مجلة المجد العلمية المتطورة العدد (5) المجلد (5) تموز 2025

إنشاء نظام إدارة أمن المعلومات للمؤسسات

creation of an information security management system for organizations

مجد ثائر حامد رشيدات، تخصص/ أمن سيبراني، جامعة اربد الأهلية، اربد، فلسطين

تاريخ الاستلام: ٢٠٢٥/٦/٩ تاريخ القبول: ٢٠٢٥ /٦/١٩ تاريخ النشر: ٢٠٢٥/٧/١٥

creation of an information security management system for organizations

الملخص:

نظام إدارة أمن المعلومات (ISMS) هو منهجية منظمة لإدارة وحماية المعلومات الحساسة للشركات والمؤسسات، لضمان توافرها وسلامتها مع الحفاظ على بيئة معلومات آمنة. يعتمد هذا النهج على مجموعة واسعة من الضوابط والإجراءات لإدارة البيانات الحساسة للمؤسسة بطريقة منظمة. يهدف تطبيق نظام إدارة أمن المعلومات (ISMS) إلى التخفيف من العديد من التهديدات والتحديات في الشركات والمؤسسات الخاصة والحكومية لحماية المعلومات. يمكن لثقافة أمن المعلومات القوية أن تقلل من التهديدات وبالتالي تقلل من خروقات البيانات أو الحوادث داخل المؤسسات. توفر هذه الدراسة فهمًا شاملاً لنظام إدارة أمن المعلومات (ISMS). تناقش هذه الورقة العديد من الأمثلة وأفضل الطرق لإنشاء نظام إدارة أمن المعلومات (ISMS) من خلال نهج متعدد الأساليب، بما في ذلك مراجعة الأدبيات والدراسات الحالية. تسلط النتائج الضوء على أهمية دعم الإدارة العليا للمؤسسة وتدريب وتوعية الموظفين لتحقيق نظام إدارة أمن معلومات قوي (ISMS). الكلمات المفتاحية: إنشاء نظام إدارة أمن المعلومات للمؤسسات.

الكلمات المفتاحية: إنشاء نظام إدارة أمن المعلومات للمؤسسات.

Abstract:

An Information Security Management System (ISMS) is a structured methodology for managing and protecting sensitive information for businesses and organizations, to ensure its availability and integrity while maintaining a secure information environment. This approach relies on a wide range of controls and procedures to manage an organization's sensitive data in an organized manner. Implementing an Information Security Management System (ISMS) aims to mitigate many threats and challenges in companies, and private and governmental institutions to protect information. A strong information security culture can reduce threats and thus reduce data breaches or incidents within organizations. this study provides a complete understanding of the Information Security Management System (ISMS). This paper discusses several examples and the best ways to create an Information Security Management System (ISMS) through a multi-method approach, including a review of the literature and existing studies. The results highlight the importance of supporting the organization's senior management and training and awareness of employees to achieve a strong information security management system (ISMS).

Keywords: creation of an information security management system for organizations.

.

Introduction

Nowadays, with rapid technological advancement, the world has become completely digitally interconnected, as information security constitutes the basic element for the organizational success of institutions and companies. Maintaining the security and integrity of information is one of the biggest electronic threats, obstacles, and increasing vulnerabilities facing organizations. As a result, it has become important to come up with strong solutions and measures for information security and protection to enable organizations to operate safely and with high efficiency. information security refers to protecting information against a wide range of threats such as electronic attacks, data breaches, and natural disasters through a wide range of different controls and measures [6]. Therefore, the Information Security Management System (ISMS) provides a systematic framework that has been designed to manage the organization's information security risks. It constitutes all policies, procedures, resources, and activities related to the organization. It is monitored, developed, and continuously improved to protect information [5]. In previous studies, information security has received the attention of researchers. The issue of information security has been a source of concern for banks and various institutions [1,9]. Therefore, this calls for developing a system to effectively protect information. Researchers have noted the need to create a flexible management system for institutions that can be integrated with other departments [8]. The information security management system was established based on ISO/IEC 27001 standards, which is an international standard that provides a series of procedures that provide an understanding of the organization, determine its needs, address risks, and commit to maintaining the system, providing resources for the system [2]. Researchers worked on creating an information security management system (ISMS) in universities based on the ISO/IEC 27001 standard and the COBIT management framework [7]. This research delves into the establishment of an information security management system (ISMS) designed in a private environment in universities, with the importance of highlighting the importance of aligning security procedures with business objectives. The study targets the basic components of an effective information security management system (ISMS), including error checking, incident response, and information protection. Through discovering best practices and case studies, therefore, establishing an information security management system (ISMS) is not just a technical goal but a strategic goal that requires a comprehensive approach, concerned with people in institutions, processes, and technology. This research aims to provide a guide for universities. And educational institutions that aim to implement their own information security management systems.

2. Related works

A great deal of ongoing research focuses on the concept of an Information Security Management System (ISMS), aiming to protect important information in educational and commercial institutions by ensuring its confidentiality, integrity, and availability at all times. Some of these studies specialize in specific areas, while others cover multiple domains [1,5,6,7,8,9]. Researchers have highlighted the importance of creating a new administrative system that is flexible and adaptable to different environments [8]. Researchers [1] suggested that banks and various institutions should pay significant attention to maintaining data security. Researchers [6] emphasized the importance of fostering an ideal information security culture,

which is based on achieving mutual trust and integrity by protecting institutional information. Researchers [9] focused on the importance of detecting threats and intrusions facing organizations. According to researchers [5], effective information security management is the foundation for the success of organizations across various sectors. Researchers [7] observed that the increasing use of information technology in certain businesses leads to information security issues, resulting in damage to resources. This necessity led to the development of a sustainable ISMS model to mitigate risks to information across various institutions. The researchers implemented this model in the university sector. research in the field of Information Security Management Systems (ISMS) highlights the important role that (ISMS) plays in enhancing security in various sectors and the important role it provides organizations in maintaining compliance with laws, preserving sensitive information, and avoiding legal action. In addition to the major role that the organization plays in training employees and those working on the system to be aware of security policies, general threats, and their role in protecting this information. This provides security awareness by completely reducing human errors. In addition, international cooperation in the field of information security provides a valuable opportunity for businesses and educational institutions to learn from each other, continuously improve security methods, and work to improve them in the future.

3. Methodology

This study focuses on developing a high-quality security plan aimed at protecting various types of systems, including commercial, economic, and private systems. The researchers have outlined a comprehensive approach to securing educational computing environments. As institutions face growing risks due to the rapid advancement of technology, the implementation of modern information technologies has increased security vulnerabilities in the workplace. Regardless of their size, objectives, or sectors, institutions rely heavily on information systems for daily operations. These systems not only connect employees and departments internally but also link the institution to external entities such as government agencies, customers, and suppliers. The widespread use of these systems has led to the generation of vast amounts of both structured and unstructured data, which are foundational to the institution’s operations. Given the critical nature of these processes, 'security protection of information systems' emerges as a fundamental concern, particularly within higher education institutions. Ensuring the security of these systems is a complex and broad issue, where the only certainty is that without robust security measures, their integrity and efficiency cannot be maintained. Currently, there are many organizations around the world interested in obtaining accreditation certificates according to the ISO/IEC 27001 standard, but some organizations have chosen to certify their information systems based on the ISO/IEC 27001:2013 standard. While obtaining these certifications is voluntary, it is increasingly becoming a critical requirement in the business sector. ISO/IEC 27001:2013 is widely recognized as the foundational global standard for information security management [2]. A survey carried out in 2020 presented several results, the most important of which was that the largest number of certificates was obtained in China (12,403), followed by Japan (5,645), and finally the United Kingdom (3,327). In the field of education, Greece topped the list.

In this section, we explain in detail the most important standard (ISO/IEC 27001:2013) used in business, and the rules that govern information technology COBIT (Control Objectives for Information and Related Technology), methodological framework, Case study.

3.1. ISO/IEC 27001:2013

The ISO/IEC 27001:2013 standard was created by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which are two global organizations responsible for designing, setting, and developing international standards in various sectors and industries. The origin of this global standard goes back to the British standard BS. 7799, this standard was first developed in 1995 by the British Standards Institute (BSI). BS 7799 provided the basic rules for information security management. The success of the British Standard can be attributed to the improvements and developments made by the ISO and IEC bodies. In 2000, the ISO/IEC 27001:2013 standard represents an evolution that reflects technological and digital advances and the increasing complexity of information security risks [2]. The concept of ISO/IEC 27001:2013 can be summarized as a recognized global standard in the field of information protection that aims to provide a complete and comprehensive framework and methodology through which organizations' information assets can be protected by implementing comprehensive security controls. The standard includes a wide set of standards that work to establish and maintain Information Security Management (ISMS) in order to reduce and eliminate the risks associated with information security. This ensures that organizations protect sensitive and important information in the company from exposure to threats, for example, cyber-attacks, theft of information, and the ability to gain unauthorized access to the system. This standard requires organizations to evaluate and monitor security risks on a regular basis and to determine appropriate controls to reduce these risks. This standard also includes a large number of comprehensive procedures that cover the largest possible number of areas such as physical security, controlling access to the system, Coding, incident management, and business continuity. This standard encourages the maintenance and continuous improvement of the information security management system to ensure its efficiency in responding to and confronting threats and developments in different business environments. Obtaining ISO/IEC 27001:2013 certification helps organizations and companies in various fields enhance their security, manage and address risks, and improve their reputation in the business world, particularly against competitive companies, by demonstrating their commitment to and compliance with the highest and most important information security standards. In fact, the ISO/IEC 27001 standard does not actually describe specific controls for all organizations. This is because different organizations and institutions in their fields, such as banks and universities, have different needs for the level of security and their use of the controls provided by the standard. Organizations that adopt this standard can choose what suits them and what will be applied to the organization. The ISO standard provides 114 safety controls and 14 safety areas, which are listed in Figure 1 [3].

Figure 1. Security controls ISO/IEC

This ISO/IEC 27001:2013 standard provides the possibility to create and design security controls according to the needs and scope of the organization. Rather than developing a single solution for all organizations, the standard provides a flexible framework that can adapt to the needs and requirements of different organizations.

3.2. COBIT

COBIT (Control Objectives for Information and Related Technology) is a special framework in business that is characterized by comprehensiveness and integration. Those responsible for developing this framework are ISACA (Information Systems Audit and Control Association) aiming to help institutions and commercial companies manage and control their information technology (IT) environments. COBIT was originally created in 1996. This framework was created to fill gaps, technical problems, business risks, and control requirements, thus providing the widest possible set of practices and services for IT management. COBIT's methodology and services have evolved to address the increasing problems facing IT systems, and the rapid development witnessed by the technical revolution in the world. The framework provides a structured and integrated approach for IT organizations to work to reduce risks, improve the decision-making process within the organization, and verify that IT operations support and improve business objectives. The COBIT framework went through a number of stages in its manufacture. The main goal of developing it was to meet business needs through monitoring information technology within organizations. The first edition focused on IT control objectives and provided advice to ensure that IT systems are compatible with business objectives. The COBIT framework has evolved over the years to become more flexible and adaptable to the problems facing organizations. Therefore, the latest edition of COBIT was (COBIT 2019) which was released. Figure 2 [4] shows the time projection of the development of the COBIT working framework

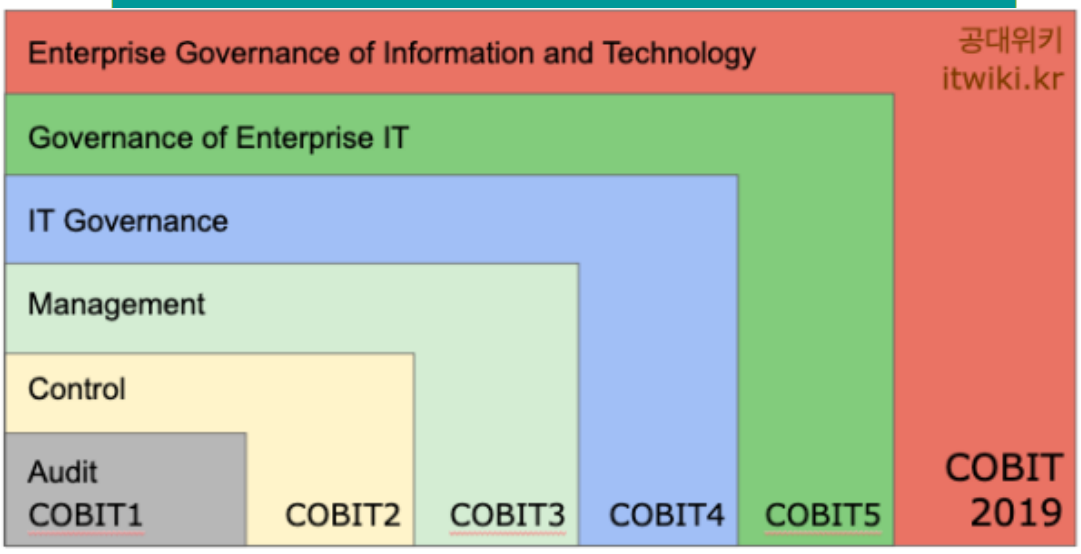


Figure 2. Time projection of the COBIT control frame development [4]

Released in 2018, this modern version reflects modern work environments and work requirements. It offers a more flexible framework, new and developed processes, and works to integrate modern technologies and practices with each other. Its main goal is to make organizations work to achieve their goals while reducing and managing risks while adhering to laws and regulations. The COBIT framework remains an important tool for organizations that aim to achieve effective and complete management of their IT environments, adapt to changes in technology, and work to achieve and implement their most important strategic goals.

3.3. Methodological framework

The researchers in [7] focused on the necessity of having a sustainable information security management system (ISMS) within higher education institutions through an organized methodology that contains a number of different levels. Although these levels are diverse and numerous in context and application in general, they are all measured to represent the organizational state of the system being measured. These typically consist of five to six levels of development, implementation, and improvement, depending on the management used. Figure 3[7] shows the framework that the researchers used in the study.

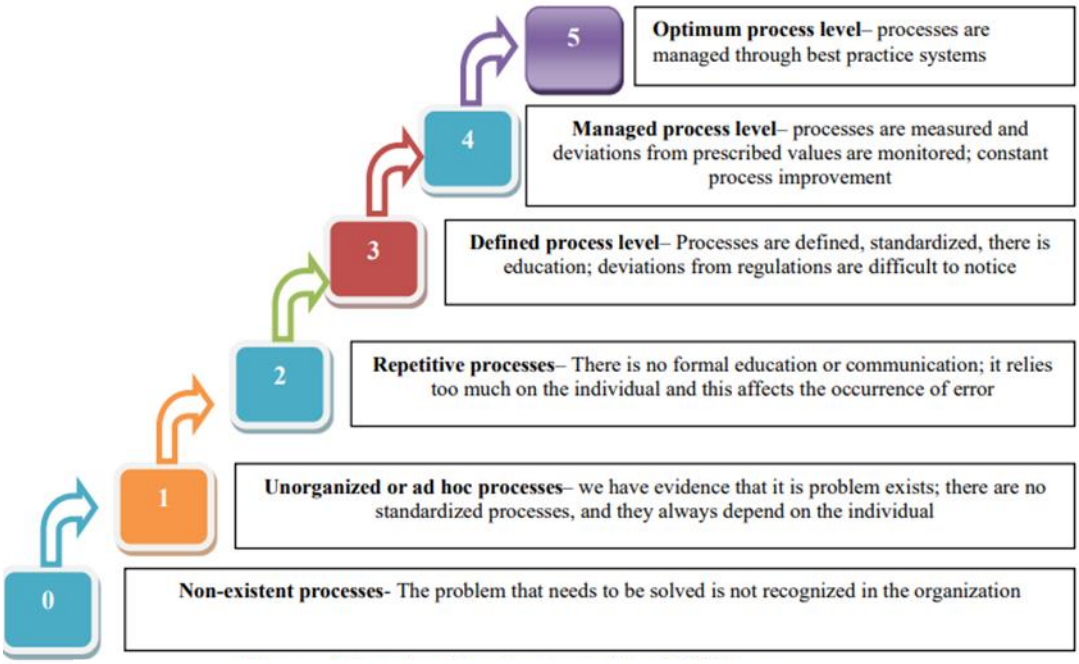


Figure 4. non−existent processes.

These levels provide a precisely structured framework for organizations. Each level of this methodology is concerned with a specific task.

Figure 4 shows the basic phase 0 of the methodology is known as (non-existent processes). This stage is based on identifying non-existent processes, when the organization is unable to identify or recognize the problem is due to the lack of awareness or understanding necessary to address the problem. The lack of awareness in the organization is due to the lack of knowledge of the potential problem, and this is due to insufficient data, communication problems, or a lack of monitoring tools. The lack or absence of processes is due to the lack of recognition of the problem, if there are no processes in place to address it or reduce it. The potential consequences facing the organization in the absence of recognition of the problem may lead to the continuation and magnification of the problem. This problem can be solved by increasing awareness and promoting a culture of continuous improvement. Awareness is increased by implementing mechanisms and methods to identify potential problems and address them before they occur, such as development methods and regular and continuous auditing. Enhancing awareness within the organization by developing an environment in which employees can discuss problems. and Providing solutions openly.

Figure 5 shows the first level of methodology involves unorganized or ad hoc processes. This level highlights the disorganized processes within the organization and reveals several reasons behind these issues, the most significant being the heavy reliance on individuals. This means that the knowledge required to execute processes may be limited to a few employees within the organization, while the rest of the staff may not have the full understanding needed to carry out these operations. Consequently, if one of these key individuals is absent, it can lead to disruptions or stoppages in the system, potentially causing losses for the organization.

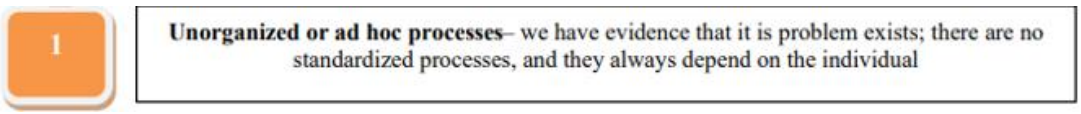


Figure 5. unorganized or ad hoc processes.

Another contributing factor is the lack of standardized procedures. This refers to the absence of a clear, organization-wide plan for how tasks should be performed, which results in inconsistent quality levels. The proposed solutions include training individuals in standardized processes and developing a unified plan for employees to follow in task execution.

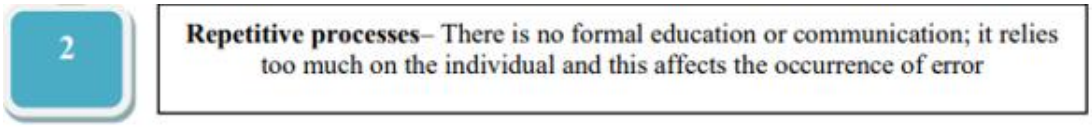


Figure 6. Repetitive processes.

Figure 6 shows the second stage of the methodology describes Repetitive processes. One of the most important reasons that lead to repetitive operations within the institution is the lack of effective communication between employees. This is due to the institution not providing effective and organized training for employees on how to perform repetitive tasks. Not providing resources so that employees can refer to them when performing repetitive tasks better. Another reason is that processes depend on the efforts of individuals in solving them separately from each other. Each employee can perform the same task in a different way, and this causes problems and errors due to misunderstanding or forgetfulness. Over time, the accumulation of these small errors can lead to major problems for the organization in the future. These mistakes can be avoided through training programs for employees and establishing effective and direct communication between employees to exchange experiences.

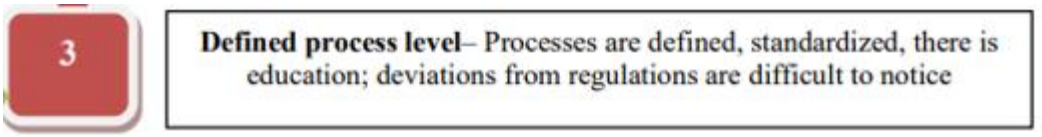


Figure 7. Repetitive processes.

Figure 7 shows the third stage of the methodology focuses on the Defined process level. One of the most important aspects of this stage is providing unified and clearly defined processes. This means that the organization has established detailed procedures that all employees must follow when performing tasks within the organization. The availability of these unified processes represents one of the most important procedures that is extremely important for the organization because it includes a kind of integration, consistency, and reliability in the performance of operations. However, it is one of the most important problems that This stage faces the inability to detect deviations during the implementation of this stage. This challenge most often stems from the lack of strong detection and monitoring mechanisms within the organization to monitor and address these deviations. One of the reasons that lead to these deviations may be the employees' feeling of being highly dependent and unsure of the implementation of tasks. Therefore, they cause unnoticed deviations that lead to inefficient performance or unnoticed errors. Among the solutions that help to avoid these deviations, it is necessary for the institution to Continuously monitor

employees and provide ongoing training to encourage open communication between employees.

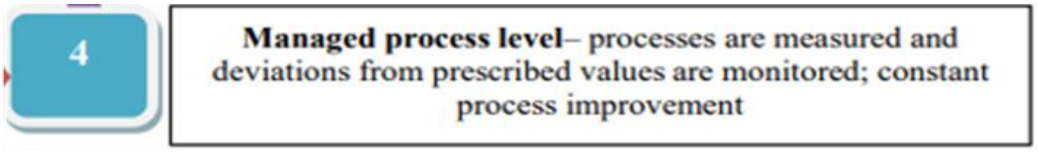


Figure 8. Managed process level.

Figure 8 shows the fourth stage of the methodology describing the Managed process level. The most important key points at this stage are that processes are measured through the application of customized and specific metrics and key performance indicators (KPIs) to track process performance. However, the organization may face deviations due to the lack of strong mechanisms to measure processes correctly and specifically, or a failure may occur in the implementation is the result of a problem in the collected data. In addition, one of the most effective aspects of this stage is the focus on continuous improvement of the process. Effective improvement requires the organization to make continuous and periodic improvements, determine the extent of these improvements, and work to implement these improvements and changes. To avoid deficiencies in this stage, work can be done to establish comprehensive monitoring systems. Encouraging a culture of continuous improvement helps maintain a high level of quality and efficiency.

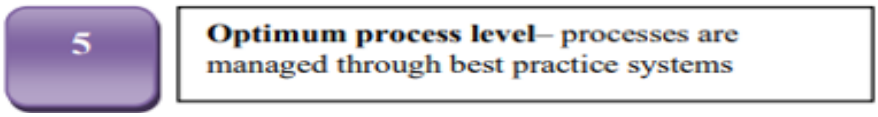


Figure 9. Optimum process-level.

Figure 9 shows the fifth and final stage of the Optimum process-level methodology. This stage is characterized by the best practices used by the organization, which are the most effective and efficient methods in the industry to manage its operations. The organization's best practices were developed through experience, continuous research, and comparison with other organizations. One of the most important features of this stage is high reliability, through the use of best practices and methods and providing results with high efficiency. The stage is also characterized by competitiveness, and this is due to the ability of institutions operating at this level to provide products and services with high efficiency greater than their competitors in the market. The advantage of reducing risks is that the organization follows the best ways to minimize problems.

3.4. Case study

In the presented case study, the researchers focused on creating a sustainable ISMS system that was applied in higher education institutions and universities in particular. They were interested in collecting the model at several levels, represented by five levels. The figure10 shows the levels that the researchers worked on. Work was done on all levels to bring

together the various elements of the system. These levels are interconnected with each other and work in an integrated manner to achieve maximum management of information security. Each level in this user framework plays an important role within the organization, which ensures the integration of all levels to achieve the best information security within various institutions.

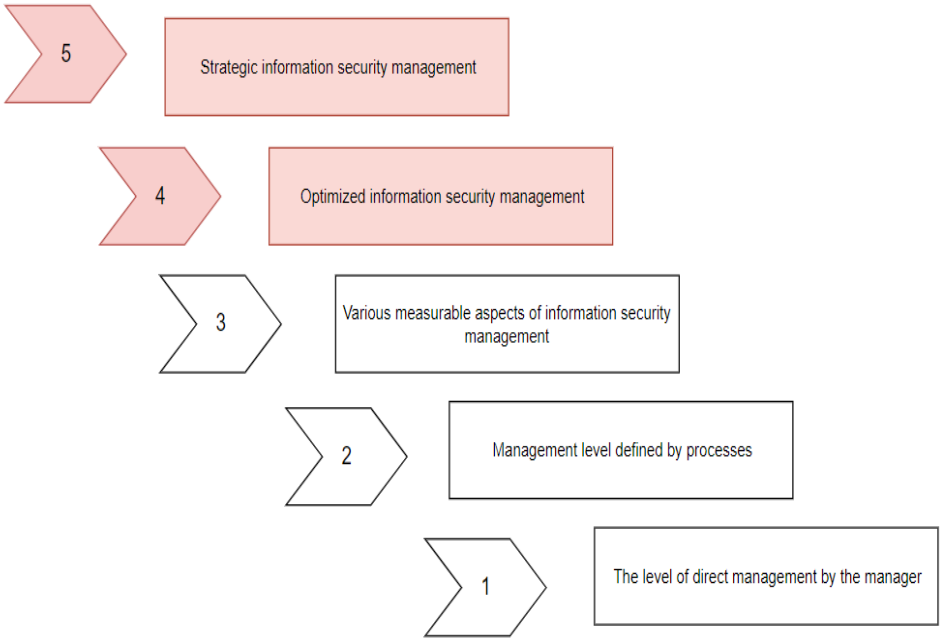


Figure 10. information security management system (ISMS)

The researchers in the study focused on the fourth and fifth levels. The elements of these levels represent the level of maintenance and security achieved in the information security management system within higher education. A survey was applied in universities in Bosnia and Herzegovina and outside Bosnia and Herzegovina. To ensure the level of security achieved. The ISMS sustainability model is shown in Figure 11 and Figure 12, where Figure 11 displays the fourth level of the methodology used. Optimal information security management represents the basic element in the use case diagram and is the main goal that the organization seeks to achieve. The researchers applied it with a weighting factor ranging from 0 to 24. The presented use case model consists of interconnected factors represented in the administrative structure and experiences, where individuals are directly involved in information security management. Additionally, special monitoring is also conducted. They presented an annual investment plan dedicated to a security management system Information, and work is being done to improve and maintain the system continuously. The system is used at the fourth level and is being improved and monitored by individuals from the organization’s administrative department, specialized experts in the field, and financial experts.

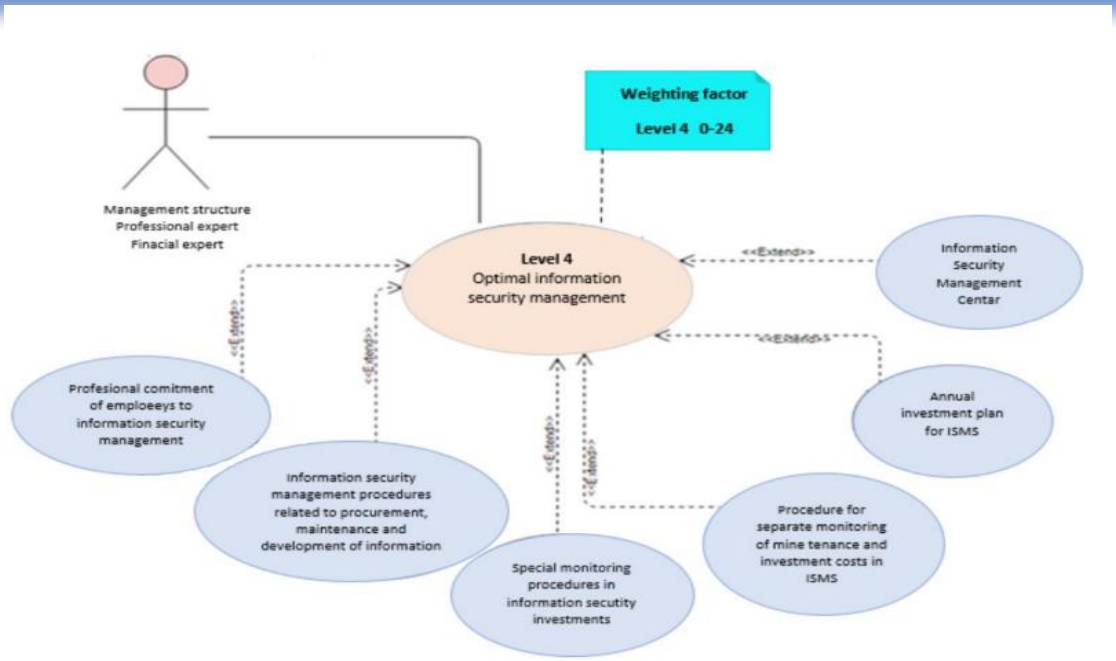
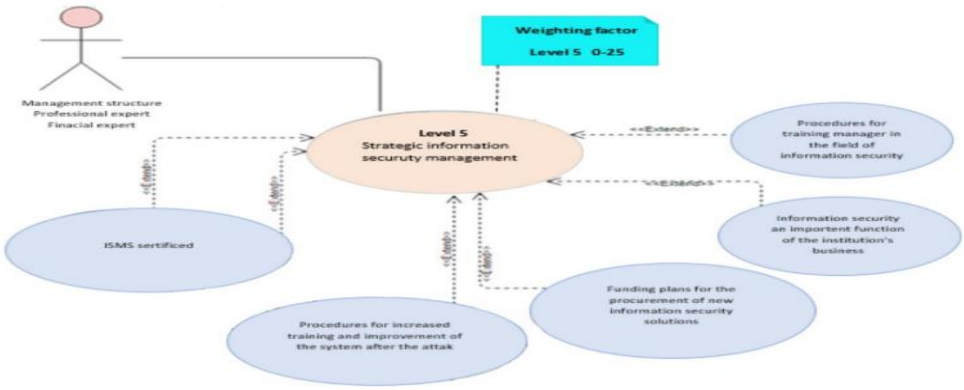


Figure 11. USE CASE diagram of optimal ISMS [7].

Figure 12 shows the fifth level of the methodology, represented by strategic information security management within the information security management framework (ISMS). This level was illustrated through the use case that the researchers worked on creating. The fifth level in the study includes five basic elements that represent the pillar of the level. These elements constitute the management structure and financial experts, the procedures for training managers, and this is done by training managers to use the system and deal with all deviations in a proper manner. and make sure that information security is the most important part of the target organization. The use case plan also included comprehensive financing plans concerned with purchasing new solutions to achieve information security. In addition to working on obtaining ISMS certificates to increase the reliability of the organization. The researchers worked to evaluate the elements through a factor A weight ranging from 0 to 25.



4. Results and discussion

The researchers in the study focused on assessing the situation in information security management systems (ISMS) in higher education institutions, specifically using the Fuzzy Expert System (FES). In order to evaluate the strength and quality of information security management in different universities, researchers in the anonymous survey used the FES model to analyze the survey data. It is particularly useful when dealing with situations of uncertainty and self-assessments, which are most commonly used in security management evaluations for various organizations. The researchers used the variables Nivo 4 and Nivo 5 to represent levels 4 and 5 in the Information Security Management Methodology (ISMS). The researchers reached a number Among the results after applying a survey to two universities, the purpose of the survey that was conducted was to obtain an assessment of the current state of information security in the participating universities. One of the participating universities outside Bosnia and Herzegovina obtained more positive results (yes). Conclusion: The analysis used focuses on the necessity of reaching the highest levels of maturity of the information security management system at levels 4 and 5, in order to work on improving information security management. The results reveal differences in the implementation of the information security management system, its quality, and its strength from one university to another. The study shows that despite the methods, efforts, and scrutiny of the work undertaken, there are some noticeable gaps and errors among universities in Bosnia and Herzegovina in implementing the system within them.

5. Conclusion

In this study, researchers demonstrated an in-depth method for creating, developing, and implementing an information security management system (ISMS) within educational institutions, specifically in the field of universities, using an organized and precise approach. The researchers in the study stressed the necessity of aligning the information security management system (ISMS) used with the proposed objectives and the necessity of focusing not only on technological objectives but also paying attention to the role of employees and internal processes. The study showed that despite the use of global standards ISO/IEC 27001:2013 and frameworks such as COBIT that provide comprehensive guidelines for establishing an information security management system (ISMS), the actual implementation and effectiveness are likely to vary from one organization to another. These differences indicate It was observed through the survey conducted at the University of Bosnia and Herzegovina and outside it that local factors and reasons have a major role, including culture, administrative commitment by managers, and the different capabilities and resources available, all of which play an important role in the success of the information security management system. Table 1 shows the most important main points in the study that play a major role in the success of the Information Security Management System (ISMS).

Table 1.

Main points	Description
Administrative Support	Strong support and involvement from senior management is critical to the success of establishing and maintaining an Information Security Management System (ISMS).
Employee Training	Continuous training programs for employees constitute one of the most important reasons for enhancing the culture of security awareness, working to reduce risks and problems resulting from human errors, and reducing internal threats to the organization.
Continuous Improvement	Periodic monitoring and improvements to the system are among the most important reasons for the continued efficiency of the information security management system (ISMS), especially when threats and intrusions facing the system develop over time.
Flexibility in Implementation	The standards used such as ISO/IEC 27001:2013 provide a strong foundation for companies and institutions, and this allows organizations to design and build their system to suit their needs and business field, allowing them flexibility in designing it in an effective and appropriate manner.

In conclusion, building and developing an effective and robust information security management system (ISMS) represents not only a technical challenge but also one of the most important strategic challenges facing organizations in all their aspects. The research focuses on the fact that while providing strong global standards, frameworks, and rules, its success ultimately depends on its ability to coexist with the organization's culture and integrate with the organization, And providing significant administrative support from the administration to work on its success, and to improve and develop it continuously to address attacks and security threats to protect information. Future research could provide an exploration of the long-term impacts of ISMS. The extent of the impact of organizational flexibility in organizations and the importance of effective training and awareness strategies for employees in enhancing the culture of information security.

References

[1] Administration: B, College; U. (2024). Research on Information Security Management and Protection Measures of Financial Enterprises in the Era of Big Data---Take the USA of Industrial and Commercial Bank of China, Journal of Education, Humanities and Social Sciences, 35(11): 39-44.

[2] ISO 27k Information security ISO/IEC 27001 certification standard (iso27001security.com).

[3] ***ISO 27001 Annex A 14 Controls & Domains 2024 [Checklist] (novelvista.com).

[4] *** Char :: COBIT 2019 (tistory.com).

[5] Jonathan, G; Lazar Rusu, E. (2024). Untangling the Link Between Digital Transformation and Information Security Management, Procedia Computer Science, 239: 575–582.

[6] Liudmila; V. Astakhova; A. Botha; A. Marlien, L. (2020). Defining organisational information security culture Perspectives from academia and industry. Published in Computers & Security. 92(1): 579-623.

[7] Sikman; L, Latinovic; T, Sarajlic, N, Sikanjic, G. (2022). A model of sustainable information security management system in higher education institutions, International Conference on Applied Sciences, 2540(2): 1-10.

[8] Tejon; J, Partearroyo; M, Osorio; D. (2024). Integrated security management model: a proposal applied to organisational resilience, Security Journal, 37(6): 375–398.

[9] Tendikov: a, Rzayeva: a, Bilal Saoud: b, Shayea: c, Azmi: d, Myrzatay: e, (2024). Security Information Event Management data acquisition and analysis methods with machine learning principles, Results in Engineering, 22(1): 102-254.