Hierarchical Models of Information Systems Security Metrics: A Comparative Sectoral Approach

Ansar Daghouri
Interdisciplinary Research Laboratory in Sciences, Education and Training, Higher Education and Training School, Hassan I University, Settat, Morocco
ansar.daghouri@uhp.ac.ma (corresponding author)

Khalifa Mansouri
Laboratory: Modeling and Simulation of Intelligent Industrial Systems, ENSET of Mohammedia, Hassan II University, Casablanca, Morocco
khmansouri@hotmail.com

Received: 2 August 2024 | Revised: 5 September 2024 and 8 September 2024 | Accepted: 14 September 2024

 DOI: https://doi.org/10.48084/etasr.8401

ABSTRACT

Information system security metrics are critical in assessing and mitigating data protection risks. Executives must improve the security of their information systems. However, it is important to note that there is a wide variety of metrics available and that generic measurements may not be effective for the broader enterprise. This article provides an overview of information system security metrics and introduces a novel hierarchical model for them. Adopting a comparative approach across five sectors (health, finance, industry, government, and education), the Analytical Hierarchy Process (AHP) was used to design and evaluate the model in each sector context. The objective was to identify the variation in security criteria based on the sector. The results obtained confirm that the criteria weights vary according to the sector involving a change in the hierarchical evaluation model.

Keywords-information systems; security; security metrics; risk management; MCDM

I. INTRODUCTION

In today's digital age, ensuring the security of Information Systems (IS) is a critical concern for organizations across multiple sectors [1]. Pursuing relevant and effective cybersecurity measures in this complex landscape presents an ongoing challenge [2]. The literature offers numerous security metrics used in various fields [3], but most of them are irrelevant or ineffective. An example of a commonly utilized metric is the number of viruses detected or deleted in a firewall, which lacks usefulness as it does not provide information on the number of undetected viruses [4]. IS security has become a crucial foundation for any organization, ensuring data confidentiality, accessibility, and integrity [5], as well as protecting processes and operations [6]. However, as cyber threats continue to evolve and businesses adapt to technological advances, it is imperative to enhance the current IS security metric models [7], especially in diverse sectoral contexts. This justification relies on several crucial aspects. First, the diversity of sectors indicates unique requirements and risks regarding IS security metrics [8]. Generic models often fail to capture sectoral nuances, which can result in unaddressed vulnerabilities [9]. This study aimed to examine sectoral differences and develop a hierarchical model adapted to each context, providing a more targeted and effective approach. Technological advancements have led to the emergence of new threats and vulnerabilities, necessitating a constant review of IS security metrics [10]. The proposed hierarchical models aim to evolve with these changes, providing greater flexibility and data adaptability to address emerging security challenges. This vision is crucial for optimizing the effectiveness of information security metrics and proactively addressing industry challenges [11]. In summary, this study is a necessary response to the evolving threats and sector-specific needs related to information security. Hierarchical models were developed and compared across five sectors, namely health, finance, industry, government, and education, to offer innovative solutions that enhance IS security resilience within modern organizations.

This study introduces a novel hierarchical model for information system security metrics, which has been specifically designed to address sector-specific needs. The model is structured into three levels: strategic, tactical, and operational. The strategic level is concerned with the overarching governance and policy frameworks, whereas the tactical level addresses operational mechanisms such as data protection and incident management. The operational level addresses technical aspects, including the security of networks

and applications. The innovation of this study lies in its sector-specific comparative approach, which employs the AHP method to evaluate and adapt the model across five distinct sectors. This approach not only elucidates sector-specific variations in security criteria, but also provides a flexible framework that is amenable to adaptation in response to emerging threats and evolving regulatory requirements. The integration of these elements into a unified model signifies a substantial advancement in the adaptation of security metrics to a multitude of organizational contexts.

II. LITERATURE REVIEW

A. Security Metrics

A metric is a measurement unit that aids in decision-making, enhancing performance and accountability by collecting, analyzing, and reporting relevant data [12]. In terms of security, metrics are a collection of quantitative and qualitative measures employed to evaluate different aspects of cybersecurity [13]. These measures aim to objectively evaluate the strength of systems, networks, applications, and security practices [14]. Security metrics quantify different aspects, such as security control performance, policy effectiveness, attack resilience, and compliance with standards. Security metrics cover areas, such as confidentiality, integrity, availability, authentication, security, and awareness [15], each offering specific criteria to assess IS security. There are multiple guidelines available for organizations to follow when implementing security metrics. Some of the frequently referenced standards are [16, 17]: ISO/IEC 27001 [18], ISO/IEC 27002 [19], NIST SP 800-53 [20], COBIT (Control Objectives for Information and Related Technologies) [21], and ITIL (Information Technology Infrastructure Library) [22]. Assessing and quantifying cybersecurity is vital to protecting systems and ensuring the safety of confidential data. According to the literature, several metrics that provide a comprehensive view of an organization are available [23-25].

- Vulnerability metrics are a crucial component in evaluating the strength of a system. They enable the quantification of the identified vulnerabilities, the duration required to resolve them, and other factors related to system security.
- Threat detection metrics assess how well threat detection systems perform. This category consists of metrics such as the detection rate of threats and the rate of false positives, providing important information on how well a system can detect suspicious behavior.
- Compliance metrics assess compliance with security standards and regulations. Such metrics gauge how well an organization follows set standards and ensure effective information governance practices.
- Security incident metrics evaluate how often and how serious security incidents are. They are crucial for determining an organization's ability to withstand threats. This group of measures also covers incident response time, which is essential for reducing potential harm.
- Patch management metrics assess the efficiency of patch management by gauging the speed at which patches are discovered, tested, and implemented to maintain system robustness.

B. MCDM Methods

Multi-Criteria Decision Making (MCDM) is an analysis method deployed to solve complicated problems utilizing numerous criteria [26]. This section aims to create a strong base by presenting the fundamental concepts of MCDM and conducting a thorough examination of the AHP [27], which will serve as a guide for assessing alternatives. The reason for choosing the AHP is that it is well-suited to the hierarchical and complex nature of this decision problem, has a systematic way of conducting pairwise comparisons [28], is flexible, includes consistency checks, is widely applicable, and promotes stakeholder participation. All of these factors work together to strengthen the reliability and credibility of this decision framework.

1) The Analytic Hierarchy Process (AHP)

Created by Thomas L. Saaty [29], AHP is based on the idea of simplifying complex decisions by breaking them down into a series of simpler comparisons. This systematic classification system helps to represent the relationships between the elements of a decision. The following steps outline the AHP [30-31]:

- Establish the hierarchy by recognizing the ultimate goal (O), criteria (C), and alternatives (A) and arranging them in a hierarchical format.
- Pairwise comparisons involve comparing elements with each other and indicating their relative preferences using a scale from 1 to 9. Next, a matrix is created to compare the criteria and another matrix to compare the alternatives:

$$A_{nn} = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \quad (1)$$

  where $a_{ij} = 1$ when $i = j$ and $a_{ji} = 1/a_{ij}$.
- Calculate the average of each column of the comparison matrices to obtain the relative weights for both criteria (W_C) and alternatives (W_A). Then, calculate the weight vector for the criteria using:

$$W_c = {}^1/_n \sum_{j=1}^{n} C_{ij} \quad (2)$$

  where n is the number of the criteria.
- Aggregate the weights to obtain the final weights of the criteria (W_{Cfinal}) and alternatives (W_{Afinal}) using:

$$W_{Cfinal} = {}^1/_m \sum_{i=1}^{m} W_c \quad (3)$$

  where m is the number of levels in the hierarchy.

III. METHODOLOGY

A. Purpose of the Study

This study aims to develop, improve, and evaluate hierarchical models of information security measures employing a comparative sectoral approach. The AHP is deployed to combine the criteria (subcriteria) of the

hierarchical model to detect important weight differences. Data were collected from the five sectors utilizing an online survey. This study focuses on the fields of health, finance, industry, government, and education, deliberately selected to provide thorough insights into the efficiency of the hierarchical models in various organizational settings. These sectors were chosen based on:

- Strategy Significance: Each of these industries has an essential role in both society and the economy. The health and financial sectors are crucial foundations, with industry and government fueling economic growth. Education is essential for future development. By selecting these industries, the study focuses on critical strategic areas.
- Variety of Sensitive Information: These industries manage and store a substantial amount of sensitive data. The healthcare field handles private medical data, the financial sector oversees important financial information, the industry manages proprietary trade information, the government deals with sensitive national security data, and education stores the personal information of students, professors, and employees.
- These sectors differ in organizational complexity, which requires for hierarchical models to be flexible.
- Regulations often impose strict data security measures on the chosen sectors. Thus, hierarchical models must consider these regulatory constraints, which are specific to the sector they need to comply.
- Each sector individually encounters different vulnerabilities and threats. An example is how the financial industry is often a common target for financial scams, whereas the healthcare industry is at risk of cyberattacks targeting medical information. It is crucial to consider these specific challenges when creating hierarchical models.
- Inter-sectoral learning: Comparative analyses across various sectors can help promote intersectoral learning. The lessons learned in one industry can be modified and implemented in different areas, promoting a joint and interdisciplinary method to secure information systems.

B. Methodology

The method followed consists of the following main steps, as summarized in Figure 1.

- Explore existing IS security metrics and standards by examining existing models and frameworks in the literature related to IS security with a particular focus on hierarchical aspects.
- Analyze the security metrics used in the five sectors (health, finance, industry, government, and education).
- Propose a hierarchical model of IS security metrics that takes into account the complexity of sectoral environments.
- Conduct a sectoral comparison by applying the model to the five sectors considering the specificities of each. Use the AHP to identify significant variations in security approaches.
- Assess the effectiveness and applicability of the proposed hierarchical model in terms of measuring IS security metrics across diverse sectors.

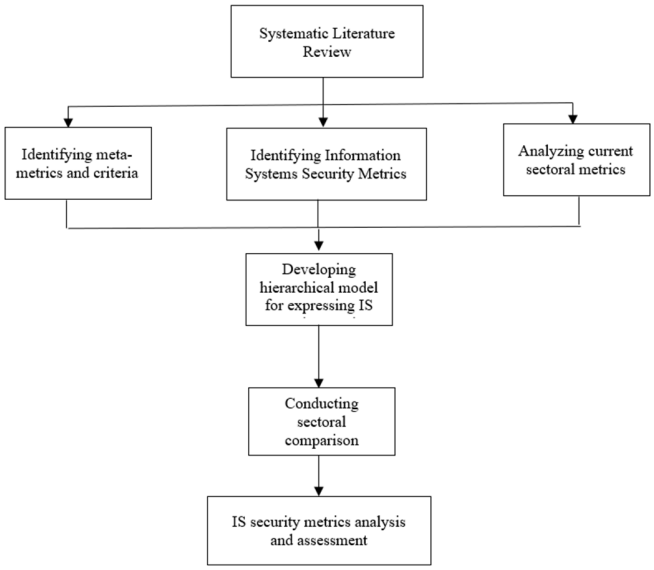

Fig. 1. The method.

C. The Proposed Model

The proposed model is inspired by information security management principles and cybersecurity best practices. The concepts incorporated can be linked to various information security standards and frameworks, such as ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-53, COBIT, and ITIL. The proposed model for evaluating IS security metrics is based on stratification into three distinct levels, as shown in Figure 2. Each level represents a crucial aspect of security and contributes cohesively to the overall organizational security posture.

- Strategic level: The strategic foundation includes important aspects, such as information security governance, security policies, standards, and regulatory compliance. This layer establishes the overall structure, defining the organization's directions and commitments regarding security. It also integrates the key elements of resource and risk management.
- Tactical level: At the tactical level, the focus is on the concrete operational mechanisms that support IS security. This includes data protection, access controls, threat management, intrusion detection, and incident management. These operational elements are essential for the effective implementation of policies and standards defined at the strategic level.
- Operational Level: Finally, this level focuses on the technical and technological aspects of security, including network, system, and application security. Daily activities at this level involve elements, such as firewalls, patch management, application security testing, and real-time monitoring to maintain a secure environment.

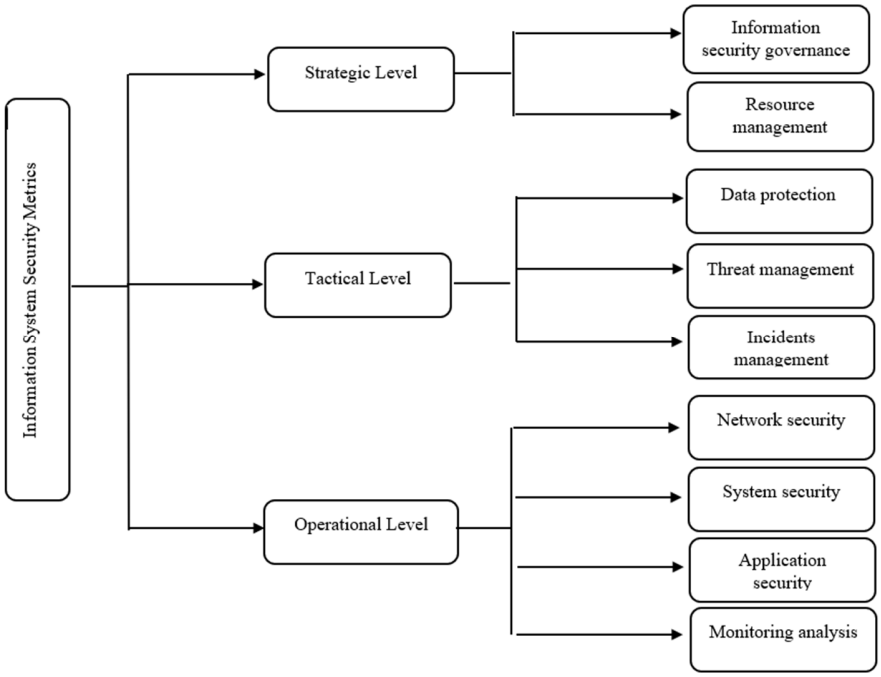

Fig. 2. The proposed model.

IV. RESULTS AND DISCUSSION

A. Implementation of AHP

As depicted in Table I, the hierarchical model consists of three levels, each composed of a set of criteria that are further decomposed into subcriteria. A questionnaire survey was conducted to collect data from decision-makers in the five sectors.

TABLE I. HIERARCHICAL PRESENTATION OF CRITERIA

Criteria	Subcriteria
Information security governance (C_{11})	Security policies (C_{111}), Security standards (C_{112}), Regulatory compliance (C_{113}), and Risk management (C_{114})
Resource management (C_{12})	Security budget allocation (C_{121}), Dedicated security personnel (C_{122}), and Training and awareness (C_{123})
Data protection(C_{21})	Access controls (C_{211}), Data encryption (C_{212}), Identity and access management (C_{213}), and Physical security of equipment (C_{214})
Threat management(C_{22})	Intrusion detection (C_{221}), Network monitoring (C_{222}), Vulnerability management (C_{223}), and Activity log analysis (C_{224})
Incidents management (C_{23})	Incident response plan (C_{231}), Incident simulation tests (C_{232}), Incident reports (C_{233}), and Post-incident analysis (C_{234})
Network security (C_{31})	Firewalls (C_{311}), Wireless security (C_{312}), Content filtering (C_{313}) and Network intrusion detection (C_{314})
System security (C_{32})	Match management (C_{321}), Antivirus and antimalware (C_{322}), Secure system configuration (C_{323}), and System monitoring (C_{324})
Application security (C_{33})	Application security testing (C_{331}), Application access controls (C_{332}), Secure development (C_{333}) and Certificate management (C_{334})
Monitoring analysis (C_{34})	Log analysis (C_{341}), Real-time monitoring (C_{342}), Abnormal behavior detection (C_{343}), and Compliance reports (C_{344})

1) The Health Sector (Sector 1)

Based on the hierarchical model presented in Table I, and following the steps of AHP, Figure 3 portrays the pairwise comparison matrix for this sector.

$$C_{I1} = \begin{bmatrix} 1 & 5 \\ 0.2 & 1 \end{bmatrix} \qquad C_{I2} = \begin{bmatrix} 1 & 3 & 5 \\ 0.33 & 1 & 7 \\ 0.2 & 0.14 & 1 \end{bmatrix}$$

$$C_{I3} = \begin{bmatrix} 1 & 0.33 & 0.2 & 5 \\ 3 & 1 & 0.2 & 5 \\ 5 & 5 & 1 & 5 \\ 0.2 & 0.2 & 0.2 & 1 \end{bmatrix}$$

Fig. 3. Aggregated pairwise comparison matrix (Sector 1).

Figure 4 shows the normalized decision matrix, calculated using (2).

$$C_{I1} = \begin{bmatrix} 0.83 & 0.83 \\ 0.17 & 0.17 \end{bmatrix} \qquad C_{I2} = \begin{bmatrix} 0.65 & 0.72 & 0.38 \\ 0.21 & 0.24 & 0.53 \\ 0.13 & 0.03 & 0.07 \end{bmatrix}$$

$$C_{I3} = \begin{bmatrix} 0.10 & 0.05 & 0.14 & 0.31 \\ 0.32 & 0.15 & 0.14 & 0.31 \\ 0.54 & 0.78 & 0.71 & 0.31 \\ 0.02 & 0.03 & 0.14 & 0.06 \end{bmatrix}$$

Fig. 4. Normalized decision matrix (Sector 1).

The priority weights for each criterion, calculated using (2), are:

W_{I11}=1.67/2=0.83 W_{I22}=0.96/3=0.32 W_{I32}=0,94/4=0,23

W_{I12}=0.33/2=0.17 W_{I23}=0.24/3=0,08 W_{I33}=2,36/4=0,59

W_{I21}=1.76/3=0.60 W_{I31}=0.61/4=0.15 W_{I34}=0,26/4=0,06

2) The Finance Sector (Sector 2)

Figure 5 displays the pairwise comparison matrix for this sector.

$$C_{II1} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \qquad C_{II2} = \begin{bmatrix} 1 & 5 & 3 \\ 0.2 & 1 & 3 \\ 0.33 & 0.33 & 1 \end{bmatrix}$$

$$C_{II3} = \begin{bmatrix} 1 & 0.2 & 0.14 & 0.33 \\ 5 & 1 & 0.33 & 3 \\ 7 & 3 & 1 & 5 \\ 3 & 0.33 & 0.2 & 1 \end{bmatrix}$$

Fig. 5. Aggregated pairwise comparison matrix (Sector 2).

Figure 6 illustrates the normalized decision matrix.

$$C_{II1} = \begin{bmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{bmatrix} \qquad C_{II2} = \begin{bmatrix} 0.65 & 0.78 & 0.42 \\ 0.13 & 0.15 & 0.42 \\ 0.21 & 0.05 & 0.14 \end{bmatrix}$$

$$C_{II3} = \begin{bmatrix} 0.06 & 0.04 & 0.09 & 0.03 \\ 0.31 & 0.23 & 0.22 & 0.32 \\ 0.43 & 0.71 & 0.68 & 0.53 \\ 0.18 & 0.07 & 0.13 & 0.11 \end{bmatrix}$$

Fig. 6. Normalized decision matrix (Sector 2).

The priority weights for each criterion are:

W_{II11}=1/2=0.5 W_{II22}=0.71/3=0.24 W_{II32}=1.1/4=0.27

W_{II12}=1/2=0.5 W_{II23}=0.41/3=0.14 W_{II33}=2.37/4=0.59

W_{II21}=1.87/3=0.62 W_{II31}=0.24/4=0.06 W_{II34}=0.51/4=0.13

3) The Industry Sector (Sector 3)

Figure 7 displays the pairwise comparison matrix for this sector.

$$C_{III1} = \begin{bmatrix} 1 & 0.2 \\ 5 & 1 \end{bmatrix} \qquad C_{III2} = \begin{bmatrix} 1 & 5 & 7 \\ 0.2 & 1 & 3 \\ 0.14 & 0.33 & 1 \end{bmatrix}$$

$$C_{III3} = \begin{bmatrix} 1 & 0.14 & 0.2 & 0.33 \\ 7 & 1 & 3 & 5 \\ 5 & 0.33 & 1 & 3 \\ 3 & 0.2 & 0.33 & 1 \end{bmatrix}$$

Fig. 7. Aggregated pairwise comparison matrix (Sector 3).

Figure 8 shows the normalized decision matrix.

$$C_{III1} = \begin{bmatrix} 0.17 & 0.17 \\ 0.83 & 0.83 \end{bmatrix} \qquad C_{III2} = \begin{bmatrix} 0.74 & 0.79 & 0.64 \\ 0.15 & 0.16 & 0.28 \\ 0.10 & 0.05 & 0.09 \end{bmatrix}$$

$$C_{III3} = \begin{bmatrix} 0.06 & 0.09 & 0.05 & 0.03 \\ 0.44 & 0.68 & 0.71 & 0.53 \\ 0.31 & 0.22 & 0.24 & 0.32 \\ 0.19 & 0.14 & 0.08 & 0.11 \end{bmatrix}$$

Fig. 8. Normalized decision matrix (Sector 3).

The priority weights for each criterion are:

W_{III11}=0.33/2=0.17 W_{III22}=0.58/3=0.19 W_{III32}=2.37/4=0.59

W_{III12}=1.67/2=0.83 W_{III23}=0.24/3=0.08 W_{III33}=1.07/4=0.27

W_{III21}=2.17/3=0.72 W_{III31}=0.24/4=0.06 W_{III34}=0.51/4=0.13

4) The Government Sector

Figure 9 displays the pairwise comparison matrix for this sector.

$$C_{IV1} = \begin{bmatrix} 1 & 0.2 \\ 5 & 1 \end{bmatrix} \qquad C_{IV2} = \begin{bmatrix} 1 & 5 & 7 \\ 0.2 & 1 & 3 \\ 0.14 & 0.33 & 1 \end{bmatrix}$$

$$C_{IV3} = \begin{bmatrix} 1 & 0.14 & 0.2 & 0.33 \\ 7 & 1 & 3 & 3 \\ 5 & 0.33 & 1 & 3 \\ 3 & 0.33 & 0.33 & 1 \end{bmatrix}$$

Fig. 9. Aggregated pairwise comparison matrix (Sector 4).

Figure 10 showcases the normalized decision matrix.

$$C_{IV1} = \begin{bmatrix} 0.17 & 0.17 \\ 0.83 & 0.83 \end{bmatrix} \qquad C_{IV2} = \begin{bmatrix} 0.75 & 0.79 & 0.64 \\ 0.15 & 0.16 & 0.27 \\ 0.10 & 0.05 & 0.09 \end{bmatrix}$$

$$C_{IV3} = \begin{bmatrix} 0.06 & 0.09 & 0.05 & 0.04 \\ 0.43 & 0.68 & 0.71 & 0.41 \\ 0.31 & 0.22 & 0.24 & 0.41 \\ 0.19 & 0.22 & 0.08 & 0.14 \end{bmatrix}$$

Fig. 10. Normalized decision matrix (Sector 4).

The priority weights for each criterion are:

W_{IV11}=0.33/2=0.17 W_{IV22}=0.58/3=0.19 W_{IV32}=2.24/4=0.56

W_{IV12}=1.67/2=0.83 W_{IV23}=0.25/3=0.08 W_{IV33}=1.18/4=0.29

W_{IV21}=2.17/3=0.72 W_{IV31}=0.25/4=0.06 W_{IV34}=0.63/4=0.16

5) The Education Sector

Figure 11 depicts the pairwise comparison matrix for this sector.

$$C_{V1} = \begin{bmatrix} 1 & 0.2 \\ 5 & 1 \end{bmatrix} \qquad C_{V2} = \begin{bmatrix} 1 & 5 & 7 \\ 0.2 & 1 & 3 \\ 0.14 & 0.33 & 1 \end{bmatrix}$$

$$C_{V3} = \begin{bmatrix} 1 & 0.14 & 0.2 & 0.33 \\ 7 & 1 & 3 & 3 \\ 5 & 0.33 & 1 & 3 \\ 3 & 0.33 & 0.33 & 1 \end{bmatrix}$$

Fig. 11. Aggregated pairwise comparison matrix (Sector 5).

Figure 12 demonstrates the normalized decision matrix.

$$C_{V1} = \begin{bmatrix} 0.17 & 0.17 \\ 0.83 & 0.83 \end{bmatrix} \qquad C_{V2} = \begin{bmatrix} 0.75 & 0.79 & 0.64 \\ 0.15 & 0.16 & 0.27 \\ 0.10 & 0.05 & 0.09 \end{bmatrix}$$

$$C_{V3} = \begin{bmatrix} 0.06 & 0.09 & 0.05 & 0.04 \\ 0.44 & 0.68 & 0.71 & 0.41 \\ 0.31 & 0.22 & 0.24 & 0.41 \\ 0.19 & 0.22 & 0.08 & 0.14 \end{bmatrix}$$

Fig. 12. Normalized decision matrix (Sector 5).

The priority weights for each criterion are:

W_{V11}=0.33/2=0.17 W_{V22}=0.58/3=0.19 W_{V32}=2.24/4=0.56

W_{V12}=1.67/2=0.83 W_{V23}=0.25/3=0.08 W_{V33}=1.18/4=0.29

W_{V21}=2.17/3=0.72 W_{V31}=0.25/4=0.06 W_{V34}=0.63/4=0.16

B. Discussion

In the context of applying the AHP, the main criteria (and subcriteria) were selected from the literature. The hierarchical model developed was tested in five sectors to identify the variance of security criteria based on the sector type and to test the possibility of having a general model to evaluate the security of the IS regardless of the sector. The model consists of three levels. At the strategic level, two main criteria are used to assess it: information security governance and resource management. Based on the AHP results, information security governance is particularly crucial for the healthcare sector (83%) due to the sensitive nature of the data processed and stored (confidentiality and protection of patient data). This goes beyond simple resource management by defining policies, procedures, and standards to ensure security. In the education sector, resource management (83%) is essential for curriculum planning, teacher and room allocation, improving the educational experience, pedagogical prioritization, and innovation.

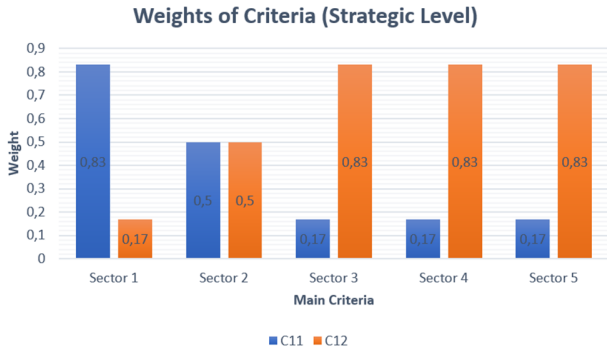

Fig. 13. Weights of main criteria (Strategic level).

Regarding the tactical level and the results provided in Figure 14, it is evident that data protection and threat management are considered more important than incident management due to their preventive and proactive roles in information security. Incident management occurs after a security incident has taken place. Focusing on data protection and threat management is substantial for mitigating damage, learning from past incidents, and improving future preparedness. This also strengthens an organization's overall resilience to potential threats on a tactical level.

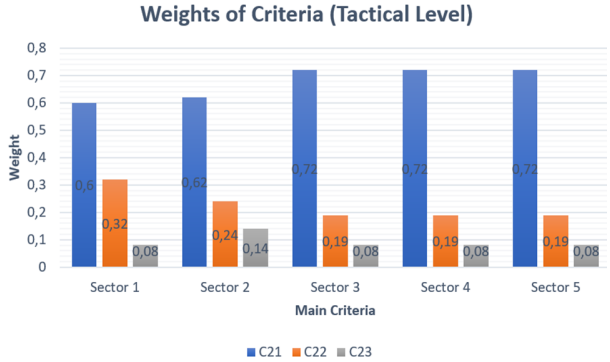

Fig. 14. Weights of main criteria (Tactical level).

Based on the weights presented in Figure 15, network security monitoring and analysis rank last among the five sectors, with respective weights of (15%, 6%, 6%, 6%, 6%) for network security, and (6%, 13%, 13%, 16%, 16%) for monitoring and analysis. While network security is undoubtedly important, it is often considered a requirement. Other security aspects, such as application and system security, may depend on a secure network infrastructure. Overall security at the operational level depends on a holistic approach. In some cases, the focus may be on system and application security due to the need to protect sensitive data, ensure the availability of critical systems, and prevent software vulnerabilities.

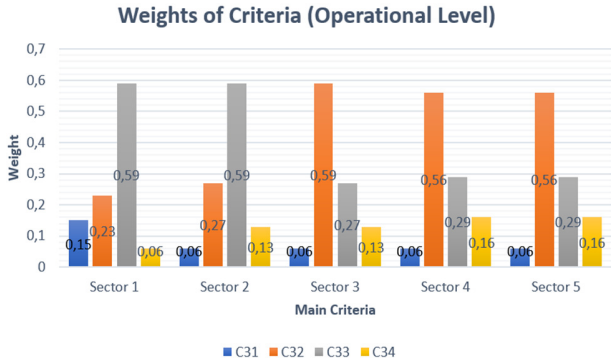

Fig. 15. Weights of main criteria (Operational level).

According to the results outlined in Figure 16, which summarizes all criteria weights in the five sectors, the criteria weights differ from one sector to another due to the specificities and unique priorities of each sector in terms of information security. For example, information security governance is more important in the financial sector. These differences in weighting highlight the adaptability of the AHP. However, these variations in weights remain minimal in the five sectors, and future work can discuss the possibility of having a general model to evaluate IS security, by focusing on the weights of the subcriteria.

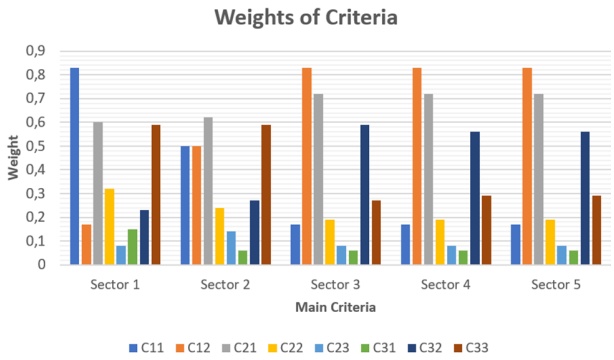

Fig. 16. Weights of main criteria across the five sectors.

V. CONCLUSION

The security of information systems has become a key concern. In light of the increasing number of threats and the

strategic importance of information systems in a range of fields, it is vital to implement robust security metrics. This study presented a novel hierarchical model of IS security metrics, developed using the AHP, across five strategically important sectors: health, finance, industry, government, and education. These sectors were selected because of the diversity of sensitive data and the distinct vulnerabilities they present. The hierarchical model offered an approach that addresses sector-specific requirements, thereby advancing beyond the generic models that are typically employed in this field. By evaluating and adapting the model across distinct sectors, this study reveals important sector-specific variations in criteria weights, thus enhancing the precision of the resulting security metrics. Although the results indicate minimal variation in the weights of the criteria across sectors, this finding highlights the necessity for further investigation into the weights of subcriteria to enhance the model's applicability. Future work should concentrate on validating the model within each sector and examining these variations in greater detail.

This study makes a significant contribution to the field by offering a more detailed and adaptable framework for the assessment of the information system security. This framework aligns with the latest threats to information systems and meets the specific requirements of different sectors. The comparative sectoral approach of the model demonstrates its relevance and potential to improve security resilience in a range of organizational contexts.

REFERENCES

[1] F. Basholli, R. Mezini, and A. Basholli, "Security in the components of information systems," *Advanced Engineering Days (AED)*, vol. 7, pp. 185–187, Jul. 2023.

[2] M. I. Khalil and M. Abdel-Rahman, "Advanced Cybersecurity Measures in IT Service Operations and Their Crucial Role in Safeguarding Enterprise Data in a Connected World," *Eigenpub Review of Science and Technology*, vol. 7, no. 1, pp. 138–158, Jul. 2023.

[3] S. Gupta Bhol, J. Mohanty, and P. Kumar Pattnaik, "Taxonomy of cyber security metrics to measure strength of cyber security," *Materials Today: Proceedings*, vol. 80, pp. 2274–2279, Jan. 2023, https://doi.org/10.1016/j.matpr.2021.06.228.

[4] A. Lakhani, "The Ultimate Guide to Cybersecurity." OSF, Jan. 31, 2024, https://doi.org/10.31219/osf.io/b6z2h.

[5] S. Duggineni, "Impact of Controls on Data Integrity and Information Systems," *Science and Technology*, vol. 13, no. 2, pp. 29–35, 2023.

[6] A. Ali, K. Ullah, and A. Hussain, "An approach to multi-attribute decision-making based on intuitionistic fuzzy soft information and Aczel-Alsina operational laws," *Journal of Decision Analytics and Intelligent Computing*, vol. 3, no. 1, pp. 80–89, Jun. 2023, https://doi.org/10.31181/jdaic10006062023a.

[7] S. Dhar, A. Khare, and R. Singh, "Advanced security model for multimedia data sharing in Internet of Things," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 11, 2023, Art. no. e4621, https://doi.org/10.1002/ett.4621.

[8] S. Ahmadi, "Cloud Security Metrics and Measurement," *Journal of Knowledge Learning and Science Technology*, vol. 2, no. 1, pp. 93–107, 2023, https://doi.org/10.60087/jklst.vol2.n1.p107.

[9] O. Safianu, F. Twum, and J. B. Hayfron-Acquah, "Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection," *International Journal of Computer Applications*, vol. 143, no. 5, pp. 8–14, Jun. 2016, https://doi.org/10.5120/ijca2016910160.

[10] H. Taherdoost, "An Overview of Trends in Information Systems: Emerging Technologies that Transform the Information Technology Industry," *Cloud Computing and Data Science*, pp. 1–16, 2023, https://doi.org/10.37256/ccds.4120231653.

[11] T. C. Herath, H. S. B. Herath, and D. Cullum, "An Information Security Performance Measurement Tool for Senior Managers: Balanced Scorecard Integration for Security Governance and Control Frameworks," *Information Systems Frontiers*, vol. 25, no. 2, pp. 681–721, Apr. 2023, https://doi.org/10.1007/s10796-022-10246-9.

[12] U. Zdun *et al.*, "Microservice Security Metrics for Secure Communication, Identity Management, and Observability," *ACM Transactions on Software Engineering and Methodology*, vol. 32, no. 1, pp. 1–34, Jan. 2023, https://doi.org/10.1145/3532183.

[13] H. U. Khan, M. Z. Malik, S. Nazir, and F. Khan, "Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis," *IEEE Access*, vol. 11, pp. 80181–80198, 2023, https://doi.org/10.1109/ACCESS.2023.3298824.

[14] M. Chauhan and S. Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions," *Network*, vol. 3, no. 3, pp. 422–450, Sep. 2023, https://doi.org/10.3390/network3030018.

[15] V. A. Desnitsky, I. V. Kotenko, I. B. Parashchuk, and E. V. Fedorchenko, "Metrics and Indicators of Security of Critical Resources in State and Corporate Objects and Processes," in *2023 Seminar on Information Computing and Processing (ICP)*, Saint Petersburg, Russian Federation, Nov. 2023, pp. 42–47, https://doi.org/10.1109/ICP60417.2023.10397416.

[16] A. Arabsorkhi and F. Ghaffari, "Security Metrics: Principles and Security Assessment Methods," in *2018 9th International Symposium on Telecommunications (IST)*, Tehran, Iran, Dec. 2018, pp. 305–310, https://doi.org/10.1109/ISTEL.2018.8661030.

[17] A. D. Khaleefah and H. M. Al-Mashhadi, "Methodologies, Requirements, and Challenges of Cybersecurity Frameworks: A Review," *Iraqi Journal of Science*, vol. 65, no. 1, 2024.

[18] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *The TQM Journal*, vol. 33, no. 7, pp. 76–105, Jan. 2021, https://doi.org/10.1108/TQM-09-2020-0202.

[19] S. Sahibudin, M. Sharifi, and M. Ayat, "Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations," in *2008 Second Asia International Conference on Modelling & Simulation (AMS)*, Kuala Lumpur, Malaysia, May 2008, pp. 749–753, https://doi.org/10.1109/AMS.2008.145.

[20] E. H. N. Safitri and H. Kabetta, "Cyber-Risk Management Planning Using NIST CSF V1.1, ISO/IEC 27005:2018, and NIST SP 800-53 Revision 5 (A Study Case to ABC Organization)," in *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*, Bogor, Indonesia, Aug. 2023, pp. 332–338, https://doi.org/10.1109/ICoCICs58778.2023.10277652.

[21] C. F. Anggraini, N. M. Estiyanti, and P. A. C. Dewi, "Governance Audit Using COBIT 5 in CV. XYZ on Accounting Information System," *ADI Journal on Recent Innovation*, vol. 4, no. 2, pp. 201–209, Jan. 2023, https://doi.org/10.34306/ajri.v4i2.870.

[22] Y. Ernawati and G. Wang, "Assessing IT Services Management with ITIL Framework V3: A Case Study," *Journal of System and Management Sciences*, vol. 14, no. 4, Aug. 2023, https://doi.org/10.33168/JSMS.2023.0409.

[23] A. Y. Abdalmagid, S. M. H. Shukry, and H. Soubra, "Towards Universal Metrics for Hardware Cybersecurity Assessment," in *2023 Eleventh International Conference on Intelligent Computing and Information Systems (ICICIS)*, Cairo, Egypt, Nov. 2023, pp. 225–232, https://doi.org/10.1109/ICICIS58388.2023.10391137.

[24] S. V. N. Santhosh Kumar, M. Selvi, and A. Kannan, "A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things," *Computational Intelligence and Neuroscience*, vol. 2023, no. 1, 2023, Art. no. 8981988, https://doi.org/10.1155/2023/8981988.

[25] M. Mastroianni, F. Palmieri, M. Ficco, R. Kozik, and M. Choraś, "Privacy risk analysis and metrics in capturing and storing network traffic," in *2023 24th International Conference on Control Systems and Computer Science (CSCS)*, Bucharest, Romania, May 2023, pp. 580–585, https://doi.org/10.1109/CSCS59211.2023.00097.

[26] A. Kumar and K. Kaur, "MCDM- Based Framework to Solve Decision Making Problems in Software Engineering," in *2022 3rd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, Ghaziabad, India, Nov. 2022, pp. 1–5, https://doi.org/10.1109/ICICT55121.2022.10064599.

[27] D. S. Costa, H. S. Mamede, and M. M. da Silva, "A method for selecting processes for automation with AHP and TOPSIS," *Heliyon*, vol. 9, no. 3, Mar. 2023, https://doi.org/10.1016/j.heliyon.2023.e13683.

[28] T. Kyrylych and Y. Povstenko, "Multi-Criteria Analysis of Startup Investment Alternatives Using the Hierarchy Method," *Entropy*, vol. 25, no. 5, May 2023, Art. no. 723, https://doi.org/10.3390/e25050723.

[29] N. Prascevic, "Application of Fuzzy AHP Method for Selection of Equipment for Concrete Works," in *Intelligent and Fuzzy Systems*, 2023, pp. 319–326, https://doi.org/10.1007/978-3-031-39777-6_39.

[30] V. Singh, V. Kumar, and V. B. Singh, "A hybrid novel fuzzy AHP-TOPSIS technique for selecting parameter-influencing testing in software development," *Decision Analytics Journal*, vol. 6, Mar. 2023, Art. no. 100159, https://doi.org/10.1016/j.dajour.2022.100159.

[31] A. Daghouri, K. Mansouri, and M. Qbadou, "Enhanced Model For Evaluating Information System Success: Determining Critical Criteria," *Engineering, Technology & Applied Science Research*, vol. 8, no. 4, pp. 3194–3198, Aug. 2018, https://doi.org/10.48084/etasr.2148.