IMPLEMENTING ISO/IEC 27001 IN SOFTWARE DEVELOPMENT: THE ROLE OF HUMAN RESOURCES IN ENSURING INFORMATION SECURITY[1]

UDC: 006.322:[004.056.5:004.4+005.963.1](478)
DOI: https://doi.org/10.53486/tids2025.06

LUCIA GUJUMAN
Associate Professor,
Academy of Economic Studies of Moldova
gujuman.lucia@ase.md
ORCID ID: 0000-0001-7940-4291

ZINOVIA TOACĂ
Associate Professor
Academy of Economic Studies of Moldova
toaca@ase.md
ORCID ID: 0000-0002-8304-1961

VITALIE URSACHI
PhD
Academy of Economic Studies of Moldova

Abstract. This paper examines the implementation of ISO/IEC 27001 in software development, emphasizing the critical role of human resources in ensuring information security. Based on international standards (ISO/IEC 27000 family, NIST CSF, COBIT, ITIL) and national legislation, the study highlights both the benefits and challenges identified through a survey of IT professionals in Moldova. The findings show that while awareness of ISO/IEC 27001 is high, training, flexibility, and organizational culture remain key factors for successful adoption. Recommendations are proposed to strengthen security practices and foster a resilient, innovation-oriented environment.

Keywords: Information Security Governance, Cybersecurity Frameworks, ISO/IEC 27001, resources, Infrastructure, standards, data.

JEL Classification: M15, M12, O32, L86

INTRODUCTION

In the digital age, the way entities collect, process, store and manage data and information is based on the use of information technologies. At the same time, the development and use of agile methodology with its Frameworks and Cloud infrastructures has accelerated the exposure of sensitive data to various types of threats. The increasing threat of cyberattacks and data leaks represents a significant challenge to the integrity of information security for all national and global entities.

According to official data published in the ENISA Threat Landscape 2024 report, by the European Union Agency for Cybersecurity, cyber threats in recent years have recorded continuous growth, affecting both private entities and public institutions. According to ENISA Threat Landscape 2024, the main risks identified at European level are the intensification of ransomware attacks, the exploitation of vulnerabilities in the supply chain and the increase in the number of attacks on critical

[1]The article was developed within the framework of Subprogram 030101 "Strengthening the resilience, competitiveness, and sustainability of the economy of the Republic of Moldova in the context of the accession process to the European Union", institutional funding.

infrastructures, which confirms the fragility of the digital environment in the face of technological and geopolitical pressures. (European Union Agency for Cybersecurity (ENISA), 2024)

According to the latest data published by Check Point Research, "the second quarter of 2025 completes this picture, highlighting a global increase in cyberattacks of 21% compared to the same period in 2024, reaching an average of 1,984 weekly attacks per organization." The same report states that "Education had 4,388 weekly cyberattacks per organization, being the most targeted sector, followed by Government (2,632) and Telecommunications (2,612)." (Check Point Research, 2025)

This growth requires the implementation of logical and standardized measures in the field of data and information security. Implementing the ISO/IEC 27001 standard in software development is not only a compliance requirement, but also an essential strategy for ensuring organizational resilience. And human resources are the most important in the successful implementation of the ISO/IEC 27001 standard within organizations. Organizations, through recruitment procedures, continuous staff training and the development of a security-oriented organizational culture, can contribute to the formation of a responsible and involved human resource in ensuring information security.

Thus, the article aims to analyze the principles and particularities of the ISO/IEC 27001 standard, with an emphasis on the ways of implementing it in the software development process and on the essential role of human resources. The paper aims to highlight the impact of applying the standard on development teams and the correlation between ISO/IEC 27001 requirements and organizational security policies, formulating conclusions and practical recommendations for strengthening information security.

THEORETICAL AND NORMATIVE FRAMEWORK OF INFORMATION SECURITY.

Security means protecting our assets. This can mean protecting them from attackers invading our networks, natural disasters, adverse environmental conditions, power outages, theft, vandalism, or other unwanted actions (Andress, 2014), and encompasses both physical protection measures and technical and organizational measures.

According to ISO/IEC 27000:2018 'Information security is defined as "maintaining the confidentiality, integrity, and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability may also be involved" (SOURCE:ISO/IEC 27000:2018, Information Security Management Systems — Overview and Vocabulary).

The National Institute of Standards and Technology (NIST) defines information security as "the protection of information and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction, in order to ensure confidentiality, integrity, and availability." (National Institute of Standards and Technology (NIST), 2018)

And the European Union Agency for Cybersecurity (ENISA) defines information security as "the set of policies, processes, and controls implemented to protect information assets and ensure the continuity of organizational activities." (European Union Agency for Cybersecurity (ENISA), 2024)

According to Law No. 299/2017 of the Republic of Moldova, information security is defined as "the state of protection of information resources, as well as the person, society, and the state, in the information space." (Parlamentul Republicii Moldova, 2017)

The analysis of the definitions presented shows that information security is based on three fundamental characteristics: confidentiality, integrity and availability, and their assurance is achieved through a management process, supported by policies, procedures and controls implemented at the

organizational level. These characteristics are considered the core of information security and recognized by major reference frameworks, such as: ISO/IEC 27000 and NIST SP 800-12.

Information security is an essential condition for the efficient functioning of contemporary institutions and organizations. The application of international standards and frameworks provides integrated methodologies for developing information security management that would contribute to reducing risks and strengthening cyber resilience.

The ISO/IEC 27000 family of standards covers a wide range of information security standards published by both the International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 27000 recommends best practices for managing information risks by implementing security controls within an overall information security management system (ISMS).

The ISO/IEC 27000 family of standards is recognized as a reference and starting point in the development of information security management systems globally, being composed of several interconnected standards, each having a specific role in the overall framework. ISO/IEC 27000 covers security, confidentiality and IT issues, and the structure of this family of standards is presented in Figure 1.

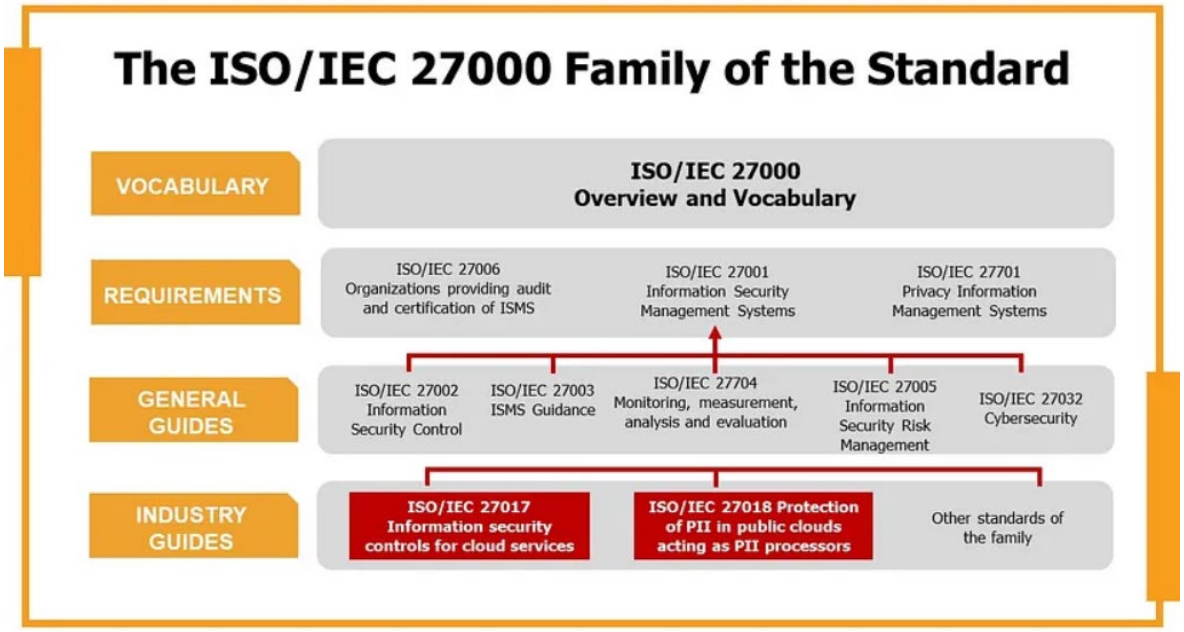

Figure1. Structure of the 27000 family of standards.

Source: *The ISO/IEC 27000 Family of Standards (CFE Certification, 2023)*

ISO/IEC 27001 is the most widely recognized international standard for information security management systems (ISMS) and their requirements. Additional practices for data protection and cyber resilience are covered by numerous other standards in the ISO/IEC 27000 family. Together, they enable organizations of all sizes and sectors to manage the security of assets such as financial information, intellectual property, employee data, and information entrusted to third parties. (CFE Certification, 2023)

ISO/IEC 27001 is a standard that helps organizations manage the security of important information in a structured and risk-focused way. It gives a clear guide for setting up, carrying out, keeping up, and regularly improving their information security practices.

The main purpose of ISO/IEC 27001 is to assist organizations in safeguarding the confidentiality, integrity, and availability of their information assets. The standard highlights the necessity of creating an information security management system (ISMS) that is customized to meet the specific requirements and risk levels of the organization, aiming to reduce confusion and frustration caused by unclear or inconsistent information security practices, which can result in operational disruptions and undermine trust. Implementing a tailored ISMS is crucial for ensuring that information is handled appropriately, securely, and in line with the organization's goals and regulatory requirements.

ISO/IEC 27001 is built on some important ideas, like being committed to managing risks in a careful and organized way, always trying to improve security practices, and making sure that security measures fit with the organization's goals and needs. A key part of this standard is the Plan-Do-Check-Act (PDCA) cycle, which helps organizations plan and set up an information security management system, carry out security controls, keep track of how well things are working, and keep making improvements over time.

An important aspect in the development of the ISO/IEC 27001 standard in our view is the role of human resources, which represents a key element in the development of an information security management system. The standard contains a specific set of human resources security controls, emphasizing the importance of staff involvement throughout the information security lifecycle.

By implementing ISO/IEC 27001, organizations demonstrate their commitment to best practices in information security and can provide assurance to stakeholders, customers, and partners that their information assets are managed with care and diligence.

Certification to ISO/IEC 27001 demonstrates that an organization has defined and implemented best practices for information security. However, not all organizations choose to obtain ISO/IEC 27001 certification; some use the standard as a framework for a best practice approach to information security management.

ISO/IEC 27001 certification can help an organization demonstrate compliance with international standards, making it more attractive to potential customers. ISO/IEC 27001 compliance helps companies demonstrate good security practices, which can improve customer relationships and give them a competitive advantage. Having an internationally recognized certification, regularly reviewed by an independent auditor, demonstrates an ongoing commitment to improving and protecting an organization’s important digital assets.

ISO/IEC 27001 is the most widely known and widely used international standard for the development of information security management systems, based on risk management principles. However, organizations are not limited to this standard alone, but also use other reference frameworks, such as the NIST series (e.g. NIST SP 800-171), COBIT, PCI DSS, SOC2, NERC-CIP, GDPR or FISMA, which provide complementary guidance and controls depending on the industry and regulatory context. Typically, in practical work, organizations combine elements from several frameworks to meet regulatory requirements and their own security objectives. In order to highlight the main differences and complementarities, the following table presents a comparative summary of the most relevant information security management standards and frameworks depending on their focus, strengths and limitations.

Table 1. Comparison of the main information security management frameworks.

Frame / Standard	Main focus	Strengths	limitation
ISO/IEC 27001 (SMSI)	Requirements for implementing an Information Security Management System (ISMS); based on risk management and PDCA.	Certified international standard; globally recognized; applicable to any organization; provides systematic and risk-based approach	Complex and costly implementation; requires mature organizational culture
ISO/IEC 27002	Good practices and control objectives (access control, cryptography, HR security, incident response).	Practical model for information asset protection; supplement to ISO/IEC 27001	Not certifiable; secondary role to 27001
NIST CSF (Cybersecurity Framework)	5 key functions: Identify–Protect–Detect–Respond–Recover; strategic and flexible orientation.	Easy to apply in any sector; widely used for assessing security maturity; good for internal/external communication	Does not provide certification; does not prescribe exactly which controls to implement
NIST SP 800-53	Detailed set of security controls (access, risks, incident response, assessment).	Very detailed technical guidance; widely adopted also in the private sector; flexible and adaptable	The statement can be rephrased as: "It is complex and challenging to implement for small organizations or those with limited resources."
COBIT 2019	IT is about governance in TI and connection to project objectives.	The framework links business and IT together, which is helpful for management and meeting compliance requirements.	It's not just about security, but also about general IT governance.
GDPR	Protection of personal data and privacy.	European laws on data protection that affect the whole world; these rules apply to any company that handles information about people living in the European Union.	It is not a management system, but a law; it only covers personal information.

Source: *developed by the author, based on (National Institute of Standards and Technology (NIST), 2018), (ISACA, 2019), (Parlamentul European și Consiliul Uniunii Europene, 2016).*

We think that ISO/IEC 27001 is still the best standard for creating an information security management system because it offers certification and is easy for any organization to use. It's not right to say that companies should only use one framework or that one is better than the others. In reality, multiple frameworks can be used together in one organization because they work well with each other and can greatly improve the safety of data and information.

IMPLEMENTING ISO/IEC 27001 IN SOFTWARE DEVELOPMENT

Knowing the details and background of the organization, as outlined in clause 4.1 of the ISO/IEC 27001 standard, helps us properly recognize the risks and weaknesses that could affect its information assets. The organizational context includes internal elements, such as organizational structure and culture, available resources, processes and contractual relationships, as well as external elements, such as market trends, legal regulations (e.g. GDPR), economic conditions and technological developments. The analysis of these factors contributes to defining the objectives of the information security management system (ISMS) and to the appropriate allocation of resources necessary for its implementation.

Risk assessment, as a fundamental part of the implementation process, aims to identify threats to the confidentiality, integrity and availability of information. In practice, this involves the involvement of security teams in the analysis of system architecture and in the development of plans to mitigate the identified risks. Examples such as those applied by companies in the software industry show how each project includes the consideration of risks and the selection of appropriate actions to minimize them.

Implementing ISO/IEC 27001 in software development means making security a key part of the whole product life cycle. Key secure practices include:

• Secure software design – making sure security needs are considered from the start, including things like user login systems, and building the software structure in line with international standards.

• Secure development and coding – following good coding rules, checking code for errors, making sure all inputs are safe, managing changes properly, and using encryption methods.

• Testing and quality assurance – including security checks at every step of development, using fake data for testing, and doing penetration tests to find any hidden weaknesses.

• Keeping environments separate and managing access – having different areas for building, testing, and running the software, setting up strict rules for who can access what, and keeping track of changes.

• Using third-party and open-source software – choosing external tools carefully, checking for security risks, and making sure the software licenses meet the needs of the customer.

• Classifying and protecting information – deciding who is in charge of data, and setting up access rules that match how important the data is.

• Keeping records, making backups, and planning for continuity – watching for security events, saving copies of data, and having a plan in place to handle emergencies so important processes can keep going without stopping.

These policies make sure that security is part of every step in making software, which helps lower the chances of problems that could put the organization's or customers' data at risk.

Using good practices for building information management systems helps organizations in several ways: it lowers the costs from security issues, makes customers more trusting, improves how processes are planned and managed, saves time on maintenance, and gives a competitive edge by showing they follow ISO/IEC 27001 standards.

Implementing ISO/IEC 27001 comes with some challenges such as: high costs, the need for a mature organizational culture and possible differences between customer and internal requirements can be major obstacles. These aspects confirm that the success of applying the standard depends on both technical integration and the organization's ability to manage change.

The first line of defense against cyberattacks is represented by employees. Awareness of the importance of policy compliance and continuous security training are essential to prevent data leaks and incidents. Thus, the role of human resources becomes a central element of the success of ISO/IEC 27001 implementation.

THE ROLE OF HUMAN RESOURCES IN ENSURING INFORMATION SECURITY

To describe the role of human resources in the implementation of the ISO/IEC 27001 standard, with the aim of ensuring information security in IT organizations in the Republic of Moldova, a questionnaire was used as a research tool. This method allowed for the collection of direct data from specialists involved in software development processes, providing an applied perspective on how

security policies influence daily activities and organizational culture. The respondents to the questionnaire were 25 specialists of an IT company employed in different roles and seniority levels, namely: 8 senior developers, 7 junior developers, 4 senior testers, 3 junior testers, 1 delivery manager, 1 scrum master, 1 business analyst. The survey aimed to identify the opinions and perceptions of development teams regarding the processes and procedures involved in the implementation of the ISO/IEC 27001 standard within the company.

Following the completion and processing of the survey data, we note that 88% of respondents consider it necessary to implement the ISO/IEC 27001 standard, because it offers an increased level of security and perceives its importance, and there is a significant recognition of the importance of implementing the standard within the company. The majority of team members perceive this implementation as necessary, recognizing the benefits brought by an increased level of security, do not identify conflicts between the requirements of the ISO/IEC 27001 standard and the daily work within the company, and regarding security policies, the majority of respondents consider them transparent, reflecting the approach to all current trends and vulnerabilities.

However, there are also divergent views among respondents. Approximately 22% of respondents perceive the implementation of the standard as necessary, but express concerns about potential obstacles and delays in development projects or believe that they are too frequent and would take away from the time that can be allocated to the activity within the project. This perspective emphasizes the importance of ensuring that all employees realize the need to be aware of the risks related to information security and the vital role that each one plays in adhering to these requirements, but also indicates an important aspect of the balance between security and flexibility within the development processes.

And 12% see room for improvement by providing more rigorous security awareness training and better assessment of understanding of the material presented, suggesting increased attention to training and awareness needs.

These findings highlight the existence of robust and extensive practices designed to ensure information security, effectively support and inform teams on the implementation of the ISO/IEC 27001 standard, and the importance of continuing efforts to adopt the ISO/IEC 27001 standard within organizations, suggesting that there is significant support, but also challenges and opportunities for improvement to ensure a harmonious integration of the standard into the company's culture and processes.

Within IT companies in the Republic of Moldova, there is awareness of the importance of adopting relevant and current practices and policies aimed at ensuring information security as well as training employees on the development of information security management through the implementation of the ISO/IEC 27001 standard.

RECOMMENDATION

The survey results provide the necessary premises for formulating recommendations, namely:

1) Intensifying and diversifying the training process - an aspect highlighted by 12% of respondents. This recommendation highlights the importance of strengthening training programs in the field of information security, through a more detailed structuring of the content and by introducing rigorous evaluation mechanisms, which would contribute to a better understanding of the key concepts associated with information security management and the ISO/IEC 27001 standard, facilitating their coherent and uniform application within entities.

2) Flexibility to maintain operational efficiency by developing a compliance strategy adapted to the specifics and complexity of ongoing projects. Identifying a balance between security and adaptability is essential to support innovation and creativity in software development processes.

3) Periodically review and update security policies to continuously adapt to technological and environmental changes. Thus, regular evaluation of policies and procedures can help maintain their relevance and ensure that they remain effective in the face of changes in the information security field. These practices must be designed and implemented in a way that promotes a deep understanding of the principles and requirements of this information security management standard.

4) Two-way communication. It is essential to develop two-way feedback mechanisms so that employees can share experiences, suggestions or concerns related to the implementation of the standard and the development of effective information security management. This open communication process would support the rapid identification of any uncertainties and would facilitate the taking of corrective measures or adjustments effectively.

By addressing these comprehensive support and awareness practices, IT companies can strengthen the commitment and involvement of the team in the implementation process of the ISO/IEC 27001 standard, thus contributing to the success and continued effectiveness of the information security program.

Implementing these recommendations can strengthen the commitment and conscious involvement of each team member in the implementation process of the ISO/IEC 27001 standard, thus contributing to ensuring information security.

REFERENCES

1. Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice.* SUA: Elsevier Science.
2. CFE Certification. (2023). *The ISO/IEC 27000 family of standards.* The ISO/IEC 27000 family of standards.
3. Check Point Research. (2025). *Global Cyber Attacks Surge 21% in Q2 2025 — Europe Experiences the Highest Increase of All Regions*. Preluat de pe Check Point Research: https://blog.checkpoint.com/research/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions
4. European Union Agency for Cybersecurity (ENISA). (2024). *ENISA Threat Landscape 2024.* Luxembourg: Publications Office of the European Union.
5. European Union Agency for Cybersecurity (ENISA). (2024). *ENISA Threat Landscape 2024.* Luxembourg: Publications Office of the European Union.
6. ISACA. (2019) *COBIT 2019 Framework: Governance and Management Objectives.* Schaumburg, IL: Information Systems Audit and Control Association (ISACA).
7. National Institute of Standards and Technology (NIST). (2018). *An Introduction to Information Security (NIST Special Publication 800-12 Rev. 1).* Gaithersburg, MD: U.S. Department of Commerce.
8. National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).* Gaithersburg, MD: National Institute of Standards and Technology.
9. Parlamentul European și Consiliul Uniunii Europene. (2016). *Regulamentul (UE) 2016/679 – Regulamentul general privind protecția datelor (GDPR).* Bruxelles: Jurnalul Oficial al Uniunii Europene.
10. Parlamentul Republicii Moldova. (2017). *Legea nr. 299/2017 privind securitatea informațională.* Chișinău: Monitorul Oficial al Republicii Moldova.