55]
3. Unless the legal provisions in force allow for a situation, in which no agreement has been concluded with a customer for the electronic access channels, such agreement should specify the principles of protection of information and the detailed conditions of providing access (in particular, the identity verification methods).
4. The capital market infrastructure entity should provide its customers with a communication channel (e.g., a mailbox, a phone number), making it possible to inform the capital market infrastructure entity of events identified by the customers, concerning security of the electronic access channels (e.g. phishing attacks).

Customer education

1. Due to the fact that a substantial part of the service channel remains beyond its direct

[55] See also: section „Cooperation with external service providers".

control, the capital market infrastructure entity should aim at providing the customers using electronic access channels with the adequate level of knowledge, allowing them to understand the threats associated with use of these channels and application of effective ways of securing themselves against such threats. The above can be implemented, for instance, in form of visible information published on the Web page of the capital market infrastructure entity, in information flyers, e-mails sent to the customers etc.

2. The capital market infrastructure entity should inform its customers of the threats, associated in particular with:

- Inadequate protection of data used for logging into electronic access channels,
- Inadequate protection of devices used to perform services, rendered via electronic access channels (mobile phones, computers), including the significance of use of anti-virus software and firewalls, physical access control, software updates on a regular basis etc.
- Other techniques aimed at taking over of information providing access to the account (e.g. phishing attacks), indicating the means of protection against these techniques.

4.10 Management of End-User Computing[56]

Guideline 17

The capital market infrastructure entity should develop formal principles of management of the so-called end user computing, effectively limiting the risk associated with use of this software.

1. Due to the threats associated with use of End-User Computing (such as high vulnerability to programming errors, probability of data loss usually higher in comparison with conventional IT systems, high vulnerability to interference with the data processing algorithms, contained in these tools, etc.), with regard to management of software of this type, the capital market infrastructure entity should in particular:

- Identify the significant EUC, that is, software used for processing of data of high significance for the capital market infrastructure entity or of high significance from the perspective of the processes implemented by the capital market infrastructure entity,
- Document the significant EUC, including its role in the business processes, the scope of data processing, the data processing algorithms etc.,
- Maintain a register of the EUC used at the capital market infrastructure entity, which is of significance,
- Ensure the proper level of security of the significant EUC (e.g. by protecting folders, in which it is saved, or blocking the form editing function) in order to prevent unauthorized modifications of the tool itself and the data stored in it,
- Have in place the formal principles of development, testing and modification of significant EUC,
- Analyze the threats and problems associated with use of EUC in individual areas of operation, and – in the case of identification of significant threats or problems in this regard - analyze the situation and make the appropriate decision with regard to replacement of EUC with functionalities of the existing or new IT systems.

[56]End-User Computing, EUC – tools developed and functioning on the basis of PC applications, such as MS Excel or MS Access, allowing users other than computer programmers to develop business applications.

5 Management of security of the ICT environment.

5.1 The ICT environment security management system

Guideline 18

The capital market infrastructure entity should use a formal, effective system for management of the ICT environment security, encompassing tasks associated with identification, estimation, control, counteracting, monitoring and reporting of risks in this regard, integrated with the overall risk management and information security system of the capital market infrastructure entity.

1. The system for management of security of the ICT environment should be rooted in the strategy of the capital market infrastructure entity with regard to security of the ICT environment and it should be based on formal internal regulations. The basic document in this regard should be the information security policy.
2. The ICT environment security management system should be subject to systematic reviews in order to make the possible improvements and to adapt it to changes in the external and internal environment of the capital market infrastructure entity.
3. The capital market infrastructure entity should analyze the benefits associated with application of international standards (or their Polish equivalents) with regard to information security (such as ISO/IEC 27000) and make the decision with regard to the potential adaptation of the ICT environment security management system of the company to the requirements of these standards.
4. The capital market infrastructure entity should, to the extent possible, ensure strict integration of the ICT environment security management system with the operating risk management system. For this purpose, the capital market infrastructure entity should, among other things, implement in the ICT environment security management system the operational risk management tools, based on the economic conditions and internal control factors,[57] operational risk self-assessment, scenario analyses or risk maps.

Identification of risks with regard to the ICT environment security

1. The purpose of identification of risks associated with security of the ICT environment is to determine the associated threats that may generate losses (including financial losses) in a given institution and to specify where, how and why these threats can materialize.
2. Risk identification with regard to the ICT environment security should be performed systematically and based on:
   - Identification of risk associated with the potential threat to security of the ICTS environment prior to materialization of threats,
   - Identification of risk associated with the potential threat to security of the ICTS environment after materialization of threats.
3. Identifying risks associated with the potential threat to security of the ICTS environment prior to materialization of threats, the capital market infrastructure entity should pay particular attention to identification of the existing vulnerabilities of the ICT environment (including the ICT infrastructure components) and the threats, which may take advantage of them. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment and the degree of exposure to risk in terms of security of this environment) and make the appropriate

[57] E.g. the number of information security incidents in a given reporting period, the number of significant security recommendations for this environment, issued by the internal audit unit, the number of non-secured vulnerabilities in the key components of the ICT environment.

decision with regard to use of the automatic tools, allowing for identification of the existing vulnerabilities. Regardless of the periodic assessment, identification of risk associated with the potential threat to security of the ICTS environment should be conducted each time in the case of planning of significant changes in the structure of IT systems [58], as well as in the mode of their use, as well as in the case of plans for implementation of new technologies.

4. Identifying risks associated with the potential threat to security of the ICTS environment after materialization of threats, the capital market infrastructure entity should collect information on events that took place, which exert impact on security of data processed by the capital market infrastructure entity and – in the case of compliance with the operating event definition, used by the company – place it in the database of operating events.

Estimation of risk with regard to security of the ICT environment

1. Estimation of risk with regard to the ICT environment security is aimed at determination of the probability and the potential impact of materialization of threats, associated with this risk, on the institution and the associated assessment of this risk.
2. The risk assessment tasks should be implemented in accordance with the classification of information and IT systems[59]. Examination of impact of the threats identified should encompass the issues associated with the component, to which a given threat pertains. As a result of the risk estimation process, the capital market infrastructure entity should gain knowledge on threats in its operation, associated with the ICT environment security, the probability of materialization of the threats identified and the possible consequences of their materialization, taking into account the potential loss of reputation, which may lead to deterioration of customer trust and termination of their cooperation with the capital market infrastructure entity, which may, in particular, impact the liquidity of the company. This knowledge should serve as a basis for adequate decisions concerning risk control and prevention.

Risk control and prevention with regard to the ICT environment security

1. Taking into account the risk estimation in terms of the ICT environment security, the capital market infrastructure entity should make the appropriate decisions with regard to approach to specific threats, consisting of:
   - Limiting of risk, that is, introduction and modification of the existing organizational and technical control mechanisms with regard to the ICT environment security,
   - Transfer of risk, that is, transferring the risk, associated with a given threat, in whole in part, to an external entity[60], in particular, by contracting tasks to external service providers [61] or purchase of insurance,
   - Risk avoidance, that is, withdrawal from acts associated with a given threat,
   - Risk acceptance, that is, intentional withdrawal from acts aimed at limiting of the probability or consequences of materialization of a given threat, including the potential provision of resources for coverage of the associated losses.
2. The control mechanisms applied should be adequate in particular to: the threats identified, estimated risk associated with these threats and significance of the associated components of the ICT environment, in particular, the IT systems [62], the scale and nature of operation of the capital market infrastructure entity, complexity of the ICT environment of the capital

[58] See also: section "Development of IT systems".
[59] See: section „Classification of information and IT systems".
[60] The capital market infrastructure entity cannot, however, treat transfer of risk as an alternative to proper risk management.
[61] See: section „Cooperation with external service providers".
[62] See: section „Classification of information and IT systems".

market infrastructure entity.

3. The capital market infrastructure entity should make sure that all exceptions to the applicable internal regulations and control mechanisms used are documented and controlled in accordance with the formal procedure, specifying, among other things, the situations, in which consent can be given for a departure from the rule, the principles of filing and acceptance of requests for such consents (making sure that the request contains a justification for a given exception), the persons authorized to give consent, the acceptable time of validity of the departure and the principles of reporting in this regard. The capital market infrastructure entity should also conduct, on a systematic basis, risk analyses with regard to these departures.
4. The capital market infrastructure entity should verify on a regular basis, whether the approved control mechanisms are adequate to the risk profile, and the mode of their functioning is appropriate. If necessary (e.g. if it is found that the applicable internal resources of the capital market infrastructure entity are not sufficient), the capital market infrastructure entity should take advantage of services rendered by external specialists, taking into account, however, the necessity to follow the legal provisions with regard to the entrustment agreement (outsourcing) and the obligation to protect business secrets and confidential information. Risk control with regard to ICT environment security should be exercised adequately to the risk level, regardless of whether the risk is associated with processing of customer data (or engaging in other operations within the framework of business activity of the capital market infrastructure entity) or with data processing for external entities.

Risk monitoring and reporting with regard to ICT environment security

1. The results of risk identification and estimation with regard to the ICT environment and results of tests of effectiveness of the control mechanisms introduced should be monitored (also from the perspective of the existing trends) and presented to the management of the capital market infrastructure entity and the board of supervisors within the framework of the functioning management information organization system[63]. Such information should be delivered on a regular basis, and the frequency and scope of delivery should be based on the risk profile of the capital market infrastructure entity and provide for the possibility of an adequate response.

5.2 Classification of information and IT systems

Guideline 19

The capital market infrastructure entity should classify IT systems and the information processed in accordance with the principles, which take into account, in particular, the security level required for these systems and information.

Classification of information

1. The capital market infrastructure entity should develop the principles of classification of information, making sure that all information processed by the ICT environment is subject to the appropriate level of protection. For this purpose, it is necessary to develop an information classification system, which would encompass all data processed by IT systems of the capital market infrastructure entity and to make sure that classification of all information is adequate to the current internal and external conditions of the capital market infrastructure entity.

[63] See also: section „The management information system".

2. Information should be classified with regard to the required security level, taking into account, in particular:
   - The significance of this information for the capital market infrastructure entity and the processes implemented,
   - The significance of this information from the perspective of management of the risk types, which have been identified as significant for the scope of operation of the capital market infrastructure entity,
   - The effects of loss or unauthorized modification of information,
   - The effects of unauthorized disclosure of information,
   - The special regulatory and legal requirements applicable to a given type of information[64].
3. Classification of all information should be taken into account in development of information security mechanisms throughout the entire processing cycle – from obtaining, through use, the potential transfer outside the capital market infrastructure entity until archiving and deletion.
4. Access to business secrets and confidential information should be granted only to persons, considered to meet the conditions of authorization by the capital market infrastructure entity in the light of the applicable legal provisions. Moreover, every person granted access to business secrets and confidential information by the capital market infrastructure entity, should be obligated to sign a confidentiality commitment (valid after such access has been withdrawn), provided that this principle does not apply in cases, if the generally applicable legal provisions impose the obligation of granting such access to information.
5. Storage of information of significance for the capital market infrastructure entity on desktop computers, laptops or mobile devices should be limited to the necessary minimum and protected accordingly with the classification of such information (e.g. through encrypting, access control mechanisms, data recovery mechanisms).
6. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment, the degree of exposure to risk in terms of security of this environment and the scale and nature of operation) and make the appropriate decision with regard to use of automation solutions with regard to control of risk associated with security of information processed in the ICT environment, such as solutions that limit the possibility of saving of information on storage media by IT system users, enable control of information sent via electronic mail and limit access to electronic mail systems other than those accepted at the capital market infrastructure entity. It should be kept in mind, however, that use of automated solutions of this type does not eliminate the necessity of employee supervision of this area of operation.

Classification of IT systems

1. The capital market infrastructure entity should develop the principles of classification of IT systems, in particular, taking into account the following:
   - Classification of information processed within a given system,
   - Significance of a given system for operation of the capital market infrastructure entity,
   - Significance of other IT systems, which are dependent on a given system.

5.3 Management of information security incidents

Guideline 20

[64] See also: section „Legal and formal security."

The capital market infrastructure entity should develop formal principles of managing information security incidents, including their identification, recording, analysis, prioritization, searching for links, undertaking corrective actions and elimination of causes.

1. The capital market infrastructure entity should develop internal regulations, describing the mode of action in the case of information security incidents, such as failures and overloading of the IT systems, loss of devices or data, human errors posing a threat to security of the ICT environment, successful or unsuccessful attempts to interfere with the means of security, uncontrolled system modifications etc. The scope and level of detail of the above regulations should be adequate to the scale and nature of operation of the capital market infrastructure entity and the level of complexity of the ICT environment.
2. The mode of proceeding in the case of information security incidents should, in particular, specify the following:
   - The methods and scope of gathering of incident information,
   - The scope of responsibility in the area of incident management,
   - The mode of conducting of analyses of impact of incidents on the ICT environment, including its security,
   - The rules of categorization and prioritization of incidents, taking into account the classification of information and IT systems, associated with a given incident[65],
   - The rules of detection of correlations between incidents (an example is a Denial-of-Service attack, preventing fast identification of another incident or removal of its causes),
   - The principles of communication, applicable to the employees of the capital market infrastructure entity, as well as the external service providers and – in the case of a significant threat of consequences of a given incident – also other third parties (customers, business partners etc.), ensuring the adequately fast notification of the interested parties and engaging in activity adequate to the level of significance of the incident,
   - The principles of collecting and securing of evidence associated with the incidents, which can be used in court (in particular, minimizing the risk of loss of such evidence or its rejection due to insufficient securing of data),
   - The principles of engaging in corrective and preventive actions, in particular, designation of persons responsible for implementation of these tasks and monitoring of progress of their completion
3. In order to, for instance, allow for preventive actions with regard to the problems identified, the capital market infrastructure entity should maintain a register of information security incidents, containing, in particular, information on:
   - Incident date and identification,
   - Reasons for occurrence,
   - The course of the incident,
   - Consequences of the incident,
   - Corrective actions undertaken.
4. The capital market infrastructure entity should make sure that all employees and other persons rendering services on behalf of the capital market infrastructure entity, who have

[65] See: section „Classification of information and IT systems".

access to the ICT environment, have been informed of the principles of management of information security incidents adequately to their tasks and scope of authorization. In particular, these persons should be obliged to report any information security incidents (including any suspicion of emergence of such incidents) as soon as possible. For this purpose, the capital market infrastructure entity should establish an appropriate contact point (e.g. within the units responsible for providing IT system users with support), dedicated to management of such notifications, which is to be known to all members of the organization, constantly available and sufficient to allow for exercising of the appropriate response times. Persons responsible for management of notifications should have the appropriate qualifications and knowledge to be able to classify each notification and to initiate the appropriate action for the purpose of its management or escalation, that is, transferring to a person with a higher level of competences in a given area (in particular, on the basis of classification of information or IT systems related to a given incident[66]).

5. It is recommended that in relation to incidents, which exert significant impact on security of the data processed, including, in particular, security of customer funds (also in the case of incidents, of which the capital market infrastructure entity has been informed by the external service provider[67]), the capital market infrastructure entity should have a fast path of reporting (including specification of the possible causes and consequences) to the high level of management of the capital market infrastructure entity. Fast flow of information with regard to the significant information security incident should allow for adequate involvement of the capital market infrastructure entity management in the corrective action undertaken. The management should also be informed of progress of this action on a regular basis.
6. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment, the degree of exposure to risk with regard to security of this environment and the scale and nature of operation) and make the appropriate decision with regard to specification of the composition of teams to be responsible for responding to incidents that exert significant impact on security of the data processed (in particular, the customer funds), having the appropriate knowledge and qualifications in this regard and authorized to undertake effective action in emergency situations.
7. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment, the degree of exposure to risk with regard to security of this environment and the scale and nature of operation) and make the appropriate decision with regard to use of SIEM (Security Information and Event Management*)* solutions, which facilitate management of information security incidents, among other things, through centralization of collection, analysis and storage of event logs generated by the IT systems and other components of the ICT environment.

5.4 Formal and legal security

Guideline 21

The capital market infrastructure entity should ensure compliance of functioning of the information technology and ICT environment security areas with the legal requirements, internal and external regulations, the contracts signed and the internal standards of the capital market infrastructure entity.

1. The capital market infrastructure entity should systematically identify, document and monitor compliance with requirements for the information technology and ICT

[66] See: section „Classification of information and IT systems".
[67] See also: section „Cooperation with external service providers".

environment security areas (including the tasks contracted to external service providers [68]) based on the applicable legal provisions, internal and external regulations, agreements concluded and standards adapted by the capital market infrastructure entity, including:

- The act of July 21st, 2005 on trade in financial instruments (Dz. U. of 2014, item 94, as amended),
- The act of October 26th, 2000 on commodities exchanges (Dz. U. of 2014 item 197),
- The act of November 16th, 2000 on counteracting money laundering and financing of terrorism, (Dz. U. of 2014 item 455)
- The act of August 29th, 1997 on protection of personal information (Dz. U. of 2002 no. 101, item 926 as amended),
- The act of August 5th, 2010 on protection of classified information (Dz. U. of 2010 no. 182, item 1228 as amended),
- The act of February 4th, 1994 on copyright and related rights (Dz. U. of 2006 no. 90, item 631, as amended),
- Implementing acts to the above,

  and agreements and licenses for the software used.

2. Compliance with the above requirements should be subject to reporting within the framework of the management information system[69].

5.5 The role of the internal and external audit

Guideline 22

The information technology and ICT environment security areas should be subject to systematic, independent audits.

1. The capital market infrastructure entity should analyze the situation (taking into account, in particular, the level of complexity of the ICT environment and the degree of exposure to risk with regard to security of this environment) and make the appropriate decision with regard to designation, within the framework of internal audit, of a unit responsible for auditing of the information technology and ICT environment security areas.

2. Persons responsible for auditing of the information technology and ICT environment security areas should have the appropriate qualifications. Audits should be based on the recognized international standards and best practices of the information technology and ICT environment security areas, such as:

- Standards for auditing of information systems of ISACA (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 (International Organization for Standardization) standards.

3. Audits of the information technology and ICT environment security areas should be conducted on a regular basis and each time after any changes that might exert significant impact on the level of security of the ICT environment. The frequency and scope of audits should be based on the level of risk associated with individual audit areas and the results of the previous reviews.

4. Ordering of additional audits to be performed by professional external institutions,

[68] See also: section „Cooperation with external service providers".
[69] See also: section „The management information system".

specializing in auditing of the information technology and ICT environment security areas, may significantly enhance control of risk in this area. Therefore, the capital market infrastructure entity should analyze the situation and make the appropriate decision with regard to complementing of the internal audit activity with external audits, conducted by entities of this kind, in particular, with regard to high risk areas.

5. Information on the audit recommendations and the mode and deadline for elimination of the potential threats should be communicated to the management board of the capital market infrastructure entity.