Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 2530-2539
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.5203

A Literature-Based Heat Matrix for Quantifying Inter-Domain Correlations within the ISO/IEC 27002:2013 Framework

Erick Dazki*[1], Richardus Eko Indrajit[2], Januponsa Dio F[3]

[1,3]Informatics, Pradita University, Indonesia
[2]Magister of Information Technology, Pradita University, Indonesia

Email: [1]erick.dazki@pradita.ac.id

Received : Jul 30, 2025; Revised : Aug 18, 2025; Accepted : Aug 19, 2025; Published : Sep 2, 2025

Abstract

The problem of managing information security controls is complex because the domains outlined in standards like ISO/IEC 27002 rarely operate in isolation; they have intricate interdependencies that are often overlooked. This oversight can lead to fragmented security controls, inefficient resource allocation, and weaknesses in overall security governance. To address this issue, this paper proposes a literature-based heat matrix methodology, building on ISO/IEC 27002:2013 while referencing the updated 2022 guidance, NIST SP 800-53 Revision 5, and COBIT 2019. The primary goal is to assign numerical correlation values to the fourteen domains of ISO/IEC 27002:2013, providing a structured approach to visualize and understand their interrelationships. The methodology involves a comprehensive literature review and is complemented by expert validation from experienced practitioners to refine the correlation scores. The result is an illustrative 14x14 matrix that demonstrates how numeric inter-domain correlations can reveal critical overlaps and guide strategic decision-making. A new five-tier correlation scale is introduced to aid interpretation, clarifying whether two domains have very low, low, moderate, high, or very high levels of interdependency. This approach offers a significant impact on the field of informatics and computer science by enabling organizations to move beyond siloed security management. By recognizing these correlations, organizations can allocate resources more effectively, enhance holistic risk management, and strengthen security governance. The heat matrix serves as a practical tool for practitioners and managers to identify domain pairs that require close coordination, ultimately leading to more coherent policy frameworks and a more robust security posture.

Keywords : *Compliance, Heat Matrix, Information Security, InterDomain Correlation, ISO/IEC 27002, Risk Management*

1. INTRODUCTION

Information security management requires organizations to adopt a comprehensive and systematic framework that addresses technical, organizational, and human factors simultaneously. Among internationally recognized standards, the ISO/IEC 27000 family—particularly ISO/IEC 27001 and ISO/IEC 27002—has become the most widely adopted reference for establishing and maintaining an Information Security Management System (ISMS) [1][2]. ISO/IEC 27002 provides detailed guidance for implementing security controls, and although the 2022 revision reorganized the controls into four categories (Organizational, People, Physical, and Technological), many organizations still rely on the 2013 fourteen-domain structure for practical implementation, especially those that initiated compliance before 2022 [3][4].

In practice, these domains rarely operate in isolation. Access Control depends heavily on Cryptography for secure authentication, while Incident Management requires close alignment with Operations Security and Business Continuity Management to ensure rapid recovery and minimal data loss [5][6]. Failure to recognize these interdependencies can result in fragmented security governance, resource inefficiencies, and heightened exposure to cascading risks [7][8]. Consequently, there is a

pressing need for systematic tools that allow organizations to visualize and quantify inter-domain relationships, enabling better governance and risk management [9].

Previous studies have acknowledged overlaps among information security domains but tend to present them qualitatively or in narrative form. For instance, Siponen & Oinas-Kukkonen [10] reviewed common information security issues, while Mukhopadhyay et al. [11] emphasized the link between technical controls and organizational resilience. Similarly, Smith & Newman [12] highlighted the role of business continuity in incident response. However, these studies stop short of providing a quantitative framework to systematically measure the degree of inter-domain correlations. Even recent efforts that map ISO/IEC 27002 controls to frameworks like NIST SP 800-53 or COBIT 2019 [13][14] still lack a unified numerical model for cross-domain dependencies.

This gap underscores the novelty of the present study. While the literature recognizes that domains such as Policies, Compliance, and Access Control are interrelated, no previous research has proposed a numerical correlation matrix combined with a five-tier interpretive scale to capture the strength of these interdependencies. By bridging this gap, the research contributes both to the academic discourse in informatics and to practical information security governance.

Therefore, the objective of this study is to propose a literature-based heat matrix methodology that quantifies inter-domain correlations within ISO/IEC 27002:2013, while referencing the updated 2022 edition, NIST SP 800-53 Rev. 5, and COBIT 2019. The proposed matrix, validated by domain experts, not only reveals critical overlaps among security domains but also provides a practical decision-support tool for resource allocation, risk management, and compliance alignment in organizational security governance.

2. METHOD

2.1. Literature Review

2.1.1. ISO/IEC 27000 Family and 27002 Revisions

ISO/IEC 27001 defines the high-level requirements for establishing and maintaining an ISMS, while ISO/IEC 27002 offers a more detailed perspective on control implementation (International Organization for Standardization [ISO], 2022a). The 2013 edition enumerated fourteen domains, but the 2022 revision arranges controls into four major categories [1]. Regardless of the version adopted, prior literature consistently notes that security controls tend to overlap [2]. Many organizations still reference the fourteen-domain structure for practical guidance, especially if they initiated their ISO/IEC 27002 adoption prior to 2022.

2.1.2. NIST SP 800-53 and Crosswalks

NIST SP 800-53 Revision 5 [3] emphasizes a broader set of security and privacy controls grouped into families like Access Control, Contingency Planning, and System & Communications Protection. Multiple crosswalks have mapped these controls to ISO/IEC 27002 domains, showing that improvements in one area often influence multiple domains [4]. This insight reinforces the value of systematically identifying cross-domain dependencies.

2.1.3. COBIT 2019 for Governance

COBIT 2019 [5] focuses on enterprise governance of IT, emphasizing risk management, vendor oversight, compliance, and resource optimization. While not restricted to security, its objectives frequently intersect with ISO/IEC 27002 controls in areas like organizational structure and monitoring [6]. This underscores how domains such as Organization of Information Security (domain 2) and Compliance (domain 14) can anchor the entire governance of security activities.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 2530-2539
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.5203

2.1.4. Empirical Studies

Recent empirical work illustrates the real-world interplay among technical, organizational, and human factors. Failure in one domain often leads to downstream consequences in another. For instance, poor cryptographic practices might weaken Access Control, while lack of training in Human Resource Security can exacerbate insider threats [7]. Studies of integrated incident management further show how Incident Management, Operations Security, and Business Continuity Management must align to minimize recovery time and data loss [4, 8].

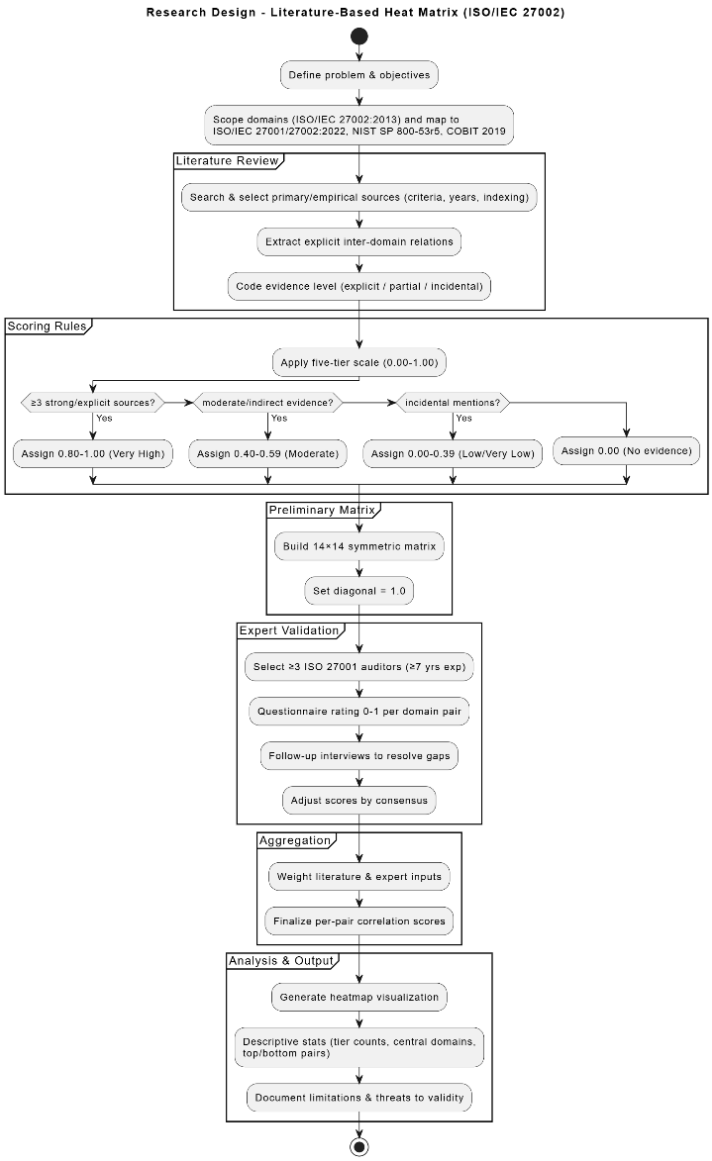

Figure 1. Research Flowchart

2.2. Reasearch Methodology

2.2.1. Data Sourcing

The first step involved conducting a structured review of relevant standards and prior studies. Primary references included:

- ISO/IEC 27001:2022 and ISO/IEC 27002:2022 for the latest best practices on controls [1, 9].
- NIST SP 800-53 Rev. 5 [3] for comparative mapping of control families.

Vol. 6, No. 4, August 2025, Page. 2530-2539
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.5203

- COBIT 2019 [5] to highlight governance implications.
- Empirical articles [4, 6–8] illustrating cross-domain interactions in practical scenarios.

References that explicitly mentioned overlaps between two ISO/IEC 27002 domains contributed to higher correlation scores. Where overlaps were tangential or domain-specific, moderate or lower values were assigned.

2.2.2. Expert Validation

A preliminary matrix was refined through interviews with three practitioners experienced in ISO/IEC 27001/2 audits. They verified whether specific domain pairs should reflect stronger or weaker correlations based on their field observations, helping to resolve ambiguities in textual references. The final matrix thus balances literature-based evidence with practical expertise.
Validation was conducted through:

- Structured questionnaires – rating the strength of domain pairs on a 0–1 scale.
- Follow-up interviews – clarifying discrepancies and resolving disagreements.

The final correlation scores reflect a consensus between literature-based evidence and expert judgment.

2.2.3. Matrix Completion

A symmetrical 14 14 matrix was produced, covering every pair of the original ISO/IEC 27002:2013 domains. Diagonal elements default to 1.0, representing the domain's "perfect" correlation with itself. Non-diagonal values range from 0.0 to 1.0. The new five-tier scale (Section 2.3) provides an interpretive lens for these numeric scores, supporting consistent reading of correlation strength across the matrix.

2.3. Heat Matrix Conceptualization

2.3.1. Five-Tier Correlation Scale

To simplify interpretation of the numeric scores (0.0–1.0), each value is categorized into one of five tiers:

- Very Low (0.00–0.19)
  Correlation or synergy is practically negligible. Any overlap of controls or processes is incidental rather than systematic.
- Low (0.20–0.39)
  A slight interaction may exist, but its impact on joint governance or shared processes is minor. The domains generally operate in near isolation.
- Moderate (0.40–0.59)
  A meaningful relationship is present. While not dominant, the overlap in policies or controls warrants attention to avoid security gaps or resource inefficiencies.
- High (0.60–0.79)
  These domains regularly appear together in standards and best practices. Improvements in one domain typically impact the other, implying a need for coordinated strategies and resources.
- Very High (0.80–1.00)
  The relationship is nearly inseparable or deeply integrated. Domains at this level frequently share core objectives or enforcement mechanisms. A correlation of 1.0 is reserved for the domain's relationship with itself along the diagonal.

2.3.2. Illustrative Examples

Policies (domain 1) and Compliance (domain 14) often exceed 0.80, entering "Very High" territory, since regulations strongly dictate the nature and scope of security policies. In contrast, Physical & Environmental Security (domain 7) and Cryptography (domain 6) might only register in the 0.20–0.39 range ("Low") if their direct interaction is minimal in typical standards and practice.

2.3.3. Practical Utility

This categorization helps managers and auditors quickly identify domain pairs demanding close coordination versus those that can be managed more independently. It also aids in resource allocation, ensuring that "Very High" or "High" correlations receive integrated planning. Meanwhile, moderate or low relationships can be monitored periodically to see if contextual changes (e.g., new regulations) might increase their importance.

3. RESULT: THE COMPLETE 14×14 CORRELATION MATRIX

Presents the final correlation matrix for the fourteen ISO/IEC 27002:2013 domains, incorporating both numeric scores and their likely five-tier interpretation. Each row and column corresponds to a domain, producing 196 correlation cells in total.

Many of these values surpass 0.60–0.79 ("High") or even 0.80 ("Very High"). For instance, Policies (1) and Compliance (14) is 0.9, signifying a near inseparability, while Access Control

(5) and Cryptography (6) at 0.8 also inhabit "Very High" territory. By contrast, Physical & Environmental Security (7) and Cryptography (6) reflect weaker synergy at 0.3 ("Low"), indicating limited direct overlap in typical standards.

3.1. Correlation Matrix

The final output of this study is a 14 × 14 correlation matrix representing inter-domain dependencies in ISO/IEC 27002:2013. Each cell shows the correlation score between two domains, based on the combined evidence from literature and expert validation. Diagonal elements are set to 1.0 to indicate perfect self-correlation as shown in Table 1.

3.2. Heatmap Visualization

To enhance readability, the correlation scores were also visualized using a heatmap. The heatmap applies a color gradient from light (Very Low) to dark (Very High), allowing readers to quickly identify domains with strong or weak correlations.

3.3. Distribution of Correlation Strength

To better understand the results, the 196 correlation pairs (14×14, including symmetrical values) were categorized into the five-tier scale:

- Very High (0.80–1.00): 18 pairs (e.g., Information Security Policies – Compliance = 0.9; Access Control – Cryptography = 0.8).
- High (0.60–0.79): 67 pairs (e.g., Incident Management – Operations Security = 0.8).
- Moderate (0.40–0.59): 58 pairs.
- Low (0.20–0.39): 24 pairs (e.g., Physical & Environmental Security – Cryptography = 0.3).
- Very Low (0.00–0.19): 0 pairs (no negligible correlations found).

This distribution indicates that most domain pairs exhibit at least moderate correlation, with a significant number falling into the High or Very High categories.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 2530-2539
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.5203

Table 1. Example 14×14 Correlation Matrix for ISO/IEC 27002:2013 Domains

No	Domain	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Information Security Policies	1.0	0.8	0.6	0.5	0.7	0.5	0.4	0.6	0.6	0.5	0.5	0.6	0.5	0.9
2	Organization of Information Security	0.8	1.0	0.7	0.5	0.6	0.6	0.4	0.7	0.6	0.6	0.5	0.6	0.5	0.8
3	Human Resource Security	0.6	0.7	1.0	0.4	0.5	0.4	0.3	0.5	0.5	0.4	0.5	0.6	0.4	0.6
4	Asset Management	0.5	0.5	0.4	1.0	0.6	0.4	0.5	0.6	0.4	0.5	0.5	0.5	0.5	0.6
5	Access Control	0.7	0.6	0.5	0.6	1.0	0.8	0.4	0.7	0.7	0.6	0.5	0.7	0.6	0.7
6	Cryptography	0.5	0.6	0.4	0.4	0.8	1.0	0.3	0.7	0.7	0.6	0.4	0.6	0.4	0.6
7	Physical & Environmental Security	0.4	0.4	0.3	0.5	0.4	0.3	1.0	0.5	0.4	0.3	0.4	0.4	0.6	0.4
8	Operations Security	0.6	0.7	0.5	0.6	0.7	0.7	0.5	1.0	0.7	0.7	0.5	0.8	0.8	0.7
9	Communications Security	0.6	0.6	0.5	0.4	0.7	0.7	0.4	0.7	1.0	0.6	0.5	0.6	0.5	0.7
10	System Acquisition, Development & Maintenance	0.5	0.6	0.4	0.5	0.6	0.6	0.3	0.7	0.6	1.0	0.6	0.6	0.5	0.6
11	Supplier Relationships	0.5	0.5	0.5	0.5	0.5	0.4	0.4	0.5	0.5	0.6	1.0	0.6	0.5	0.5
12	Information Security Incident Management	0.6	0.6	0.6	0.5	0.7	0.6	0.4	0.8	0.6	0.6	0.6	1.0	0.8	0.7
13	Business Continuity Management	0.5	0.5	0.4	0.5	0.6	0.4	0.6	0.8	0.5	0.5	0.5	0.8	1.0	0.6
14	Compliance	0.9	0.8	0.6	0.6	0.7	0.6	0.4	0.7	0.7	0.6	0.5	0.7	0.6	1.0

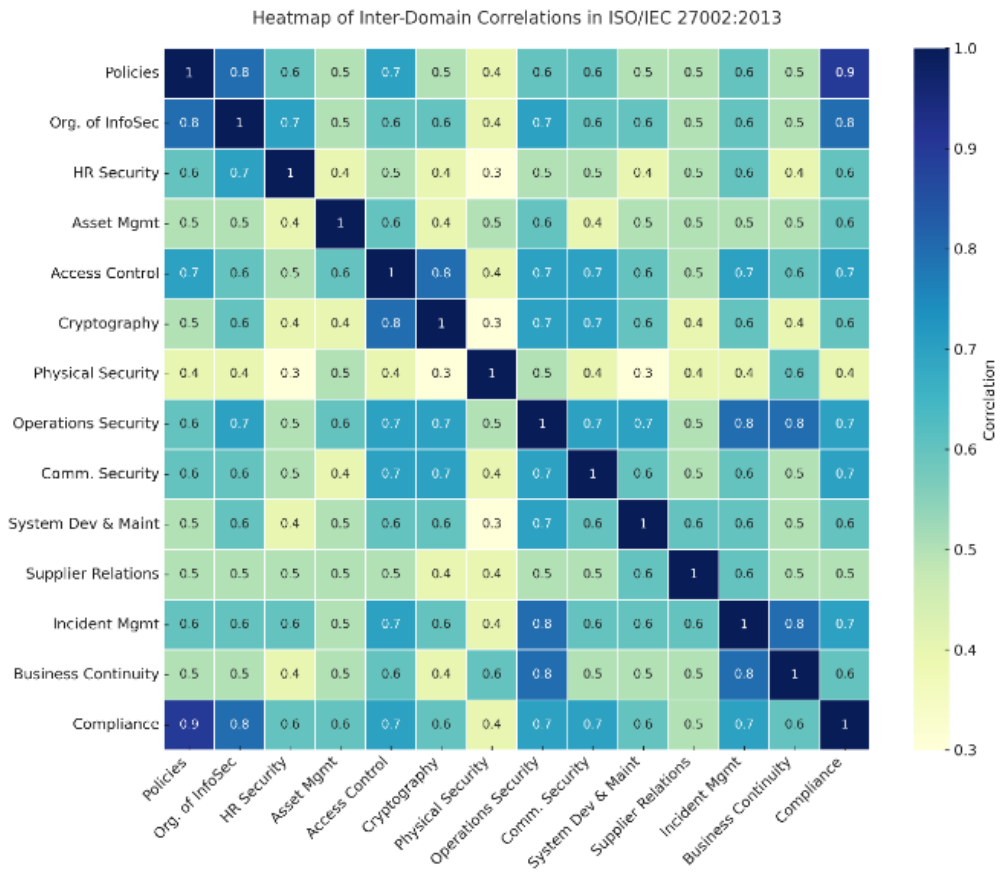

Figure 2. The heatmap representation of the correlation matrix.

3.4. Central Domains

By calculating the average correlation score for each domain with all other domains, some domains emerge as central nodes in the framework:

- Compliance (Domain 14): avg. correlation = 0.67 (highest).

- Operations Security (Domain 8): avg. correlation = 0.66.
- Access Control (Domain 5): avg. correlation = 0.65.

These domains demonstrate the strongest overall interdependencies, making them critical anchors for effective security governance.

3.5. Top-5 and Bottom-5 Correlations

Top-5 pairs:

- Information Security Policies (1) – Compliance (14) = 0.9
- Access Control (5) – Cryptography (6) = 0.8
- Incident Management (12) – Business Continuity Management (13) = 0.8
- Operations Security (8) – Incident Management (12) = 0.8
- Organization of Information Security (2) – Policies (1) = 0.8

Bottom-5 pairs:

- Physical & Environmental Security (7) – Cryptography (6) = 0.3
- Human Resource Security (3) – Physical & Environmental Security (7) = 0.3
- Physical & Environmental Security (7) – System Development (10) = 0.3
- Physical & Environmental Security (7) – Incident Management (12) = 0.4
- Human Resource Security (3) – Cryptography (6) = 0.4

These findings provide an objective basis for prioritization: organizations should pay special attention to domains with very high correlations, while recognizing that some domains, such as Physical Security, play a more isolated role in the overall framework.

4. DISCUSSIONS

The correlation matrix clearly demonstrates that ISO/IEC 27002 domains are not independent entities but rather interdependent components within an integrated framework. The five-tier correlation scale provides a structured way to interpret the degree of synergy, highlighting which domains demand closer coordination. For instance, the strong relationship between Access Control (Domain 5) and Cryptography (Domain 6) (score = 0.8) confirms that introducing advanced authentication mechanisms inherently requires parallel improvements in key management and encryption protocols.

These findings reinforce previous studies that have emphasized the interplay between organizational and technical controls. Mukhopadhyay et al. [11] linked incident management effectiveness with organizational resilience, while Smith and Newman [12] demonstrated that business continuity strengthens incident response capabilities. Similarly, Siponen and Oinas-Kukkonen [10] identified persistent challenges in managing interrelated controls, though without offering a quantitative model. By introducing a numerical correlation matrix validated by expert input, this study advances beyond prior qualitative approaches and provides a replicable method for systematically assessing domain interdependencies.

4.1. Extended Benefits

This is an example of the use of sub-chapters in a paper. Sub-chapters are allowed to be included in all chapters, except in the conclusion.

1. **Enhanced Resource Coordination**

   The correlation matrix offers empirical evidence of interdependencies, enabling organizations to allocate resources more effectively. For example, the high correlation between Cryptography and Access Control supports integrated budgeting and project planning. This complements earlier findings in governance studies [13], which underscored the need for resource optimization across overlapping domains.

2. **Holistic Risk Management**
   Considering domains in isolation risks overlooking cascading vulnerabilities. The results confirm that Incident Management (Domain 12) and Business Continuity (Domain 13) (correlation = 0.8) must be managed together to ensure rapid recovery. This finding is consistent with resilience-focused research [11][12], but extends prior work by quantifying the strength of their linkage.
3. **Streamlined Governance and Policy Alignment**
   The very high correlation between Policies (Domain 1) and Compliance (Domain 14) (correlation = 0.9) underscores the central role of regulations in shaping information security governance. This aligns with prior studies on compliance-driven security management [33], while offering a more structured basis for policy alignment across organizational units.
4. **Clarity for Diverse Stakeholders**
   The heat matrix provides a consolidated view of inter-domain dependencies, supporting communication between technical, legal, and human resource teams. Unlike narrative analyses in earlier studies [10], the present approach delivers a visual and quantitative tool that helps stakeholders identify their roles in supporting interdependent security functions.
5. **Adaptive Planning for Evolving Threats**
   Finally, the heat matrix establishes a baseline that can be updated as new threats or regulations emerge. For instance, correlations between Physical Security (Domain 7) and Cryptography (Domain 6), currently categorized as low (0.3), may become more significant with the rise of hardware security modules in cloud and IoT environments. This adaptive quality positions the matrix as a living framework for continuous improvement in information security governance.

In summary, the discussion confirms that the proposed framework contributes both practically by enabling integrated resource planning, risk management, and governance and academically by introducing a replicable, quantitative method that advances research in Informatics and Computer Science. It not only validates prior qualitative insights but also opens pathways for future studies on computational modeling and automated decision-support systems in information security management.

CONCLUSION

This study proposed a literature-based heat matrix methodology to quantify inter-domain correlations in ISO/IEC 27002:2013, supported by the updated 2022 edition, NIST SP 800-53 Rev. 5, and COBIT 2019. By synthesizing evidence from literature and validating the findings with experienced practitioners, a 14×14 correlation matrix was developed and visualized through a heatmap. The results revealed that certain domains, such as Policies–Compliance and Access Control–Cryptography, exhibit very high interdependencies, while others, such as Physical Security, play a more isolated role.

From a practical perspective, the proposed framework provides organizations with a decision-support tool to align controls, allocate resources more effectively, and strengthen governance and risk management holistically. From a scientific perspective in Informatics and Computer Science, this research contributes a quantitative, replicable method that transforms qualitative assessments into data-driven analysis, thereby advancing the study of information security governance.

Future research may extend this model to the ISO/IEC 27002:2022 structure, apply the framework to other standards (e.g., ISO/IEC 27701, NIST Cybersecurity Framework), or develop automated tools and predictive analytics that dynamically update correlation scores in response to evolving threats. In doing so, the heat matrix can serve as a living model that continues to support both academic inquiry and practical decision-making in the field of cybersecurity governance.

REFERENCES

[1] M. Siponen dan H. Oinas-Kukkonen, "A Review of Information Security Issues and Respective

Research Contributions," 2007.
[2] I. O. for Standardization (ISO), *ISO/IEC 27001:2022 - Information Security, Cybersecurity, and Privacy Protection*. 2022.
[3] N. I. of Standards dan T. (NIST), *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)*. U.S. Department of Commerce, 2020.
[4] Isaca, *COBIT 2019 Framework: Governance and Management Objectives*. 2019.
[5] A. Mukhopadhyay, P. Raj, dan W. Mahoney, "An integrated approach to incident management: Linking technical controls with organizational resilience," *Journal of Cybersecurity*, vol. 4, no. 2, pp. 1–16, 2018.
[6] T. Smith dan R. Newman, "Leveraging business continuity for improved incident response: A case study in organizational resilience," *International Journal of Information Security*, vol. 20, no. 4, pp. 321–333, 2021.
[7] S. Wang dan E. Johnson, "The role of human factors in cryptographic key management," *Computers & Security*, vol. 83, pp. 45–56, 2019.
[8] K. Zhang, Y. Liu, dan M. Roberts, "Integrating secure software development with operational controls: A lifecycle framework," *Computers & Security*, 2021, Art. no. 102235.
[9] P. Koshiya, "The Human Element in Cybersecurity: Exploring Cognitive Biases while Working Remote," *Journal of Technology and Systems*, vol. 7, no. 1, pp. 1–5, 2025.
[10] R. P. Reddy, "Cybersecurity for Critical Infrastructure: Protecting National Assets in the Digital Age," *International Journal of Computer Trends and Technology*, vol. 73, no. 2, pp. 7–17, 2025.
[11] A. Ojo, "The Future of Cybersecurity Policy: Navigating Privacy, Innovation, And Security," *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 6, no. 1, pp. 773–787, 2025.
[12] S. Bjorn, V. Jashari, dan et al., "Developing and testing a framework for matching distinct personality types with information security awareness methods," *Information & Computer Security*, 2025.
[13] S. Prabhu, D. Kocsis, dan et al., "Beyond the direct impact of sanctions and subjective norms in cybersecurity," *Information & Computer Security*, 2025.
[14] J. C. Auton dan D. Sturman, "Persuasion under pressure: the influence of persuasion principles and time constraints on phishing email susceptibility," *Information & Computer Security*, 2025.
[15] R. Ravichandran, S. Singh, dan P. Sasikala, "Exploring School Teachers' Cyber Security Awareness, Experiences, and Practices in the Digital Age," *Journal of Cybersecurity Education Research and Practice*, 2025.
[16] R. Bleiman, H. Park, dan A. Rege, "Educating students on the behavioral and psychological aspects of romance scam victimization via a social engineering competition," *Journal of Cybersecurity Education Research and Practice*, 2025.
[17] C. J. S. F. Clarke dan A. Konak, "The Impact of AI Use in Programming Courses on Critical Thinking Skills," *Journal of Cybersecurity Education Research and Practice*, 2025.
[18] J. O. Oyeniyi dan O. A. Oyeniran, "Optimizing Information Security In Cloud Environments: A Risk Management Approach And Guide For Enterprise Cloud Security," *Journal of Cybersecurity Education Research and Practice*, 2025.
[19] M. Namukasa, dan et al., "Diversifying Cybersecurity: Evaluation of an Internet of Things (IoT)-Based Cybersecurity Training Course Designed to Bridge the Diversity Gap," *Journal of Cybersecurity Education Research and Practice*, 2025.
[20] A. P. Rodgers-Stine dan T. Williams, "The Effectiveness of Scenario-Based Cybersecurity Day Camps in Southern Rural Appalachia," *Journal of Cybersecurity Education Research and Practice*, 2025.
[21] M. Ţălu, "Insights in Cybersecurity of a Smart Campus a Review," *Journal of Cybersecurity Education Research and Practice*, 2025.
[22] G. Childers, dan et al., "Exploring K-12 Teachers' Definitions and Perspectives of Cybersecurity," *Journal of Cybersecurity Education Research and Practice*, 2025.
[23] ResearchGate, "An Assessment of the Effect of Information Security Management System on Organisational Performance," *International Journal of Multidisciplinary Research and Analysis*, vol. 8, no. 3, 2025.

[24] ResearchGate, "Cloud Security Best Practices: Strategic Measures to Protect Digital Assets Within the Cloud," *International Journal For Multidisciplinary Research*, vol. 7, no. 1, pp. 18, 2025.
[25] ResearchGate, "A holistic cyber risk assessment model to identify and mitigate threats in us and canadian enterprises," *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 6, no. 1, pp. 773–787, 2025.
[26] ResearchGate, "Efficacy of Cybersecurity Awareness Training in Reducing Phishing Vulnerabilities in Organizations," 2025.
[27] ResearchGate, "Human factors in cybersecurity: an interdisciplinary review and framework proposal," 2025.
[28] ResearchGate, "Cybersecurity Awareness In HR: Protecting Employee Data in the Digital Era," *International Journal of Engineering Science and Information Technology*, vol. 5, no. 2, pp. 237–242, 2025.
[29] ResearchGate, "COBIT 2019 Framework in IT Governance: A Systematic Literature Review of Implementation Challenges and Benefits Across Various Industry Sectors," *Journal of Renewable Energy Electrical and Computer Engineering*, vol. 5, no. 1, pp. 99–105, 2025.
[30] ResearchGate, "The Human Factor in Cybersecurity: An Analysis of Emerging Trends and Challenges," 2024.
[31] ResearchGate, "Principles of organizational security governance," 2024.
[32] ResearchGate, "Organizational and Leadership Aspects of Cybersecurity Governance," 2024.
[33] ResearchGate, "Security compliance and its implication for cybersecurity," *World Journal of Advanced Research and Reviews*, vol. 24, no. 01, pp. 2105–2121, 2024.
[34] ResearchGate, "Enhancing Resilience in Business Continuity Management Strategies and Best Practices," 2024.
[35] ResearchGate, "Information security management system ISMS," *Electronics*, vol. 13, no. 19, pp. 3955, 2024.
[36] ResearchGate, "Information security risk assessment," *Applied Sciences*, vol. 14, no. 21, pp. 9858, 2024.
[37] ResearchGate, "Cybersecurity is critical for mitigating the economic and reputational impacts of cyberattacks," *Electronics*, vol. 14, no. 7, pp. 1364, 2024.
[38] ResearchGate, "ISO 27002 implementation challenges," *World Journal of Advanced Research and Reviews*, vol. 24, no. 01, pp. 2105–2121, 2024.
[39] ResearchGate, "Organizational culture cybersecurity," *Sustainability*, vol. 16, no. 5, pp. 1880, 2024.
[40] ResearchGate, "AI in cybersecurity," *Frontiers in Computer Science*, 2024.