International Journal for Quality Research 19(2) 371-386
ISSN 1800-6450

Agnieszka Górka–Chowaniec [1]

Adam Popek

Article info:
Received 20.05.2024.
Accepted 15.11.2024.

DOI – 10.24874/IJQR19.02-01

ATTEMPT TO USE THE DEMING CYCLE (PDCA) IN THE PROCESS OF IMPLEMENTING AN INFORMATION SECURITY MANAGEMENT SYSTEM

Abstract: *Information security, nowadays, when both states, institutions, companies and societies increasingly use information in digital form, is becoming a critical factor of the organization's activity. Therefore, the purpose of this paper is to discuss the issues of building an information security management system in a modern company.*

This systemic approach is a response to the expectations of modern organizations and a very important issue, due to the fact that with regard to the security of information systems, each organization should verify its activities in terms of sufficient information protection.

Keywords: *Deming Cycle, PDCA, management, information security, information security management systems, enterprise, ISO, ISO/IEC 27001*

1. Introduction

In addition to human, infrastructure and financial resources, information is becoming another extremely important resource (Pigłowski & Żak, 2021; Culot et al., 2021; Mirtsch et al., 2021; Legowo & Juhartoyo, 2022; Podrecca et al., 2022).

Access to information is currently a fundamental factor for the dynamic development of an organization, with the reservation that it should be efficient, but above all safe. All organizations, regardless of their business profile, produce, store, process and transmit sensitive information, whose unauthorized disclosure or destruction may cause serious harm to an individual or institution (Achmadi et al., 2018; Hamdi et al., 2019; Kitsios & Kamariotou, 2017; Dospinescu & Dospinescu, 2018). Increasing cybercrime, its simplification and accessibility for incompetent ICT users are actively attacking enterprise information assets

Therefore, the purpose of this work is to discuss the problem of building an information security management system in a modern company. This systemic approach is a way to meet the expectations of modern organizations and a very important issue, given the fact that, with regard to the security of information systems, every organization should verify its activities for adequate information protection.

2. System management of information security

It is information, not events, that is changing today's economic reality. Their value is now undeniable, because they determine the successes and failures of the organization, becoming one of the main resources (information resources) with the help of

[1] Agnieszka Górka–Chowaniec
a.chowaniec@awf.katowice.pl

which companies are in the wall to build a long-term competitive advantage (European Commission, 2022).

More and more often managers pay more and more attention to the value that information generates for the company (its possession, processing, protection, use, modification or management). Remote work, increased mobility of members of the organization, outsourcing, flat structures in the organizations, constantly changing relationships in the business – increasingly established very quickly with a short time horizon, often with entities that have a short history is today's reality that must face modern entrepreneurial environments (Bolek et al., 2023). The subject of information security is not a new subject, but the attempts made in the area of systematic standardisation of information safety practices are relatively short-lived (in the early 1990s). In economic practice, comprehensive care for information security is a new issue, however, the scale and scope of problems that we can observe and which arise as a result of the non-acceptance of risks arising, among other things, from the loss of information assets generates a significant danger to the efficiency and efficiency of the operation of enterprises and cannot be overlooked (Wu et al., 2021; Varghese, 2022). Information is a key part of any undertaking. The collection, processing, storage and confidentiality of information are among the most important activities in the entire life cycle of an enterprise (Mou et al., 2020). Maintaining security and taking action to protect information assets is essential in relation to every party involved, such as customers, employees, business partners, suppliers or other strategic allies. As other authors stress, security pathologies result from a lack of recognition of the importance of information security management (Huo et al., 2015; Juma'h & Alnsour, 2021).

There are currently five main reasons why organizations should focus on information security (Ernst & Young, 2014):

1. Changes in the enterprise environment that take place in relatively short intervals of time. The rapid movement of enterprises in the era of multi-crisis is due to the emergence of new mergers, acquisitions, market expansion and new technologies. These changes are complex, with many negative consequences for enterprise information security.
2. Ecosystem: We live in an ecosystem of entities, people and data connected digitally. The likelihood of exposure to cybercrime affects every area of human existence.
3. Infrastructure: Internet access is now unlimited even for traditionally closed operating technologies, so threats to information security affect critical infrastructures (e.g. transport systems, energy distribution or the world of science).
4. Cloud: Third-party data management and storage services pose unknown risks that previously did not exist or existed on a significantly smaller scale).
5. Mobility and customer orientation: the widely accepted use of mobile technology weakens corporate boundaries and delivers IT closer to the user and beyond the enterprise environment. The widespread use of the Internet, smartphones combined with the positive approach of enterprises to BYOD has led to almost unlimited access to sensitive corporate data.

With the development of information and communication technologies and the expansion of industry competition, it is necessary to attach increasing importance to the protection of confidential information, as information technology has become a tool or object of cybercrime.

According to PN-EN ISO/IEC 27001:2023-08, information security is the preservation of the confidentiality, integrity and availability of information, with confidence being defined as an attribute consisting of information not being made available or disclosed to unauthorized persons, entities or processes; integrity as a property consisting in ensuring accuracy and completeness; and accessibility as the property of being accessible and useful at the request of an authorized entity (PN-EN ISO/IEC 27001; Chu & So, 2020; Ali et al., 2021).

Security is associated with the uninterrupted operation of systems, however, bear in mind that there are many factors that can interfere with it, and the source of threat can be unauthorized access to resources, not only from outside, but also from within the organizational network (Shojaie et al., 2015; Di Bona et al., 2020).

According to the type of threat, you can distinguish between active attacks that seek to modify the flow of information or create false information, and passive attacks, which consist of intercepting and monitoring the transmitted information (Diefenbach et al., 2019; Barton et al., 2016).

Maintaining a high level of security of the strategic resources of the IT system requires, among other things:

- classification of resources, by determining their degree of sensitivity,
- constant monitoring and periodic review of the security status of all components of the system,
- selection and implementation of appropriate infrastructure (hardware-software) solutions (system: antivirus, firewall, breach detection),
- application of protection measures affecting increasing the reliability of the equipment and enabling the system to restore after a crash,
- training of users of the organizational network in the prevention and detection of breaches of IT security,
- raising the qualifications of system administrators through specialized training in the field of information security (Eling & Wirfs, 2019; Mirtsch et al., 2021; Oleksiewicz, 2017; Marhavilas et al., 2020).

ISO/IEC 27001 defines information security management as an information security management system (ISMS) that "protects the confidentiality, availability, and integrity of information by implementing a risk management process and providing confidence to stakeholders that risks are well-managed."

According to PN-EN ISO/IEC 27001, organizations of all types and sizes: collect, process, store and transmit information, understand that information and related processes, systems and networks and staff are important assets for achieving the goals of the organization, are exposed to risks that may affect the operation of assets, take into account these risks by implementing security measures related to information security (Gonçalves et al., 2020; Mazurek, 2014).

All information that the organization holds and processes is subject to: threats related to attacks and errors, threats arising from natural causes (e.g. flood, fire), vulnerabilities inherently related to their use (Pałęga, 2016; Tigre-O et al., 2019).

The protection of information assets is achieved by defining, obtaining, ining and improving information security in such a way that the company achieves its goals, acting in accordance with the law and preserving its image. It should therefore carry out coordinated actions related to the implementation of appropriate safeguards and the appropriate handling of unacceptable risks in information security (Janczak & Nowak, 2013; Jeong et al., 2019). Information security risks and the effectiveness of security changes depend on changing circumstances, which is why organizations should: monitor and evaluate

the efficacy of implemented security and procedures; identify emerging risks that require action; select, implement and improve appropriate security as needed.

In order to link and coordinate these activities, the organization defines its own information security policy and objectives, using a management system (Pigłowski & Żak, 2021; PN-EN ISO/IEC 27001).

Organizations may decide to implement an information security management system for the following reasons: requirements for qualifying and evaluating suppliers, ability to operate in service and supply chains (stability and predictability), expectation of effective risk transfer, increasing competition, need to adjust to industry standards and requirements, e.g. in the financial sector (Finance Supervision Commission – KNF) or key services (National Cyber Security System – KSC), need to meet legal requirements (Zawistowski, 2020)

In order to ensure reliability in the operation of the implemented security system and to create the possibility of fulfilling its assumed role, it is necessary to update it systematically, due to the fact that those systems (spyware, antivirus), which are not updating, become vulnerable to all kinds of hacking attacks.

According to PN-EN ISO/IEC 27001, data protection against unauthorized, accidental, deliberate disclosure, modification or destruction is based on the fulfilment of security aspects such as confidentiality, integrity and accessibility, where confidentialism is defined as the attribute that information is not to be made available or disclosed to unauthorised persons, entities or processes, integrity as a property that ensures accuracy and completeness, and availability as the property of being accessible and useful at the request of an authorized entity (PN-EN ISO/IEC 27001).

It should be noted that the fact that the implementation of the information security management system, confirmed by the certificate, is a signal to internal and external clients that the organization:

- appreciates the value of information,
- meets legal requirements,
- has a qualified team to watch over the security of its operations; that is, it is proof of the credibility of the organization (Tigre-O et al., 2019).

Standard PN-EN ISO/IEC 27001 Information security, cybersecurity and privacy – Information security management systems; provides a practical guide to information security management. It emphasizes risk management and contains statements that make it possible to conclude that it is not necessary to apply all the recommended safety control guidelines, but only those that are appropriate to the situation and the level of acceptable risk. The scope of application of the recommendations contained in the standard, the organization chooses for itself (PN-EN ISO/IEC 27001; Leszczyna, 2018).

The scope can include all the information processed within an organization.

It is also worth noting that, despite the fact that the mentioned standard contains information on what actions should be taken to increase information security, it does not specify at the same time how to this, and guidelines for this are contained in other standardization documents (PN-EN ISO/IEC 27002:2017-06. Information technology. Security techniques. Practical principles for information security; PN-EN ISO/IEC 27005:2017-01; PN-EN ISO/IEC 27001 Information technology. Security techniques. Risk Management in Information Security; PN-ISO 31000:2018-08. Risk management. Guidelines) (PN-EN ISO/IEC 27001).

ISO, the International Organization for Standardization, grants certificates in accordance with ISO/IEC 27001 to any organization that meets specific requirements. However, the entire certification process can be perceived by some entrepreneurs as an organizational,

time and financial burden. However, the research results available in the subject literature (ISO, 2017) on the distribution of certificates according to ISO/IEC 27001 in 2015 show a 20% increase compared to 2014 (27,536 organizations that obtained certificates in 2015). The countries with the most certified organizations are Japan (8 240), the United Kingdom (2 790) and India (2,490). Of the V4 countries, Poland has the most certificates. (448). Further studies also reveal the growing interest of companies in the topic of their distribution From the survey (ISO, 2019) in 2019 on the distribution of certificates according to ISO/IEC 27001 it can be concluded that 36 362 certificates have been issued.

As already mentioned, this standard allows an organization to informedly choose the safeguards appropriate to the profile of its operations. Based on risk analysis, it is possible to eliminate areas where the implementation and maintenance of safeguards significantly exceeds the estimated losses or gains achieved (Setyadji et al., 2023).

Furthermore, as research results show (Wu et al., 2021) the financial effectiveness of enterprises becomes greater as they gain experience in the implementation of ISO 27001. Such evidence will undoubtedly enable modern managers to gain confidence in the use of information security certification.

3. Risk Management Elements

Risk is defined as the impact of uncertainty on goals. The consequence of risk is a positive or negative deviation from expectations. The risk involves uncertainty, i.e. a state, even partial, of lack of information related to understanding or knowledge of an event, its consequences or probability. A risk may be presented in relation to potential events and consequences, or a combination thereof, and expressed as the combination of the consequences of an event (including a change in circumstances) and the associated probability of the event.

Risk management is the process of assessing risk with the aim of reducing it to an acceptable level. It should consist of the following phases: planning, acquisition, development, testing, appropriate deployment of IT systems. Risk management is the entire process of identifying, controlling and eliminating or minimizing the likelihood of uncertain events that may affect the resources of an IT system. Risk analysis, on the other hand, is the process of identifying a risk, determining its magnitude and identifying areas requiring safeguards. Whitman and Mattord (2006) point out the interrelationship between risk assessment and risk mitigation – which is the essence of risk management, while pointing to the following steps of risk Management:

1. Identification of risks.
2. Impact assessment on operations.
3. Assessment of vulnerabilities and threats.
4. Evaluation of current risk mitigation measures.
5. Development and review of a risk reduction plan.
6. Implementation of the risk mitigation plan.
7. Compliance measurement.
8. Measurement of the impact on activities.
9. Review and monitoring.

Risk is therefore the probability that a particular vulnerability may be used by a particular threat to cause loss or destruction of an asset or group of assets, thereby negatively affecting the organization's operations directly or indirectly. One or more threats can exploit one or more vulnerabilities (Table 1).

Table 1. Risk Categories

Risk	***Description***
Major business risks	Mergers, acquisitions, the introduction of a new website, legal regulations, risks related to turbulence and volatility of the environment, the risk related to the lack of acceptance by the market of generated value for the customer.
Major IT risks	Introduction of new technologies supporting internal and external processes of the enterprise
Project risks	Threat to business continuity caused by the implementation of the project, risk in terms of achieving assumed project benefits, risk of failure to the expected success
Individual risks and incidents	Inherent in the work and activities related to the use of IT, ***loss and acquisition of information resources***

Source: own work based on (Whitman & Mattord, 2006, p. 52–53).

In the case of an information security management system, the risk may be expressed as the impact of uncertainty on information security objectives. In the case of information security, a risk involves the possibility of a situation in which the risks arise from the vulnerability of one or more information assets and thus cause harm to the organization (paragraph 2.68) (Pałęga, 2016; PN-EN ISO/IEC 27001).

Risk management is defined as coordinated actions for guiding and controlling an organization in relation to risk, and the risk management process as the systematic application of management policies, procedures and practices to information, consultation, context-building and risk identification, analysis, evaluation, risk management, monitoring and review activities (Pigłowski & Żak, 2021; Topa & Karyda, 2019; Mesquida & Mas, 2015).

All necessary information related to the implementation of the information security management system of the organization can be obtained by classifying the information processed in the organization and estimating the risk of loss of valuable information. A properly developed classification of information can be the basis for estimating the risk of loss of information. The main objective of such analysis is to identify such risks to information processed in the organization that are most likely and may be the cause of the greatest losses. For a specified level of risk, specify the level to which the organization intends to minimize the risk.

Risk assessment requires systematic actions that allow, to:

- identify assets (inventory of information, equipment, software, services related to the scope of the implementation of an organization's security management system),
- identification of the risks to these assets,
- identifying the vulnerabilities that may be exploited by these risks,
- determining the effects that the exploitation of the vulnerability by threats may have (Mirtsch et al., 2021).

4. Information Security Management System Implementation Process

The subject literature presents many models applicable in the management of information security. The most famous are: PDCA, Activate-Adapt -Anticipate, Confidentiality – Integrity – Availability, Domain Model ISSRM, General Model of Influence Factors,

BMIS, Process map SRIB, Model according to Cybernetic Security Framework.

For further analysis, the authors took into account We evaluate the overall PDCA model as one of the most complex models that companies can use to manage information security and operations without major constraints.

The Deming Cycle, also called the PDCA cycle, is a cycle that consists of four stages, representing the following successive actions:

1. **PLAN** – Establish and plan actions to a given goal.
2. **DO** – Realize the established actions for a trial.
3. **CHECK** – Check whether the implemented plan was effective, brings results and how the process can be improved.
4. **ACT** – A perfect process that has proved or corrected errors in an unsuccessful process (Hamdi et al., 2019; Łuczak & Tyburski, 2010).

The Deming cycle is a universal approach that gives an organization the opportunity to self-improvement. The most important thing in its implementation is consistency and systematic implementation of its individual stages. Otherwise, this cycle will be interrupted and the organization will not the desired results.

The creation, implementation and operation of an information security management system according to PN-EN ISO/IEC 27001 is also carried out in the Deming cycle, and the entire family of standards in the field of **information safety management system** contains mutually complementary documents, which describe the requirements for establishing, implementing, reviewing, as well asining and improving the management system (Figure 1) (Hamdi et al., 2019; Łuczak & Tyburski, 2010; Diéguez et al., 2020).

PN-EN ISO/IEC 27001 provides the following description of these stages (table 2).

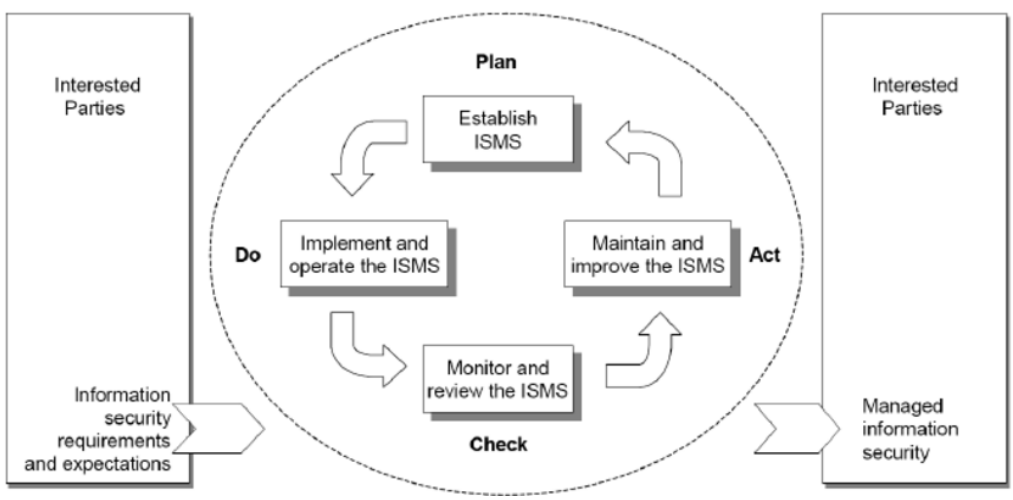

Figure 1. Information security management system and Deming cycle
Source: own work based on (https://ictinstitute.nl/pdca-plan-do-check-act/).

Table 2. Description of the phases of the PDCA cycle in relation to the organization's security management system

L.p.	Stage	Stage Description
1.	Plan	Establish security policies, scope, processes and procedures that match risk management and enhance information security in such a way that results are consistent with the general principles of the organization's objectives.
2.	Do	Implement and operate security policies, security, processes and procedures and use these tools to protect information.
3.	Check	Assessing and possibly measuring the performance of the processes in relation to the security policy, objectives and practical experience and communicating to management the results of the review regarding the functioning of the system and the possibility of its possible improvement.
4.	Act	Take corrective and preventive action based on the results of the management review to the effect of improving the information security management system.

Source: own work based on (PN-EN ISO/IEC 27001).

The most important features of the information security management system, namely:

- Making decisions based on facts. The standard requires the decision to apply safeguards on the basis of a risk analysis. The primary objective should be to maintain the continuity of the organization. It is worth stressing that the approach to the implementation of the recommendations of the standard, consisting of duplicating the template actions that fulfil their task in the general case, has little chance of success, because most often leads to so-called overinvestment or underinvestment in ensuring information security, and often also omission of the range of threats, characteristic of a given organization.
- The ability to "self-correct" the system. The information security management system should be constructed in such a way that it is capable of detecting shortcomings and improving. This means that the system must have "built-in" procedures to respond to noticed problems and non-compliance and procedures for periodic reviews, as well as, in case of non-conformity detected, procedures aimed at both the current problem correction and its modification in order to reduce the risk of the problem occurring in the future (Goldberg et al., 2019; Janczak & Nowak, 2013; Łuczak & Tyburski, 2010; Nasir et al., 2019).

With regard to **phase 1, Planning** (establishing an ITSB), the implementation of an information security management system should begin with defining the scope of the system. The policy of the information security management system should then be defined, and PN-EN ISO/IEC 27001 provides that it is a document that sets out the general direction and principles of action with regard to information security. When designing it, it should take into account the business and legal requirements of the organization, define the criteria according to which the risk will be assessed and determine the organizational structure. This document must be adopted and accepted by the management of the organization. Once the policy of the information security management system has been defined, a risk analysis should be defined and carried out, and it is important that it be a repeatable process. The requirements of the standard do

not specify a specific method of risk analysis, they only require the definition and description of this process and the establishment of risk acceptance criteria. The next action taken by the organization at this stage is to conduct a risk analysis, according to the adopted methodology. In a well-organized company, where business processes are described and there is an up-to-date inventory of resources necessary for the operation of these processes, this is a process that is less burdensome. As a rule, organizations that have other management systems implemented (e.g. quality management system, according to ISO 9001), are well prepared for the risk analysis process. Once the risk has been defined, it is necessary to specify what action should be taken for each risk identified. It is possible to:

- Reduce the risk by applying safeguards. In addition to the safeguards described in the standard, others can be implemented if deemed necessary. This is important, because the list of security proposed in the standard may not keep up with technological developments.
- Risk transfer (np. na dostawce lub ubezpieczyciela).
- Avoiding risk.
- Risk acceptance. The modern approach to security clearly assumes that there are no fully secure systems (PN-EN ISO/IEC 27001; PN-EN ISO/IEC 27005:2017-01, 2014; Diesch et al., 2020).

Always, despite the use of the most sophisticated safeguards, there is a minimum of risk that the organization accepts, and it is important that this is an informed decision.

In the context of the management of the method of selection of security, the basic objective of the implementation of the information security management system should be to ensure the continuity of the organization's operation, that is, in the process of choosing the way to respond to a given threat, it should be taken into account its effects on the maintenance of this continuity (Pelnekar, 2011).

At the end of the process of establishing an information security management system, management approval must be obtained. This concerns, above all, the acceptance of residual risk and the issuance of internal regulations allowing the system to be implemented.

In stage 2 – Implement - (Implementation and operation of the ITSB), procedures to ensure the smooth functioning of the entire information security management system, i.e. procedures related to risk management, operations and resources management procedures and procedures capable of detecting and responding to incidents related to security breaches as quickly as possible and safeguards chosen at the stage of the establishment of the Information Security Management System, should first be implemented. In this case, particular attention should be paid to so-called awareness-raising training, which covers all staff and training on the procedures implemented (PN-EN ISO/IEC 27000; PN-EN ISO/IEC 27005; PN-EN ISO/IEC 27001).

Step 3 – Check – (Monitoring and review of SBI), in practice leads to the realization of the idea of self-improvement. To this, mechanisms to respond to system errors and security-related incidents and procedures for periodic reviews of the information security management system must be somehow embedded in the system. Given the fact that the process of responding to errors and incidents is initiated in a necessity arising from the situation, it is therefore difficult to speak here of any specific stage that has its beginning and end. Therefore, within defined periods of time, it is necessary to undertake:

- reviews of the effectiveness of the information security management system (according to the adopted

objectives, you can take into account the results of external and internal audits, information generated during the management of incidents, suggestions from employees regarding the modification of the system),
- audits of acceptable risk (because each organization and its environment change over time, assumptions about acceptable risks need to be periodically verified and, if necessary, modified),
- internal audit of the management system of information security (checking the functioning of the whole system according to the requirements of PN-EN ISO/IEC 27001).
- reviews of information security management system carried out by management (PN-EN ISO/IEC 27001; PN-EN ISO/IEC 27000; PN-EN ISO/IEC 27005).

Step 4 – Apply – (Maintaining and improving an information security management system). At this stage, the procedures for responding to errors, incidents and non-compliance identified during the review must result in documented corrective or preventive actions (PN-EN ISO/IEC 27000:2017-06, 2018; PN-EN ISO/IEC 27005:2017-01, 2014).

In summary, the processes conducted under stages 3 and 4, i.e. Verify and Apply, are in practice the result of the application of the procedures of stage 1 – Plan and implemented in stage 2 – Execute. Therefore, the critical role of the documentation, which is being developed in phase 1 – Plan, is clearly outlined, as it contains both measures relating to the implementation of safeguards and control procedures and procedures aimed at taking corrective action. At the planning stage, attention should also be paid to the business aspects of the organization's operations, as the information security management system cannot be a ballast in the context of its daily activities. Therefore, when considering building an information security management system, it is necessary to move away from template solutions and always use an individual approach, adapted to the specifics of the organization.

Information security does not mean that the organization has implemented the best possible safeguards, but appropriate to ensure that the activities and services of the organization meet the requirements:
- customers and other stakeholders,
- legal and regulatory,
- standards, own,
- contained in offers and standards,
- their own, designed in response to risk.

In making the final conclusions, the authors asked themselves the question of the benefits that the implementation of the Information Security Management System can bring to enterprises?. Modern managers should be aware that many companies, both Polish and foreign, currently expect suppliers to meet certain criteria in the area of information security. In addition to questions related to guaranteeing customer satisfaction, questions about the reliability and security of management procedures related to the protection of the information entrusted to them also arise. For this reason, many organizations implement or declare the need to implement an information security management system, providing their "strategic allies" with information protection (e.g. confidentiality of products ordered by the customer or projects being developed and information concerning the architecture of a given product).

Among the most common benefits mentioned from the implementation of an information security management system, are those revolving around ***business benefits*** (including the prevention and minimization of the frequency of leaks of confidential information to the press, competition, the market; destruction of information and

media due to fire, flooding, sabotage; financial losses, prestige, loss of credibility due to negligence about the reliability of the information processed and held or more certain action in the situation of threats caused by internal and external factors – business continuity); ***internal benefits*** (e.g. avoidance of penalties for infringement of information security, ensuring compliance with legal requirements – a systemic approach to meeting legal requirements rather than immediate actions, protection of information in the organization, increased awareness of employees in the area of information protection, fulfilment of tendering requirements in the field of information safety or credibility of the company in the eyes of the customer, for whom in today's times quality is very often identified with security); **marketing benefits** (i.e. improvement of the image and prestige of the organization and its products both in the sight of its current and potential customers, brand protection, building the professional image of a trustworthy organization or obtaining the effect of being perceived as an organization offering services at the highest level in terms of security).

5. Summary

At the moment, information is the most valuable element in the organization's activities, due to the fact that in the event of its loss, the recovery process is very expensive and problematic, much more difficult to recreate than its other resources. Disclosure of relevant information can also lead to a loss of competitive position by the organization. Therefore, information should be subject to special protection within the organization. This is served by a tool, which is systemic information security management.

An information security management system is part of a comprehensive management system, based on a business-risk approach, relating to establishing, implementing, operating, monitoring, ining and improving information security within an organization. The process approach to information security, according to the Deming cycle (PDCA), enables the construction of an effective security management system.

Implementation of this system brings with it measurable benefits (Mishra, 2015), which can be included:

1. The ability to apply for orders / contracts.
2. Improvement of competitiveness and credibility, thereby increasing the likelihood of acquiring a customer.
3. Additional points in evaluations.
4. Reduction of consequences of non-compliance with legal requirements.
5. Avoidance of contractual penalties.
6. Increased awareness of employees.
7. Improved internal communication.
8. Reduced stress of employees.

Information security does not mean that the organization has implemented the best possible safeguards, but appropriate to ensure that the activities and services of the organization meet the requirements:

- customers and other stakeholders,
- legal and regulatory,
- standards, own, contained in offers and standards,
- their own,
- designed in response to risk.

This paper in a sense fills the gap identified in the literature of the subject and represents an attempt to present the use of the Deming cycle (PDCA) in the process of implementing an information security management system in modern enterprise environments.

The paper presents the requirements for establishing, implementing, ining and continuously improving the information security management system in relation to the modern organization The authors also draw attention to requirements for the

assessment and management of information security risks, tailored to the needs of the organization. These requirements are general and apply to all organizations, regardless of type, size and nature. Faced with increasing cybercrime and constantly emerging new threats, managing information security in any organization is a key strategic element and at the same time may seem difficult or even impossible.

Searching for different solutions in this area helps organizations to consciously protect the information collected, build secure processes for its processing, taking into account changing external and internal risks. This paper promotes a holistic approach to information security by identifying strategic areas in building security such as: people, processes and technologies.

References:

Achmadi, D., Suryanto, Y., & Ramli, K. (2018). On developing information security management system (ISMS) framework for ISO 27001-based data center. *2018 International Workshop on Big Data and Information Security (IWBIS)*, 149–157. IEEE.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences, 11*(8), 3383. https://doi.org/10.3390/app11083383

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security, 59*, 9–25.

Bolek, V., Romanova, A., & Korcek, F. (2023). The information security management systems in E-business. *Journal of Global Information Management, 31*(1), 1–29. https://doi.org/10.4018/jgim.316833

CERTIOS. (n.d.). *Cykl PDCA*. https://www.certios.pl/113-bezpieczenstwo-informacji/96-cykl-pdca (accessed December 6, 2021)

Chu, A. M., & So, M. K. (2020). Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective. *Sustainability, 12*(8), 3163. https://doi.org/10.3390/su12083163

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal, 33*(7), 76–105.

Di Bona, G., Forcina, A., Falcone, D., & Silvestri, L. (2020). Critical risks method (CRM): A new safety allocation approach for a critical infrastructure. *Sustainability, 12*(12), 4949. https://doi.org/10.3390/su12124949

Diefenbach, T., Lucke, C., & Lechner, U. (2019). Towards an integration of information security management, risk management and enterprise architecture management – A literature review. In *2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)* (pp. 326–333). IEEE.

Diéguez, M., Bustos, J., & Cares, C. (2020). Mapping the variations for implementing information security controls to their operational research solutions. *Information Systems and e-Business Management, 18*(2), 157–186. https://doi.org/10.1007/s10257-020-00470-8

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security, 92*, 101747. https://doi.org/10.1016/j.cose.2020.101747

Dospinescu, O., & Dospinescu, **N.** (2018). The use of information technology toward the ethics of food safety. *Ecoforum Journal, 7*(1), 1–11.

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research, 272*(3), 1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021

Ernst & Young. (2014). *Cyber Threat Intelligence – How to get ahead of cybercrime*. https://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.pdf

European Commission. (2022). *The European Commission's priorities*. https://ec.europa.eu/info/strategy/priorities-2019-2024_en

Gonçalves, E., Teixeira, P., & Silva, J. P. (2020, June). Development of GDPR-compliant software: Document management system for HR department. In *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1–6). IEEE.

Hamdi, Z., Norman, A. A., Molok, N. N. A., & Hassandoust, F. (2019, December). A comparative review of ISMS implementation based on ISO 27000 series in organizations of different business sectors. In *Journal of Physics: Conference Series* (Vol. 1339, No. 1, p. 012103). IOP Publishing.

Huo, C., Meng, L., & Chen, K. (2015). Research on the university network information security risk. *[Brak danych wydawniczych]*.

ICT Institute. (n.d.). *PDCA – Plan Do Check Act*. https://ictinstitute.nl/pdca-plan-do-check-act/

Internet sources and institution pages

ISO. (2017). *The ISO survey of management system standard certifications (2006–2015)*. https://www.iso.org/iso/iso_27001_iso_survey2015.xls

ISO. (2019). *The ISO survey of management system standard certifications 2019*. https://www.iso.org/the-iso-survey.html

Janczak, J., & Nowak, A. (2013). *Bezpieczeństwo informacyjne. Wybrane problemy*. Warszawa: AON.

Jeong, C. Y., Lee, S. Y. T., & Lim, J. H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management, 56*(5), 681–695.

Juma'h, A. H., & Alnsour, Y. (2021). How do investors perceive the materiality of data security incidents. *Journal of Global Information Management, 29*(6), 1–32. https://doi.org/10.4018/JGIM.20211101.oa4

Kitsios, F., & Kamariotou, M. (2017). Decision support systems and strategic information systems planning for strategy implementation. In A. Kavoura, D. Sakas, & P. Tomaras (Eds.), *Strategic Innovative Marketing; Springer Proceedings in Business and Economics* (pp. 327–332). Cham, Switzerland: Springer.

Legowo, N., & Juhartoyo, Y. (2022). Risk management; risk assessment of information technology security system at bank using ISO 27001. *Journal of System and Management Sciences, 12*(3), 181–199. https://doi.org/10.33168/JSMS.2022.0310

Leszczyna, R. (2018). A review of standards with cybersecurity requirements for smart grid. *Computers & Security, 77*, 262–276. https://doi.org/10.1016/j.cose.2018.03.011

Łuczak, J., & Tyburski, M. (2010). *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*. Poznań: Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu.

Marhavilas, P. K., Filippidis, M., Koulinas, G. K., & Koulouriotis, D. E. (2020). A HAZOP with MCDM based risk-assessment approach: Focusing on the deviations with economic/health/environmental impacts in a process industry. *Sustainability, 12*(3), 993. https://doi.org/10.3390/su12030993

Mazurek, P. (2014). Realizacja szacowania ryzyka w wybranym przedsiębiorstwie. In J. Brdulak & R. Sobczak (Eds.), *Wybrane problemy zarządzania bezpieczeństwem informacji*. Warszawa: Wydawnictwo SGH.

Mesquida, A. L., & Mas, A. (2015). Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension. *Computers & Security, 48*, 19–34. https://doi.org/10.1016/j.cose.2014.09.003

Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the adoption of the international information security management system standard ISO/IEC 27001: A web mining-based analysis. *IEEE Transactions on Engineering Management, 68*(1), 87–100.

Mishra, S. (2015). Organizational objectives for information security governance: A value focused assessment. *Information & Computer Security, 23*(2), 122–142. https://doi.org/10.1108/ICS-02-2014-0016

Mou, J., Cui, Y., & Kurcz, K. (2020). Trust, risk and alternative website quality in B-buyer acceptance of cross-border E-commerce. *Journal of Global Information Management, 28*(1), 167–188. https://doi.org/10.4018/JGIM.2020010109

Nasir, A., Arshah, R. A., Ab Hamid, M. R., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications, 44*, 12–22. https://doi.org/10.1016/j.jisa.2018.11.003

Oleksiewicz, I. (2017). Bezpieczeństwo informacyjne jako wyzwanie w XXI wieku. *Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie, 15*(4[41]), 5–14.

Pałęga, M. (2016). Ocena poziomu zagrożeń bezpieczeństwa informacji za pomocą macierzy ryzyka. In M. Ogórek & T. Bajor (Eds.), *Wybrane zagadnienia dotyczące usprawniania procesów w przedsiębiorstwie*. Częstochowa: Wydawnictwo WiPiTM Politechniki Częstochowskiej.

Pelnekar, C. (2011). Planning for and implementing ISO 27001. *ISACA Journal, 4*, 28–34.

Pigłowski, M., & Żak, N. (2021). *Management of information security*. Gdynia: Department of the Maritime University of Gdynia.

PN-EN ISO/IEC 27000:2017-06. (2018). *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. Warsaw: Polish Standards Committee.

PN-EN ISO/IEC 27001:2023-08. (2023). *Information security, cybersecurity and privacy – Information security management systems*. Warsaw: Polish Standards Committee.

PN-EN ISO/IEC 27005:2017-01. (2014). *Information technology – Security techniques – Information security risk management*. Warsaw: Polish Standards Committee.

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry, 142*, 103744. https://doi.org/10.1016/j.compind.2022.103744

Setyadji, A. E., Putrananda, A. R., Permadi, D. H., Nustara, R. I., Pratama, R. B., Masyhuda, T. A., & Hariyanti, E. (2023). Causes of ineffective implementation of IT governance in risk management: A systematic literature review. *JIKO (Jurnal Informatika dan Komputer), 6*(2), 88–96. https://doi.org/10.33387/jiko.v6i2.6182

Shojaie, B., Federrath, H., & Saberi, I. (2015, August). The effects of cultural dimensions on the development of an ISMS based on the ISO 27001. In *2015 10th International Conference on Availability, Reliability and Security* (pp. 159–167). IEEE. https://doi.org/10.1109/ARES.2015.27

Tigre-O, F., Tubón-Núñez, E. E., Carrillo, S., Buele, J., & Salazar-L, F. (2019, June). Quality management system based on the ISO 9001:2015: Study case of a coachwork company. In *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1–6). IEEE. https://doi.org/10.23919/CISTI.2019.8760890

Topa, I., & Karyda, M. (2019). From theory to practice: Guidelines for enhancing information security management. *Information and Computer Security, 27*(3), 326–342. https://doi.org/10.1108/ICS-09-2018-0108

Varghese, J. (2022). Ecommerce security: Importance, issues & protection measures. *Astra Security*. https://www.getastra.com/blog/knowledge-base/ecommerce-security/ (accessed March 2, 2024)

Whitman, M. E., & Mattord, H. J. (2006). *Readings and cases in the management of information security* (pp. 52–53). Boston: Thomson Course Technology.

Wu, W., Shi, K., Wu, C. H., & Liu, J. (2021). Research on the impact of information security certification and concealment on financial performance: Impact of ISO 27001 and concealment on performance. *Journal of Global Information Management, 30*(3), 1–16.

Zawistowski, T. (2020). Materiały szkoleniowe „Asystent Systemu Zarządzania Informacją" na Uniwersytecie Morskim w Gdyni, 10–14.02.2020. Warszawa: Polskie Centrum Badań i Certyfikacji.

Agnieszka Górka–Chowaniec
Faculty of Sport and Tourism Management of Academy of Physical Education in Katowice, Katowice,
Poland
a.chowaniec@awf.katowice.pl
ORCID 0000-0001-6087-6299

Adam Popek
Department of Recreology and Biological Recovery of Academy of Physical Education in Krakow, Krakow,
Poland
adam.popek@awf.krakow.pl
ORCID 0000-0001-9322-4692