

**INFORMATION SECURITY MANAGEMENT IN CRISIS (ISMC)  
ACCORDING TO THE STANDARD PN- ISO/IEC 27001: 2017.  
INTRODUCTION TO USEFUL OF THE SYSTEM IN SMALL  
AND MEDIUM ENTERPRISES (SME)**

Natalia JAGODZIŃSKA

BTCH Systemy Zarządzania Gdańsk; natalia.jagodzinska@outlook.com

**Purpose:** The aim of the article is to indicate the requirements and tools for the implementation of an information security management system according to the PN- ISO/IEC 27001: 2017 standard.

**Design/methodology/approach:** The author presents the requirements of the standard PN- ISO/IEC 27001: 2017 that relate to Information Security Systems (ISS) in terms of their usefulness in small and medium enterprises (SME).

**Findings:** The paper identified requirements of implementation and functioning of an information security management system.

**Practical implications:** The requirements for the information security system indicated in the article are the basis for data security in the organization. Data security is required by potential customers, which is to ensure, m.in, security of contract implementation.

**Social implications:** The information security management system according to the standard PN- ISO/ IEC 27001: 2017 is an extension and support for the requirements of the personal data protection requirements.

**Originality/value** The requirements of the information security management system adapted to the requirements of small and medium sized enterprises are presented.

**Keywords:** PN- ISO/ IEC 27001: 2017, Information Security Management System.

**Category of the paper:** Review article.

## 1. Introduction

In times of crisis, many small and medium organizations, in a very short time, changed the form of work. These organizations have moved from stationary to on-line mode. Such a change can also be seen in the area of small and medium-sized enterprises. As a result, information security threats that have not been identified so far have arisen. In crisis, companies began to pay special attention to the security of their resources, which are information resources in

electronic form. There is a significant interest in introducing security policies and procedures to ensure information security. One of the most frequently used solutions in this area is the introduction of the ISO 27001 standard in the organization – information security management system. The introduction of data supervision rules according to PN- ISO/IEC 27001: 2017 significantly increases the level of security of both electronic and paper information. The use of solutions according to the PN- ISO/IEC 27001: 2017 express standard increases data security and a colder risk of data loss, data modification or data theft.

## 2. The concept of information security

In Poland, there are legal regulations that specify requirements for data protection. Such regulations are:

- The Act on the Protection of Personal Data (Journal of Laws of 2002, No. 101, item 929).
- Act on the Protection of Persons and Property (Journal of Laws of 1997, No. 114, item 740).
- Act on the Protection of Classified Information (Journal of Laws of 1999, No. 11, item 95).
- Competition and Consumer Protection Act (Journal of Laws of 2000, No. 122, item 1319).

These requirements are necessary to build an appropriate information security management system in a given organization. The Information Security Management System is an organized and documented process aimed at ensuring information security. The construction of such a system should be carried out based on the guidelines that we can find in the following ISO standards:

- ISO 27000 – Terminology.
- ISO 27001 – Requirements.
- ISO 27002 – Practical Principles of Information Security Management.
- ISO 27003 – Implementation Guidelines.
- ISO 27004 – System Measurements.
- ISO 27005 – Risk Management.
- ISO 27006 – ISMS Auditing.

When talking about information security, the term "information" should be defined. **INFORMATION (PN-EN ISO/IEC 27000:2020-07...)** – an asset that, like other important business assets, has value to the institution and should therefore be adequately protected.

**INFORMATION (Łuczak, p. 194)** (business approach) – processed data (arranged, filtered, grouped, etc.) in such a way that on their basis you can draw conclusions, make business decisions.

The standard (PN-ISO/IEC 27001: 2017...) identify the following types of information that can be covered by the information security management system:

- internal – information that should not reach the competition, because we do not want it;
- consumer/customer information – information that should not be disclosed because they do not want it;
- information provided to other business partners.

It should be remembered that information can: create, store, destroy, process, use, lose, damage.

In order for the information security management system and information security risk management to be effective, it is recommended to apply the principles included in the PN-ISO/IEC 27001: 2017 standard – Information security management systems – Requirements. PN-ISO/IEC 27001: 2017 contains a specification of requirements for the establishment, implementation and documentation of information security management systems and a specification of security requirements to be introduced according to the needs of individual organizations. It is important that the standard PN-ISO/IEC 27001: 2017 consists of two parts:

- Part I – discusses approaches, principles and practices, condemns to the most vulnerable areas and discusses the best of safety practices used.
- Part II – contains 114 safeguards to be considered during the implementation of isms.

### **3. Information Security Management System**

The already mentioned PN- ISO/IEC 27001: 2017 standard contains many guidelines and information on where and how to apply the requirements to secure information. The standard applies to all kinds of organizations, regardless of the size of the company or the scope of activity.

Purpose of the Information Security Management System (ISMS) is to ensure the selection of adequate and proportionate safeguards for the protection of information assets and to ensure trust in stakeholder organisations. It is not possible to exclude any requirements contained in the clauses of the standard if the organization declares compliance with this international standard. Any exclusion of the safeguards deemed necessary should be justified and proof should be provided that the associated risks have been accepted by authorised persons. If an organization makes inclusions, compliance with the standard is declared when the exclusions do not affect the organization's ability and responsibility to ensure information

security. Hence, there are sometimes difficulties in the implementation of the Information Security Management System. These are difficulties in interpreting the requirements of the standard, difficulties in creating a risk estimation model, burdening the system with a large number of procedures and instructions, formalizing the system, financial outlays incurred on infrastructure/security and the involvement of qualified personnel and/or external consultants.

The Information Security Management System according to the PN- ISO/IEC 27001: 2017 standard should be established, implemented, applied, monitored, and should be reviewed. An organization that has a system should maintain and improve it. In addition, such a system should be documented, included in the context of the overall business activities of the organization and refer to the risks it faces.

The PN-ISO/IEC 27001: 2017 standard proposed by the standard is based on the PDCA model. The PDCA model used in the processes of the information security management system operates on the basis of 4 steps:

Step 1 – Plan – establishing an information security management system; establishing security policies, tasks, objectives, processes and procedures appropriate for risk management and improving information security in order to meet the provisions of the organization's policy and objectives.

Step 2 – Perform - implementation and operation of the information security management system - implementation and application of security security policies, processes, procedures.

Step 3 – Check – monitoring and review of the information security management system – evaluation and possible measurement of the execution of processes in relation to security policies, objectives and practical experiences and providing data management for review.

Step 4 – Act – maintenance and improvement of the information security management system – taking corrective and preventive actions based on the results of reviews carried out by the management in order to continuously improve the ISMS.

Sources of requirements for information security are the results of risk estimation and legal, statutory, regulatory and contractual requirements in relation to organizations, contractors, suppliers. The basis of the requirements of the system is also developed by the organization, a set of rules, goals and requirements for information processing. Speaking about the required standards, in order to understand its content, it is necessary to define the following concepts:

- Threat – a potential cause of an undesirable incident that may result in damage to the system or institution.
- Vulnerability – the weakness of an asset or group of assets that can be exploited by a threat.
- Effect – the result of an undesirable incident.
- Probability – the degree of certainty that an incident will happen.
- Information security event – an identified occurrence of a state in a system, service or network that indicates the possibility of a breach of information security policy or failure

to act security, or a previously unknown situation that may be important for information security.

- Information security incident – an identified occurrence of a state in a system, service or network that indicates the possibility of a breach of the information security policy or failure to act security, or a previously unknown situation that may be important for information security.
- Risk – the probability that a particular threat will exploit the vulnerability of an asset or group of assets to cause losses or destruction of assets.
- Residual risk – the risk remaining after the process of dealing with the risk.
- Risk assessment – the process of comparing the estimated risk with the assumed risk criteria in order to determine the risk weight.
- Risk management – coordinated actions to direct and control the organization taking into account the risk.
- Collateral – a practice, procedure or mechanism to reduce risk.

When small and medium-sized enterprises are already familiar with the specifics and terminology of the information security standard, they should determine the stages of creating a management structure. That structure should define the scope of the system and establish a framework for the policy of the management system. The next step is to create a systematic approach to risk estimation, determine the risk, estimate the risk and assess the options for dealing with risk. As a result of these activities, the organization selects objectives and safeguards, draws up a declaration of use and a risk management plan. The final step is to implement the safeguards, determine how to measure effectiveness and improve the security, and reassess the risk. These activities exhaust the requirements of PN- ISO/IEC 27001: 2017.

## **4. Detailed requirements of the information security management system according to PN- ISO/ IEC 27001: 2017**

### **4.1. Information Security Management System Policy**

According to the PN-ISO/IEC 27001:2017 standard, an organization should be an information security management system policy that takes into account the nature of the business, the organization, its location and assets. A well-designed policy:

- provides the basis for setting objectives and sets out the basic direction and principles of action in relation to information security,
- takes into account business, legal and regulatory requirements and security obligations arising from contracts,

- is consistent with the strategic risk management context in which the ISMS will be established and maintained,
- establishes the criteria on the basis of which the risk will be assessed.

The information security management system policy should be accepted by management, communicated to employees and applied.

#### **4.2. Risk assessment**

The information security standard obliges entrepreneurs implementing the system to determine the risk estimation methodology that is appropriate for the information security management system, identify legal and business requirements in the field of information security. In addition, the organization should develop criteria for accepting risk and define acceptable levels of risk. In carrying out these tasks, entrepreneurs should adhere to the following principles of risk management: creates and protects value, is an integral part of all processes in the organization, is part of decision-making, clearly refers to uncertainty, is systematic, structured and up-to-date, uses the best available information, is tailored, takes into account human and cultural factors, is transparent and holistic, is dynamic, interactive and responsive to change, facilitates continuous improvement of the organization

#### **4.3. Identification of risks and choice of safeguards**

An organization maintaining an information security management system should identify the system assets and the owners of those assets, identify the risks to those assets, identify the vulnerabilities that can be exploited by the threats, identify the effects that the loss of confidentiality, integrity and availability may have on the assets. That identification should also address the risks to those assets, the vulnerabilities that may be exploited by the risks and the effects that the loss of confidentiality, integrity and availability may have on the assets.

Each company should identify and evaluate options for dealing with risk. This applies to the use of appropriate safeguards, conscious and deliberate acceptance of risks, provided that they meet the requirements of the organization's policies and risk acceptance criteria. It also applies to risk avoidance and transfer of related business risks to other parties, e.g. insurers, suppliers.

The choice of objectives and safeguards should be adequate to the size of the organisation and the technical capabilities. The safeguards chosen should meet the requirements arising from the risk assessment and the decisions taken as to how to deal with it. The selection should take into account risk acceptance criteria, legal, regulatory and contractual requirements. Acceptance of residual risks and authorization is part of risk management. For this purpose, the company should obtain management approval for the proposed residual risks and obtain authorization to implement and apply an information security management system. In some

situations, management may accept residual risks beyond the acceptable level. This decision should be formally documented.

#### **4.4. Risk identification and estimation**

In order to ensure an effective information security management system, it is necessary to estimate the risk associated with the possibility of losing security. To do this properly, describe the chosen risk estimation method and determine why it is appropriate in relation to security requirements, business environment and the size of the business. It is recommended that each company documents the tools and techniques that have been selected to identify and estimate the risk. The values of the assets covered by the system should be documented, including information about the valuation scale used (if it is not financial). Identified threats and vulnerabilities and a threat assessment using vulnerabilities that may lead to incidents should also be documented.

An organization with a security system should create a detailed schedule or plan for risk treatment. This plan for each identified risk should include: the methodology of treatment, the implemented safeguards, the proposed additional safeguards, the time frame within which the safeguards are to be implemented. An acceptable level of risk should be specified. For each risk with an unacceptable level, it is recommended to choose one of the actions: risk transfer, risk avoidance, reduction of risk to an acceptable level, decision to accept risk. The risk estimation process includes asset identification, asset valuation, requirements identification, requirements weight estimation, risk calculation, identification and assessment of risk management and the use of safeguards to reduce the level of risk to an acceptable level. Risk estimation aims to reduce the risk to an acceptable level. The safeguards selected by the organization are carried out on the basis of the results of risk estimation. This action is supported by periodic analysis of the collateral applied, taking into account the costs incurred.

#### **4.5. Asset management**

Risk estimation and determination of collateral cannot be carried out without identifying assets. Therefore, all assets of the organization should be classified. In small and medium-sized enterprises, this action is carried out thanks to the involvement of management staff at all levels. The most frequently identified assets among entrepreneurs are information assets (databases, files, procedures, plans, training materials), paper documents (contracts, official reports), software (applications, programs), hardware (computer, data carriers), people (staff, customers, Co-operators), services (telecommunications, data processing), image of the organization. Once an organization has identified assets, it must assess their value to determine what assets to protect. Asset valuation is carried out from the point of view of the organization and assesses the impact of the loss of security along with replacement costs. The most effective assessment is therefore when the estimate is in quantitative form (PLN). When estimating, an important element is the weight of the requirements and the most commonly used scale: significant,

important, very important. It usually determines the resources allocated to meet the requirement.

#### **4.6. Implementation and maintenance of the information security management system in small and medium-sized organizations**

In order for a small organization to implement the system well, it should develop a risk management plan that identifies the right actions, resources, responsibilities and priorities related to the management of information security risks. That plan should include rules for dealing with risks in order to achieve the identified objectives of the hedges, including consideration of the financing and allocation of roles and responsibilities and collateral. The documents required by the information security management system should be protected and supervised. Records should also be created and maintained to provide evidence of compliance with the requirements of the standard and the effectiveness of the system. In the success of system maintenance, the main role is played by the management of the organization. Management should demonstrate a commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the system. The organization should identify and provide the human resources and infrastructure necessary to maintain the system. It is essential for the effectiveness of the system that all personnel with the responsibilities specified in the system have the competence to perform the required task.

The tool verifying the functioning of the system is the internal audit of the system. The organization should conduct internal audits of the information security management system at scheduled intervals to determine whether security objectives, safeguards, processes and procedures are being met. The closing element of the system verification is the review of the system management, where the management should review the system in terms of: audit results, feedback from stakeholders, status of preventive and corrective actions, results of performance measurements, actions taken after previous management reviews and changes affecting the information security management system.

### **Summary**

The PN- ISO/IEC 27001: 2017 standard indicates many safeguards necessary to implement and maintain an information security system. The system functioned constantly the organization should constantly improve the effectiveness of the system through the use of resources, policies and goals of information security, analysis of monitored events, corrective actions. By monitoring non-compliance and taking corrective action, the organization can take action to eliminate the causes of non-compliance with system requirements.



## References

1. Journal of Laws of 1997, No. 114, item 740, as amended.
2. Journal of Laws of 1999, No. 11, item 95, as amended.
3. Journal of Laws of 2000, No. 122, item 1319, as amended.
4. Journal of Laws of 2002, No. 101, item 929.
5. Journal of Laws of 2002, No. 153 item 1271 as amended.
6. Łuczak, M. *Tyburcki Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*.
7. PN-ISO/IEC 27001:2007 standard – Information security management systems – Requirements.
8. PN-ISO/IEC 27001:2017 – Information security management systems – Requirements.