The International Journal of Engineering and Science (IJES)
|| Volume || 14 || Issue || 1 || Pages || PP 62-67 || 2025 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Implementation of Iso 27001:2022 In The City Of Cazin: Awareness, Challenges And Opportunities

Nejra Mesić
University „Džemal Bijedić“ Mostar
Bosnia and Herzegovina

--*ABSTRACT*--

The paper ''Implementation of ISO 27001:2022 in the City of Cazin: Awareness, Challenges, and Opportunities'' analyzes the level of awareness, implementation, and benefits of applying the international standard ISO 27001:2022, which is crucial for all institutions whose business functions are in any way related to information technology and the need to protect the confidentiality of information resources. Considering the enhanced digitalization of business operations, the establishment and development of information security systems in all segments of a country represent an important prerequisite for creating an information society. The creation of an information society, in a broader sense, not only serves as a condition for integrating a country into international processes but also as a means for its survival in the society of developed nations. Therefore, through a survey conducted in the public and private sectors of the City of Cazin, data was collected regarding the motivations and challenges organizations face in implementing the standard. The results indicate a low level of awareness. However, organizations that have adopted the standard report increased level of security and reduced risks. The IT sector is recognized as critical for the modernization of business operations, and raising awareness of the ISO 27001:2022 standard could further enhance information systems, increase the competitiveness of enterprises, and attract investments to the City of Cazin.

KEYWORDS: *system, security, standard, ISO 27001:2022*

Date of Submission: 14-01-2025 Date of acceptance: 27-01-2025

I. INTRODUCTION

In the modern business environment, there is a need for efficient management and secure information, which has become a key resource of every organization. Protecting daily activities involving critical data, information and intellectual property from cyber threats presents a significant challenge in modern society [1]. In this context, the international standard ISO 27001:2022 represents a modern framework for assessing information security and implementing an information security management system (ISMS) for organizations of all sizes, structures or orientations. The main subjects of the information society are the state administration, business subjects and general population, while the basis of its development is the trust of these subjects in electronic services and electronic business [2]. Although ISO 27001:2022 is recognized as a leading standard at the global level, its application in Bosnia and Herzegovina, and especially in the city of Cazin, is still at the beginning. This paper investigates the level of awareness of the existence of this standard, as well as the degree of its implementation among organizations in the public and private sectors of the city of Cazin. The analysis of the data collected through the survey provides insight into the motivation of organizations for applying this standard, as well as the challenges they face during implementation. In addition, research results indicate that although awareness of ISO 27001:2022 is low, organizations that have already adopted it are seeing improvements in security and risk reduction. The key catalysts for the development and modernization of business in this region have been identified in the IT sector, which can play a crucial role in strengthening the information security and competitiveness of local companies. This paper not only provides an overview of the current state of awareness and implementation of ISO 27001:2022, but also provides recommendations for the future development and improvement of information security in the city of Cazin, with an emphasis on the importance of the IT sector as a driver of change.

II. WORK METHODOLOGY

For the purpose of this paper, a quantitative approach was used to investigate the level of awareness and implementation of the ISO 27001:2022 standard in the city of Cazin. Data collection was carried out through a survey that covered the public and private sectors.

The survey is designed to contain structured questions related to:

- Degree of familiarity with the ISO 27001:2022 standard,
- Reasons for implementing the standard,
- Identification of challenges and benefits recognized by organizations after implementation.

The research sample included various organizations in the city of Cazin, including public companies, institutions, administrative bodies, police station, IT companies and banks. The objective was to provide a representative overview of the state of awareness and implementation practices of the ISO 27001:2022 standard within various sectors. The survey was distributed electronically and was created using the Microsoft Forms platform, which enabled efficient data collection. The chosen method of data collection allowed the respondents to answer the questions simply and quickly. The collected data were analyzed using a combination of quantitative and qualitative methods. Quantitative data were processed using statistical techniques to determine the level of awareness and the degree of implementation of the standard, while qualitative data were analyzed through open-ended responses, enabling a deeper understanding of the motivations and challenges faced by organizations.The research was conducted in compliance with ethical principles, including the informed consent of the participants, data confidentiality and the possibility to withdraw from the research at any time. This methodology provides a comprehensive insight into the state of implementation of the ISO 27001:2022 standard in the city of Cazin, providing a basis for recommendations for future development and improvement of information systems.

III. LEGAL REGULATION IN BOSNIA AND HERZEGOVINA

Based on Article 10 of the Law on Ministries and Other Bodies of Bosnia and Herzegovina (‘’Official Gazette of Bosnia and Herzegovina’’, No. 5/03, 42/03, 26/04, 42/04, 45/06, 88/07, 35/09 , 103/09, 87/12 and 61/13) and Article 17 of the Law on the Council of Ministers of Bosnia and Herzegovina (‘’Official Gazette of Bosnia and Herzegovina’’, no. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 and 24/08), Council of Ministers of Bosnia and Herzegovina, at the 95th session, held on March 22, 2017 adopted the Decision on the adoption of the information security management policy in the institutions of Bosnia and Herzegovina for the period 2017-2022. The information security management policy implies a hierarchically organized set of documents that represents the basis for the implementation of the information security management system in the institutions. The policy treats the field of information security management in accordance with the ISO/IEC 27001 standard [2]. From a legal point of view, the controls crucial for the institution relate to the protection of confidentiality of personal data and information, the preservation of institutional reports and respect for intellectual property rights. When implementing an information security management system, the controls that achieve good results in practice are the following:

- security policy,
- division of responsibility for information security,
- awareness of information security, education and training,
- correct data processing in applications,
- vulnerability management,
- business continuity management,
- management of security incidents and system improvements.

Information and associated processes, systems and networks in institutions are of exceptional importance. In order to meet legal norms and ensure reputation, defining, implementing, maintaining and improving information security management can be of crucial importance. Computer fraud, espionage, sabotage, vandalism, fire, floods, etc. are security threats that institutions often face. Institutional damage in the form of malicious code, computer hacking and denial of service is an increasingly common phenomenon. Information security management requires the participation of all employees in institutions [2]. The final version of the preliminary draft of the Law on Information Security of the FBiH dated 6/9/2021 is available on the official website of the Federal Ministry of Transport and Communications [3]. Although the Law on Information Security has not yet been adopted, institutions must ensure the security of their information, and ISO 27001 provides a well-structured and internationally recognized framework for this. Relying on this standard can help institutions to bridge the legal gap while ensuring compliance with future legislation.

IV. ISO 27001:2022 AND CHANGES BROUGHT BY THE STANDARD

The ISO 27001 standard is important for all institutions whose business functions are in any way connected to the information technologies and the need to protect the confidentiality of information resources. By introducing this standard, organizations show their clients and all interested parties that they perform their business functions based on security principles and that their business plans are aimed at continuous improvement of the information security management system [1]. The new version of the ISO/IEC 27001:2022 standard was published on October 25, 2022. Unlike ISO/IEC 27001:2013, the full name of the new version is ISO/IEC 27001:2022 Information security, cyber security and privacy protection. The part that has gone through the most significant changes is Annex A of the ISO/IEC 27001 standard, which is aligned with the amendments of ISO/IEC 27001:2022. Annex A of the ISO/IEC 27001:2022 standard contains changes in the number of controls and their list in groups. The number of controls from Annex A was reduced from 114 to 93. The reduction in the number of controls occurred due to the merging of certain controls. 35 controls remained the same, 23 controls were renamed, 57 controls were merged into 24 controls, and one control was split into two. Thus, 93 controls were restructured into four control groups or sections [4]. It is not mandatory to implement all controls. Certification bodies may exclude certain controls if the associated risks have not been identified or if there are no legal requirements for the establishment of such controls. The advantages of the new version of the standard can be defined as follows:

- improved risk management,
- simplified and improved access to the standard and presentation of controls,
- concern for cyber security and privacy protection,
- assistance in risk assessment and implementation of controls.

All these advantages contribute to strengthening information security and enable organizations to better manage their information resources in today’s complex and dynamic environment [1].

V. COMPARISON OF ISO CERTIFICATIONS: BOSNIA AND HERZEGOVINA IN THE REGIONAL AND WIDER CONTEXT

According to the data available on the official website of the ISO (International Standard Organization) and the report on certifications in 2023, Bosnia and Herzegovina shows modest results in the field of ISO certifications, with a total of 60 certificates. This number indicates the existence of awareness of the importance of standardization, but also the need for further development and support in the implementation of these systems. Serbia stands out in the region with a significant number of certificates, 555, Croatia records 325 and Slovenia records 164 certificates. Austria, as a developed country, has 75 certificates, while Germany leads the region with 1.563 certificates. Compared to Bosnia and Herzegovina, all the mentioned countries record a higher number of certificates, which indicates a stronger culture of standardization and greater market pressure on organizations to adhere to international standards. This analysis can serve as a basis for further research and recommendations for improving ISO 27001 certification in Bosnia and Herzegovina.

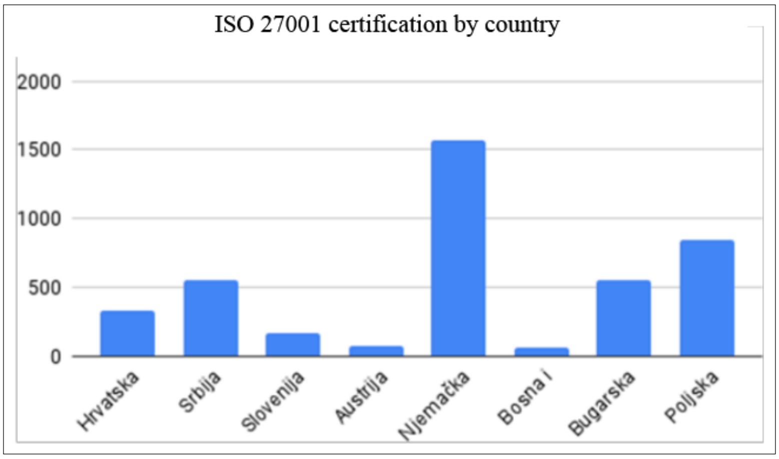

Figure 1. ISO certification by country: Bosnia and Herzegovina in the context of the region and wider

VI. ISO 27001:2013 and 2022: KEY AREAS OF APPLICATION IN 2023

Based on the data on the official page of the ISO (English International Standard Organization) in the form of results for 2023, one can notice the variability of the number of certificates awarded to different sectors. This data highlights the sectors with the most certificates, as well as those that are less represented.The Information Technology sector records 11.515 certificates, which shows the need for information security in this area. Transport, storage and communications records 1.086 certificates, which can be linked to the growth of e-commerce and the need for data protection and reliable communication systems. The financial and construction sectors record a significant number of certificates, while other sectors such as agriculture, health and education record a smaller number of certificates. This analysis shows that information technology, transport and the financial sector are the leaders in the field of ISO/IEC 27001 certification. Increasing awareness of risks and the need for data protection can also encourage organizations from less represented sectors to consider implementation and certification, as a basis for improving security practices.

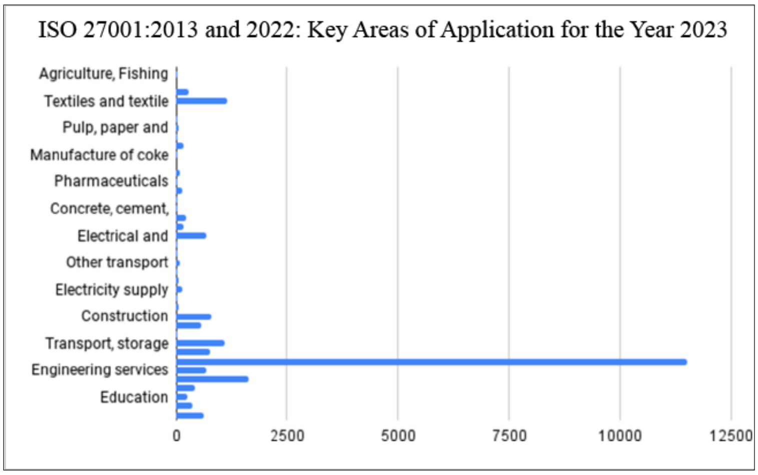

Figure 2. ISO/IEC 27001 standard - sector with the largest number of certificates in the world in 2023 (ISO Survey, 2023)

VII. IMPLEMENTATION OF THE ISO 27001:2022 STANDARD IN PUBLIC COMPANIES, INSTITUTIONS AND THE FINANCIAL SECTOR OF THE CITY OF CAZIN

As part of this research, a survey was conducted in the city of Cazin, which included public companies and institutions, government administration office, police station, IT companies and banks. The aim of the survey was to examine the level of familiarity and implementation of the ISO 27001:2022 standard for information security management, as well as to identify the main motivations and steps in the implementation process. According to the results of the survey, a significant number of organizations are not familiar with the ISO 27001:2022 standard. This data suggests the need for greater awareness of the importance of information standards and the need for their implementation.

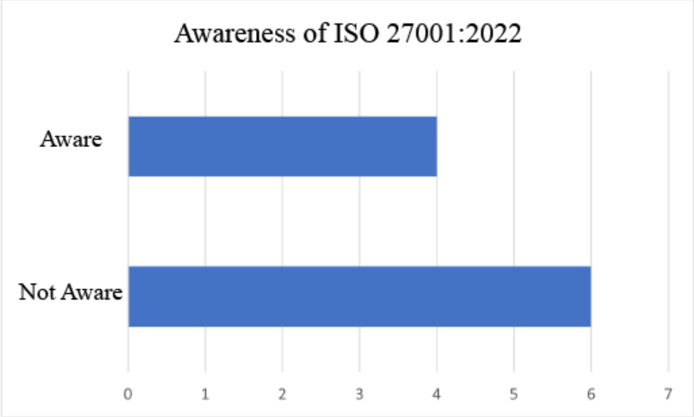

Figure 3. Awareness of the existence of the ISO 27001:2022 standard

Among organizations that have recognized the importance of the standard, the most common motivations for implementing ISO 27001:2022 include: improving information security, requirements from clients and/or partner organizations, improving business reputation, and reducing the risk of incidents.

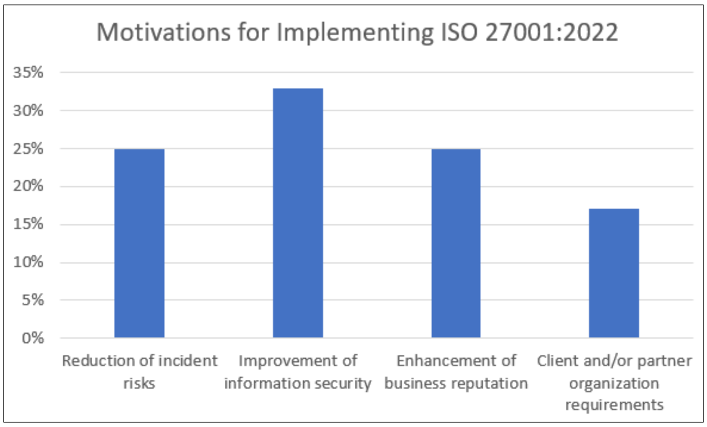

Figure 4. Motivation for implementing ISO 27001:2022 in the city of Cazin

The respondents mentioned several steps they took in the implementation process, including: planning, creating an information security policy, and training of employees.

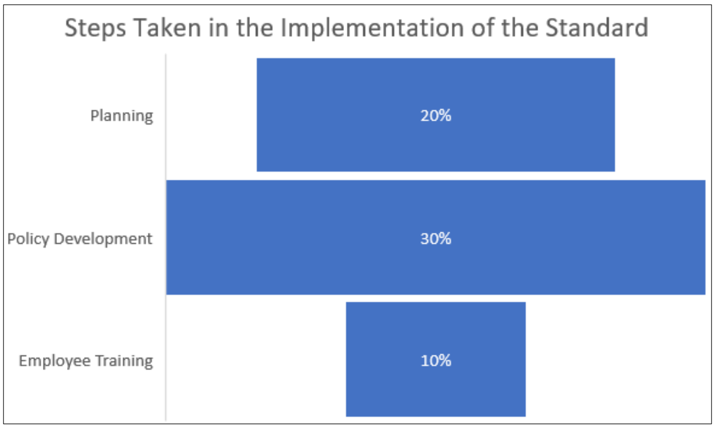

Figure 5. Steps taken in the implementation of ISO 27001:2022

Two organizations noticed moderate improvements in information security management after the implementation of the ISO 27001:2022 standard, while two organizations recorded significant improvements but also an increase in costs. It is important to note that all organizations that implemented the standard expressed their desire to further improve and expand the implementation of the ISO 27001:2022 standard, which indicates a commitment to improving information systems. Although the city of Cazin is developing, its economy still relies on small and medium-sized enterprises. Increasing the number of IT companies in Cazin would open the door for significant changes in the implementation of modern systems, including standards such as ISO 27001:2022. The IT sector, dynamic and innovative, can serve as a catalyst for the development and modernization of business in the region.

VIII. CONCLUSION

The implementation of ISO 27001:2022 in the city of Cazin represents a significant step towards improving information security, but the research results show that awareness of this standard is relatively low among organizations. Although some organizations in the city have recognized the importance of applying the standard, most respondents are only partially aware of its existence and the possibilities it offers. Those who implemented the standard recognized key benefits, such as improving security and reducing risk, while the IT sector was identified as the most important catalyst for future development and digital transformation in the region. Considering the current level of awareness, one of the main challenges is education and raising awareness of the benefits of ISO 27001:2022, especially in public companies and institutions.

Based on the conducted research, it is recommended:

1. Organization of educational workshops and seminars on the importance of the Law on Information Security in BiH.
2. Development of support strategies for organizations in the private sector to facilitate the implementation of standard.

3. Strengthening cooperation between institutions, educational institutions and the IT sector in order to improve capacities and exchange knowledge in the field of information security standards.
4. Continuously informing the public about security threats and events.

The recommendations aim to ensure that organizations in the city of Cazin recognize the importance of implementing ISO 27001:2022, and that they successfully build and maintain information security management systems that will contribute to the protection of their resources and increase the trust of clients and partner organizations.

REFERENCE

[1]. Lj. Šikman, D. Savanović, T. Latinović, „Information security in the function of corporate management of information technologies", June 2023.

[2]. Službeni glasnik BiH, br. 38/17. Available at: http://www.sluzbenilist.ba/page/akt/bM0k8gNBNCU= (accessed on: 20 October 2024)

[3]. „Prijedlozi i nacrti", [Online]. Available at: https://fmpik.gov.ba/bh/dokumenti/prijedlozi-i- nacrti.html (accessed on: 19 October 2024)

[4]. New version of the Standard ISO/IEC 27001:2022 was published on 25 October 2022, [Online]. Available at: https://issbih.ba/view-more/nova-verzija-standarda-iso-iec-27001-2022-objavljena- je-25-oktobra-2022/330 (accessed on: 18 October 2024)

[5]. „ISO/IEC 27001:2022", [Online]. Available at: https://www.iso.org/committee/54998.html?t=KomURwikWDLiuB1P1c7SjLMLEAgXOA7e mZHKGWyn8f3KQUTU3m287NxnpA3DIuxm&view=documents#section-isodocuments-top (accessed on: 20