

MODEL FOR ASSESSING MEASURABLE ASPECTS OF INFORMATION SECURITY IN HIGHER EDUCATION

Ljilja Šikman¹, Tihomir Latinović^{2✉}, Nermin Sarajlić³,
Biljana Vranješ⁴, Ljubica Figun⁵, Aleksandar Gaćina⁶

Received on February 3, 2025

Presented by Ch. Roumenin, Member of BAS, on May 27, 2025

Abstract

In the higher education sector, there is a growing need to ensure the security and protection of information resources. The implementation of the ISO 27001 standard and the Information Security Management System (ISMS) helps in assessing the risks of security threats and attacks. Organizations, including universities, exhibit varying levels of commitment to information security, leading to variations in the development and implementation of ISMS. This highlights the need for a model to assess the current situation in the field of information security for each business institution. The model creation considers advice from the IT management framework – COBIT. Components are defined that indicate the level of quantitative characteristics and measurable criteria in managing ISMS. The research on the development level of the proposed model was conducted at several universities, applying fuzzy logic to specific elements. This model shows the results in a sequence from the lowest to the highest rating or weighted factor value, representing an assessment of the information security state at an academic institution. The model can also be used to assess the effectiveness of other parameters in areas such as ecology, health, workplace safety, and the economic business sector.

Key words: information security management, ISO 27001, risk assessment, fuzzy logic, measurable criteria

Introduction. The development of information and communication technologies is constantly growing, and as a result, threats and attacks on information

<https://doi.org/10.7546/CRABS.2025.07.07>

security are on the rise. In Bosnia and Herzegovina, in 2022, the Cyber Security Excellence Centre in Bosnia and Herzegovina (CSEC BiH) and the Balkan Investigative Reporting Network Bosnia and Herzegovina (BIRN BiH) created the first annual report on cyber security threats [1]. Data from the report show that in November 2022, there were 9.2 million different cyber-attacks. This situation demonstrates that data and information are poorly protected and that strategies and regulations for protection against cyber-attacks are lacking. Also, in Bosnia and Herzegovina, there is no national CERT (Computer Emergency Response Team), so one of the activities to mitigate cyber-attacks is the application of the ISO 27001 standard in relation to the information security management system (ISMS). By implementing the ISO 27001 standard, institutions gain numerous economic and technical advantages, some of which include: ensuring customer trust; reducing risks in business activities; improving the business environment; enhancing the security and availability of information flows [2].

Many businesses and educational institutions need to manage information security as a guarantee for long-term and stable operations. Most institutions have adopted remote work and use virtual applications for their operations. The ISO/IEC 27001:2022 standards provide solutions to the growing challenges of implementing information security measures in each institution [3]. SUNNY et al. [4] dealt with a model for assessing the information security management system in a public institution, considering ISO 27002 and 27004. A security management system in a public institution, considering ISO 27002 and 27004. A good plan and protection system enable the establishment of security at all critical points of the system, in any segment of security, and such a problem is addressed by establishing an information security management system [5]. ŠIKMAN et al. [6] applied fuzzy logic to develop a methodology for assessing ISMS within higher education, based on the recommendations of the ISO/IEC 27001 standard. This presents a new approach to solving complex system problems, applicable to other areas (economics, ecology, occupational safety, etc.), which is difficult to describe using specific mathematical models. This paper explores and presents a model for measurable aspects of ISMS in higher education, which is part of the methodology presented in [7]. Elements representing the level of measurable aspects of management in higher education are defined. ISMS levels are tailored according to the recommendations of the COBIT (Control Objectives for Information and Related Technology) management framework.

Why is ISO/IEC 27001:2022 important? ISO/IEC 27001:2022 is an internationally recognized standard that defines the requirements for establishing, implementing, maintaining, and continuously improving the Information Security Management System (ISMS). This standard plays a crucial role in modern organizations that want to ensure the confidentiality, integrity, and availability of their information, especially in times when cyber threats are ubiquitous and increasingly sophisticated. The importance of ISO/IEC 27001:2022 lies in its ability

to provide organizations with a framework to identify and manage risks related to information security. By implementing this standard, organizations not only secure their business processes but also build trust with clients, partners, and regulatory bodies. The standard enables proactive action against cyber threats, thereby minimizing potential losses and reputational damage [8].

One of the main advantages of implementing ISO/IEC 27001:2022 is increasing the organization's resilience to threats that could compromise information security. In addition to providing technical and organizational protection, the standard promotes the improvement of business processes and contributes to transparency. Clients and partners often prefer to collaborate with organizations certified according to this standard, which can contribute to gaining a competitive advantage and opening new markets. Compliance with ISO/IEC 27001:2022 also facilitates adherence to legal and regulatory requirements, further strengthening the organization's reputation.

Key components of ISMS include security policies, risk assessment, security controls, and continuous system improvement. Security policies form the foundation of any ISMS, as they define the objectives and rules that the organization follows to secure its information. Risk assessment allows for the identification and analysis of potential threats, while security controls provide specific measures to mitigate risks. Continuous improvement ensures that ISMS remains relevant and effective, adapting to changes in the business environment and technological innovations.

The implementation process of the standard requires a detailed analysis of the current state within the organization to identify existing weaknesses. Afterward, the scope of ISMS is defined, and a risk assessment is carried out, which involves developing strategies to manage the identified threats. Implementation includes the application of technical and organizational measures, employee training, and the establishment of a system for continuous monitoring and auditing. Certification is the final phase, confirming compliance with the standard's requirements.

ISO/IEC 27001:2022 is often associated with other standards, such as ISO 9001 (Quality Management System), ISO 22301 (Business Continuity Management System), and ISO/IEC 27002:2022 (Code of Practice for Information Security Controls). For example, ISO/IEC 27002:2022 provides detailed guidelines for implementing controls from ISO/IEC 27001:2022, while combining it with ISO 22301 enables organizations to ensure business continuity in emergency situations. This compatibility allows organizations to integrate various management systems, leading to more efficient and consistent operations. The application of ISO/IEC 27001:2022 brings organizations not only greater information security but also better organization of internal processes and increased market trust. In the digital age, compliance with this standard has become a fundamental step for all organizations seeking to be recognized as reliable and responsible.

Management-functional framework of information security through the lens of modern information space within higher education. The concept of the management-functional framework of information security is based on a combination of legal regulations, national and international standards, as well as internal regulations, contractual obligations, and strategic planning for each public institution, business entity, or legal person. Today the public and business sectors are closely linked, leading to overlapping security mechanisms. The complexity of the management-functional framework increases further when business/public institutions have international cooperation. Considering the specifics of higher education institutions, it is essential to specifically address the strategic importance of information security in managing these institutions. Within an institution, it is necessary to identify strategic and operational units responsible for implementing the information security plan, where their responsibilities overlap, as do the risks that span the entire organizational structure of public and business institutions.

For any institution to improve its business success, it needs to continuously develop its information system. One of the methodologies for improving the information system is the COBIT (Control Objectives for Information and Related Technology) methodology. The key features of this methodology include the development, research, publication, and promotion of everything that enhances the quality of the information system. The latest alignment for the COBIT methodology was in 2019. The COBIT management framework contains 6 development levels. COBIT 2019 increases business value, reduces business risk, and helps meet the requirements of standards and laws in the field of information security, which is now crucial in institutions/business entities for IT and business alignment. It also aims to provide senior management with insight into how technology can be aligned with corporate goals [9].

Example of measurable aspects of ISMS in higher education institutions. The methodology for the development and functioning of ISMS, which includes the recommendations of the COBIT management framework, contains five levels of management [6]:

- Level 1 – Direct management of information security by the manager;
- Level 2 – Defined process management of information security;
- Level 3 – Measurable aspects of information security management;
- Level 4 – Optimal information security management;
- Level 5 – Strategic management of information security.

Each level is represented by a numerical value that shows the current value and state of ISMS management in the observed information system. This paper analyzes and investigates Level 3, which contains a numerical value – a weight factor (0–42). The weight factor for all levels is within the interval 0–108. Therefore, the development and state of ISMS in higher education institutions can be depicted by applying development levels that represent a quantified depiction of

development from the initial to the strategic management state of ISMS. Basic elements representing the measurement mechanism for each level, which distinguishes the states of development and operation of the information system, have been defined. In Fig. 1, the structural elements of the third level are presented using a USE CASE diagram. The third level of the model is the level of measurable aspects of information security management, shown with a use case diagram, extended with fourteen elements, and includes a weight factor of 0–42; there is an adopted information security policy at the University (Fig. 1).

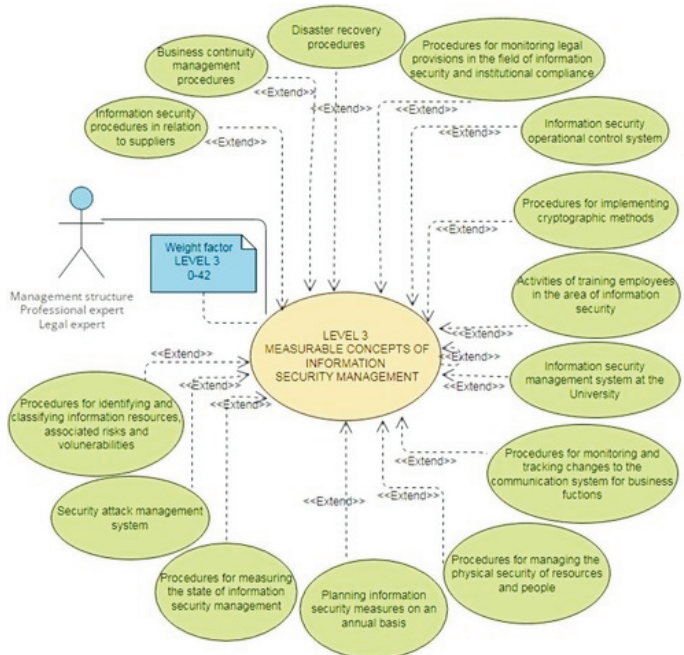


Fig. 1. USE CASE diagram of the third level of ISMS management

The diagram includes various components that represent the functions and processes in the system, with an emphasis on ensuring the adoption and execution of a security policy at the university. Each component or use case has a specific weight factor, illustrating how different aspects of information security are quantified and assessed. This model helps to evaluate the development of ISMS in a structured and measurable way.

This level contains the most elements, and they are a prerequisite for achieving higher levels of system functionality, which corresponds to the practical aspect of ISMS functioning in higher education institutions. The processes at this level are documented, standardized, and represent the formalization of existing practices. Interaction with the system at the third level is carried out by individuals from the management structure, field experts, and legal experts.

Research results. The research results were based on the FES model presented in [6], in which responses from an anonymous survey conducted among universities abroad and universities in Bosnia and Herzegovina were analyzed. The research determined the current state of ISMS at the surveyed universities. A program in Visual Basic for calculating the weight value and entering survey results for the third level is shown in Fig. 2.

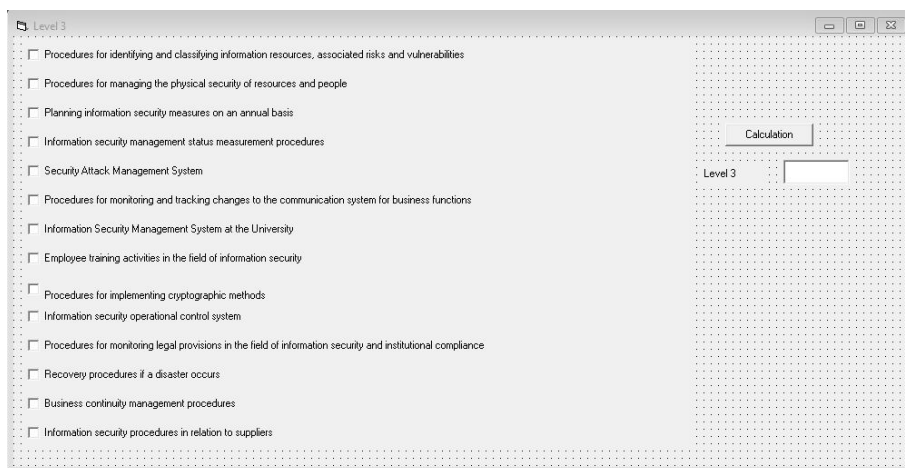


Fig. 2. Program for calculating the weight value of the third level

Figure 2 shows a program in Visual Basic designed to calculate the weight value of the third level of ISMS management. The program processes survey results from universities and determines the corresponding weight value based on the responses.

The results are then used to assess the development and implementation of ISMS in the surveyed institutions. Universities abroad and in Bosnia and Herzegovina with the highest number of “Yes” responses were considered. A program was created in Visual Basic to present the results of each level, displaying the quantified values of the weight factor for each level. In this paper, we are interested in the results for level 3. After entering the obtained results into the model for the third level, the following values are obtained, as shown in Fig. 3a.

Figure 3a presents the survey results for a university in Bosnia and Herzegovina at the third level, with a weight factor of 3. The data shown reflects the responses received from the survey, which were then analyzed to assess the level of ISMS development and implementation at the institution.

Figure 3b presents the survey results for a university outside of Bosnia and Herzegovina at the third level, with a weight factor of 39. The data shown reflect the responses received from the survey, which were then analyzed to assess the level of ISMS development and implementation at the institution.

The fuzzy rules describe the behaviour of the system and the interdependence

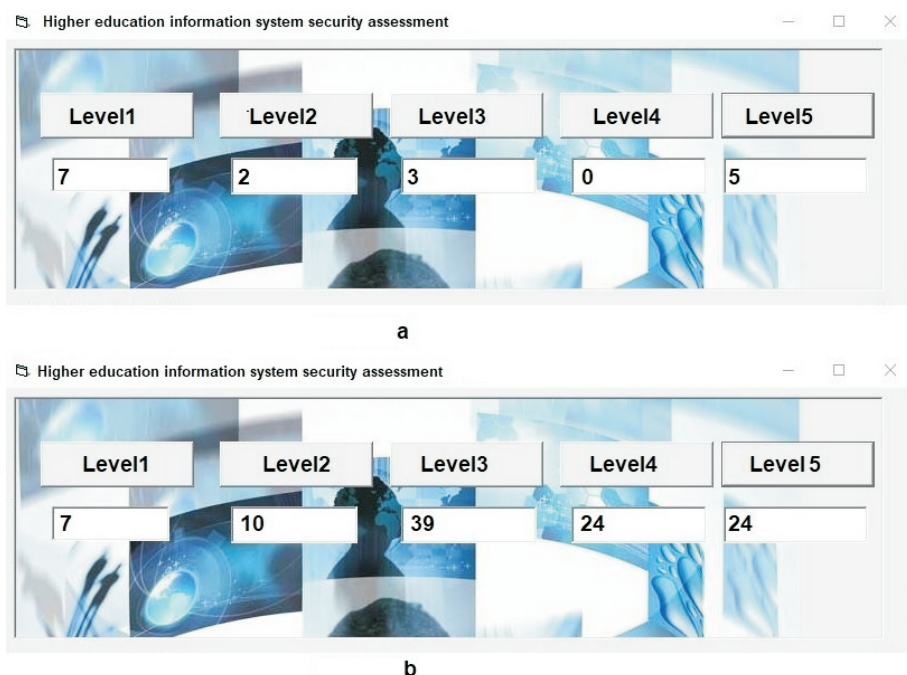


Fig. 3. Survey results from the University in Bosnia and Herzegovina (a) and a University outside of Bosnia and Herzegovina (b)

of fuzzy sets of different descriptive variables. These rules have a limited set of language expressions and strict syntax, typically in the form: IF $x = A_i, \dots$ and $y_i = B_i$, THEN $z = C_i$, where $i = 1, 2, \dots, n$. The Mamdani fuzzy inference process, which includes fuzzification of input variables, estimation of rules, aggregation of output data, and defuzzification, is used. A Visual Basic program was used to find the optimal number of rules, and in this study, 1084 rules were reduced to 284 to achieve a good result. The Fuzzy expert system uses these rules to connect the input (Levels 1–5) to the output parameter (Evaluation 1). The Rule Viewer displays a roadmap of the fuzzy inference process.

The Visual Basic program in the paper is used to determine the numerical weights for individual levels of information security management and to generate fuzzy rules. A special program is created in Visual Basic to determine the numerical weights for the individual levels. Subroutines can be called from this program to calculate levels and prepare them for input into MATLAB commands for the Fuzzy Inference System (FIS). The program contains pre-defined subroutines for each level of the information security management system. For example, Level 1 has three checkboxes, each with a different weight. When a checkbox is selected, its corresponding weight is included in the numerical value of the level. The more checkboxes selected, the higher the numerical value, indicating that more conditions are satisfied.

A Visual Basic program is used to find the optimal number of rules for the fuzzy system. The program generates rules based on 5 inputs (Levels 1–5) and one output (grading with an output score of 5 to 10). The program uses nested loops to iterate through different combinations of input values and assign an output score based on those combinations. The code writes these rules to a text file. The program determines the minimum number of rules that can be used in the system while still providing approximately the correct result.

The Visual Basic program is used to determine the fuzzy rules. It uses one sheet box and one text file for data output to create rules based on 5 inputs and one output, grading with an output score of 5 to 10. The code is as follows:

```
Private Sub Form_Load()
Dim n(5) As Integer
Dim counter1(5, 5) As Integer
Open "D:\Output1.txt" For Output As #1
counter = 0
b5 = 0
b6 = 0
b7 = 0
b8 = 0
b9 = 0
b10 = 0

n(1) = 7
n(2) = 10
n(3) = 42
n(4) = 25
n(5) = 24
For i = 0 To 5
For j = 0 To 5
For k = 0 To 5
For l = 0 To 5
For m = 0 To 5
If i = j Or i = k Or i = l Or i = m Or j = k Or j = l Or j = m Or k = l
Or k = m Then
Else
counter = counter + 1
counter1(i, j) = n(i) + n(j) + n(k) + n(l) + n(m)
If counter1(i, j) < 56 Then
List1.AddItem "Five " + Str(n(i)) + " " + Str(n(j)) + " " + Str(n(k)) +
" " + Str(n(l)) + " " + Str(n(m)) + " " + Str(counter1(i, j))
Write #1, "Five " + Str(n(i)) + " " + Str(n(j)) + " " + Str(n(k)) + " " +
```

```

Str(n(l)) + " " + Str(n(m)) + " " + Str(counter1(i, j))
b5 = b5 + 1
ElseIf counter1(i, j) > 56 And counter1(i, j) < 66 Then
List1.AddItem "Six " + Str(n(i)) + " " + Str(n(j)) + " " + Str(n(k)) +
" " + Str(n(l)) + " " + Str(n(m)) + " " + Str(counter1(i, j))
Write #1, "Six " + Str(n(i)) + " " + Str(n(j)) + " " + Str(n(k)) + " " +
Str(n(l)) + " " + Str(n(m)) + " " + Str(counter1(i, j))
b6 = b6 + 1
ElseIf counter1(i, j) > 67 And counter1(i, j) < 77 Then
List1.AddItem "Seven " + Str(n(i)) + " " + Str(n(j)) + " " + Str(n(k))
+ " " + Str(n(l)) + " " + Str(n(m)) + " " + Str(counter1(i, j))
Write #1, "Seven " + Str(n(i)) + " " + Str(n(j)) + " " + Str(n(k)) + " "
+ Str(n(l)) + " " + Str(n(m)) + " " + Str(counter1(i, j))
b7 = b7 + 1
ElseIf counter1(i, j) > 78 And counter1(i, j) < 88 Then
List1.AddItem "Eight " + Str(n(i)) + " " + Str(n(j)) + " " + Str(n(k))
+ " " + Str(n(l)) + " " + Str(n(m)) + " " + Str(counter1(i, j))
Write #1, "Eight " + Str(n(i)) + " " + Str(n(j)) + " " + Str(n(k)) + " "
+ Str(n(l)) + " " + Str(n(m)) + " " + Str(counter1(i, j))
b8 = b8 + 1
ElseIf counter1(i, j) > 89 And counter1(i, j) < 99 Then
List1.AddItem "Nine " + Str(n(i)) + " " + Str(n(j)) + " " + Str(n(k))
+ " " + Str(n(l)) + " " + Str(n(m)) + " " + Str(counter1(i, j))
Write #1, "Nine " + Str(n(i)) + " " + Str(n(j)) + " " + Str(n(k)) + " "
+ Str(n(l)) + " " + Str(n(m)) + " " + Str(counter1(i, j))
b9 = b9 + 1
ElseIf counter1(i, j) > 100 And counter1(i, j) < 110 Then
List1.AddItem "Ten " + Str(n(i)) + " " + Str(n(j)) + " " + Str(n(k)) +
" " + Str(n(l)) + " " + Str(n(m)) + " " + Str(counter1(i, j))
Write #1, "Ten " + Str(n(i)) + " " + Str(n(j)) + " " + Str(n(k)) + " " +
Str(n(l)) + " " + Str(n(m)) + " " + Str(counter1(i, j))
b10 = b10 + 1
End If
End If

Next m
Next l
Next k
Next j
Next i

```

```
List1.AddItem Str(b5) + " " + Str(b6) + " " + Str(b7) + " " + Str(b8)
+ " " + Str(b9) + " " + Str(b10)
List1.AddItem counter
End Sub
```

In this way, 1084 rules were found, and after further analysis, the rules were reduced to 284 that give a good result.

Figure 4 shows the created Fuzzy expert system for this problem and its input and output variables. In this phase, fuzzy rules are selected, the number and form of which depend on the quality of the information available. By applying these rules, the explicit values (crisp) of all input variables are associated with as many values of the membership functions of each output variable as the rules are selected. The fuzzy expert system takes Level 1–5 on input and produces Evaluation 1 for the output parameter.

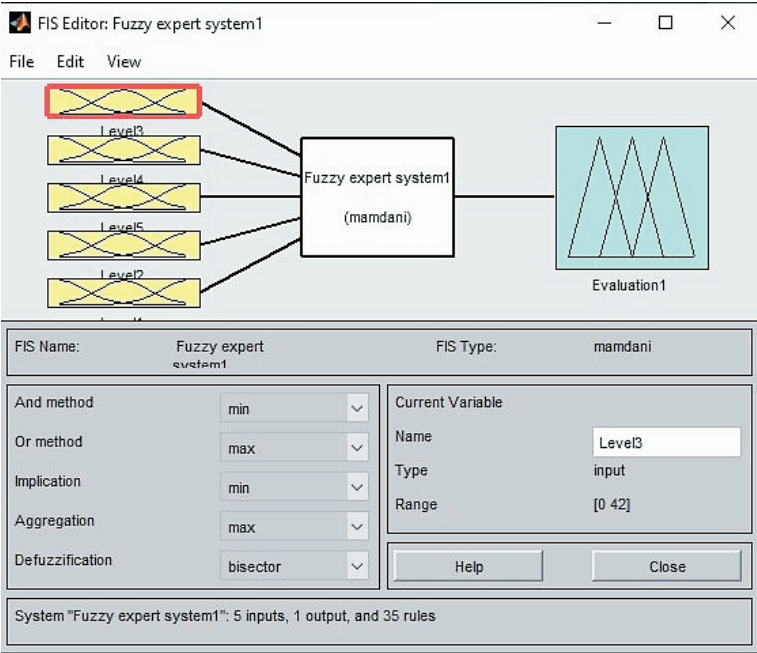


Fig. 4. Fuzzy expert system with Level 1–5 on input and Evaluation 1 for Output parameter

Conclusion. The analysis and evaluation of the measurable aspects of ISMS (Level 3) are expressed based on the weight factor for the third level, ranging from 0 to 42, and represent the number of "Yes" responses. After comparing the results shown in Fig. 3a with weight factor for Level 3 is 3 (university in Bosnia and Herzegovina) and 39 in Fig. 3b, (university outside Bosnia and Herzegovina), the lower weight factor is caused by the smaller number of "Yes" responses, indicating that there are no defined elements within Level 3.

Based on the results presented for Level 3, the following conclusions can be made:

1. The application of the methodology for calculating measurable aspects of ISMS allows for the creation of a quality management framework for information system protection.
2. By using input data prescribed by the requirements of ISO/IEC 27001 and the COBIT management framework, it is possible to implement corrective measures and offer solutions for improving ISMS.

Information systems form an integrated set of components tasked with collecting, storing, processing, and communicating information [10]. Higher education institutions rely on information systems to use their operations, services, and improve the user and business environment. Information systems are becoming larger and more complex, mainly due to the increase in data volume, growing user needs, and the development of new technologies. A quality education strategy requires appropriate investment in tools, accessibility, content, and skills development, as well as training for teaching and administrative staff. We must not forget the infrastructure, including the availability of high-speed internet (new 5G internet) [11]. To enable the execution of business operations, it is essential to protect information resources (information, processes and services, software, physical equipment, and people). By applying the methodology presented in this paper, it is possible to achieve an adequate level of management for measurable aspects of ISMS within higher education.

REFERENCES

- [1] Report on CYBERSECURITY THREATS in Bosnia and Herzegovina (2022) CSEC, BIRN BiH, <https://detektor.ba/wp-content/uploads/2023/04/Cyber-prijetnje-u-BiH-BOS-WEB.pdf>.
- [2] ŠIKMAN L., T. LATINVIĆ, D. PASPALJ (2019) ISO 27001 – Information systems security, development, trends, technical and economic, ANNALS of Faculty Engineering Hunedoara, Int. J. Eng., **XVII**(4), 45–48.
- [3] ŠIKMAN L., D. SAVANOVIĆ, T. LATINVIĆ, A. GAĆINA (2023) Information security in the function of corporate management of information technologies, XII International conference on social and technological development, Trebinje, BiH, 15–18, 362–369.
- [4] SUNNY K., A. FAJRI, R. HARWAHYU (2024) Information Security Management System Assessment Model by Integrating ISO 27002 and 27004, Indonesian Journal of Machine Learning and Computer Science, **4**(2), 498–506.
- [5] ŠIKMAN L., T. LATINOVIC, N. SARAJLIC, G. ŠIKANJIC (2023) A model of sustainable information security management systems in higher education institutions, J. Phys: Conf. Ser., 2540, <https://doi.org/10.17559/TV-20200721154801>.

- [6] ŠIKMAN L., T. LATINOVIC, N. SARAJLIC (2022) Modeling of Fuzzy Expert Systems for of security Information Management System UIS (University Information System), *Gazette (Leiden Netherlands)*, **29**(1), 60–65.
- [7] SIKMAN L. (2021) Modeling of information security management systems within higher education, University of Tuzla, Bosnia and Herzegovina, PhD Thesis.
- [8] PANEVSKI A. (2024) Applicable international standardized basis in defining data for security systems development, *C. R. Acad. Bulg. Sci.*, **77**(8), 1193–1200.
- [9] ISACA® , COBIT® (2019) Framework: Introduction and Methodology, USA, 2018, <https://www.isaca.org/resources/cobit>.
- [10] Encyclopedia Britannica “Information and information systems”, 2004.
- [11] LATINOVIC T., L. SIKMAN (2022) Impact of COVID 19 on the Information Technology for Online Education, Education 4.0, Challenges and Solutions. In: *Advanced Technologies, Systems, and Applications*, https://doi.org/10.1007/978-3-031-17697-5_54.

¹*Faculty of Technology, University of Banjaluka, V. Stepe Stepanovica 73, 78000 Banjaluka, Bosnia and Herzegovina*
e-mail: ljilja.sikman@tf.unibl.org

²*Faculty of Information Technology, University of Vitez, Skolska 23, 72270 Travnik, Bosnia and Herzegovina*
e-mail: tihomir.latinovic@unvi.edu.ba

³*Faculty of Electrical Engineering, University of Tuzla, Franjevačka 2, 75000 Tuzla, Bosnia and Herzegovina*
e-mail: nermin.sarajlic@untz.ba

⁴*Faculty of Mechanical Engineering, University of Banjaluka, V. Stepe Stepanovica 71, 78000 Banjaluka, Bosnia and Herzegovina*
e-mail: biljana.vranjes@mf.unibl.org

⁵*Faculty of Mining, University of Banjaluka, Aleja kozarskog odreda 1, 79101 Prijedor, Bosnia and Herzegovina*
e-mail: ljubica.fugun@rf.unibl.org

⁶*University Computer Center, University of Banjaluka, 1A V. Petra Bojovića Blvd, Bosnia and Herzegovina*
e-mail: aleksandar.gacina@unibl.org