The International Journal of Engineering and Science (IJES)
|| Volume || 14 || Issue || 1 || Pages || PP 81-87 || 2025 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Data Protection Challenges and Compliance with ISO 27001:2022 and GDPR: Guidelines for Application Development and Implementation of RFID and Biometric Systems For The Purpose Of Monitoring Working Hours

MA Nejra Mesić, Ph.D. Emina Junuz
Faculty of Information Technologies, University "Džemal Bijedić" in Mostar, Bosnia and Herzegovina
Corresponding Author: MA Nejra Mesić

ABSTRACT

The accelerated digitalization of business processes is transforming work organization and time management. The development of time-tracking technology, such as RFID and biometric systems, introduces significant changes in business process management and brings challenges concerning employee data protection compliance with legal regulations. This paper examines the challenges associated with the use of these technologies and analyzes the extent of users understanding of them. Additionally, it emphasizes the importance of aligning time-tracking systems with legal regulations, such as GDPR and the ISO 27001:2022 standard.

KEYWORDS: *digitalization, ISO 27001:2022, GDPR, data*

Date of Submission: 14-01-2025 Date of acceptance: 28-01-2025

I. INTRODUCTION

Flexible working hours and remote work, on the one hand, and working in public institutions and companies, on the other hand, make monitoring working hours a challenging task. The introduction of technologies such as RFID (Radio-Frequency Identification) and biometrics is becoming more and more desirable, not only in the private sector, but also in public institutions. In addition to reducing administrative work, automatic monitoring of employee attendance enables accurate recording of working hours, which can provide valuable insights into employee behavior and identify potential abuses, with the aim of improving operations and making informed decisions based on the collected data. However, employers face challenges related to data protection and compliance with regulations such as GDPR (General Data Protection Regulation) and ISO 27001:2022. This paper investigates the key aspects that employers and public institutions should take into account when implementing a system for monitoring working hours, in order to ensure the protection of personal data and improve business efficiency.

II. OBJECTIVES AND METHODOLOGY

The aim of this research is multifaceted and includes several key aspects. Firstly, to provide employers with guidance on the factors they should consider when implementing a time tracking system. Secondly, to strive towards the popularization of this topic, emphasizing the numerous benefits that automated monitoring of working hours brings, namely: reduction of bias, increase in productivity, creation of new business opportunities and improvement of economic efficiency. The research methodology includes literature analysis, implementation of the system in practice, and surveying of employees in order to define guidelines for the applicability of the system in practice.

III. RFID TECHNOLOGY

RFID (Radio-Frequency Identification) is a wireless form of communication based on radio waves that is used to identify objects, collect information, process and enter information into systems. The basic principle of RFID technology is a radio frequency signal, or rather its transmission via an antenna from the sender to the recipient. The two basic components of an RFID transponder are a microchip and an antenna, which are most often sealed in a housing resistant to environmental influences. The microchip contains a radio receiver, a radio modulator for sending responses to the reader, control logic, memory, and a power management system. Transponders can be divided into groups according to: power supply method, programming capabilities, frequencies used, and physical design. According to the power supply method, transponders are divided into: passive, partially active, and active. According to the programming capabilities, transponders are divided into:

- read-only transponders (in the production process they receive a unique serial number that cannot be changed),
- transponders that enable one-time programming (data written for the first time remain permanently on the responder),
- transponders with the possibility of multiple programming (they usually have a unique and permanent serial number to which recorded data is added, and are used in more demanding applications).

According to the frequencies used, they are divided into:

- low frequencies (around 125 kHz),
- high frequencies (13.56 MHz),
- ultra-high frequencies (UHF- 860 to 960 MHz) and
- microwave frequencies (2.45 GHz).

As for the physical implementation, RFID tags, RFID stickers and RFID printed circuit boards are used. The range of RFID transponder signals is related to the frequency used, but also to the type of power supply.Ease of use and ubiquity are great advantages of RFID systems, but also sources of their vulnerabilities. The main problem with RFID systems is privacy protection because transponders respond to a reader's query by sending information that can be sensitive and that can allow an unauthorized user to compromise the system [1].

IV. BIOMETRICS

Biometrics is a set of automated methods for unique recognition of people, based on one or more of their physical and behavioral characteristics. In information technology, biometric authentication refers to technologies that measure and analyze physical (fingerprints, cornea, facial recognition, etc.) and behavioral characteristics (handwriting, gait, etc.). Biometrics is becoming an increasingly common form of authentication in various spheres of life and has been a part of reality for a long time. The great advantage of biometrics is over codes. Passwords can be lost or discovered by attackers. Therefore, wherever possible, biometric methods are implemented to access the local network. Biometrics is also used in monitoring the working hours of employees. The use of RFID cards or codes allows one employee to record the presence of another employee, while biometrics prevents this. However, for applications of biometrics, it is necessary to have specialized devices that will process the obtained data [2].As part of the implementation of the working hours' record system in the N.N organization, a terminal that supports both RFID and biometric technologies was used. These options offer different advantages and disadvantages that have been demonstrated during use. RFID functionality enables employees to quickly and easily record working hours via cards, which contributes to the efficiency of the process. However, there are security challenges, including the possibility of cards being lost or damaged. Biometric functionality provides accuracy and security in employee identification, reducing the possibility of identity abuse. However, higher implementation costs and privacy concerns present significant drawbacks.
Table 1 shows the advantages and disadvantages of the mentioned technologies.

	Biometrics	**RFID**
Accuracy	High accuracy in identification	Accuracy depends on the quality of the marking
Security	High level of security	Lower level of security
Uniqueness	Each person has unique biometric characteristics, which reduces the risk of identification errors.	Labels may be duplicated which may affect accuracy
User experience	Quick identification, with or without physical contact	Quick identification and easy use
Costs	More expensive implementation costs	Lower implementation costs, higher accessibility
Privacy	Special category of data; processing in exceptional situations	Less concern for privacy, but high possibility of misuse
Access	Possible technical difficulties in case of health problems	Loss or damage of the tag prevents access to the system
Maintenance	Regular maintenance required	Regular checking and timely replacement of tags (cards)

Table 1. Biometrics vs. RFID: Advantages and disadvantages

V. DATA TRANSFER AND PROCESSING IN WORKING HOURS MONITORING SYSTEMS: CHALLENGES AND REGULATIONS

In modern business, time tracking applications are essential for optimizing human resource management and improving work efficiency. However, the use of such systems brings with it significant challenges regarding the protection of employees' personal data. At the moment when employees log in and log out of the workplace, their personal data is collected and processed, including name, surname, time of arrival and departure, and location data. This data is stored in a database, which increases the need for appropriate protection mechanisms. Data transfer and processing takes place when logging into the system, when different systems communicate with each other, and during data analysis with the aim of identifying patterns of employee behavior. Because of these processes, compliance with legislation such as the General Data Protection Regulation and standards such as ISO 27001:2022 becomes mandatory. The General Data Protection Regulation presents strict requirements for the protection of personal data defining how, when and why this data can be processed, while ISO 27001:2022 provides a framework for managing system security. Following these regulations in the process of developing an application for tracking working hours, apart from being a legal obligation, is a key element for building employee trust in the system itself because it minimizes the risks to which all data are exposed [3].

VI. GUIDELINES FOR THE APPLICATION OF THE RELEVANT ARTICLES OF THE GENERAL DATA PROTECTION REGULATION (GDPR) IN THE DEEVELOPMENT, MAINTENANCE AND USE OF THE WORKING HOURS MONITORING APPLICATION

The General Data Protection Regulation is a European regulation on the protection of personal data that entered into force on May 25, 2018 [4]. The general data protection regulation establishes detailed requirements for organizations regarding the collection of personal data, their storage and management of personal data. They apply to European organizations that process personal data of individuals in the European Union and organizations outside the European Union that target people living in the European Union. The Law on the Protection of Personal Data in Bosnia and Herzegovina is not identical to the GDPR, but it contains similarities with the GDPR, such as the rights of data subjects and the obligations of data controllers. Bosnia and Herzegovina, as a candidate country for membership in the European Union, is not legally obliged to implement the GDPR. However, due to harmonization with European standards, more and more organizations in Bosnia and Herzegovina apply GDPR principles, especially those that process the data of citizens of the European Union. In an application for tracking working hours that includes the use of biometrics and RFID technology, it is necessary to ensure compliance with the General Regulation on the Protection of Personal Data due to the processing of personal data of employees, because, at the time of developing the system for commercial purposes, it is not possible to determine in advance the scope of use and the users who will access the system. Key Articles of the General Data Protection Regulation relevant for this type of application are the following [5]:

Article 5 Principles of personal data processing
This article defines the basic principles of data processing, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality. This article establishes basic guidelines for the responsible handling of personal data.
Article 6 Legality of processing
Article 6 states the conditions under which the processing of personal data is legal, such as the consent of the data subject, execution of contracts, compliance with legal obligations, protection of vital interests, tasks of public interest and legitimate interests of the controller.
Article 7 Conditions for giving consent
This article lays down the rules on how and when consent must be given, with an emphasis on voluntariness and the possibility of withdrawing consent. Consent must be informed and unambiguous.
Article 9 Processing of special categories of data
Special categories of personal data are processed, such as racial or ethnic origin, political opinions, biometric data, religious beliefs, health data, and it is stipulated that the processing of this data is prohibited, except in specific situations.
Article 13 Information provided when collecting personal data
Article 13 requires the controller to provide transparent information to data subjects when collecting their data, including the purpose of the processing, the identity of the data controller and the data subject's rights.
Article 32 Security of processing
The Article defines the security measures that the controller must take to protect personal data, including encryption, pseudonymization and securing the system against unauthorized access or accidental loss.

Article 35 Data Protection Impact Assessment (DPIA)
A DPIA is mandatory in cases where there is a high risk to the rights and freedoms of individuals. This article requires the controller to assess the impact of the planned processing operations on data protection.

Article 83 Fines
This article specifies the fines that may be imposed for violations of the GDPR, depending on the seriousness and nature of the violation. The fines can be significant, which underlines the importance of complying with the GDPR rules.

VII. RELEVANT CONTROLS OF ISO 27001:2022

The ISO/IEC 27001 standard is one of the most widespread and accepted standards for information security worldwide [6]. ISO/IEC 27001:2022, as the third edition of the 27001 standard, was published on October 25, 2022 with the aim of solving global challenges in cyber security [7]. When developing and implementing a time tracking application that uses RFID technology and biometrics, the following ISO 27001:2022 data security controls are essential, especially in the context of sensitive personal data:

A 5.1 Information security policies
Control: Defining and regularly updating information security policies that include rules for data protection within the application. Control role: Establishing clear guidelines and rules for data handling within the time tracking application.

A 9.1 Access management
Control: Limiting access to employee data to authorized users only, using access controls such as username and password, two-factor authentication, or biometric identification. Control role: This control ensures that only authorized personnel can access sensitive employee data, such as biometrics, thus reducing the risk of unauthorized access.

A 10.1 Cryptographic controls
Control: Use of encryption to protect data in transit and in storage, especially for biometric data. Control role: Reduces the risk of unauthorized access and abuse in case of data leakage or system attack.

A 12.1 Safety of operations
Control: Ensuring safe operating procedures including regular monitoring and supervision of systems that process personal data. Control role: Enables continuous monitoring of application operation and timely detection of potential security incidents.

A 12.6 Management of Technical Vulnerabilities
Control: Regularly identifying and managing technical vulnerabilities in the software and hardware used by the application. Control role: Ensures timely detection and remediation of vulnerabilities to reduce the risk of attacks.

A 13.2 Security of Communications
Control: Protecting information transmitted over networks, including the use of encryption and VPNs. Control role: Security of communications between client devices and server infrastructure. It ensures that data is not intercepted or altered during transmission.

A 14.2 Security of system development
Control: Application of security measures throughout the application development life cycle, from design to implementation and testing. Control role: This control ensures that security measures are integrated into the development process, reducing the possibility of security vulnerabilities in the application.

A 16.1 Management of information security incidents
Control: Defining procedures for reporting, responding, and recovering from security incidents, including data leaks or application attacks. Role of control: Enables quick and efficient response to incidents, minimizing damage and risk to employee data.

A 18.1 Compliance with legal and regulatory requirements
Control: Ensuring that the application complies with applicable data protection laws, such as GDPR, and that changes in laws are monitored. Control role: Ensures that all aspects of data processing within the application are compliant with legal frameworks, reducing the risk of fines or legal consequences [8].Biometric data and data collected with RFID technology are among sensitive personal data, which means that any inadequate protection of this data can result in serious security incidents and legal consequences. The implementation of the ISO 27001:2022 standard and the listed controls helps to ensure the integrity, confidentiality and availability of data and enables the organization to fulfill legal obligations and reduce the risk arising from sensitive data.

VIII. ANALYSIS OF THE RESEARCH RESULTS OF THE SURVEY

As part of research related to the challenges of data protection and working hours monitoring, a survey was conducted among employees of various companies and institutions. The objective of the survey was to collect relevant information that will enable a better understanding of users' perceptions and experiences regarding current working hours monitoring systems, as well as the degree of familiarity with relevant data protection standards, such as ISO 27001:2022 and legal regulations on data protection. The survey included fifty-one participants, and the questions related to several key aspects, including the importance of monitoring working hours, challenges in implementation, as well as views on technical and legal principles of data protection. In addition, awareness of technologies such as RFID and biometrics, as well as expectations from future systems for monitoring working hours, was examined. The results of this survey will provide insight into the current attitudes and perceptions of employees, which can enable informed decisions to be made regarding the improvement of the working hours tracking system and data protection within the organization. The majority of respondents, 78.4%, consider the monitoring of working hours important, which emphasizes the need to monitor the activities of employees and respect work discipline. Figure 1 indicates the need for reliable systems that ensure accuracy in monitoring and facilitate the management of working hours.

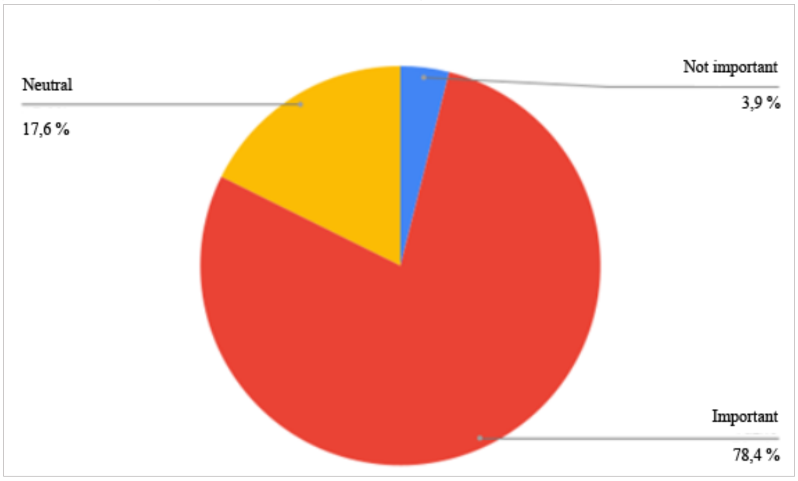

Figure 1. The Importance of Tracking Working Hours

From the results on knowledge of ISO 27001:2022, it can be concluded that the majority of respondents are not familiar with the mentioned standard, as shown in Figure 2, which indicates the need for continuous training in order to strengthen the safety culture of employees.

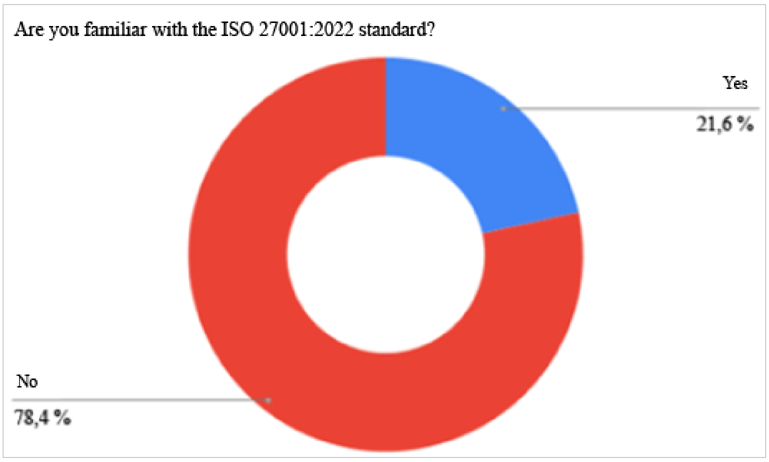

Figure 2. Degree of knowledge of the ISO 27001:2022 security standard

Figure 3 shows an assessment of current challenges related to privacy and data protection. This result justifies the implementation of security measures.

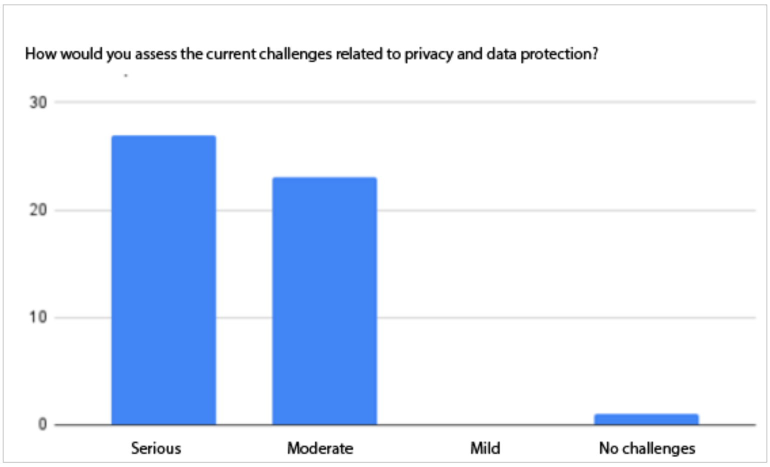

Figure 3. Challenges related to privacy and data protection

The majority of respondents are not familiar with RFID technology, which is one of the causes of distrust in systems for monitoring records of employee activities. Figure 4 indicates the need to educate employees with the aim of gaining trust in the system.

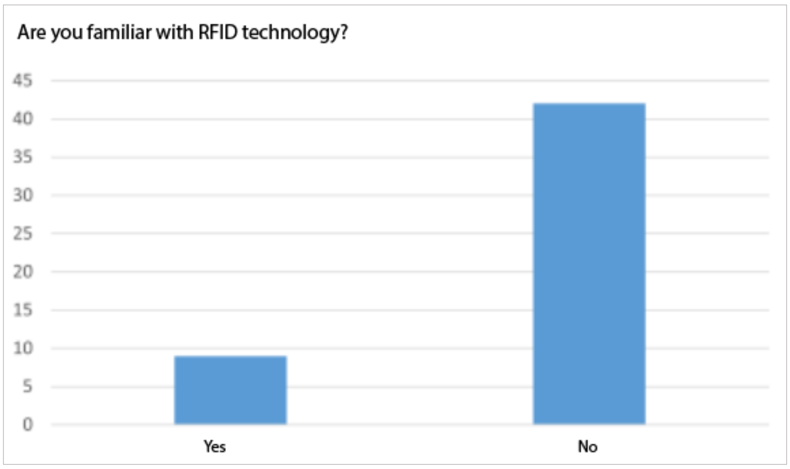

Figure 4. Knowledge of RFID technology

Figure 5 shows the preferences regarding the time tracking platform. Respondents expressed the need for a solution that enables monitoring of working hours via web and mobile applications. This preference suggests the importance of accessibility and flexibility in the use of a time tracking system, which provides an adaptable way of recording work engagement. The implementation of web and mobile applications can contribute to greater system adoption and user satisfaction, as it enables access to monitoring functions in real time from different work environments.

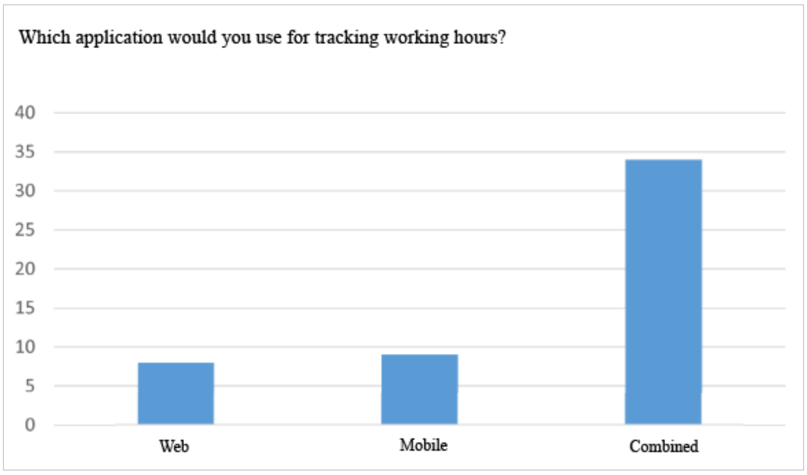

Figure 5. Mobile vs. web application

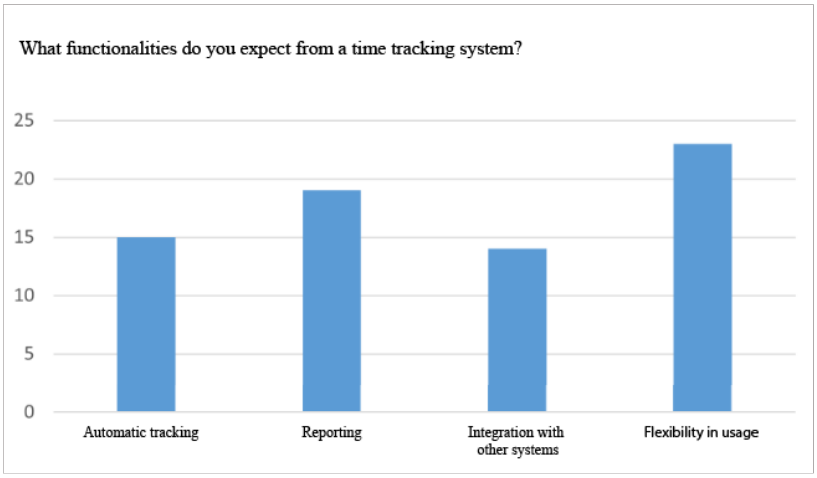

Figure 6. Expected functionalities of the working hours monitoring system

Figure 6 shows the functionalities expected by the user from the working hours monitoring system, namely: automatic monitoring and report generation, integration with other systems (e.g. ERP) and flexibility in use. Such functionalities enable more efficient collection and analysis of data, reduce manual work and facilitate informed decisions regarding working time management. Flexibility in using the application, both through the web and through the mobile version, allows employees easy and quick access to the system, regardless of whether they are in the office, in the field or working from home. These characteristics can positively influence the adoption of systems in organizations as well as the accuracy and timeliness of data, which are vital to efficient business operations.

IX. CONCLUSION

The introduction of RFID and biometric systems for monitoring working hours brings a number of benefits, including greater efficiency and precision in monitoring the presence of employees, but at the same time poses challenges in terms of privacy protection and ethical application of the technology. The research presented in this paper indicates the need for a comprehensive understanding of the benefits and potential risks of these technologies among employers and employees, as well as the importance of respecting the legal frameworks that regulate this area, such as state laws, GDPR and the ISO 27001:2002 standard. The results indicate that transparent communication, employee training and clearly defined rules and policies on data collection and processing can significantly reduce resistance to the use of these systems. By complying with legal regulations and implementing best practices in privacy protection, organizations can achieve a balance between increasing productivity and preserving employee rights. Through the responsible use of these technologies, it is possible to ensure business efficiency that respects privacy rights and ethical standards.

REFERENCES

[1]. RFID identification. Available at: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-01-179.pdf (accessed on: 29 September 2024)

[2]. Biometrics. Available at: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-11-167.pdf (accessed on: 29 September 2024)

[3]. Oral interview with an employee of SYSTECH, [14 October 2024]. Topic: The Attendo system for tracking working hours and challenges related to the protection of personal data.

[4]. General Data Protection Regulation (GDPR). Available at: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_hr.htm (accessed on: 1 October 2024)

[5]. GDPR – Info portal. Available at: https://gdpr-info.eu/ (accessed on: 1 September 2024)

[6]. Management of Enterprise Cyber Security: A Review of ISO/IEC 27001:2022.

[7]. Institut za standarde i sigurnost BiH. 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)

[8]. Institut za standarde i sigurnost. Prezentacija o sigurnosnom standardu ISO 27001:2022.