Journal of Process Management and New Technologies
Vol. 14, Issue 1-2, 2026, pp. 31-49

A FRAMEWORK FOR QUANTITATIVE CYBER RESILIENCE ASSESSMENT OF NETWORK ARCHITECTURES IN EDUCATIONAL INSTITUTIONS

Ana BAŠIĆ[1*], Dejan VIDUKA[2], Dražen JOVANOVIĆ[3]

[1]*Information Technology School—ITS, Belgrade, Serbia, ana.basic@its.edu.rs*
https://orcid.org/0009-0009-4137-3296

[2]*Faculty of Mathematics and Computer Sciences, University Alfa BK, Belgrade, Serbia, dejan.viduka@alfa.edu.rs*
https://orcid.org/0000-0001-9147-8103

[3]*Faculty of Technical Sciences, European University Brčko District, Brčko, Bosnia & Herzegovina, jdrazen13@gmail.com*
https://orcid.org/0000-0002-1218-6231

Abstract: *This paper investigates the development and application of an integrated framework for the quantitative assessment of cyber resilience of network architectures in educational institutions. Resilience assessment criteria were identified and mapped to the NIST Cybersecurity Framework to cover key functional areas of cybersecurity, while the ISO 31000 standard was applied to assess disruption scenarios, including cyber-attacks and network infrastructure failures. The PIPRECIA-S method enables precise weighting of criteria based on expert assessments, and the H-SCRM methodology allows quantitative evaluation of network alternatives according to defined criteria and scenarios. The results show that the hybrid cloud-managed network architecture achieves the highest level of cyber resilience, while software-defined networking and traditional LAN architecture achieve lower global resilience index values. Sensitivity analysis confirms the stability of the ranking of alternatives and the robustness of the proposed model. The paper provides practical guidelines for improving network security and decision-making in educational institutions through an integrated approach to risk and resilience management.*
Keywords: *Cyber resilience, educational institutions, NIST CSF, ISO 31000, PIPRECIA-S, H-SCRM.*

Original scientific paper
Received: 16.04.2026
Accepted: 25.05.2026
Available online: 28.05.2026
DOI: 10.5937/jpmnt14-66564

1. Introduction

The development of information and communication technologies has significantly transformed the way educational institution's function (Liu et al., 2025; Shetelia et al., 2024). Schools, colleges and universities are increasingly using digital systems for teaching

* Corresponding author

management, administration and communication with students and teachers (Pacheco et al., 2025; Olowo et al., 2026). Modern educational institutions integrate wireless networks, e-learning servers, cloud services and various software platforms, creating a complex information ecosystem that improves efficiency and continuity of educational processes (Kiryakova, 2017). However, at the same time, the exposure of institutions to various cyber threats is also increasing. Attacks on network systems, server compromise or unauthorized access to data can lead to the interruption of teaching and administrative processes, endanger the security of users and damage the reputation of the institution (Lallie et al., 2025; Ibrahim, 2024). Due to the limitations of traditional approaches to cyber security, contemporary research increasingly emphasizes the importance of cyber resilience, which implies the ability of a system to maintain functionality, quickly recover and adapt after an incident (Bellini et al., 2025).

The network architecture of educational institutions plays a key role in cyber resilience, as it enables communication between all digital components of the system and directly affects the availability, performance and security of services (Wibowo et al., 2025; Afolalu & Tsoeu, 2025). Different approaches to managing networks exhibit different levels of resilience to disruptions. Therefore, it is necessary to develop a methodological framework that enables a systematic and comparable assessment of the resilience of network architectures in the educational environment.

Existing research usually focuses on the identification of individual vulnerabilities, the analysis of specific attacks or the application of protective mechanisms (Jawaid, 2023). However, there is a lack of an integrated methodological framework that enables a quantitative assessment of cyber resilience, considering different scenarios and criteria importance, which makes it difficult to plan and improve network systems in educational institutions.

In educational institutions, there is often a problem of insufficient integration of security and operational aspects of network systems. The primary goal is for the systems to function, while less attention is paid to their behavior under disturbance conditions. Incidents such as DDoS attacks, power outages or network overloads can lead to significant interruptions in work and threaten the continuity of educational processes (Jawaid, 2023). Therefore, it is necessary to apply an integrated approach that includes risk assessment, defining crisis scenarios, assessing the criticality of components and ranking alternative network architectures.

Existing standards and frameworks, such as the NIST Cybersecurity Framework (CSF) and ISO 31000, provide guidelines for security and risk management, but do not allow direct assessment and ranking of different network architectures. The goal of this research is the development of a unique methodological framework for assessing the cyber resilience of network architectures in educational institutions, which enables systematic and quantitative comparison of architectural solutions under cyber disturbances.

The integrated framework envisages the application of the following components:

- standardized cybersecurity and risk management frameworks (NIST CSF and ISO 31000);
- methodology of scenario analysis of resilience (H-SCRM);
- multi-criteria decision-making and determination of criteria weights using the PIPRECIA-S method.

This approach enables not only the identification of vulnerabilities and risk assessment, but also the ranking of alternatives, which provides a practical basis for improving network architectures and strengthening the cyber resilience of educational institutions.

2. Literature review and theoretical framework

2.1. Educational institutions as cyber-physical systems and challenges of cyber resilience

Educational institutions represent complex digital environments in which information and communication technologies are used for the realization of teaching, administrative and research activities (Liu et al., 2025; Pacheco et al., 2025). Modern schools and universities rely on an integrated network infrastructure that connects computer networks, cloud services, learning management systems, wireless networks, server platforms and various digital services, making network architecture a key element in their functioning (Güntem & Kılıç, 2025; Dong & Xie, 2025).

In literature, educational institutions are often viewed as cyber-physical systems in which digital components are directly connected to physical resources and teaching processes (Gallon et al., 2024; Tariq et al., 2025). The large number of users, heterogeneity of devices and constant changes in network traffic create a dynamic environment that is susceptible to various cyber threats (Afolalu & Tsoeu, 2025). Cyber incidents in educational institutions can lead to disruption of the teaching process, loss of data, compromise of research results and damage to the institution's reputation (Lallie et al., 2025).

Traditional approaches to cyber security that focus solely on attack prevention are not sufficient to protect such complex systems. Therefore, in modern research, the concept of cyber resilience is increasingly emphasized, which implies the system's ability to maintain functionality, mitigate the consequences of an attack and recover quickly after a disruption.

Choosing the right network architecture plays a key role in achieving cyber resilience (AlHidaifi et al., 2024). Different network architectures enable different levels of control, segmentation, automation and monitoring of network traffic, which directly affects the system's ability to respond to cyber threats and disruptions.

Existing research mainly focuses on individual vulnerabilities or protective mechanisms. An integrated approach that enables a quantitative assessment of the resilience of network architectures is lacking. Therefore, this paper proposes a framework that combines: NIST CSF for defining criteria, ISO 31000 for risk management and disruption scenarios, PIPRECIA-S method for determining criteria weights and H-SCRM methodology for quantitative assessment of resilience.

2.2. The concept of cyber resilience and cyber security

The traditional approach to cyber security involves protecting the system from unauthorized access, abuse, integrity breaches and data loss through preventive technical and organizational measures such as authentication, access control, encryption and network protection (Li & Liu, 2021). However, in dynamic environments such as educational institutions, prevention cannot eliminate risks completely.

Cyber resilience represents an evolution of the approach to security and involves the design of systems that function even in conditions of disruption (Araujo et al., 2024). It covers the full lifecycle of a cyber incident, including preparation, detection, response and recovery. In the context of network architectures in educational institutions, cyber security focuses on protecting individual components, while cyber resilience considers the system as a whole and its behavior under disruption, including limiting the spread of incidents and minimizing their impact on critical services.

Cyber resilience is a dynamic process that evolves over time and incorporates learning from previous disruptions, further enhancing security and operational mechanisms (Singh et al., 2025). In this paper, cyber resilience is defined as the ability of network architecture to maintain an

acceptable level of availability, performance and security in the face of disruption, with the ability to quickly recover.

Systematic approaches to cyber resilience often rely on standardized frameworks, such as the NIST Cybersecurity Framework and ISO 31000. The NIST framework provides a structured assessment and improvement of an institution's ability to detect, respond to, and recover from incidents (Salas Riega et al., 2025). Its functions include risk management, critical resource identification, system protection, anomaly detection, incident response, and disaster recovery (National Institute of Standards and Technology, 2024).

ISO 31000 enables the definition and evaluation of risk scenarios, including the assessment of the likelihood and impact of a cyber-attack, which is critical to the preparation and planning of an institution's response (International Organization for Standardization, 2018). Risk management within ISO 31000 includes a continuous process: context definition, risk identification, analysis and evaluation, risk treatment, monitoring and communication with stakeholders.

ISO 31000 and NIST CSF are complementary frameworks. ISO 31000 allows the definition and evaluation of different disruption scenarios that are later mapped to NIST CSF functions. Their integration enables cyber resilience evaluation from both technical and organizational perspectives.

2.3. H-SCRM (Hybrid Scenario-Based Comparative Resilience Method)

For the quantitative assessment of resilience, the H-SCRM methodology (Hybrid Scenario-Based Comparative Resilience Method) is applied in the research, which integrates the analysis of disruption scenarios and multi-criteria evaluation of network performance (Rezvani et al., 2025). Each scenario represents a specific form of risk, and the analysis includes partial resilience indices that reflect the system's ability to quickly recover and minimize the consequences of disruptions.

A scenario-based approach enables a detailed assessment of the system's behavior under different conditions, identification of critical points and prioritization of resources to preserve the continuity of operations (Rathnayaka et al., 2024). This way, educational institutions can strategically plan their security policies, improve technological infrastructure and develop operational protocols that increase resistance to cyber incidents.

The multi-criteria part of the H-SCRM method enables the quantification of complex and often difficult to measure characteristics of cyber resilience, such as the ability to detect an incident, the speed of response or the efficiency of recovery. These characteristics are expressed through a set of criteria, the relative importance of which is determined with the help of expert knowledge.

One of the key features of the H-SCRM method is multi-level aggregation of results. The first level involves evaluating the performance of each alternative in relation to the defined criteria, especially for each disruption scenario. These results are then aggregated into partial resilience indices by scenario. The second level of assessment implies that a global index of resilience is calculated based on the obtained partial indexes of resilience, considering the relative severity of the scenario. The value of the global level of resilience allows ranking and comparative analysis of alternative network architectures.

A particular advantage of the H-SCRM method is its flexibility and the possibility of integration with different frameworks and methods, such as NIST CSF, ISO 31000 and PIPRECIA-S. In this way, the theoretical concepts of cyber resilience are operationalized in the practical evaluation of networks.

2.4. Multi-criteria decision-making methods within the H-SCRM approach

Cyber resilience is a multidimensional concept that includes technical, organizational and operational aspects of a system. These dimensions of the system cannot be represented by a single indicator, but rather evaluation is necessary using a set of criteria that can often have conflicting goals. The application of multi-criteria decision-making methods enables the simultaneous consideration of several resistance criteria, the determination of the relative importance of criteria, the comparison of alternative solutions in real conditions of disturbance and the ranking of alternatives based on quantitative indicators (Avramova et al., 2025).

Multi-criteria decision-making methods (MCDM) include different approaches that enable the selection of optimal solutions when it is necessary to consider multiple criteria with possible conflicts (Taherdoost & Madanchian, 2023). Among the most famous methods are: AHP (Analytic Hierarchy Process), which is used for hierarchical weighting of criteria; ANP (Analytic Network Process), suitable for systems with interdependent criteria; TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution), which ranks alternatives according to the distance from the ideal solution; and VIKOR, which is particularly useful for compromise solutions in conflict situations (Avramova et al., 2025; Park et al., 2025). These methods are widely applied in education, smart buildings, technology selection, energy efficiency and security systems, enabling transparent and quantitative evaluation of complex systems (Veljić et al., 2025; Theilig et al., 2025; Madanchian & Taherdoost, 2025).

In this paper, the PIPRECIA-S method is used for weighing the resistance criteria, because it reduces the burden on experts compared to classical methods such as AHP. So far, the PIPRECIA-S model has been used to evaluate various criteria in the context of the selection of optimal solutions for the selection of electronic learning materials (Jauković et al., 2020), for the selection of AI tools in education (Popović et al., 2025), for the selection of operating systems in education (Marinović et al., 2025), for the selection of software testing methods (Bašić & Viduka, 2025), for research in sustainable development, decision-making in the IT industry (Bašić et al., 2024), as well as in studies dealing with the evaluation of cognitive skills.

The integration of multi-criteria methods into the H-SCRM framework enables a multi-level analysis:

- determining the relative importance of the criteria;
- combining normalized values with scenario weights and obtaining partial resilience indices;
- aggregation into a global resilience index and ranking of alternatives.

This approach enables the quantification of complex aspects of cyber resilience, reduces subjectivity and increases the transparency and repeatability of research.

3. Methodological framework

The methodological framework of this research combines multi-criteria decision-making methods and a scenario-based approach to the assessment of the cyber resilience of the network infrastructure of educational institutions. The aim is to enable a quantitative assessment of the performance of different network architectures under conditions of real cyber disruptions, taking into account the relative importance of criteria and scenarios. The methodology includes defining criteria and alternatives, determining criteria weights using the PIPRECIA-S method, creating disruption scenarios, forming scenario-based decision matrices and calculating the cyber resistance index.

3.1. Defining criteria based on the NIST CSF framework

The key step in the process of assessing the cyber resistance of the network infrastructure of educational institutions is the definition of criteria because it enables a structured and objective evaluation of alternative network architectures. The criteria are derived from the NIST Cybersecurity Framework, which defines five basic cybersecurity functions: identify, protect, detect, respond, and recover (NIST, 20204). Based on the above, a set of cyber resistance criteria $C = \{C_j | j = 1, \dots, n\}$ was defined, where n represents the total number of defined criteria:

- Availability of network infrastructure (C_1) - continuity of communication and availability of critical services;
- System recovery time (C_2) – the speed of returning the system to a functional state after an incident;
- Network traffic management (C_3) – efficient management of increased load;
- Failure tolerance and system redundancy (C_4) – backup communication paths and devices for automatic traffic redirection;
- Resilience to cyber threats (C_5) – detection and mitigation of attacks and unauthorized access;
- System scalability and adaptability (C_6) – integration of new devices and services without compromising security;
- Supervision and management (C_7) – continuous monitoring and coordinated response to security incidents.

The defined criteria enable the quantitative evaluation of alternative network architectures by assessing their ability to ensure business continuity, resilience to cyber threats and effective recovery after incidents. Each criterion is associated with the corresponding functions of the NIST CSF framework and classified as a benefit or cost criterion, depending on whether a higher value represents better or worse system performance. The rating scale is defined in the range from 1 to 5, where a higher value indicates a higher level of network infrastructure performance, except for the recovery time criterion, where a lower value represents a better result.

3.2. Determination of criterion weights using the PIPRECIA-S method

To determine the weights of the criteria objectively, the PIPRECIA-S method (Simplified Pivot Pairwise Relative Criteria Importance Assessment) was applied, which represents an improved version of the PIPRECIA method and is used to determine the weighting coefficients of the criteria in multi-criteria decision-making. The advantages of the PIPRECIA-S method are that it does not require complete matrices of pairwise comparisons, enables a flexible choice of reference criteria, reduces the burden on experts during assessment, and is suitable for group decision-making (Stanujkić et al., 2021).

The procedure for determining the weight coefficients of criteria using the PIPRECIA-S method consists of several steps. In the first step, a set of criteria C_j is defined, where $j = 1, \dots, n$, and n represents the total number of criteria that are taken into account when solving the problem. The criteria are determined on the basis of relevant literature, cyber security standards and professional opinions of experts.

In the second step, each expert independently determines the reference criterion C_{ref}, which is used as a basis for comparing other criteria. The remaining criteria are assigned the relative importance of criteria s_j based on equation (1).

$$s_j = \begin{cases} 1, & for\ C_j = C_{ref} \\ [0.6, 1.4], & for\ C_j \neq C_{ref} \end{cases} \quad (1)$$

In f criterion C_j is more important than criterion C_{ref}, a value s_j that is greater than 1 is assigned to it. If criterion C_j is less important than criterion C_{ref}, a value less than 1 is assigned to

it. If criteria C_{ref} and C_j are equally important, then both criteria have an importance value of 1. The relative importance of the reference criterion always has a value of 1.

In this research, it was adopted that the range $s_j \in [0{,}6,\ 1{,}4]$ (Bašić et al., 2025). This choice is in accordance with the recommendations from the literature on PIPRECIA-S methods, but it is additionally adapted to the specifics of cyber resistance evaluation, where the criteria are often found at similar levels of importance, and extreme differences are very rare. Limiting the range to [0,6, 1,4] avoids extreme estimates that could damage the stability of the model and lead to a disproportionate impact of certain criteria.

In the next step, the coefficient of relative importance of the criterion k_j is calculated based on equation (2).

$$k_j = \begin{cases} 1, & j = 1 \\ 2 - s_j, & j > 1 \end{cases} \tag{2}$$

Then, based on the coefficient k_j, the value of the preliminary weight of the criterion q_j is calculated, according to equation (3).

$$q_j = \begin{cases} 1, & j = 1 \\ \dfrac{q_{j-1}}{k_j}, & j > 1 \end{cases} \tag{3}$$

In order to obtain the final criteria weights that can be used in further multi-criteria analysis, the preliminary weights are normalized according to equation (4):

$$w_j = \frac{q_j}{\sum_{i=1}^{n} q_i} \tag{4}$$

where $0 \leq w_j \leq 1$ and $\sum_{j=1}^{n} w_j = 1$.

Considering that group decision-making is applied to the research, each member of the expert group independently determines the reference criterion and evaluates the relative importance of the remaining criteria, after which the preliminary weights of the criteria are calculated. Based on the obtained values, expert assessments are aggregated using the arithmetic mean, which results in the aggregated value of the preliminary weights. In order to assess the reliability of expert assessments, the standard deviation of the preliminary weights of the criteria is calculated. The degree of conformity of expert assessments is checked using the coefficient of variation. Values of the coefficient of variation less than 0,2 indicate a high level of agreement among experts and confirm the stability of the obtained weight coefficients. In the final step, the aggregated preliminary weights are normalized. The obtained weight coefficients represent the relative importance of the criteria and are used in the next phase of the research to assess the cyber resilience of the network infrastructure of different network architectures of educational institutions.

3.3. Defining alternative network architectures

In order to conduct a comparative assessment of the cyber resilience of the network infrastructure of educational institutions, a set of alternatives $A = \{A_l | l = 1, \dots, m\}$ is defined, where m represents the total number of considered alternatives. Three alternatives were chosen that represent different approaches to the design, implementation and management of network architecture, and are most often applied in educational institutions.

Traditional hierarchical LAN architecture (A_1) – a multi-layer model with locally managed devices. It is simple and stable, but limits rapid response and recovery in the event of a cyber disruption.

Software Defined Networking SDN (A_2) – control plane separated from data transmission plane. A centralized controller enables dynamic management, flexible traffic policies and quick response to incidents. It is suitable for digital platforms and cloud services.

Hybrid cloud-managed network architecture (A_3) – combines local infrastructure with cloud services for monitoring and management. It enables scalability, advanced security and process automation, especially for universities with a large number of users.

3.4. Defining cyber disruption scenarios

Defining the cyber disruption scenario is based on the principles of the ISO 31000 standard for risk management. The set of scenarios $S = \{S_i | i = 1, \dots, k\}$ is analyzed, where k is the total number of considered cyber disturbances. Each scenario S_i is defined to reflect real threats that are characteristic of educational institutions. For each scenario, in the phase of quantitative evaluation, the relative importance of the scenario and the impact of the scenario on the cyber resistance criteria are determined. Five scenarios were defined in the research.

Failure of a critical network device (S_1) - This scenario includes the failure of the main router, switch or controller of the central part of the network infrastructure. Consequences include reduced network availability, disruption of communication between segments, and difficult access to information systems, learning platforms, and administrative services.

Interruption of communication links (S_2) – The scenario refers to the interruption of wired or wireless connections within the network or to the Internet. The consequences are loss of connection, reduced performance and difficult use of digital educational platforms and cloud services.

Network traffic overload (S_3) - This scenario simulates an increased number of users, e.g. during online classes or electronic testing. The consequences are increased data transfer delays, reduced network speed and degradation of service quality.

Distributed Denial-of Service attack (S_4) - This scenario involves external attacks that burden network resources and prevent access to key services. Consequences include loss of system availability, platform outages, and reduced network infrastructure resiliency.

Compromise of cloud or educational information services (S_5) – This scenario involves the compromise of cloud platforms, LMS systems, servers or network services for teaching and administration. The consequences are loss of data access, system downtime and reduced network security.

3.5. Determining scenario weights based on the ISO 31000 framework

The ISO 31000 risk management framework is used to determine the relative importance of scenarios. The assessment of the probability of occurrence of the scenario P_{S_i} for each of the scenarios S_i is determined based on the relevant literature, available statistical data on cyber incidents and the professional opinion of experts in the field of network security and information systems. When assessing the probability, factors such as the reliability of network devices, the frequency of attacks on educational platforms, the vulnerability of network services and the level of exposure of educational institutions to cyber threats are taken into account. Probability values are assigned in a range from 0 to 1, where a value of 0 indicates a virtually impossible scenario, while a value of 1 indicates an almost certain scenario.

The potential impact of the scenario I_{S_i} is evaluated based on the consequences that the disruption may have on the network infrastructure and the functioning of the educational institution's information systems. The impact assessment includes the impact on the availability of network services, system recovery time, fault tolerance, network security, scalability and infrastructure manageability. The impact of the scenario is evaluated on a scale from 1 to 5, where the value 1 indicates minimal consequences, and the value 5 maximum consequences for the functioning of the educational institution. The weight of the scenario w_{S_i} for each of the scenarios S_i, is determined by applying equation (5).

$$w_{S_i} = P_{S_i} \cdot I_{S_i} \tag{5}$$

When a group of experts participates in the research, where each expert independently assesses the weight of each scenario, the preliminary weight of each scenario per expert is calculated. The obtained values are aggregated using the arithmetic mean, after which they are normalized, so that the sum of the weights of all scenarios is equal to 1. Before normalizing the weight coefficients of the scenarios, the consistency of expert assessments is examined to ensure the reliability of the obtained results. Checking the homogeneity of grades is done by calculating the coefficient of variation. All values of the coefficient of variation below 0,2 are acceptable and confirm that expert assessments are homogeneous and reliable.

3.6. Formation of scenario-based decision-making matrices and calculation of cyber resilience index

After the scenarios of cyber disruptions have been defined and their severity assigned through expert assessment, the next step in the H-SCRM methodology is the formation of scenario-based decision-making matrices and the quantification of the cyber resistance of the considered alternatives to the network infrastructure of educational institutions. For each scenario S_i, a decision matrix is formed according to equation (6):

$$X^{(i)} = \left[x_{lj}^{(i)}\right]_{m\times n}, i = 1,2,\dots,k \tag{6}$$

where:

$X^{(i)}$ - decision-making matrix for scenario S_i,

m - the total number of network architecture alternatives,

n - total number of cyber resilience criteria,

$x_{lj}^{(i)}$ – performance evaluation of alternative A_l according to criterion C_j in scenario S_i.

Each element $x_{lj}^{(i)}$ is evaluated on the basis of an independent expert assessment and represents the expected level of cyber resistance of the observed alternative in relation to the given criteria and a specific disruption scenario.

To allow comparability between criteria of different units and scales, each decision-making matrix must be normalized. Normalization results in a normalized matrix $R^{(i)}$ defined by equation (7) for each scenario.

$$R^{(i)} = \left[r_{lj}^{(i)}\right]_{m\times n}, i = 1,2,\dots,k \tag{7}$$

For benefit criteria, normalization is performed according to equation (8).

$$r_{lj}^{(i)} = \frac{x_{lj}^{(i)}}{\sqrt{\sum_{l=1}^{m}\left(x_{lj}{}^{(i)}\right)^2}} \tag{8}$$

For cost criteria, normalization is performed according to equation (9).

$$r_{lj}^{(i)} = \frac{1/x_{lj}^{(i)}}{\sqrt{\sum_{l=1}^{m}\left(1/x_{lj}^{(i)}\right)^2}} \tag{9}$$

With this procedure, the normalized values become dimensionless and mutually comparable, which enables their further aggregation and calculation of the resistance index. In this work, Root Mean Square normalization was used, instead of the classic min-max normalization. This type of normalization was chosen because it takes into account all criteria values through the sum of squares, which enables proportional scaling of grades so that extreme values are not overemphasized.

After forming the normalized decision matrices, the next step is to calculate the partial resilience indices for each alternative within each scenario. The partial resistance index of the alternative A_l in the scenario $S_i$is calculated as a weighted sum of the normalized criteria values according to equation (10):

$$R_l^{(i)} = \sum_{j=1}^{n} w_j \cdot r_{lj}^{(i)} \quad (10)$$

where:
$R_l^{(i)}$ - partial cyber resistance index of alternative A_l in scenario S_i,
w_j - weight coefficient of criterion C_j,
$r_{lj}^{(i)}$ - normalized value of alternative A_l according to criterion C_j in scenario S_i,
n - total number of resistance criteria.

The partial resilience index enables a quantitative assessment of the performance of the network architecture within an individual scenario, taking into account the relative importance of the criteria. In order to obtain the overall cyber resilience of the network architecture in all considered scenarios, the partial resilience indices are aggregated into the global cyber resilience index of the alternative A_l according to equation (11):

$$GR_l = \sum_{i=1}^{k} w_{S_i} \cdot R_l^{(i)} \quad (11)$$

where:
GR_l - global cyber resilience index of alternative A_l,
w_{S_i}– normalized weight of scenario S_i,
$R_l^{(i)}$– partial resistance index of alternative A_l in scenario S_i,
k - total number of defined disturbance scenarios.

The Global Cyber Resilience Index enables a comparable quantitative assessment of all considered network architectures, whereby a higher value of the index indicates a higher level of resilience of the educational institution's network architecture in conditions of various cyber disruptions. Based on the obtained values of the global index, it is possible to rank the alternatives and identify the optimal solution from the aspect of cyber resistance.

3.7. Expert sample and evaluation method

Considering the complexity of cyber resilience of educational systems and the fact that a large part of the relevant parameters cannot be reliably quantified solely on the basis of measurement data, in this research an expert assessment with two independent groups of experts was applied.

The first group consists of five members with more than five years of professional experience in designing, implementing and managing network systems in educational institutions and critical infrastructure. Experts come from the fields of communication networks, ICT, cyber security and IT infrastructure management in schools and universities. All experts are familiar with the functional requirements of educational systems, as well as with the architectural and operational characteristics of the analyzed network architectures.

This group is responsible for determining the relative importance of cyber resilience criteria using the PIPRECIA-S method. Each expert independently selects a reference criterion and evaluates other criteria relative to it in order to obtain preliminary weights. The same group also assesses disruption scenarios using the ISO 31000 approach, where probability and impact of each scenario are evaluated and then aggregated and normalized.

The second group of five experts is responsible for the operational evaluation of system performance. They have practical experience in network architecture design, cybersecurity and IT systems in educational institutions. Based on their knowledge, they evaluate the performance of each alternative under different disruption scenarios. These evaluations form decision matrices used for further analysis. To reduce subjective bias, all assessments are performed independently, and final values are obtained by aggregating results using the arithmetic mean across criteria, alternatives and scenarios.

4. Results and discussion

This chapter presents the results of the application of the H-SCRM methodology for the quantitative assessment of cyber resilience of network architectures in educational institutions, based on defined criteria, disruption scenarios and expert assessments.

4.1. Determination of weight coefficients of resistance criteria

Table 1 shows the choice of reference criteria of each member of the first expert group, as well as the relative importance of criteria s_j. Although the experts independently chose the reference criterion based on which they evaluated the relative importance of the other criteria, the mathematical structure of the PIPRECIA-S method remained the same for all experts.

Table 1. Selection of the reference criterion and determination of the relative importance of the criteria

Expert	Reference criterion	s_j						
		C_1	C_2	C_3	C_4	C_5	C_6	C_7
Expert 1	C_1 – Availability of network infrastructure	1.0	1.0	0.8	1.0	1.2	1.0	1.0
Expert 2	C_3 – Network traffic management	1.0	0.8	1.0	1.0	1.2	1.0	0.8
Expert 3	C_6 – System scalability and adaptability	1.0	0.8	1.0	0.8	1.2	1.0	1.0
Expert 4	C_1 – Availability of network infrastructure	1.0	1.0	0.8	1.0	1.2	1.0	0.8
Expert 5	C_5 – Resilience to cyber threats	1.0	0.8	1.0	0.8	1.0	1.0	1.0

Source: Authors' calculation

Expert ratings were processed using the PIPRECIA-S method, and the coefficient of variation less than 0.2 confirms a high degree of agreement among experts. The final values of weight coefficients and ranking criteria are shown in Table 2.

Table 2. Weight coefficients of cyber resistance criteria

C_j	w_j	Rank
C_1	0.160	1
C_2	0.144	3
C_3	0.133	5
C_4	0.124	6
C_5	0.150	2
C_6	0.150	2
C_7	0.139	4

Source: Authors' calculation

The analysis of the obtained weight coefficients shows that the criteria Availability of network infrastructure (C_1), Resistance to cyber threats (C_5), as well as the criterion Scalability and adaptability (C_6) have the greatest importance in the assessment of cyber resistance of network architectures of educational institutions. These results indicate that experts believe that the key factors of overall resilience are stable network availability, the system's ability to withstand attacks and flexibility in adapting to new conditions. The criteria Recovery time (C_2) and Supervision and management (C_7) occupy a medium level of importance, which indicates that their role is not negligible, but not dominant in relation to the first three criteria. The Network Traffic Management (C_3) and Failure Tolerance (C_4) criteria have the lowest importance, but still contribute to the cyber resilience rating.

4.2. Determination of severity of disturbance scenarios

To calculate the relative importance of disturbance scenarios, five experts evaluated the probability of occurrence P_{S_i} and the impact I_{S_i} of each of the five defined scenarios. The results of expert assessments are shown in Table 3.

Table 3. Assessment of the probability of occurrence and impact of cyber disruption scenarios

Expert 1		Expert 2		Expert 3		Expert 4		Expert 5	
P_{S_1}	I_{S_1}	P_{S_2}	I_{S_2}	P_{S_3}	I_{S_3}	P_{S_4}	I_{S_4}	P_{S_5}	I_{S_5}
0.8	5	0.8	5	0.7	5	0.8	5	0.8	5
0.6	4	0.6	4	0.6	4	0.7	4	0.6	4
0.5	3	0.5	3	0.6	3	0.5	3	0.5	3
0.6	5	0.6	5	0.6	5	0.5	5	0.6	5
0.7	5	0.7	5	0.6	5	0.7	5	0.7	4

Source: Authors' calculation

The preliminary weights of the scenarios are aggregated by the arithmetic mean, and the coefficient of variation less than 0,2 confirms the consistency of the ratings. The normalized values enable a quantitative comparison of the importance of the scenarios. Table 4 shows the normalized values of the weights of the disturbance scenarios and their ranking.

Table 4. Disturbance scenario weights and ranking

S_i	w_{S_i}	Rang
S_1	0.28	1
S_2	0.17	4
S_3	0.12	5
S_4	0.20	3
S_5	0.23	2

Source: Authors' calculation

The obtained results show that the scenario S_1- Failure of a critical network device has the highest aggregated weight, which confirms that the centralized network infrastructure represents a key point of system dependency and that its interruption directly affects the availability of communication services and control over distributed components. Scenario S_5 – compromise of cloud or educational information services takes second place, emphasizing the strategic role of external information services in the work of educational institutions, where their disruption can lead to a decrease in operational efficiency and control over teaching and administrative processes. Scenario S_4 - DDoS attack has a significant impact, which indicates the importance of protection against external cyber threats. The medium-ranked scenarios S_2 – interruption of communication links and S_3 – network traffic overload represent scenarios with a moderate operational impact, which can be partially mitigated by applying redundancy and alternative communication paths.

4.3. Quantifying the performance of alternatives by scenario

The next step in the application of the H-SCRM methodology is the quantification of the performance of the network architecture alternatives according to the defined cyber resilience criteria within each disruption scenario. For each disruption scenario S_i, a decision-making matrix was formed based on the assessment of another group of experts who evaluated three network architectures A_l according to each of the cyber resilience criteria C_j. Scores are assigned on a scale from 1 to 5, where a higher value indicates a better level of performance for the benefit criteria, while for the cost criteria, a lower value represents a more favorable solution. The values of expert ratings are aggregated using the arithmetic mean. The coefficient of variation, which in all cases

has a value less than 0,2 indicates a high degree of agreement between the experts and the stability of the alternative evaluation model. The normalized values of criteria scores by alternatives for each of the defined scenarios are shown in Table 5.

Table 5. Normalized values of criteria by alternatives for each scenario

A_l	S_i	C_1	C_2	C_3	C_4	C_5	C_6	C_7
A_1		0.471	0.500	0.448	0.463	0.45	0.352	0.466
A_2	S_1	0.581	0.500	0.588	0.550	0.588	0.616	0.611
A_3		0.665	0.708	0.673	0.695	0.673	0.705	0.640
A_1		0.511	0.520	0.485	0.450	0.485	0.391	0.536
A_2	S_2	0.483	0.465	0.571	0.534	0.571	0.559	0.631
A_3		0.681	0.631	0.686	0.703	0.686	0.699	0.631
A_1		0.424	0.488	0.424	0.424	0.457	0.352	0.468
A_2	S_3	0.566	0.517	0.566	0.566	0.571	0.588	0.624
A_3		0.707	0.586	0.679	0.707	0.685	0.735	0.686
A_1		0.449	0.500	0.424	0.424	0.449	0.316	0.468
A_2	S_4	0.561	0.500	0.566	0.566	0.561	0.574	0.624
A_3		0.702	0.567	0.679	0.707	0.702	0.718	0.749
A_1		0.424	0.569	0.424	0.424	0.449	0.316	0.424
A_2	S_5	0.566	0.675	0.566	0.566	0.561	0.574	0.566
A_3		0.707	0.432	0.707	0.707	0.702	0.718	0.707

Source: Authors' calculation

The analysis of normalized values shows that alternative A_3 in every scenario achieves the highest values according to benefit criteria, especially in relation to the criteria of flexibility, scalability and continuity of system operation. Alternative A_2 shows stable but moderate performance, while alternative A_1 achieves the lowest values in most scenarios, which indicates a lower level of network infrastructure resilience in educational institutions.

4.4. Calculation of partial resistance indices according to scenarios

A partial resistance index is calculated for each alternative under individual scenarios, taking into account the calculated relative weights of the criteria obtained by the PIPRECIA-S method. The partial resilience index represents a weighted sum of normalized criteria values and shows the level of resilience of the network architecture in a specific disruption scenario. The values of the partial resistance indices of the alternatives according to the scenarios are shown in Table 6.

The results shown in Table 6 indicate that the differences between the alternatives in scenarios S_1, S_2 and S_3 are relatively uniform. This means that in conditions of failure of a critical network device, interruption of communication links and network traffic overload, all alternatives can maintain the basic level of functionality, but with different degrees of efficiency. Alternative A_3achieves the best performance in these scenarios, which confirms its stability and ability to maintain the continuity of the educational institution's information system.

Table 6. Partial indices of resistance of alternatives according to each scenario

A_l	$R_l^{(1)}$	$R_l^{(2)}$	$R_l^{(3)}$	$R_l^{(4)}$	$R_l^{(5)}$
A_1	0.449	0.484	0.421	0.411	0.414
A_2	0.575	0.541	0.570	0.566	0.568
A_3	0.678	0.675	0.706	0.716	0.721

Source: Authors' calculation

In scenario S_4, which represents a DDoS attack, there is a more pronounced separation of alternatives. Alternative A_3 reaches a significantly higher value of the partial resistance index,

while alternative A_1 records the lowest value. This result indicates that DDoS attacks represent one of the most critical disruptions for network architectures of educational institutions and that only more robust configurations can provide an adequate level of protection and continuity of information services.

In scenario S_5, which represents the breach of cloud or educational information services, the dominant position of alternative A_3, which achieves the highest partial resistance index, is additionally confirmed. This result indicates the pronounced ability of this alternative to ensure continuity of work, stability of information systems and data protection even in complex cyber incidents.

4.5. Calculation of the global resistance index

The global resilience index is calculated by applying the H-SCRM aggregation of partial resilience indices taking into account the relative weights of the disturbance scenarios. This index represents the overall level of resilience of network architecture in educational institutions and enables the final ranking of alternatives. Figure 1 shows the values of the global resilience index, as well as the ranking of the analyzed alternatives.

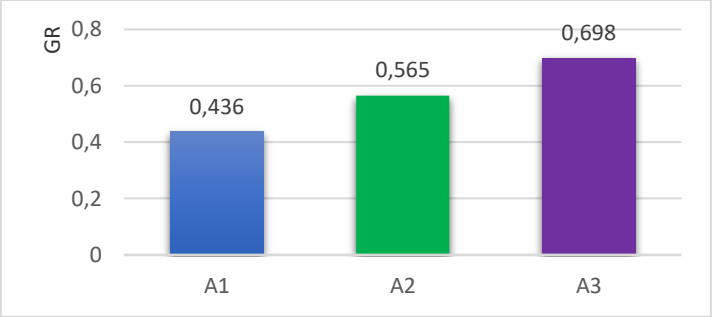

Figure 1. Global index of resilience of alternatives
Source: Authors' calculation

The results presented in Figure 1 show that the introduction of scenario weights did not change the ranking of the alternatives, which confirms the stability and robustness of the H-SCRM decision model. Alternative A_3 achieves the highest value of the global resilience index and maintains a dominant position even after weighting the scenarios, while alternative A_1 remains the least resilient network architecture.

5. Sensitivity analysis of the H-SCRM model

Sensitivity analysis allows examining the impact of changes in input parameters on the final results of the model and the ranking of alternatives. In this way, it can be determined whether the global resilience index and the ranking of network architectures depend on the initial weights of criteria and scenarios or whether the model maintains stability under different decision conditions.

Within this research, two types of sensitivity analysis were conducted: (1) changing the weights of criteria to simulate different expert priorities of cyber resilience, and (2) changing the weights of disruption scenarios to examine the impact of cyber incidents on the global resilience index of network architectures.

5.1. Criteria weight variation

The sensitivity analysis was carried out by changing the weight of an individual criterion, while the weights of the remaining criteria are proportionally adjusted in order to preserve the normalization condition. If we assume that the weight of the criterion changes, the variable

weight of this criterion represents a decrease or increase in weight by ±20%. The remaining weights of the criteria are proportionally adjusted in order to preserve the normalization condition. In this way, it is ensured that the sum of the new weights of the criteria remains equal to one, thus maintaining the consistency of the decision model. The partial index of resistance of the alternative in the scenario after changing the weights is recalculated based on the normalized values of alternatives according to the observed criteria. On the basis of the obtained partial resistance indices, the global resistance index of the alternatives is recalculated, which enables the analysis of the impact of changes in the weights of the criteria on the final ranking of network architectures.

The sensitivity analysis is focused on criteria C_1, C_5 and C_6 because these are the criteria with the highest weights. Given that these three criteria have the greatest weight, they proportionally have a greater impact on the partial resilience indices, as well as on the global resilience index. Figure 2 shows a graphic representation of the sensitivity analysis of the global resilience index after changing the weight of the key criteria by ±20%. The results indicate a high robustness of the model, because even with extreme changes in the weight of the most important criteria, there are no changes in the ranking of alternatives. The graphic lines visually highlight the impact of certain criteria on the global resilience index. Changing the weight of criterion C_6 gives the largest jump or fall of the index, which indicates that this criterion has the greatest impact on the evaluation of resilience. This information is important in strategic decision-making and prioritization of investments in the field of cyber resilience.

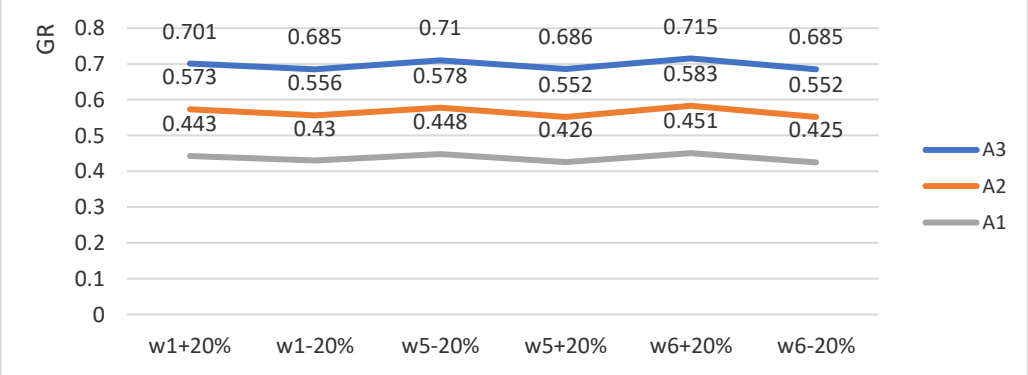

Figure 2. Global resilience index after changing the weight of key criteria
Source: Authors' calculation

5.2. Scenario weight variation

The weights of the scenarios represent the relative importance of various cyber incidents and network infrastructure disruptions in educational institutions, and their impact is directly reflected in the value of the global alternative resilience index. Therefore, it is necessary to examine whether the change in the importance of individual scenarios affects the final ranking of network architectures and the stability of the decision-making model.

In order to check the stability of the model, additional sets of scenario weights were defined that simulate different priorities of cyber incidents in educational institutions. Changing the weight of the scenario enables the analysis of the behavior of the model in conditions of different security priorities, such as the increased importance of DDoS attacks, greater dependence on cloud services or even risk distribution. Within the sensitivity analysis, three sets of scenario weights are defined:

- Model A – an even distribution of scenario weights, which represents a neutral environment in which all cyber incidents have the same importance;

- Model B – increased importance of DDoS attacks, where scenario S_4 gets the most weight, thus simulating an environment with frequent network attacks;
- Model C – increased importance of cloud and information services, where scenario S_5 gets the most weight, which simulates the high dependence of educational institutions on digital services.

The scenario weights for all analyzed models are shown in Table 7.

Table 7. Scenario weights by models for sensitivity analysis

S_i	Basic model	**Model A**	**Model B**	**Model C**
S_1	0.28	0.20	0.20	0.20
S_2	0.17	0.20	0.15	0.15
S_3	0.12	0.20	0.10	0.10
S_4	0.20	0.20	0.35	0.20
S_5	0.23	0.20	0.20	0.35

Source: Authors' calculation

Based on the new scenario weights, the global resistance index of the alternatives was recalculated, and the results are shown in Figure 3.

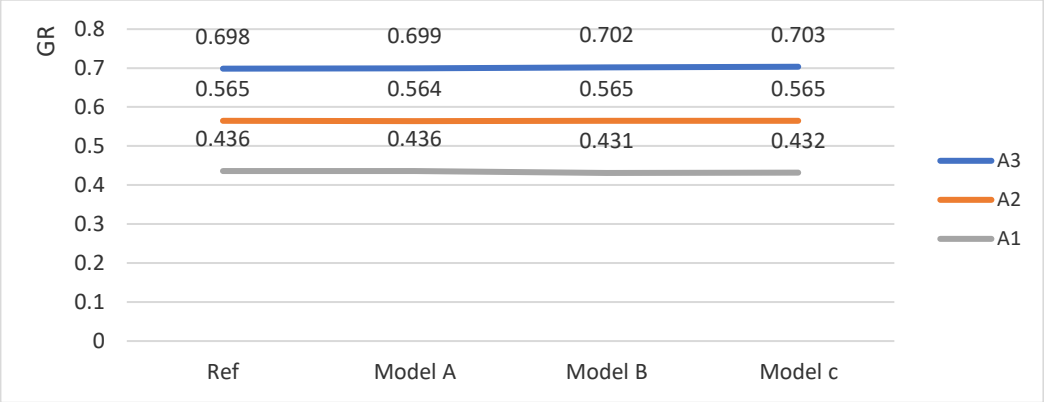

Figure 3. Stability of the ranking of alternatives when the weights of the scenarios change
Source: Authors' calculation

The analysis shows that, even with changes in scenario weights, the ranking of alternatives remains stable. Alternative A_3 retains the dominant position in all cases, which confirms the robustness of the proposed decision model. Alternatives A_2 and A_1 also keep their orders, which indicates that the variations of scenario weights do not lead to significant changes in the choice of the optimal network architecture for educational institutions.

6. Conclusion

In this work, the H-SCRM methodology was applied for the quantitative assessment of the cyber resilience of network architectures of educational institutions. Through the identification of seven key criteria ($C_1 - C_7$) and the definition of five disruption scenarios ($S_1 - S_5$), aggregated and normalized matrices were formed that enabled the calculation of partial resilience indices by alternatives, as well as a weighted global resilience index. The obtained results show that alternative A_3 consistently achieves the highest resistance index, which indicates that this architecture best responds to potential cyber threats in the analyzed context.

The analysis of normalized values and partial indices shows that the criteria Availability of network infrastructure (C_1), Resistance to cyber threats (C_5) and Scalability and adaptability (C_6) have a dominant influence on the global resilience index, while the other criteria contribute to a

lesser extent, but are significant for the overall assessment. The sensitivity analysis, performed by changing the weights of the three dominant criteria ±20%, shows that the ranking of the alternatives remains stable, which confirms the robustness of the model and the practical applicability of the results.

The proposed model allows managers of educational institutions to identify critical points of their network architectures and implement protection measures as a matter of priority. In addition, the methodology contributes to the application of multi-criteria decision-making in the specific context of network architectures of educational institutions, filling a gap in the literature that mainly focuses on IT infrastructure in a general sense.

The research conducted has several limitations. The first limitation is that the criterion ratings were collected by five experts, which limits the generalization of the results. A larger sample of experts would increase the reliability of the assessment and reduce the risk of individual biases. On the other hand, the number of disruption scenarios is fixed and does not include all possible situations in a real cyber environment. Adding new scenarios or combinations of risk events could affect the values of the partial and global resilience indices. The ratings were made on a scale from 1 to 5, which, despite the confirmed homogeneity through the coefficient of variation, may reflect the subjective preferences of experts. Additionally, dynamic changes in network infrastructure and unexpected attacks are not included in the analysis, which may affect the actual level of resilience in practice.

Future research directions include expanding the number of criteria and scenarios to include advanced cyber-attacks, insider threats, and IoT device failures, as well as integrating predictive algorithms and machine learning to adaptively adjust weights and scenarios based on real-world events. The proposed methodology can be applied to other sectors and systems that require multi-criteria resilience assessments, thus enabling a wider application of the model.

References

Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions. *Future Internet*, *17*(12), 575. https://doi.org/10.3390/fi17120575

AlHidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). Towards a cyber resilience quantification framework (CRQF) for IT infrastructure. Computer Networks, 247, 110446. https://doi.org/10.1016/j.comnet.2024.110446

Araujo, M., Machado, B., & Passos, F. (2024). Resilience in the context of cyber security: A review of the fundamental concepts and relevance. Applied Sciences, 14, 2116. https://doi.org/10.3390/app14052116

Avramova, T., Peneva, T., & Ivanov, A. (2025). Overview of Existing Multi-Criteria Decision-Making (MCDM) Methods Used in Industrial Environments. Technologies, 13(10), 444. https://doi.org/10.3390/technologies13100444

Bašić, A., & Viduka, D. (2025). Multi-criteria decision-making in the evaluation of software testing methods. Sinteza 2025 – International Scientific Conference on Information Technology, Computer Science, and Data Science, 150–157. https://doi.org/10.15308/Sinteza-2025-150-157

Bašić, A., Viduka, D., Kraguljac, V., Lavrnić, I., Jevremović, M., Balaban, P., Sajfert, D., Gligorijević, M., & Barzut, S. (2024). Multi-Criteria Decision Analysis of Wireless Technologies in WPANs for IoT-Enabled Smart Buildings in Tourism. Buildings, 14(10), 3275. https://doi.org/10.3390/buildings14103275

Bellini, E., D'Aniello, G., Flammini, F., & Gaeta, R. (2025). Situation awareness for cyber resilience: A review. International Journal of Critical Infrastructure Protection, 49, 100755. https://doi.org/10.1016/j.ijcip.2025.100755

Dong, X., & Xie, Y. (2025). Research on cloud computing network security mechanism and optimization in university education management informatization based on OpenFlow. Systems and Soft Computing, 7, 200225. https://doi.org/10.1016/j.sasc.2025.200225

Gallon, L., Salameh, K., Chbeir, R., Bachir, S., & Aniorté, P. (2024). Educational Cyber–Physical Systems (ECPSs) for University 4.0. Information, 15(12), 790. https://doi.org/10.3390/info15120790

Güntem, O., & Kılıç, Y. (2025). Efficiency and Sustainability in Online Education: An Evaluation of LMS Platforms and University Websites in Northern Cyprus. Sustainability, 17(9), 4166. https://doi.org/10.3390/su17094166

Ibrahim, F. (2024). Importance of cybersecurity in educational institutions. https://doi.org/10.13140/RG.2.2.34745.99681

International Organization for Standardization. (2018). *ISO 31000:2018 Risk management — Guidelines*. ISO.

Jauković Jocić, K., Karabasević, D., & Jocić, G. (2020). The use of the PIPRECIA method for assessing the quality of e-learning materials. Ekonomika, 66, 37–45. https://doi.org/10.5937/ekonomika2003037J

Jawaid, S. A. (2023). Cyber security threats to educational institutes: A growing concern for the new era of cybersecurity. International Journal of Data Science and Big Data Analytics, 2, 11–17. https://doi.org/10.51483/IJDSBDA.2.2.2022.11-17

Kiryakova, G. (2017). Application of cloud services in education. Trakia Journal of Science, 15(4), 277–284. https://doi.org/10.15547/tjs.2017.04.001

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector. Computers, 14(2), 49. https://doi.org/10.3390/computers14020049

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. Energy Reports, 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Liu, T., Luo, Y. T., Pang, P. C.-I., & Kan, H. Y. (2025). Exploring the Impact of Information and Communication Technology on Educational Administration: A Systematic Scoping Review. Education Sciences, 15(9), 1114. https://doi.org/10.3390/educsci15091114

Madanchian, M., & Taherdoost, H. (2025). Applications of Multi-Criteria Decision Making in Information Systems for Strategic and Operational Decisions. Computers, 14(6), 208. https://doi.org/10.3390/computers14060208

Marinović, M., Viduka, D., Lavrnić, I., Stojčetović, B., Skulić, A., Bašić, A., Balaban, P., & Rastovac, D. (2025). An Intelligent Multi-Criteria Decision Approach for Selecting the Optimal Operating System for Educational Environments. Electronics, 14(3), 514. https://doi.org/10.3390/electronics14030514

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. https://www.nist.gov/cyberframework

Olowo, B., Ahamefula, N., & Chukwu, B. (2026). Digital school management system in the 21st century education: Necessary, not a luxury. Federal University Gusau Faculty of Education Journal, 6, 338–346. https://doi.org/10.64348/zije.2026284

Pacheco, A., Yupanqui, R., Mogrovejo, D., Garay, J., & Uribe-Hernández, Y. (2025). Impact of digitization on educational management: Results of the introduction of a learning management system in a traditional school context. Computers in Human Behavior Reports, 17, 100592. https://doi.org/10.1016/j.chbr.2025.100592

Park, C., Son, M., Kim, J., Kim, B., Ahn, Y., & Kwon, N. (2025). TOPSIS and AHP-Based Multi-Criteria Decision-Making Approach for Evaluating Redevelopment in Old Residential Projects. Sustainability, 17(15), 7072. https://doi.org/10.3390/su17157072

Popović, S., Viduka, D., Bašić, A., Dimić, V., Djukic, D., Nikolić, V., & Stokić, A. (2025). Optimization of Artificial Intelligence Algorithm Selection: PIPRECIA-S Model and Multi-Criteria Analysis. Electronics, 14(3), 562. https://doi.org/10.3390/electronics14030562

Rathnayaka, B., Robert, D., Adikariwattage, V., Siriwardana, C., Meegahapola, L., Setunge, S., & Amaratunga, D. (2024). A unified framework for evaluating the resilience of critical infrastructure: Delphi survey approach. International Journal of Disaster Risk Reduction, 110, 104598. https://doi.org/10.1016/j.ijdrr.2024.104598

Rezvani, S. M. H. S., Silva, M. J. F., & de Almeida, N. M. (2024). Urban resilience index for critical infrastructure: A scenario-based approach to disaster risk reduction in road networks. Sustainability, 16, 4143. https://doi.org/10.3390/su16104143

Salas Riega, J., Riega, Y., Soto, M., & Salas-Riega, J. (2025). Cybersecurity and the NIST framework: A systematic review of its implementation and effectiveness against cyber threats. International Journal of Advanced Computer Science and Applications, 16. https://doi.org/10.14569/IJACSA.2025.0160672

Shetelia, N., Apshay, F., Telep, O., Ahiy, Y., & Maslov, V. (2024). The role of information communications in the educational environment of higher education institutions. Journal of Educational Technology Development and Exchange, 17(1), 188–204. https://doi.org/10.18785/jetde.1701.11

Singh, K., Chatterjee, S., Mariani, M., & Wamba, S. F. (2025). Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment. Technovation, 143, 103219. https://doi.org/10.1016/j.technovation.2025.103219

Stanujkić, D., Karabasević, D., Popović, G., & Sava, C. (2021). Simplified pivot pairwise relative criteria importance assessment (PIPRECIA-S) method. Romanian Journal of Economic Forecasting, 24(4), 141–154.

Taherdoost, H., & Madanchian, M. (2023). Multi-Criteria Decision Making (MCDM) Methods and Concepts. Encyclopedia, 3(1), 77-87. https://doi.org/10.3390/encyclopedia3010006

Tariq, R., Casillas-Muñoz, F., Hassan, S., & Ramírez-Montoya, M.-S. (2025). Synergy of Internet of Things and education: Cyber-physical systems contributing towards remote laboratories, improved learning, and school management. https://doi.org/10.6084/m9.figshare.24927696

Theilig, K., Vollmer, M., Lang, W., & Albus, J. (2025). Multi-criteria decision-making for energy building renovation: Comparing exterior wall structures with the AHP, ANP, utility analysis, and TOPSIS. Building and Environment, *280*, 113075. https://doi.org/10.1016/j.buildenv.2025.113075

Veljić, A., Viduka, D., Ilić, L., Karabasevic, D., Šijan, A., & Papić, M. (2025). Sustainable Decision-Making in Higher Education: An AHP-NWA Framework for Evaluating Learning Management Systems. Sustainability, 17(22), 10130. https://doi.org/10.3390/su172210130

Wibowo, B., Ibrahim, N., Yuswanto, A., & Hidayat, T. (2025). Cyber resilience to digital threats for education institutions 4.0. International Journal of Management Science and Application, 4, 35–45. https://doi.org/10.58291/ijmsa.v4i1.370