European Research Studies Journal
Volume XXVII, Issue 2, 2024

pp. 35-46

Chief Information Security Officer: A Vital Component of Organizational Information Security Management

Submitted 18/02/24, 1st revision 10/03/24, 2nd revision 22/03/24, accepted 15/04/24

Marek Ciekanowski[1], Sławomir Żurawski[2], Zbigniew Ciekanowski[3], Yury Pauliuchuk[4], Artur Czech[5]

Abstract:

Purpose: *The article aims to identify the role of the Chief Information Security Officer (CISO) in managing information security within an organization.*

Design/Methodology/Approach: *The research problem was formulated as follows: What role does the CISO play in ensuring information security within an organization? To address this research problem, appropriate research methods were employed, such as literature analysis, both domestic and foreign, about information security, ISO 27000 standards, the role of the CISO, and information security threats. This method facilitated understanding existing theories, research frameworks, and practices in the field of information security, as well as the analysis of documents and reports containing current research, data, and information, enabling an understanding of practices and standards applicable in a given organization or sector.*

Findings: *The process of developing, implementing, maintaining, improving, and auditing the quality management system impacts the security level of the organization. Consequently, it serves as a modern tool focused on instilling organizational order in the company, encompassing both the structure and creativity of all employees.*

Practical implications: *The article addresses the topic of information security, emphasizing its significance in today's digital world, where data is a critical asset for organizations, and it focuses on the ISO 27000 standard, which is one of the most important standards related to information security management. It discusses its main assumptions, scope, and benefits resulting from its implementation. Another aspect addressed is the role of the CISO (Chief Information Security Officer) in the organization. The authors analyze the tasks, responsibilities, and expectations placed on the individual fulfilling this role. They explain that the CISO is a key player in ensuring the integrity, confidentiality, and availability of data within the organization, while also being a leader in the field of information security.*

[1]*University of Social Sciences, Poland, ORCID: 0009-0009-1271-0652, e-mail: marek@ciekanowski.pl;*
[2]*State School of Higher Education in Chełm, Poland, ORCID: 0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl;*
[3]*Faculty of Economics, John Paul II University of Applied Sciences in Biała Podlaska, Poland, ORCID: 0000-0002-0549-894X, e-mail: zbigniew@ciekanowski.pl;*
[4]*Siedlce University of Natural Sciences and Humanities, Poland, ORCID 0000-0002-2077-5124, e-mail: y.pauliuchuk@wp.pl;*
[5]*Warsaw Management University, Poland, ORCID: 0000-0003-4854-1466, e-mail: artur.czech@mans.org.pl;*

The article also discusses the threats that CISOs must contend with in their work, encompassing both technical threats and those associated with human factors, such as lack of employee awareness regarding information security or neglect in security policies and procedures. The authors emphasize that the role of the CISO is becoming increasingly strategic in ensuring information security in organizations.

Originality/Value: *The authors accentuate in this article the fact that organizations must provide adequate support for their CISO and enable access to appropriate resources, including financial and human resources, to effectively fulfill their duties. Furthermore, they emphasize that continued research in the field of information security management is crucial because cyber threats are constantly evolving, and organizations must stay updated with the latest methods and tools for data protection. This research may include new technologies, best practices, risk management, and the development of skills and competencies for information security personnel. Pursuing the continuous improvement of information security processes and strategies will be crucial for maintaining data protection at an appropriate level in a dynamic and changing business environment.*

Keywords: *Information security, CISO, management, organization, ISO 2700 standard*.

JEL: *D89, M10, M15.*

Paper type: *Research article.*

1. Introduction

In today's digital world, where data is one of the most valuable assets, information security has become a key element for organizations in every sector. In order to effectively manage information security, many companies appoint a CISO (Chief Information Security Officer) or director of information security as a key leader responsible for protecting data and systems from threats.

The CISO serves as a strategic advisor, who is not only responsible for overseeing operations related to information security but also participates in shaping the organization's policies, procedures, and strategies regarding data protection. His duties include identifying, analyzing, and managing risks, implementing appropriate tools and technologies, overseeing compliance with security regulations and standards, and conducting incident response activities.

The CISO acts as a crucial bridge between the IT department and management, conveying essential information regarding risk and investment needs in the field of information security. His role becomes particularly significant in the face of increasingly complex cybersecurity threats, such as ransomware attacks, phishing, or data breaches. Therefore, organizations increasingly recognize the CISO as a key element in ensuring operational continuity, protecting reputation, and building customer trust through effective information security management.

2. Information Security- ISO 27000 Standard

ISO standards are safety standards or standards established by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), responsible for establishing norms and guidelines related to management systems applicable to every type of international and global organization.

These standards aim to facilitate trade, ease information exchange, and contribute to technology transfer. The 27000 series aims to establish best practices for implementing, maintaining, and managing an Information Security Management System (ISMS). ISO/IEC 27001 is the most globally recognized standard concerning Information Security Management Systems (ISMS) and their requirements.

Additional best practices in information protection and cyber resilience are covered by several standards within the ISO/IEC 27000 family. Selected standards are presented in the table below (Vasquez, 2023).

Table 1. *Selected standards from the ISO/IEC 27000 series. Information technology. Security techniques.*

Standards containing requirements	**Standards describing main guidelines**	**Standards containing measures for particular sectors**
ISO/ IEC 27001 Informatics - Techniques security - Systems security management information - Requirements	**ISO/IEC 27002** Practical information security principles (list of measures)	**ISO/IEC 27011** Technological information Security techniques – Code of conduct in the field of information security control based on ISO/IEC 27002 for telecommunications organizations
ISO/ IEC 27006 **ISO/IEC 27006** Information technology Security techniques Requirements for bodies providing audit and certification of information security management systems	**ISO/ IEC 27005** ISO/IEC 27005 Risk management in information security (the standard includes, among others, a catalogue of threats that should be considered in risk analysis).	**ISO/IEC 27015** Information technology Security techniques Guidelines concerning information security management in the field of financial services.
	ISO/IEC 27014 Information technology Security techniques Management of information security	**ISO/IEC 27799** Informatics in the protection of health Management of security in health with the use of ISO / IEC 27002 norms
	ISO/IEC 27007	

	Information security, Cybersecurity and data privacy - Measures concerning the auditing of systems managing information security	
Standard integrated with the family of standards ISO/IEC 27000: **ISO/IEC 29134** Information techniques – Security techniques – Measures concerning the assessment of the effects for privacy **ISO/IEC 27032** Information techniques – Security techniques – Measures concerning cybersecurity		

Source: Antczak, 2021.

In Annex A, four areas affecting information security have been identified. These are:

- The organizational security domain.
- The personnel security domain.
- The physical security domain.
- The technological security domain.

The implementation of ISO 27001 and/or obtaining certification for compliance with the standard involves many benefits. The most important of them are:

- Ensuring that informational assets are appropriately protected.
- Maintaining data privacy and integrity.
- Increasing the awareness of threats and the need for appropriate security measures among employees.
- Strengthening the organization's resilience to incidents.
- Supervising information processing processes.
- Assisting in defining roles and responsibilities related to information processing.
- Meeting legal requirements and expectations of customers, contractors, and business partners,
- Improving service quality and increasing customer reliability and trust.
- Avoiding financial losses resulting from security breaches.
- Increasing competitiveness in the market.
  https://resilia.pl/blog/iso-27001-czym-jest-jakie-daje-korzysci/.

In an increasingly technological environment, management standards, particularly ISO 27000 standards, are essential to guarantee information security in organizations. These standards offer a range of benefits, such as improving security, increasing efficiency, and reducing costs.

Additionally, they help maintain the confidentiality, integrity, and availability of information (G.S.B. Presentacion, Benefits of ISO 27000 standards, 2023).

Implementing ISO 27000 standards is necessary to protect informational resources and manage risk effectively. These standards apply to organizations of all sizes and sectors, making them versatile and valuable in any business context.

Furthermore, they promote continuous improvement in information security management, enabling organizations to adapt to changes in both internal and external environments (G.S.B. Presentacion, Benefits of ISO 27000 standards, 2023). In summary, adopting ISO 27000 standards is a key means of protecting information and ensuring the successful development of organizations in an increasingly digital world susceptible to cyber threats. These standards serve as a valuable source for maintaining competitiveness and customer trust.

3. CISO Tasks

Under the acronym CISO hides an employee who holds one of the most important roles in the organization. It is the Chief Information Security Officer (CISO). His task is to ensure a comprehensive approach to cybersecurity. The CISO supports threat detection, prevents their materialization, and mitigates the consequences, all while keeping the organization's mission in mind.
https://www.karierawfinansach.pl/artykul/wiadomosci/kim-jest-ciso-szef-bezpieczenstwa-informacji.

One of the main challenges facing Chief Information Security Officers is the invisibility of security success. Success often goes unnoticed, while breaches can attract enormous attention. Success is not commonly perceived as a result of proactivity (Hooper and McKissack, 2016). Several areas of work and responsibilities should be reported to the CISO. For example, we can find them in the following four organizational units.

***Figure 1**. Tasks of the Chief Information Security Officer*

***Source:** The tasks of the Chief Information Security Officer (CISO), https://pl.itpedia.nl/2017/11/11/taken-van-de-chief-information-security-officer-ciso/.*

In light of growing threats and ever more complicated regulatory requirements, the tasks of the CISO have never been more critical or key. https://www.ey.com/pl_pl/ciso/how-do-you-see-more-clearly-when-cyber-threats-cross-boundaries.

Below are the most important tasks of the CISO. In the Figure below the main tasks of a CISO are presented.

***Figure 2**. What are the typical tasks of a CISO?*

***Source*:** https://advisera.com/27001academy/knowledgebase/what-is-the-job-of-chief-information-security-officer-ciso-in-iso-27001/

Tasks placed before cyber security directors are very important and serious, more than one would think. With the increased level of threats caused by rapid technological development, CISOs must determine the exposure level of all processes, establish risk-limiting structures, develop responses to threats, and simultaneously meet the organization's expectations by responding to market needs.

This change carries some risk, but every risk can also be an opportunity for CISOs. If the transformation succeeds, their function within the organization will significantly increase (https://www.ey.com/pl_pl/ciso/how-do-you-see-more-clearly-when-cyber-threats-cross-boundaries).

An important element of information security in the organization, as well as collaboration with the CISO, is the Information Security Committee. The Information Security Committee acts as a steering group for the CISO. This steering group ensures that the tasks of the CISO are aligned with all organizational objectives. The steering committee also ensures compliance with management

policy and obligations. Members of the steering committee for the CISO may include:

- The Managing Director.
- The Chief Information Officer.
- The Chief Financial Officer.
- The Privacy Inspector.
- A Lawyer.
- The HR Officer.
- The Communication / Marketing Specialist.
- IT Staff (e.g. Network Administrator).
- Executive Unit Employees.
- An external Consultant (https://pl.itpedia.nl/2017/11/11/taken-van-de-chief-information-security-officer-ciso/).

When management and boards take responsibility for cybersecurity, they will most likely require the CISO to be part of the management team. If the organization does not have a CISO with the required knowledge and skills, they will certainly hire one from outside (Shayo and Lin, 2019).

The role of the Chief Information Security Officer (CISO) in an organization is crucial for ensuring information and data security. The CISO is responsible for developing, implementing, and overseeing the information security strategy throughout the organization.

Their tasks include risk management, protection against cyber attacks, ensuring compliance with regulations and industry standards, conducting investigations in the event of security incidents, educating employees on security, and continuously improving and updating security strategies in response to changing threats. The CISO plays a key role in building a culture of security in the organization and supporting business goals through effective information risk management.

4. Role and Threats for the CISO in Ensuring Information Security

Information has always been and continues to be one of the most valuable assets for individuals, institutions, states, economies, cultures, and societies (Łuczak and Tyburski, 2009). Information security is very often understood as the protection of information from unwanted (accidental or intentional) disclosure, the modification, destruction, or disruption of its processing (Liedel, 2008). Information security manifests itself in every sphere of entity activity, including within organizations (Grzebiela, 2018).

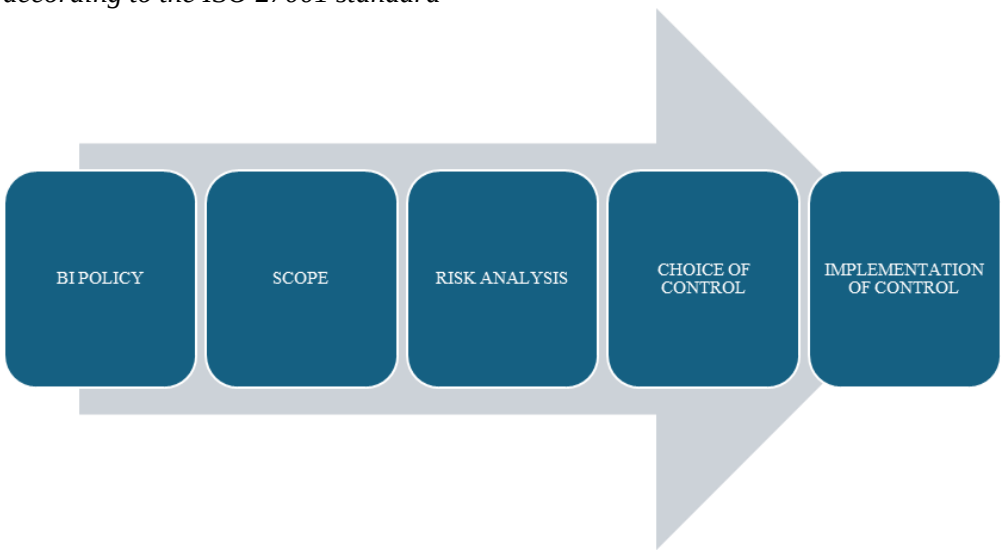
The information security strategy, in particular, must support the organization's overall strategic plans (Ghelani, 2022). Any organization that decides to build,

maintain, and improve an Information Security Management System based on the requirements of the ISO/IEC 27001 standard can ensure:

- the maximum protection of information,
- very good access to IT services.

It is possible thanks to technical and organizational frameworks ensuring the effective assessment of efficiency and introducing process optimization loops in the company (https://cis-cert.com.pl/blog/czym-jest-iso-27001). Below is presented the functioning of the Information Security Management System according to the ISO 27001 standard.

Figure 3. *The functioning of the Information Security Management System according to the ISO 27001 standard*



Source: *The ISO 27001 Standard.*

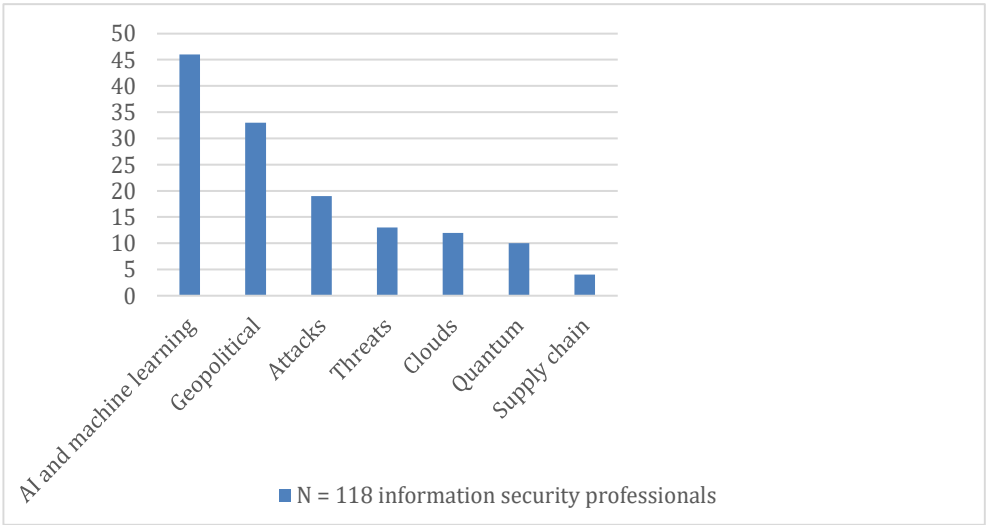
Needs of corporate organizations in terms of security are evolving. Our increased dependence on cloud-based technologies and IoT in the workplace requires appropriate people, processes, and technologies for the continuous monitoring and improvement of the organization's security status. Organizations must adapt their teams to defend against threats and protect critical business data.

For the proper functioning of the Information Security Management System, an essential element is the CISO. The CISO (Chief Information Security Officer) position is crucial for ensuring information security in the organization. There are many factors that can affect the effectiveness of the CISO's work and the overall level of information security in the company. While IT and security teams focus on incidents, the CISO is responsible for the broader risk and compliance picture.

Once CISOs focused solely on technology, but their role has evolved, focusing on business and processes. It is a multidimensional role that requires the understanding of enterprise resources, long-term goals, and the ability to build relationships with various business units (https://www.trgsolutions.com/pl/resources/blog/enterprise-cybersecurity-ciso).

The importance of the role of the Chief Information Security Officer (CISO) is constantly growing with the proliferation of digital technologies, particularly artificial intelligence, and the increasing concerns related to cyber attacks. Below are presented the most significant cyber threats from the past five years that individuals occupying this position are exposed to.

Figure 4. *The most significant cyberthreats for CISO in the last 5 years (%)*



Source: *Global research of Heidrick & Struggles concerning directors of information security (CISO), 2022, 2023.*

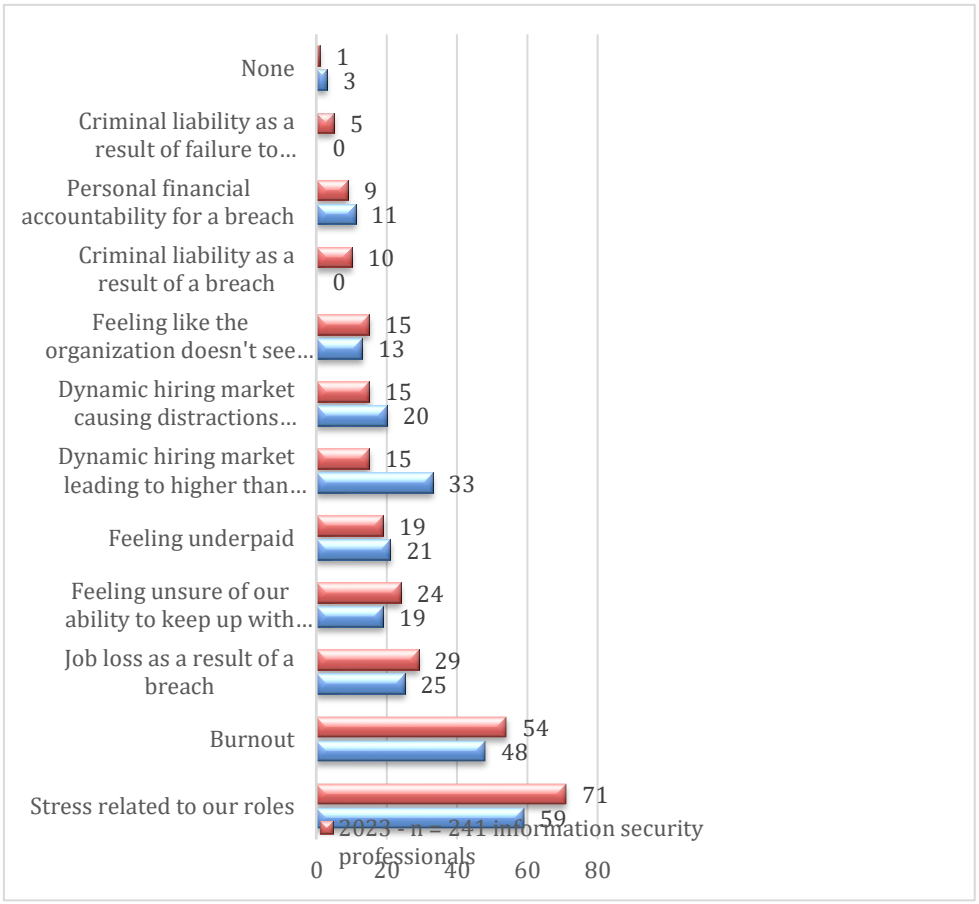
The Director of Information Security (CISO) is responsible for safeguarding the organization's information from breaches, leaks, and other threats. The CISO must stay current with the latest trends in information security and implement appropriate control measures to protect the organization. The challenges facing the CISO include:

- Technology complexity: Technologies are becoming increasingly complex, making it difficult for the CISO to understand and protect all of the organization's systems.
- Cyber threats: Cyber threats are constantly evolving, and the CISO must stay abreast of the latest threats and implement appropriate control measures to mitigate them.

- Lack of personnel: There is a shortage of qualified information security professionals, making it difficult for the CISO to find and retain suitable employees.

The work of the CISO is highly demanding and entails a range of personal risks. The CISO can minimize these risks by taking appropriate steps, such as maintaining their health, building a strong team, implementing appropriate control measures, and staying abreast of the latest trends. Below are the key personal risks in the role of CISO.

Figure 5. *The most significant personal risks in the CISO position (%)*



Source: *Global research of Heidrick & Struggles concerning directors of information security (CISO), 2022, 2023.*

When it comes to personal risk, the main problems, which grow from year to year, are stress and professional burnout. Also, a slight increase in concerns regarding the ability to keep up with rapidly changing threats, as well as job loss due to breach, to 29% from 25% in 2022, have been noted.

(https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/2023-global-chief-information-security-officer-survey.pdf).

The role of the CISO is increasingly important in today's digital world. The CISO must stay up to date with the latest trends in information security and implement appropriate control measures to protect the organization from breaches, leaks, and other threats.

5. Conclusions

In summary, the role of the CISO as a key element of information security management in the organization is extremely important in the face of growing cybersecurity threats and the increasing value of data. The CISO serves as a strategic advisor, who not only oversees operations related to information security but also actively collaborates with management in shaping policies, procedures, and data security strategies.

His role is not limited to the technical side of security but also includes risk identification, analysis, and management, as well as the supervision of compliance with regulations and security standards. The CISO acts as a crucial communication bridge between the IT department and management, conveying essential information regarding risk and investment needs in the area of information security.

The conclusion drawn from this is that organizations must ensure adequate support for their CISO and provide access to appropriate resources, including financial and human resources, to effectively fulfill their duties. Furthermore, continuing research in the field of information security management is crucial because cyber threats are constantly evolving, and organizations must stay up-to-date with the latest methods and tools for data protection.

This research may include new technologies, best practices, risk management, and the development of skills and competencies for information security personnel. The pursuit of continuous improvement in information security processes and strategies will be crucial for maintaining data protection at an appropriate level in a dynamic and changing business environment.

References:

Antczak, J. 2021. Zarządzanie przedsiębiorstwem w cyberprzestrzeni. ASzWoj, Warszawa.
Co to jest norma ISO 27001 i dlaczego jest tak ważna dla organizacji? https://resilia.pl/blog/iso-27001-czym-jest-jakie-daje-korzysci/.
Czym jest ISO 27001? https://cis-cert.com.pl/blog/czym-jest-iso-27001/.
Ghelani, D. 2022. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. American Journal of Science, Engineering and Technology, Vol. 3, No. 6.

Global Chief Information Security Officer (CISO) Survey. 2023. https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/2023-global-chief-information-security-officer-survey.pdf.

Globalne badanie Heidrick & Struggles dotyczące dyrektorów ds. bezpieczeństwa informacji (CISO), 2023 oraz globalne badanie Heidrick & Struggles dotyczące dyrektorów ds. bezpieczeństwa informacji (CISO), 2022.

Grzebiela, K. 2018. Pojęcie i istota bezpieczeństwa informacyjnego. Kultura Bezpieczeństwa. Nauka-Praktyka-Reflekse, nr. 30.

Hooper, V., McKissack, J. 2016. The emerging role of the CISO. Business Horizons, Volume 59, Issue 6, November - December. https://www.sciencedirect.com/science/article/abs/pii/S0007681316300635.

Kim jest CISO? Portret współczesny, https://www.karierawfinansach.pl/artykul/wiadomosci/kim-jest-ciso-szef-bezpieczenstwa-informacji.

Liedel, K. 2008. Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego. Wydawnictwo Adam Marszałek, Toruń.

Łuczak, J., Tyburski, M. 2009. Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001. Wyd. Uniwersytetu Ekonomicznego w Poznaniu, Poznań.

Nowa rola CISO - od ochrony danych do transformacji i rozwoju, https://www.ey.com/pl_pl/ciso/how-do-you-see-more-clearly-when-cyber-threats-cross-boundaries.

Presentacion G.S.B. 2023. Beneficios de las normas ISO 27000, HT. High Tech Engineering Journal, Vol 3, nr. 2.

Shayo, C., Lin F. 2019. An Exploration of the Evolving Reporting Organizational Structure for the Chief Information Security Officer (CISO) Function. Journal of Computer Science and Information Technology, Vol. 7, No. 1.

Vasquez, J.D. 2023. ISO/IEC 27000. HT. High Tech Engineering Journal, Vol. 3.

What is the job of Chief Information Security Officer (CISO) in ISO 27001? https://advisera.com/27001academy/knowledgebase/what-is-the-job-of-chief-information-security-officer-ciso-in-iso-27001/.

Zadania głównego inspektora bezpieczeństwa informacji (CISO). https://pl.itpedia.nl/2017/11/11/taken-van-de-chief-information-security-officer-ciso/.