European Research Studies Journal
Volume XXVII, Issue 3, 2024

pp. 128-141

Information Security Management as the Basis for the Functioning of an Organization

Submitted 18/05/24, 1st revision 16/06/24, 2nd revision 29/06/24, accepted 24/07/24

Julia Nowicka[1], Zbigniew Ciekanowski[2], Anna Milewska[3]

Abstract:

Purpose: *This article aims to identify and determine the role of information security (across its various dimensions) in the functioning of an organization. An important aspect is also defining the key challenges and threats associated with it. The first part presents the essence of information security within an organization. Next, the role of auditing as a leading tool in ensuring information security is defined. The subsequent section identifies and analyzes contemporary challenges and threats in the area of organizational information security.*
Design/Methodology/Approach: *The research conducted in the article utilized information from secondary sources. The study engaged the method of literature review. Additionally, the information and data used were sourced from available internet sources. The method of data analysis from national and international industry reports was also employed, with conclusions drawn through induction and deduction.*
The research problem concerned the level of information security in an organization, and to define it precisely, a research question was posed: how does it impact the organization's functioning? The effectiveness of current information security practices was evaluated, as well as the identification of areas needing further improvement and innovation.
Findings: *Based on the conducted research, it was concluded that the analysis of information security requires a holistic approach that considers both technological and regulatory aspects. Moreover, there is a need and expectation for the continuous improvement of practices to protect the data and resources of an organization against growing digital threats. This includes personal, financial, as well as specific and strategic data, depending on the nature of the particular organization or entity.*
Practical Implications: *The identified and indicated scopes and dimensions related to data protection (from creating security policies, identifying elements to ensure an appropriate level of security in teleinformatics systems to auditing and its conclusions) can and should be particularly utilized by entities that are starting to operate in the market. This will first allow them to realize the problem of data security and then choose the instruments that, due to the specifics of their operation, will be appropriate for them.*

[1]*War Studies University, Poland, ORCID: 0000-0002-0778-0519,*
e-mail: j.nowicka@akademia.mil.pl
[2]*Warsaw Management University, Poland, ORCID: 0000-0002-0549-894X;*
e-mail: zbigniew@ciekanowski.pl
[3]*Institute of Economics and Finance, Warsaw University of Life Sciences-SGGW, Poland, ORCID: 0000-0003-4776-6049, e-mail: anna_milewska1@sggw.edu.pl*

Moreover, the information provided in the article will also help prevent a routine approach by entities already functioning but changing their business profile, market segment, or seeking new solutions due to the development of technology and techniques.
***Originality/Value**: The authors present the needs and possibilities related to data protection in an enterprise. Their identification and implementation will allow for meeting formal and legal requirements and also rationalize the expenses associated with this service. In the event of theft or other loss of data, the organization incurs costs, both those anticipated by public entities and those that may arise from court rulings based on civil lawsuits.*

***Keywords:** Organization, data, management, finance, security, cybersecurity, audit.*

***JEL codes:** K24, L2.*

***Paper type:** Research article*

1. Introduction

Information security is a crucial aspect of an organization's operations in the digital age, ensuring the protection of data, resources (including financial), and the integrity of business operations. It is a fundamental element of every organization's strategy, encompassing the assurance of data confidentiality, availability, and integrity.

This security forms the foundation upon which modern organizations operate. In the digital era, where data is an extremely valuable asset, its protection gains paramount importance. Information security includes a variety of practices, procedures, and technologies aimed at safeguarding data from unauthorized access, modification, disclosure, or destruction. This is especially critical due to the diverse nature of the data involved.

First and foremost, information security focuses on the confidentiality, integrity, and availability of data. Confidentiality ensures that only authorized individuals have access to specific information. Integrity guarantees that data is accurate, complete, and unaltered by unauthorized persons. Availability ensures that information is accessible when needed by those who have the right to it.

The importance of information security cannot be overstated. Modern organizations handle vast amounts of data, including personal, financial, commercial, and other critical information essential to their operations. Any security breach can lead to serious consequences—legal, financial, and reputational. Data breaches involving personal information of customers or employees can result in penalties under regulations such as GDPR, as well as loss of customer trust.

Moreover, security breaches can lead to financial losses due to data theft, business interruptions, or costs associated with damage repair.

In the era of cyberattacks, such as ransomware, where criminals block access to systems and data demanding ransom, securing information becomes a strategic priority. Organizations must implement comprehensive information security strategies, which include technologies, procedures, and employee training. Information Security Management Systems (ISMS), security policies, regular audits and risk assessments, and continuous staff training in best security practices are essential elements of effective data protection.

Security cannot rely on internal safeguards alone, ignoring external threats. The boundaries between internal and external environments have become blurred in an open, highly heterogeneous, distributed setting.

This is especially true for data subject to complex usage patterns and aggregation, such as in multinational corporations or financial institutions. Security must therefore be ubiquitous and dynamically linked to the data and its metadata, allowing entities in different ecosystems to apply relevant policies (Lopez, 2013).

An organization must recognize that some security measures will incur costs, such as upgrading software licenses or implementing physical security measures. However, many security measures are organizational, involving different types of costs, primarily labor (Wiśniewska, 2009).

Summarizing this thread, information security is not only a legal requirement but also a key management element that ensures the stability and efficiency of organizational operations. Protecting data from both internal and external threats is essential to maintaining customer trust, avoiding financial losses, and ensuring business continuity in a dynamic and often unpredictable digital environment. While these efforts may initially require financial resources, they yield tangible benefits in the long run.

2. Information Security in the Organization

Information security is a critical aspect and plays a significant role in protecting an organization's business. Organizations must safeguard their information and resources to ensure their security and maintain their reputation. Effective information security management requires the support and commitment of top-level management in implementing policies and procedures (AlGhamdi *et al.*, 2020).

A practical way to identify existing vulnerabilities and threats is to initiate diagnostic processes that assess the current state of security within the organization, considering current regulations and risk analysis processes (Velinov *et al.*, 2023).

Organizations must recognize that some necessary security measures will incur costs, such as updating software licenses and implementing physical safeguards.

However, many security measures are organizational in nature, involving different costs, mainly in terms of labor.

To achieve adequate protection of IT resources, systems, and data, the entire organization must be involved. Initially, it is essential to understand the ISO/IEC 27001 standard in each relevant area to determine its scope of application.

This diagnosis will enable the organization to design, implement, and maintain an Information Security Management System (ISMS) in compliance with ISO/IEC 27001. This system will be capable of controlling vulnerabilities, threats, and security risks that the organization may face (Solarte Solarte *et al.*, 2015).

The ISO/IEC 27001 standard outlines regulations that must be implemented to establish, maintain, and improve an information security management system (ISMS) within an organization (ISO 27001, 2024). Organizations that choose to adopt the ISO 27001 standard must commit to a comprehensive management system that:

1. encompasses the entire organization or selected parts of it;
2. engages both the Management Board and various levels of the organizational structure;
3. requires organizational effort and financial resources proportionate to the requirements;
4. is viewed by the organization as a support to the company's development, not a hindrance (ISO 27001, 2024).

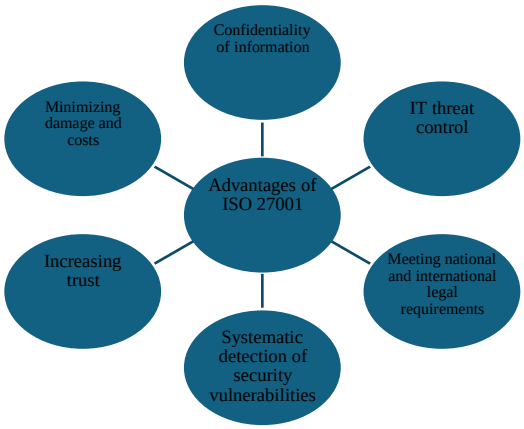
Figure 1 presents the advantages of ISO 27001 for information security in an organization. From the data in Diagram 1, it can be inferred that all these features are equally advantageous. This is because it functions as a system of interconnected vessels. Increased trust is a result of the care and due diligence associated with adhering to the organization's policies and procedures.

This includes formal-legal procedures following applicable law, as well as those specific to the entity's nature and culture. Monitoring the required areas allows for the detection of deficiencies (gaps) and helps mitigate potential negative effects, which could be financial, legal, or business-related.

The ISO/IEC 27001 standard is recognized as an international standard for information security management systems (ISMS). Its implementation and certification bring numerous benefits to organizations, both in terms of data protection and overall operational efficiency.

Table 1 below outlines the benefits of implementing the ISO 27001 standard, detailing the specific areas it addresses.

Figure 1. *Advantages of ISO 27001 for information security in the organization*



Source: *Own elaboration.*

Table 1. *Benefits of implementing ISO 27001 distinguishing certain areas*

Advantage	Benefits
Increased information security	**Risk management:** A systemic approach to the identification of, assessment, and risk management associated with information security **Threat protection:** The implementation of appropriate technical and organizational measures to protect against a variety of threats (e.g. cyberattacks, data breaches, human error).
Compliance with laws and regulations	**Compliance with Laws:** Helping comply with legal and regulatory requirements for data protection and privacy (e.g., GDPR, HIPAA). **Proof of compliance:** Provide evidence of compliance during external and internal audits.
Increased stakeholder trust	**Customer and partner trust:** ISO/IEC 27001 certification is proof that an organization takes information security seriously, which can increase the trust of customers and business partners. **Competitive advantage:** Organizations that are ISO/IEC 27001 certified can stand out in the market and win new contracts, especially in industries that require a high level of security.
Improve operational efficiency	**Standardization of processes:** Implementation of structured and standardized processes for information security management. Reduce operational risk: Reduce operational risk by better managing information and minimizing potential downtime and waste.
Continuous improvement	**PDCA methodology:** Use of the Deming cycle (Plan-Do-Check-Act) for continuous improvement of the information security management system. **Auditing and monitoring:** Regular internal audits and management reviews allow you to identify areas for improvement and implement corrective actions.
Increased employee awareness	**Training and education:** Increasing employee awareness and knowledge of the importance of information security and its role in maintaining it.

	Safety Culture: Promoting a safety culture within the organization where each employee understands their duties and responsibilities in terms of information protection.
Reduce costs associated with security breaches	**Incident prevention:** Reducing the number and impact of information security incidents through proactive risk management. **Resource savings:** Avoid costly responses to security breaches, including legal costs, reputational damage, and operational downtime.
Scalability and flexibility	Adapted to different organizations: ISO/IEC 27001 is suitable for organizations of all sizes and industries, allowing you the flexibility to adapt your information security management system to your specific needs and requirements.

Source: *Own elaboration.*

Implementing the ISO/IEC 27001 standard brings tangible benefits that help organizations secure their information, manage risk, and build trust among stakeholders. Through a systematic approach to information security management, organizations can achieve higher levels of data protection and operational efficiency.

One method of continuous improvement is the Deming Cycle. The Deming Cycle, also known as PDCA (Plan-Do-Check-Act), is a fundamental methodology for managing continuous process improvement. It is widely used in various standards, including ISO/IEC 27001, which pertains to Information Security Management Systems (ISMS). The specifics of the Deming Cycle (PDCA) as applied to the ISO/IEC 27001 standard are presented in Table 2.

Table 2. *Deming cycle (PHVA) applied to ISO/IEC 27001*

PHVA cycle process	**Action**
1. Planning	**Organizational Context Analysis**: Identify internal and external issues that may affect the ISMS. **Stakeholder identification:** Understanding stakeholder requirements for information security. **Risk assessment and risk management planning:** Developing a risk management plan, including identifying hazards and determining an acceptable level of risk.
2. Implementation	**ISMS Policy and Purpose:** Implementation of appropriate information security policies. **Asset Management:** Ensuring adequate resources to implement and maintain an ISMS. **Communication and training:** Ensuring that all employees are aware of their responsibilities and duties related to information security.
3. Monitoring	**Monitoring and Review:** Regularly monitor and review the ISMS to ensure that it is effective and compliant with ISO/IEC 27001. **Internal audit:** Conducting regular internal audits to identify potential non-conformities and areas for improvement.

4. Corrective actions	**Correction of non-conformities:** Implementation of corrective actions in response to nonconformities identified during audits and reviews. Continuous improvement: Striving for ongoing enhancement of the ISMS by analyzing results and implementing improvements.

Source: *G. Pallas Mega, Metodología de Implantación de un SGSI en un grupo empresarial jerárquico: Tesis de Maestría (Ingeniería en Computación): Universidad de la República, Montevideo – Uruguay, 2009, p. 10.*

The use of the Deming cycle in ISO/IEC 27001 helps organizations maintain and improve their information security management systems. With the PDCA approach, organizations can systematically identify and manage risks, monitor and improve their operations, and ensure compliance with the requirements of the standard, leading to better information security and protection against threats.

3. Audit as a Leading Tool in Ensuring Information Security

Audits are a crucial tool in managing information security, particularly regarding compliance with standards such as ISO/IEC 27001. Regularly conducting audits helps organizations identify weaknesses, ensure compliance with requirements, and continuously improve the information security management system. An organization should conduct internal ISMS audits at planned intervals to determine whether the security objectives, controls, processes, and procedures are:

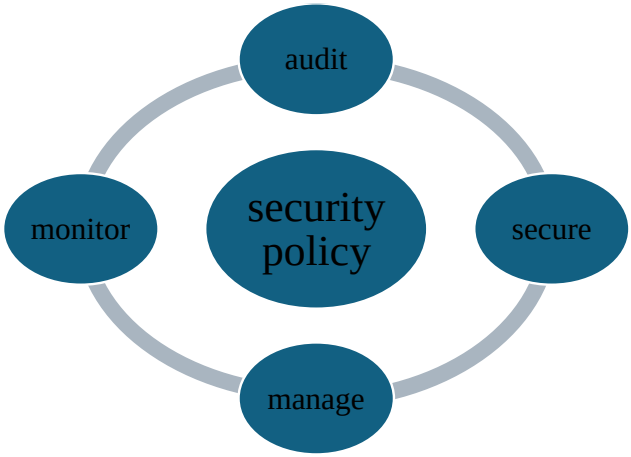
- in line with the recommendations of standards and relevant laws and regulations;
- consistent with identified information security requirements;
- effectively implemented and maintained, meeting expectations (Audit, 4itsecurity.pl, 2024).

Information security audits are a fundamental element in managing risk and protecting an organization's information assets. Despite technological advancements and emerging threats, the auditing process remains fundamentally unchanged and includes planning, preparation, conducting the audit, reporting results, and implementing corrective actions.

These audits can be carried out by external specialists or internal audit teams, each offering specific benefits (Jezierska and Koziara, 2017). Therefore, auditing is one of the most important components of an organization's security policy (Figure 2).

External audits are characterized by complete independence of assessment, which enhances their objectivity and impartiality. External auditors often have extensive experience gained across various sectors, allowing them to introduce best practices into the audited organization.

Figure 2. *Security policy – actions*



Source: *Own study.*

Certificates and reports from external audits are also valuable evidence of compliance that may be required by clients, business partners, or legal regulations. However, these audits can be costly and may take more time to understand the specifics of the organization.

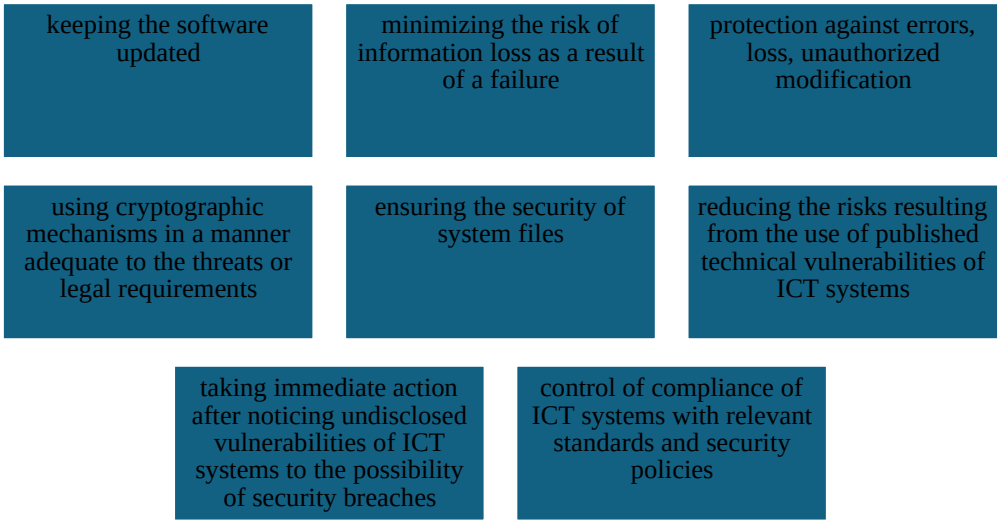
In contrast, internal audits guarantee an in-depth understanding of the organization, its processes, structure, and culture, enabling more accurate identification of potential threats. Internal auditors can conduct audits regularly and continuously monitor the implementation of recommendations, providing greater flexibility in responding to new threats.

Nevertheless, internal teams may be less objective and may not have access to the same breadth of knowledge and experience as their external counterparts.

In Polish legislation, the obligation to ensure periodic (but not less than once a year) internal audits of information security processed in the ICT system was introduced by § 19 sec. 2 point 14 of the Regulation of the Council of Ministers of May 22, 2022, on the National Interoperability Framework, minimum requirements for public registers and electronic information exchange, and minimum requirements for ICT systems (Regulation, 2022).

The legislator also addresses the elements that must be implemented to ensure an adequate level of security in ICT systems, particularly through the activities presented in Figure 3.

Figure 3. *Elements of ensuring an appropriate level of security in ICT systems*



Source: *Regulation of the Council of Ministers of 22 May 2022 on the National Interoperability Framework for minimum requirements for public registers and exchange of information in electronic form and minimum requirements for ICT systems, § 19, paragraph 2, item 12 (Rozporządzenie Rady Ministrów z dnia 22 maja 2022 r. w sprawie Krajowych Ram Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2024 poz. 773).*

With the above in mind, the audit planning stage can be divided into the following phases:

- understanding of business;
- defining the regulation and legal environment;
- review of previous audits, OSINT;
- identification of policies, standards and procedures;
- conducting a risk analysis;
- determining the scope and objectives of the audit;
- developing a strategy and programme;
- designation of resources;
- establishing a plan for the implementation of tasks (Wygodny, 2021).

The information security audit process is multi-stage and requires thorough preparation and understanding of the organization's specifics. Conducting an information security audit requires careful preparation and understanding of many aspects of the organization's activities.

Each stage of the audit process – from understanding the business, through risk analysis, to developing an audit strategy and program – is crucial to achieving

success. Proper preparation and execution of the audit allow for the identification of security gaps, ensuring compliance with regulations, and implementing effective corrective actions, thereby contributing to an increased level of information security within the organization.

Audit practice indicates that there are actions or even certain catalogs of actions aimed at complicating the operations of criminals. This pertains to computer hackers, system intruders, as well as procedures and policies suitable for organizations to prevent data leaks.

Data leak prevention is a priority for organizations in the face of globalization, the development of the FinTech industry, and threats related to terrorism and cyber warfare. Increasing engagement and expenditures on security is inevitable and seems to focus primarily on the following areas (Kifner, 2016):

- monitoring;
- providing technical measures;
- managing the organization based on risks.

Perpetrators of computer crimes can be both internal employees of the organization, regular staff, as well as individuals with higher privileges in IT systems, and external entities. The most dangerous perpetrators of security breaches are internal personnel working in IT departments (Podgórski, 2019; Auzina *et al.*, 2023).

Organizations identify obligations and recognize the ever-changing needs associated with data protection and the need to organize financial resources for this purpose. However, (despite many common features for all), the directions of expenditure, their structure, and scale will depend on the specifics of the entity in question.

Entities that want to effectively protect their information should therefore apply a systemic approach, involving holistic management of their information resources, the infrastructure for processing them, and the risks inevitably associated with information security (Wiśniewska, 2009).

To summarize, information security audits, whether conducted internally or externally, are key tools in managing risk and protecting information assets. Each of these forms of audit has its unique advantages, which can be utilized depending on the specific needs and goals of the organization. By integrating modern technologies, the auditing process becomes even more effective, which is essential in the face of increasingly advanced security threats.

4. Information Security of Organizations - Challenges and Threats

Information security within an organization is a crucial aspect that requires constant attention and commitment. In the era of rapid digital technology development and

the global network, threats related to information security are becoming increasingly complex and varied. Table 3 presents data published by KPMG in Poland regarding the number of security incidents reported by companies.

Based on the data (Table 3), it can be inferred that from 2019 to 2023, there was an increase in incidents (in the group of 30 and more) by 6 percentage points. This confirms the general opinion that along with technological advancements and technical capabilities, there will also be an upward trend in incidents related to data security threats.

Table 3. *Number and structure of security incidents registered by companies*

Specification	**Years**				
	2023	**2022**	**2021**	**2020**	**2019**
	(%)				
0	32	42	31	36	46
1-3	29	25	23	26	29
4-9	17	9	23	23	14
10-29	9	12	14	11	6
30 i więcej	11	12	9	4	5

Source: *KPMG in Poland based on a survey.*
https://kpmg.com/pl/pl/home/insights/2024/02/barometr-cyberbezpieczenstwa-2024.html

In the face of challenges and threats, it is necessary to develop appropriate data protection mechanisms and establish information security standards. This requires cooperation among the scientific community, the private sector, the government, and international organizations (Frączek and Spaliński, 2023).

Only in this way can an adequate level of security be ensured within an organization. Table 4 presents the selected challenges and threats considered by the authors to be the most important for organizations in the area of information security.

Table 4. *Challenges and threats faced by organizations in the area of information security – selected aspects*

Challenges	**Threats**
1. Dynamic development of technology Technology is advancing at a rapid pace, which means that organizations must constantly update their security systems and procedures. New technologies such as artificial intelligence, the Internet of Things (IoT) and blockchain introduce new challenges and require adaptation in terms of security management.	**1. Cyberattacks** Cybercrime is one of the biggest threats to organizations. Hacker attacks, ransomware, phishing, DDoS (Distributed Denial of Service) are just some of the methods used by cybercriminals. Effective defense against them requires advanced protection measures and continuous monitoring.

2. The complexity of IT systems Today's organizations often use extensive and complex IT systems that integrate different technologies and platforms. Managing such systems requires advanced knowledge and skills to ensure their security.	**2. Insider threats** Employees of an organization can unknowingly or intentionally cause security breaches. Human error, misuse, lack of awareness of threats - all this can lead to serious incidents. Therefore, education and training are an essential part of a security strategy.
3. Competence gap There is a high demand for information security specialists, and at the same time, there is a shortage of suitably qualified employees on the labor market. Organizations need to invest in training and development for their IT teams to keep up with the growing demands.	**3. Malware** Viruses, trojans, spyware, and other types of malware are a constant threat to information systems. Protection against them requires the use of advanced antivirus tools and regular software updates.
4. Legal regulations and compliance Data protection laws such as the GDPR in Europe impose numerous information protection obligations on organizations. Meeting these legal requirements is crucial, but at the same time it is challenging from an organizational and technological perspective.	**4. Physical threats** Information security is not only digital protection, but also physical protection. Equipment theft, sabotage, or natural disasters can lead to data loss and downtime for an organization. Putting in place appropriate physical protection measures and contingency plans is essential.

Source: *Own elaboration.*

Organizational information security is a multifaceted process that requires a holistic approach. Effective information protection requires understanding of both technical and organizational aspects, continuous monitoring of threats and adaptation to a dynamically changing technological environment. Organizations must invest in the development of their employees' competences, the implementation of advanced protection tools and building awareness of threats at all levels of their structure.

5. Conclusions

Information security is the foundation of modern organizations, ensuring the protection of data, resources, and the integrity of business operations. In the era of digitalization and widespread data access, its importance is increasing, becoming a crucial element of every organization's strategy. Information protection includes ensuring data confidentiality, availability, and integrity. The rise in cyber threats necessitates the continuous improvement of security practices and quick responses to incidents.

Legal regulations, such as GDPR in Europe and HIPAA in the USA, impose obligations on organizations to adhere to specific standards for personal data

protection. Implementing appropriate procedures and policies has become an essential part of business operations.

The development of technologies, such as artificial intelligence, opens new opportunities for data security, enabling more effective threat detection and faster incident response.

Findings from existing research indicate the need for investment in employee education and awareness, cross-sector collaboration, and continuous improvement of security practices. Further research and analysis should focus on new technologies and global security standards to better address the growing challenges in information protection.

References:

Auzina, I., Volkova, T., Norena-Chavez, D., Kadłubek, M., Thalassinos, I.E. 2023. Cyber Incident Response Managerial Approaches for Enhancing Small–Medium-Size Enterprise's Cyber Maturity. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 175-190). Emerald Publishing Limited.

Audyt Systemu Zarządzania Bezpieczeństwem. At: https://4itsecurity.pl/blog/4-Audyt-bezpiecze%C5%84stwa/92-audyt-systemu-zarzadzania-bezpieczenstwem-informacji.html.

AlGhamdi, S., Khin-Than, W., Vlahu-Gjorgievska, E. 2020. Information security governance challenges and critical success factors: Systematic review. Computers & Security, Volume 99, December. https://www.sciencedirect.com/science/article/abs/pii/S0167404820303035?via%3Dihub.

Frączek, M., Spaliński, K. 2023. Bezpieczeństwo informacji w dobie sztucznej inteligencji: analiza ryzyka i wyzwania związane z ChatGPT. Zeszyty Naukowe Pro Publico Bono, Nr 1(1).

Jezierska, A., Koziara, A. 2017. Audyt wewnętrzny a bezpieczeństwo informacji. In: Bezpieczeństwo informacyjne w dyskursie naukowym, red. H. Batorowska, E. Musiał, UP w Krakowie IBiEO KKIiZI, Kraków.

Kifner, T. 2016. Elementy kultury IT wspomagające wdrażanie systemu bezpieczeństwa teleinformatycznego i bezpieczeństwa informacji. In: Bezpieczeństwo danych w sektorze publicznym (T. Szatkowski red.), Biblioteka Izby Rzeczoznawców, Warszawa, s. 23, 7-28. https://ir.pti.org.pl/wp-content/uploads/2017/02/Biblioteczka-Izby-Rzeczoznawc%C3%B3w-PTI-Tom-4.pdf.

KPMG w Polsce na podstawie badania ankietowego. https://kpmg.com/pl/pl/home/insights/2024/02/barometr-cyberbezpieczenstwa-2024.html.

Lopez, D.R. 2013. Data Security. Data Science Journal, Volume 12. DOI: 10.2481/dsj.GRDI-012, s. 2.

Solarte Solarte, N.F., Rosero, E.R.E., Carmen Benavides, del M. 2015. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica – ESPOL, 28(5).

Norma ISO 27001. https://lexdigital.pl/norma-iso-27001.

Pallas Mega, G. 2009. Metodología de Implantación de un SGSI en un grupo empresarial jerárquico: Tesis de Maestría (Ingeniería en Computación): Universidad de la República, Montevideo – Uruguay.

Podgórski, G. 2019. Bezpieczeństwo danych. In: Zarządzanie danymi w organizacji (B. Gontar red.), Wydawnictwo Uniwersytetu Łódzkiego, Łódz, s. 178. https://doi.org/10.18778/8142-629-9.06. https://dspace.uni.lodz.pl:8443/xmlui/handle/11089/44772.

Rozporządzenie Rady Ministrów z dnia 22 maja 2022 r. w sprawie Krajowych Ram Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2024 poz. 773

Velinov, E., Kadłubek, M., Thalassinos, I.E., Grima, S., Maditinos, D. 2023. Digital Transformation and Data Governance: Top Management Teams Perspectives. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (Vol. 111, pp. 147-158). Emerald Publishing Limited.

Wiśniewska, M. 2009. Kompleksowe podejście do zarządzania bezpieczeństwem informacji – systemy zarządzania bezpieczeństwem informacji. Zeszyty Naukowe Politechniki Łódzkiej, Organizacja i Zarządzanie Nr, z. 45(1064), s. 80, 89.

Wygodny, A. 2021. Metody prowadzenia audytu cyberbezpieczeństwa: Ustawa o KSC. Kontrola Państwowa, nr 2(397).