Strengthening resilience against cyberattacks in Moroccan Universities through AHP, TOPSIS, and ITIL v4

Abdelilah Chahid, Souad Ahriz, Kamal El Guemmat, Khalifa Mansouri
Department of Mathematics and Computer Science, Higher Normal School of Technical Education of Mohammedia, Mohammédia, Morocco

Article Info

Article history:

Received Jun 19, 2024
Revised Sep 29, 2024
Accepted Oct 7, 2024

Keywords:

AHP
Cybersecurity
Digital transformation
ITIL V4
TOPSIS

ABSTRACT

This study addresses the complex challenges of digital transformation in higher education by enhancing IT governance to combat cyber threats in Moroccan universities. By adopting a hybrid multi-criteria decision-making (MCDM) framework, the research combines the analytic hierarchy process (AHP) and the TOPSIS method to evaluate fourteen IT governance criteria, categorized into structural, procedural, and relational dimensions. Using TOPSIS, the study identifies the most relevant SVC services from the ITIL v4 value chain for each category, with the aim of developing an optimized strategic approach against cyberattacks. The input from ten academic experts was crucial in prioritizing these services. The results show that SVC services A5 and A2 are fundamental for optimizing the resources of structural and procedural mechanisms, while A4 and A2 play a key role in relational mechanisms. This strategic alignment enhances the resilience of Moroccan universities to cyber threats by ensuring a more efficient allocation of security resources and providing a robust defense against potential attacks.

Corresponding Author:

Abdelillah Chahid
Department of Mathematics and Computer Science
Higher Normal School of Technical Education of Mohammedia
Bd Hassan II, Mohammédia 28830, Morocco
Email: chahidabdelillah@gmail.com

1. INTRODUCTION

Digital transformation, driven by social change, is driving economic development and impacting all sectors [1]. Experts are therefore analyzing digital transformation in detail to understand its effects, advantages and disadvantages, especially for companies that could fail without it [2]. In higher education, digital transformation encompasses social, organizational and technological changes, affecting teaching, infrastructure, curriculum, administration, research, operations, human resources, knowledge dissemination, governance and information management, while encouraging this transformation [3]. During the COVID-19 pandemic, higher education institutions have been rapidly pushed to adopt digital technologies and revise their teaching methods to adapt to new and specific constraints [4]. This rush towards digitalization has unfortunately increased their exposure to the risks of cyberattacks, making the information systems of these institutions more vulnerable in an already complex context [5], [6]. This situation requires the establishment of robust information systems governance mechanisms, based on solid structures, well-defined processes and effective interpersonal relationships [7]. The effective implementation of these best practices not only helps to secure information systems but also facilitates the adoption of digital solutions essential to ensure educational continuity, thereby minimizing the risks of cyberattacks and enabling institutions to effectively navigate the integration of technology and the protection of infrastructures against increasing and complex threats [8].

Several approaches have been proposed to enhance cybersecurity in higher education institutions. Among these, the implementation of information systems governance frameworks, such as ISO27001 and COBIT, is one of the most commonly adopted strategies. These frameworks provide structured guidelines for managing IT services and protecting sensitive data [9]. Additionally, decision-making methodologies, such as the analytic hierarchy process (AHP) and the TOPSIS method, are frequently used to evaluate and prioritize security practices based on their specific relevance and effectiveness in various contexts [10], [11].

Despite these solutions, several constraints limit their adoption and effectiveness. Budget constraints are one of the main barriers to the implementation of robust security systems [12]. Additionally, the complexity of university IT infrastructures, often associated with organizational resistance to change, complicates the rapid adaptation to new security technologies. As the cybersecurity threat landscape continuously evolves, institutions must also contend with the need to maintain constant technological vigilance and perform frequent updates, which adds an additional burden. This allows institutions to prioritize the most critical actions while ensuring an optimal allocation of resources [13].

The primary objective of this research is to evaluate and prioritize the most effective cybersecurity governance practices for Moroccan universities, using AHP and TOPSIS methodologies to determine those that offer the greatest relevance in this specific context. The integration of these practices within the ITIL v4 framework aims to develop a targeted and optimized cybersecurity strategy that meets the unique needs of academic institutions while maximizing their resilience against cyber threats. The final goal is to provide academic decision-makers with a practical framework to improve their security posture, aligning these practices with strategic objectives while considering resource constraints [13].

2. THEORETICAL BACKGROUND

2.1. IT governance

In higher education institutions, structural IT governance capabilities include establishing clear roles and responsibilities [14], having an IT Strategy Committee [15]-[19] and IT Steering Committees [20]-[22], as well as appropriate organizational structuring [23], [24] and integrating the CIO into executive committees [25]. These structures are essential for effective IT governance and positively influence the absorptive capacity of IT governance in universities. Process capabilities encompass strategic information system planning [26], [27], portfolio management [28]-[30], and the adoption of IT governance frameworks such as COBIT, ITIL, ISO, PRINCE2, PMBOK, and BSC [31]-[36]. These processes play a crucial role in setting priorities and enhancing the operational efficiency of IT governance. Relational capabilities include IT leadership [37], formal communication [26], [32], [38], and knowledge management [26], [32], [39]. These capabilities facilitate strategic dialogue, shared learning, and effective collaboration between IT and business functions, thereby strengthening the performance of IT governance.

2.2. Digital transformation and cyberattacks

Rapid digital transformation has created significant security gaps for organizations, necessitating a shift in focus towards protecting data distributed across multiple platforms [40]. In higher education institutions, digital transformation enhances accessibility and personalization of education through digital technologies [41], facilitates efficient management of administrative and academic operations, and supports pedagogical innovation with new online tools. However, this increased reliance on technologies raises the risks of cyberattacks [42], making the protection of sensitive data and the implementation of cybersecurity strategies tailored to modern threats crucial. Therefore, it is essential that the securing of digital infrastructures accompanies the transformation to protect stakeholders and digital assets, requiring close collaboration between IT and cybersecurity departments to align transformation initiatives with best security practices [43].

2.3. ITIL v4

Risk management is an intrinsic component of any business, whether explicitly acknowledged or not. How a company handles these risks is crucial to its ongoing success. At the heart of the service value system (SVS), risk management ensures that the organization effectively addresses potential challenges. Chahid *et al.* [44], ITIL as a whole can be considered a risk management framework. Risk assessment is defined as a key element of risk management for the successful implementation of an information security management system (ISMS), as studied by [45]. This practice is critical not only for the SVS but also for the survival of an organization.

Haufe *et al.* [46] found that the risk assessment process is standardized not only in ITIL but also in COBIT and the ISO 27000 series. These same authors identified risk management as one of the most recognizable core processes of the ISMS [47]. Without adequate risk management, an organization would overlook many other areas of IT management. Given its importance, we deem it necessary to review value chain activities in the domain of cyberattack risk management, aligning SVC services with established governance methods. Figure 1 illustrates that, within the SVS, the service value chain represents a flexible operational model designed for the creation, delivery, and continuous improvement of the following services.

- Planning: Integrates threat monitoring and legal requirements to anticipate and mitigate potential risks. Emphasis is placed on continuous assessment of vulnerabilities and their impacts on university operations.
- Improvement: Focuses on assessing and testing the resilience of IT systems against cyberattacks, with regular updates and security patches to maintain system integrity.
- Engagement: Identifies key stakeholders and evaluates their risk tolerance, integrating cybersecurity perspectives to align policies and procedures.
- Design and transition: New IT services are designed with robust security mechanisms, and security impact assessments are conducted before deployment to prevent vulnerabilities.
- Acquisition and development: Purchase and development decisions are guided by security risk management, ensuring that products and services comply with high security standards.
- Delivery and support: Integrate proactive security risk management strategies, with real-time monitoring and incident response plans for quick action against threats.

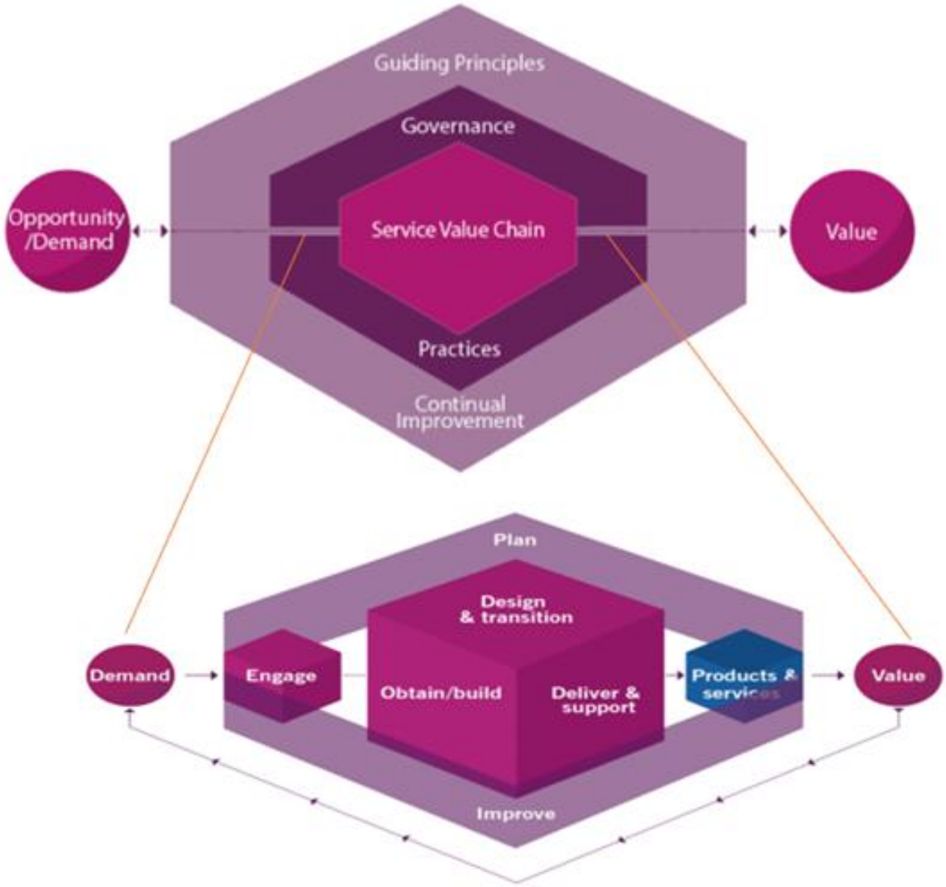

Figure 1. The ITIL 4 service value system [48]

2.4. AHP

Thomas Saaty developed AHP in the 1970s as a systematic decision-making method [49], incorporating both qualitative and quantitative techniques. This method is particularly useful for deriving a single assessment value based on various indicators or criteria. It simplifies the decision-making process by breaking down a complex problem into a series of structured steps, where each element in the criteria hierarchy is assumed to be independent of the others, simplifying complex decision-making by breaking down the problem into a hierarchy of independent criteria.

However, when criteria are interdependent, the Analytic Network Process is more appropriate. AHP involves creating a hierarchy of decision elements and comparing them in pairs to generate a matrix. These paired comparisons yield weighting scores that reflect the relative importance of each item or criterion. Decision-makers assess two alternatives based on a specific criterion, using a standard numeric scale from 1 to 9, where 1 indicates "equal importance" and 9 indicates "extreme importance" between factors. Each level of the hierarchy results in an n×nn \times nn×n matrix, where nnn represents the number of elements at that level.

AHP facilitates consensus building among decision-makers, allowing them to compare their judgments and understand the impact of their priorities. The decision process in AHP involves the following steps [50]:

- Define the problem and establish the goal.
- Identify the criteria influencing the goal, organizing them into levels and sublevels.
- Conduct paired comparisons of each factor to form a comparison matrix, calculate weights, rank eigenvalues, and assess consistency.
- Synthesize the alternative rankings to arrive at the final decision.

Similarly, the technique for order of preference by similarity to ideal solution (TOPSIS), developed by Hwang and Yoon in 1981, is another multi-criteria decision analysis method [51]. TOPSIS operates by hypothesizing two artificial alternatives: the ideal solution (IS), representing the best possible level for all attributes, and the negative ideal solution (NIS), representing the worst attribute values. The method prioritizes alternatives based on their geometric distance from these ideal and negative solutions. The decision process in TOPSIS unfolds as follows [51]:

- Step 1: Calculate the normalized decision matrix. The normalized value n_{ij} is calculated as:

$$n_{ij} = \frac{x_{ij}}{\sqrt{\sum_{j=1}^{m} x_{ij}^2}}, i = 1, \ldots, n, j = 1, \ldots, m \tag{1}$$

- Step 2. Calculate the weighted normalized decision matrix. The weighted normalized value v_{ij} is calculated as:

$$v_{ij} = w_i n_{ij}, i = 1, \ldots, n, j = 1, \ldots, m \tag{2}$$

where w_i is the weight of the ith attribute or criterion, and $\sum_{i=1}^{n} w_i = 1$.

- Step 3. Determine the positive ideal (A^+) and negative ideal (A^-) solutions:

$$A^+ = \{v_1^+, \ldots, v_n^+\} = \left\{\left(\max_i v_{ij} | j \in J_1\right), \left(\min_i v_{ij} | j \in J_2\right)\right\} \; A^- = \{v_1^-, \ldots, v_n^-\} = \left\{\left(\min_i v_{ij} | j \in J_1\right), \left(\max_i v_{ij} | j \in J_2\right)\right\}, i = 1, \ldots, m. \tag{3}$$

where J_1 is associated with benefit criteria, and J_2 is associated with cost criteria.

- Step 4. Calculate the separation measures using the n-dimensional Euclidean distances. The distance of each alternative for positive ideal solution (d_j^+) and for negative ideal solution (d_j^-) are given as, respectively,

$$d_j^+ = \left\{\sum_{i=1}^{n} \left(v_{ij} - v_j^+\right)^2\right\}^{1/2} \; d_j^- = \left\{\sum_{i=1}^{n} \left(v_{ij} - v_j^+\right)^2\right\}^{1/2} \tag{4}$$

- Step 5. Calculate the relative closeness to the ideal solution R_j.

$$R_j = \frac{d_j^-}{d_j^+ + d_j^-}, j = 1, \ldots, m \tag{5}$$

If $d_j^- \geq 0$ and $d_j^+ \geq 0$, then $R_j \in [0,1]$.

3. RESEARCH METHOD

This article details a structured approach to cybersecurity risk management in higher education institutions in Morocco, within the context of digital transformation. Utilizing the international ITIL v4 framework and its service value chain (SVC), this method focuses on selecting and prioritizing defense mechanisms against cyberattacks. Through a literature review and semi-structured interviews with risk management experts, our study proposes an evaluation process based on three key IT governance criteria: structure, processes, and relationships. These criteria allow for the prioritization of defense mechanisms using the AHP method. Once these mechanisms are prioritized, the TOPSIS method is employed to evaluate and rank the six ITIL v4 SVC services based on their effectiveness in integrating these defense mechanisms. This dual approach ensures that the choices made are both effective and aligned with the institution's strategic objectives, thereby enhancing its capacity to manage cybersecurity risks. Table 1 presents the three ITG mechanisms identified in Moroccan universities [36]. Table 2 details the various SVC alternatives for countering cybersecurity threats.

Table 1. IT Governance criteria

Structural mechanisms criteria	Process mechanisms criteria	Relational mechanisms criteria
CS1: Roles and responsibilities	CP1: Information system planning strategy	CR1: IT leadership
CS2: IT strategic committee	CP2: Portfolio management	CR2: Internal communication
CS3: IT steering committee	CP3: Budget control and reports	CR3: Active participation and collaboration between main stakeholders
CS4: Structure of the IT organization	CP4: Frameworks	CR4: Knowledge sharing on IT governance
CS5: CIO to the executive committee		CR5: IT staff training

Table 2. List of SVC Alternatives

Alternative	Description
Plan (A1)	Defines strategies to meet security requirements.
Improve (A2)	Enhances security services and practices.
Engage (A3)	Improves communication and relationships for risk management.
Design and Transition (A4)	Ensures the security of services in the operational environment.
Obtain/Build (A5)	Builds necessary components for secure services.
Deliver and Support (A6)	Provides support and resolution of cybersecurity incidents.

4. RESULT AND DISCUSSION

The following tables present the results of the evaluation of cybersecurity governance criteria (CS), process criteria (CP), and risk criteria (CR) using AHP and TOPSIS methods. Table 3 shows the pairwise comparison matrix for CS criteria, illustrating the relative importance of each criterion. Table 4 presents the weight calculation for each CS criterion according to the AHP method, determining the priorities. Table 5 describes the data set used to evaluate the alternatives in terms of CS criteria. Table 6 normalizes this decision matrix for more precise analysis. Table 7 and Table 8 display the separation distances and proximity scores of CS alternatives, respectively, with their final ranking. For process criteria, Table 9 and Table 10 provide the pairwise comparison matrix and the weights calculated via AHP for CP criteria. The separation distances and proximity scores of CP alternatives are presented in Table 11 and Table 12. Regarding risk criteria, Table 13 and Table 14 show the pairwise comparison matrix and AHP weights for CR criteria. Table 15 and Table 16 conclude with the separation distances and proximity scores of CR alternatives, respectively. These tables highlight the importance and effectiveness of each alternative in managing cybersecurity, processes, and risks within academic institutions.

Table 3. Pairwise comparison (CS)

	CS1	CS2	CS3	CS4	CS5
CS1	1	3	4	2	5
CS2	1/3	1	2	1/2	3
CS3	1/4	1/2	1	1/3	4
CS4	1/2	2	3	1	2
CS5	1/5	1/3	1/4	1/2	1

Table 4. Weight calculation with AHP method (CS)

Criterion	Criterion weight	Priority
CS1	42.58%	1
CS2	16.34%	3
CS3	11.42%	4
CS4	23.39%	2
CS5	6.27%	5

Table 5. Data set description (CS)

	CS1	CS2	CS3	CS4	CS5
A1	80%	60%	75%	70%	65%
A2	85%	80%	80%	75%	70%
A3	70%	65%	70%	65%	80%
A4	75%	70%	85%	80%	75%
A5	90%	75%	80%	85%	60%
A6	65%	85%	65%	60%	85%

Table 6. Normalized decision MATRIX (CS)

	CS1	CS2	CS3	CS4	CS5
A1	41.89	33.55	40.22	39.15	36.35
A2	44.51	44.74	42.90	41.94	39.15
A3	36.65	36.35	37.54	36.35	44.74
A4	39.27	39.15	45.58	44.74	41.94
A5	47.12	41.94	42.90	47.54	33.55
A6	34.03	47.54	34.86	33.55	47.54

Table 7. Separation distance of alternatives (CS)

Alternative	Distance to S+	Distance to S-
A1	0.0386	0.0365
A2	0.0188	0.0530
A3	0.0556	0.0157
A4	0.0369	0.0380
A5	0.0130	0.0667
A6	0.0658	0.0245

Table 8. Prioritized SVC (CS)

Alternative	Proximity score	Ranking
A1	48.57%	4
A2	73.80%	2
A3	22.01%	6
A4	50.72%	3
A5	83.65%	1
A6	27.12%	5

Table 9. Pairwise comparison (CP)

	CP1	CP2	CP3	CP4
CP1	1	2	3	4
CP2	1/2	1	2	3
CP3	1/3	1/2	1	2
CP4	1/4	1/3	1/2	1

Table 10. Weight calculation with AHP (CP)

Criterion	Criterion weight	Priority
CP1	46.68%	1
CP2	27.76%	2
CP3	16.03%	3
CP4	9.53%	4

Table 11. Separation distance of alternatives (CP)

Alternative	Distance à S+	Distance à S-
A1	0.0473	0.0380
A2	0.0160	0.0599
A3	0.0603	0.0153
A4	0.0435	0.0353
A5	0.0161	0.0680
A6	0.0649	0.0388

Table 12. Prioritized SVC (CP)

Alternative	Score de Proximité	Ranking
A1	44.55%	4
A2	78.89%	2
A3	20.28%	6
A4	44.80%	3
A5	80.84%	1
A6	37.43%	5

Table 13. Pairwise comparison (CR)

	cR1	cR2	cR3	cR4	cR5
CR1	1	4	5	2	3
CR2	1/4	1	3	1/2	2
CR3	1/5	1/3	1	1/4	1/2
CR4	1/2	2	4	1	3
CR5	1/3	1/2	2	1/3	1

Table 14. Weight calculation with AHP (CR)

Criterion	Criterion weight	Priority
CR1	41.88%	1
CR2	15.18%	3
CR3	6.17%	5
CR4	26.42%	2
CR5	10.36%	4

Table 15. Separation distance of alternatives (CR)

Alternative	Distance à S+	Distance à S-
A1	0.0151	0.0178
A2	0.0140	0.0189
A3	0.0229	0.0100
A4	0.0100	0.0229
A5	0.0200	0.0129
A6	0.0214	0.0116

Table 16. Prioritized SVC (CR)

Alternative	Score de Proximité	Ranking
A1	54.10%	3
A2	57.52%	2
A3	30.38%	6
A4	69.62%	1
A5	39.29%	4
A6	35.12%	5

The integration of AHP and TOPSIS methods in cybersecurity governance within higher education has proven effective in various studies, particularly for managing security risks and developing targeted defense mechanisms against cyber threats. Our research on imminent threats and cybersecurity solutions in the higher education context highlights significant research gaps and the need for strategic protection. These studies show that the combined use of AHP and TOPSIS techniques allows the development of a strategic vision to counter cyber threats while aligning IT governance practices with the specific cybersecurity requirements of Moroccan universities. The integration of ITIL v4 in this context offers a significant advantage by going beyond simple service management to create value, an aspect that was absent in earlier versions like ITIL v3. This approach not only facilitates the identification of risks but also the development of response strategies tailored to the specific needs of the Moroccan academic context. The study results show that SVC services A5 and A2 are crucial for structural and process mechanisms, underscoring their importance in creating and maintaining a robust and secure IT infrastructure, as well as in the effective management of IT resources. The role of SVC services A4 and A2 in relational mechanisms is also vital, particularly in ensuring the security of new services and transitions, thereby minimizing the risks associated with the introduction of new technologies or processes. These results align with the strategic objectives of academic institutions.

Our study stands out from previous research, such as those by [43], [52] adopting a specific and contextualized approach to strengthening cybersecurity in Moroccan universities. Cheng and Wang [43] propose general strategies for institutional governance and [52] focus on a systematic review of information security management frameworks based on international standards like ISO 27000 and COBIT, our study distinguishes itself by integrating AHP and TOPSIS methods to prioritize IT governance mechanisms specific to the local context. This approach allows for a more precise assessment of cybersecurity needs, taking into account the cultural and institutional particularities of Morocco, often overlooked in other research. In contrast, Gamilla and Palaoag [53] emphasizes the security of infrastructures in smart campuses but does not delve deeply into the strategic alignment of cybersecurity initiatives with institutional objectives, which our research successfully integrates through the application of the ITIL v4 framework. Additionally, the study by Joshi and Singh [54], which focuses on risk management in university networks, offers a useful perspective but remains limited to threat assessment and action planning. It does not provide the analytical depth and strategic direction that we have developed with our multi-level methodology.

The strengths of our study lie in its ability to combine a rigorous methodology with a contextual application, which not only strengthens the cyber-resilience of Moroccan universities but also optimizes the allocation of security resources. However, our study has limitations, including the need for a deeper exploration of long-term implementation mechanisms and potential interactions between different governance criteria. Finally, unexpected results emerged, such as the identification of the critical importance of specific ITIL v4 services, which proved essential for enhancing resilience against cyber threats, even though they are often underestimated in the existing literature. These results highlight the need to review and adjust cybersecurity priorities in university environments based on local realities and emerging challenges.

The primary objective of this study was to demonstrate the effectiveness of an integrated approach using AHP, TOPSIS, and ITIL v4 to improve cybersecurity in Moroccan universities. The significance of this study lies in its ability to align IT governance practices with the specific cybersecurity requirements of academic institutions while optimizing resource utilization and strengthening resilience against cyber threats. Although the study successfully demonstrated how a structured approach can improve cybersecurity risk management, questions remain unanswered, particularly regarding how this approach could be adapted and applied to other contexts or academic sectors. Future research could explore the long-term impact of this integration and assess its effectiveness in various academic environments while examining other IT governance frameworks that could complement or enhance the effectiveness of AHP, TOPSIS, and ITIL v4 methodologies.

5. CONCLUSION

This study provides valuable insights into the intricate challenges of digital transformation in higher education, particularly in the context of Moroccan universities. By integrating AHP and TOPSIS methodologies within the ITIL v4 framework, the research effectively addresses the critical need for enhanced IT governance to combat cyber threats. The study demonstrates that the combined use of these decision-making tools allows for the strategic prioritization of IT governance mechanisms, aligning them with the specific cybersecurity needs of academic institutions. The findings reveal the importance of key ITIL v4 SVC services, highlighting their role in optimizing resource allocation and bolstering the resilience of universities against cyberattacks. Despite its contributions, the study also identifies areas for further exploration, such as the long-term implementation of these strategies and their adaptation to different contexts. Future research should focus on assessing the broader applicability of this integrated approach and exploring additional IT governance frameworks to further enhance cybersecurity in academic environments. Overall, this study underscores the critical importance of strategic IT governance in safeguarding the digital transformation efforts of higher education institutions.

REFERENCES

[1] A. Kozarkiewicz, “General and specific: the impact of digital transformation on project processes and management methods,” *Foundations of Management*, vol. 12, no. 1, pp. 237–248, Jan. 2020, doi: 10.2478/fman-2020-0018.
[2] T. M. Siebel, “Digital Transformation,” in *RosettaBooks*, 2019.

[3] L. M. Castro Benavides, J. A. Tamayo Arias, M. D. Arango Serna, J. W. Branch Bedoya, and D. Burgos, "Digital transformation in higher education institutions: a systematic literature review," *Sensors*, vol. 20, no. 11, p. 3291, Jun. 2020, doi: 10.3390/s20113291.

[4] T. Jensen, "Higher education in the digital era. The current state of transformation around the world." International Association of Universities, pp. 28–42, 2019. [Online]. Available: https://www.iau-aiu.net/Higher-Education-in-the-Digital-Era-The-Current-State-of-Transformation-Around

[5] V. Kyva, "Analysis of factors affecting cyber security of a higher military educational institution," *Cybersecurity: Education, Science, Technique*, vol. 3, no. 15, pp. 53–70, 2022, doi: 10.28925/2663-4023.2022.15.5370.

[6] K. A. Yousif Yaseen, "Importance of cybersecurity in the higher education sector 2022," *Asian Journal of Computer Science and Technology*, vol. 11, no. 2, pp. 20–24, Dec. 2022, doi: 10.51983/ajcst-2022.11.2.3448.

[7] A. Chahid, S. Ahriz, K. El Guemmat, and K. Mansouri, "Towards an effective baseline of it governance mechanisms in higher education institution," in *17th International Conference on e-Learning and Digital Learning 2023, ELDL 2023 and 11th International Conference on Sustainability, Technology and Education 2023, STE 2023*, IADIS Press, Jul. 2023, pp. 107–116. doi: 10.33965/el_ste2023_202303l014.

[8] A. B. Nassoura, "Cybersecurity technologies and practices in higher education institutions: a systematic review," Webology. Accessed: Aug. 04, 2024. [Online]. Available: https://www.researchgate.net/publication/360835004_Cybersecurity_Technologies_And_Practices_In_Higher_Education_Institutions_A_Systematic_Review.

[9] A. Aborujilah, A. Z. Al-Othmani, N. S. Hussien, S. A. Mokhtar, Z. A. Long, and M. Nizam, "Cybersecurity risk assessment approach for Malaysian organizations: Malaysian Universities as case study," in *2022 9th International Conference on Electrical and Electronics Engineering, ICEEE 2022*, IEEE, Mar. 2022, pp. 440–450. doi: 10.1109/ICEEE55327.2022.9772546.

[10] M. Dos Santos, S. Bessa, A. Gomes, and L. Carvalho, "Application of the AHP-TOPSIS-2N method to prioritize vulnerabilities in solution development in cybersecurity," *Researchgate.Net*. pp. 1–4, 2021.

[11] A. Agrawal *et al.*, "Software security estimation using the hybrid fuzzy ANP-TOPSIS approach: Design tactics perspective," *Symmetry*, vol. 12, no. 4, p. 598, Apr. 2020, doi: 10.3390/SYM12040598.

[12] Y. Bin Du and P. Zhu, "Collective relations of fuzzy relational structures," *Journal of Intelligent and Fuzzy Systems*, vol. 34, no. 4, pp. 2807–2816, Apr. 2018, doi: 10.3233/JIFS-17969.

[13] P. Żebrowski, A. Couce-Vieira, and A. Mancuso, "A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber-Physical Systems," *Risk Analysis*, vol. 42, no. 10, pp. 2275–2290, Oct. 2022, doi: 10.1111/risa.13900.

[14] A. R. Jamali, A. Bhutto, M. Khaskhely, and W. Sethar, "Impact of leadership styles on faculty performance: Moderating role of organizational culture in higher education," *Management Science Letters*, vol. 12, no. 1, pp. 1–20, 2022, doi: 10.5267/j.msl.2021.8.005.

[15] R. B. Z. Putz, V. I. Rasoto, and E. Ishikawa, "Brazilian federal universities information technology governance: An analysys of the strategic alignment dimension," in *Iberian Conference on Information Systems and Technologies, CISTI*, IEEE, Jun. 2017, pp. 1–7. doi: 10.23919/CISTI.2017.7975955.

[16] S. Ahriz, N. Benmoussa, A. El Yamami, K. Mansouri, and M. Qbadou, "An elaboration of a strategic alignment model of University information systems based on SAM model," *Engineering, Technology & Applied Science Research*, vol. 8, no. 1, pp. 2471–2476, Feb. 2018, doi: 10.48084/etasr.1696.

[17] S. Ghosh, "An exploration of IT governance in university: Its drivers, how it maps to theoretical frameworks, and the committee structure characteristics abstract," *International Journal of Business and Applied Social Science (IJBASS)*, vol. 4, no. 11, pp. 45–71, 2018.

[18] R. S. Dlamini, "The role of the strategic and adaptive chief information officer in higher education," *Education and Information Technologies*, vol. 20, no. 1, pp. 113–140, Mar. 2015, doi: 10.1007/s10639-013-9269-5.

[19] C. Abdelilah, S. Ahriz, K. El Guemmat, and K. Mansouri, "Building a specialized it governance strategy for higher education: a strategic model," *Journal of Computer Science*, vol. 20, no. 7, pp. 768–782, Jul. 2024, doi: 10.3844/jcssp.2024.768.782.

[20] I. S. Bianchi, R. D. Sousa, R. Pereira, and I. M. de Souza, "Effective it governance mechanisms in higher education institutions: An empirical study," *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, no. E25, pp. 412–423, 2020.

[21] P. K. Addo and A. Adusei, "Risk management in Higher Education: The Role of Educational Leaders in Translating Policy into Practice in the Ghanaian Context," *The IEA Classroom Environment Study*, vol. 49, no. May, p. ii, 2021.

[22] T. Soobaroyen, C. G. Ntim, M. J. Broad, D. Agrizzi, and K. Vithana, "Exploring the oversight of risk management in UK higher education institutions: the case of audit committees," *Accounting Forum*, vol. 43, no. 4, pp. 404–425, Oct. 2019, doi: 10.1080/01559982.2019.1605872.

[23] I. S. Bianchi, R. D. Sousa, R. Pereira, and E. Luciano, "IT governance structures in brazilian, dutch and Portuguese Universities," *Procedia Computer Science*, vol. 121, pp. 927–933, 2017, doi: 10.1016/j.procs.2017.11.120.

[24] M. Attaran, S. Attaran, and B. G. Celik, "Promises and challenges of cloud computing in higher education: a practical guide for implementation construction management education view project sustainability rating systems view project," *Journal of Higher Education Theory and Practice*, vol. 17, no. 6, pp. 20–38, 2017, [Online]. Available: https://www.researchgate.net/publication/320719465

[25] Anwar Fattah, Hoga Saragih, and Resad Setyadi, "Determinants effectiveness of information technology governance and IT performance in higher education institution (HEI): a conceptual framework," *International Journal of Science, Technology & Management*, vol. 2, no. 1, pp. 36–47, Jan. 2021, doi: 10.46729/ijstm.v2i1.135.

[26] B. A. Ajayi and H. Hussin, "IT governance from practitioners' perspective: Sharing the experience of a Malaysian university," *Journal of Theoretical and Applied Information Technology*, vol. 88, no. 2, pp. 219–230, 2016.

[27] M. D. Richardson and P. A. Lemoine, "Planning for higher education institutions: chaos and the covid-19 pandemic," *Educational Planning*, vol. 27, no. 3, pp. 43–57, 2020, [Online]. Available: https://eric.ed.gov/?id=EJ1279907

[28] F. Bi and W. Wu, "Research on portfolio management of university education funds taking harvard university for example," in *4th International Conference on Industrial Economics System and Industrial Security Engineering, IEIS 2017*, IEEE, Jul. 2017, pp. 1–5. doi: 10.1109/IEIS.2017.8078578.

[29] S. Ahriz, A. El Yamami, K. Mansouri, and M. Qbadou, "Cobit 5-based approach for IT project portfolio management: Application to a Moroccan university," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 4, pp. 88–95, 2018, doi: 10.14569/IJACSA.2018.090416.

[30] P. Sangiumvibool and S. Chonglerttham, "Performance-based budgeting for continuing and lifelong education services: the Thai higher education perspective," *Journal of Higher Education Policy and Management*, vol. 39, no. 1, pp. 58–74, Jan. 2017, doi: 10.1080/1360080X.2016.1211977.
[31] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez-Fonseca, and D. Quiroz, "Information security management frameworks and strategies in higher education institutions: a systematic review," *Annales des Telecommunications/Annals of Telecommunications*, vol. 76, no. 3–4, pp. 255–270, Apr. 2021, doi: 10.1007/s12243-020-00783-2.
[32] I. S. Bianchi, R. D. Sousa, and R. Pereira, "Information technology governance for higher education institutions: A multi-country study," *Informatics*, vol. 8, no. 2, p. 26, Apr. 2021, doi: 10.3390/informatics8020026.
[33] A. Ishlahuddin, P. W. Handayani, K. Hammi, and F. Azzahro, "Analysing IT governance Maturity Level using COBIT 2019 Framework: a case study of small size higher education institute (XYZ-edu)," in *2020 3rd International Conference on Computer and Informatics Engineering, IC2IE 2020*, IEEE, Sep. 2020, pp. 236–241. doi: 10.1109/IC2IE50715.2020.9274599.
[34] C. Abdelilah, A. Souad, K. El Guemmat, and K. Mansouri, "Evaluating IT governance in the DSS domain (delivery, service, and support) through COBIT 5 framework at a Moroccan University," in *2024 4th International Conference on Innovative Research in Applied Science, Engineering and Technology, IRASET 2024*, IEEE, May 2024, pp. 1–5. doi: 10.1109/IRASET60544.2024.10548341.
[35] I. S. Bianchi and R. D. Sousa., "Frameworks used for IT governance at universities: An exploratory study." International Business Information Management Association (IBIMA), 2018. [Online]. Available: https://repositorium.sdum.uminho.pt/handle/1822/71305
[36] C. Abdelilah, S. Ahriz, K. El Guemmat, and K. Mansouri, "Implementation of suitable information technology governance frameworks for Moroccan higher education institutions," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 3, p. 3116, Jun. 2024, doi: 10.11591/ijece.v14i3.pp3116-3126.
[37] A. Fattah and R. Setyadi, "Determinants Effectiveness Information technology governance in higher education institution (HEI) using partial least squares structural equation modeling approach (PLS-SEM)," *Journal of Physics: Conference Series*, vol. 1807, no. 1, p. 012007, Apr. 2021, doi: 10.1088/1742-6596/1807/1/012007.
[38] T. Ngqondi and H. Mauwa, "Information technology governance model for a low resource institution with fragmented IT portfolio," *South African Journal of Higher Education*, vol. 34, no. 3, Jul. 2020, doi: 10.20853/34-3-3326.
[39] C. W. Montenegro and D. A. Flores, "An integrated model for ICT governance and management applied to the council for evaluation, accreditation and quality assurance of higher education institutions in Ecuador (CEAACES)," in *2015 International Conference on Computing, Communication and Security, ICCCS 2015*, IEEE, Dec. 2016, pp. 1–9. doi: 10.1109/CCCS.2015.7374158.
[40] S. Mishra and S. Gochhait, "Emerging cybersecurity attacks in the era of digital transformation," in *Proceedings of the 7th International Conference on Intelligent Computing and Control Systems, ICICCS 2023*, IEEE, May 2023, pp. 1442–1447. doi: 10.1109/ICICCS56967.2023.10142357.
[41] A. Chahid, S. Ahriz, K. El Guemmat, and K. Mansouri, "Conceptualizing a model for information technology governance for successful digital transformation in higher education: an approach focused on absorptive capacity," in *Lecture Notes in Networks and Systems*, vol. 1098 LNNS, 2024, pp. 192–201. doi: 10.1007/978-3-031-68650-4_19.
[42] E. Pavlova, "Enhancing the organisational culture related to cyber security during the university digital transformation," *Information & Security: An International Journal*, vol. 46, no. 3, pp. 239–249, 2020, doi: 10.11610/isij.4617.
[43] E. C. K. Cheng and T. Wang, "Institutional strategies for cybersecurity in higher education institutions," *Information*, vol. 13, no. 4, p. 192, Apr. 2022, doi: 10.3390/info13040192.
[44] A. Chahid, S. Ahriz, K. El Guemmat, and K. Mansouri, "Strategic Selection of ITIL V4 Services for Cybersecurity Defense: An AHP and TOPSIS Approach for Moroccan Universities," in *Lecture Notes in Networks and Systems*, vol. 1156 LNNS, 2024, pp. 361–372. doi: 10.1007/978-3-031-73125-9_22.
[45] G. Mirela and B. D. Maria, "Information security management system." Scribd, p. 1353, 2008. [Online]. Available: https://www.scribd.com/document/335514261/249-pdf
[46] K. Haufe, R. Colomo-Palacios, S. Dzombeta, K. Brandis, and V. Stantchev, "Security management standards: a mapping," *Procedia Computer Science*, vol. 100, pp. 755–761, 2016, doi: 10.1016/j.procs.2016.09.221.
[47] K. Haufe, R. Colomo-Palacios, S. Dzombeta, K. Brandis, and V. Stantchev, "ISMS core processes: a study," *Procedia Computer Science*, vol. 100, pp. 339–346, 2016, doi: 10.1016/j.procs.2016.09.167.
[48] Y. Al-Ashmoery, H. Haider, A. Haider, N. Nasser, and M. Al-Sarem, "Impact of IT Service Management and ITIL Framework on the Businesses," in *International Conference of Modern Trends in ICT Industry: Towards the Excellence in the ICT Industries*, MTICTI 2021, IEEE, Dec. 2021, pp. 1–5. doi: 10.1109/MTICTI53925.2021.9664763.
[49] T. L. Saaty, "Principles of the analytic hierarchy process," in *Expert Judgment and Expert Systems*, Berlin, Heidelberg: Springer Berlin Heidelberg, 1987, pp. 27–73. doi: 10.1007/978-3-642-86679-1_3.
[50] T. L. Saaty, "Decision making with the analytic hierarchy process," *International Journal of Services Sciences*, vol. 1, no. 1, p. 83, 2008, doi: 10.1504/IJSSCI.2008.017590.
[51] G.-H. Tzeng and J.-J. Huang, *Multiple attribute decision making*. Chapman and Hall/CRC, 2011. doi: 10.1201/b11032.
[52] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez-Fonseca, and D. Quiroz, "Information security management frameworks and strategies in higher education institutions: a systematic review," *Annals of Telecommunications*, vol. 76, no. 3–4, pp. 255–270, Apr. 2021, doi: 10.1007/s12243-020-00783-2.
[53] A. P. Gamilla and T. D. Palaoag, "Building A Barrier: A Security Operations Center Framework For A Sustainable Smart Campus Network," in *6th International Conference on Information Technology, InCIT 2022*, IEEE, Nov. 2022, pp. 256–261. doi: 10.1109/InCIT56086.2022.10067377.
[54] C. Joshi and U. K. Singh, "Information security risks management framework – A step towards mitigating security risks in university network," *Journal of Information Security and Applications*, vol. 35, pp. 128–137, Aug. 2017, doi: 10.1016/j.jisa.2017.06.006.

BIOGRAPHIES OF AUTHORS

Abdelilah Chahid was born in Casablanca, Morocco. He is currently a doctoral student at the ENSET Institute in Mohammedia. Her doctoral work focuses on the governance of university information systems within an innovative education system. In 2011, he obtained a master's degree in computer networks at Hassan II University in Casablanca. He can be contacted at chahidabdelillah@gmail.com.

Souad Ahriz is a Ph.D. and member of the "Distributed Computer Systems" team within the research laboratory "Signals, Distributed Systems, and Artificial Intelligence" at ENSET Institute of the University Hassan II of Casablanca-Morocco. She graduates form ENSETM, in 1991 an received her master and doctoral degrees in Computer science from Hassan the 2nd University. She works as a computer science teacher at ENSET Mohammedia. Her research fields include cloud computing, e-learning system, educational modeling, information systems, IT governance, programming language, and database management. She can be contacted at ahrizsouad@gmail.com.

Kamal El Guemmat is a Ph.D. candidate and a member of the "Distributed Computer Systems" team within the research laboratory "Signals, Distributed Systems, and Artificial Intelligence" at ENSET Institute of the University Hassan II of Casablanca, Morocco. His research fields include semantic indexing, semantic web, information retrieval systems, and e-learning. He can be contacted at k.elguemmat@gmail.com.

Khalifa Mansouri was born in 1968 in Azilal, Morocco. He is currently a researcher-professor in computer science, Training Director and Director of the M2S2I Research Laboratory at ENSET of Mohammedia, Hassan II University of Casablanca. His research interests include information systems, e-learning systems, real time systems, artificial intelligence and industrial systems (modeling, optimization, numerical computation). Graduated from ENSET of Mohammedia in 1991, CEA in 1992 and Ph.D. (Computation and Optimization of Structures) in 1994, HDR in 2010 and National Ph.D. (in computer science-distributed systems) in 2016. He is the author of 10 books in computer science, a scientific book with the publisher Springer, 425 research papers including 236 in the Scopus library and supervised 35 defended doctoral theses. He can be contacted at email: khalifa.mansouri@enset-media.ac.ma.