Providing a Framework to Support the Analysis and Implementation of Information Security Management Systems Based on the ISO/IEC 27001 ISMS Standard in Several Subsidiary Companies of the Ministry of Roads and Urban Development

Abdullateef Haghighat[1], Majid Kalantari[2*] Mostafa Kolahdoozi[3]

[1] Master's Student, Business Administration (MBA), Technology Specialization, Electronic Campus, Islamic Azad University, Tehran, Iran
[2] Assistant Professor, Faculty of Management, Department of Information Technology Management, Electronic Campus, Islamic Azad University, Tehran, Iran
[3] Assistant Professor, Faculty of Management, Department of Information Technology Management, South Tehran Branch, Islamic Azad University, Tehran, Iran

*** Corresponding author email address**: Eng.m.klt@gmail.com

Received: 2024-12-11 **Reviewed:** 2025-01-21 **Revised:** 2025-01-30 **Accepted:** 2025-02-23 **Published:** 2025-03-11

Abstract

The purpose of the present study is to provide a model-based framework to support the analysis and implementation of information security management systems based on the ISO/IEC 27001 ISMS standard in several subsidiary companies of the Ministry of Roads and Urban Development. The research strategy used in this study is a sequential exploratory mixed-methods approach. In the present research, by utilizing the results of this phase and through in-depth and semi-structured interviews with seven relevant managers from ten examined companies, the components related to the objectives and prerequisites for implementing information security management systems based on the ISO/IEC 27001 ISMS standard were identified. The collected data were then analyzed using thematic analysis, which is one of the efficient and flexible methods, and the MAXQDA10 software. Subsequently, to validate and prioritize the identified components, a questionnaire was distributed among the employees of the ten companies, including deputies, managers, and operational staff, as another step of the research. By leveraging the obtained results, the final framework for the objectives and prerequisites for the establishment of organizational security management based on the ISO/IEC 27001 ISMS standard in the intended dimensions was presented. Furthermore, structural equation modeling (SEM) was applied using the Smart PLS software to examine the causal relationships between variables. In the case study, the framework was planned to be implemented in several subsidiary companies of the Ministry of Roads and Urban Development to evaluate its effectiveness, which will confirm or reject the proposed framework's objectives. Accordingly, 430 questionnaires derived from the qualitative research section were distributed among the statistical sample. The research findings indicate that five categories—compliance with other standards, organizational motivation, implementation, consequences and outcomes, and context—emerged from the qualitative thematic analysis. In the quantitative section, structural equation modeling demonstrated that context, implementation, integration with other standards, and organizational motivation significantly impact the outcomes and consequences of implementing information security management systems based on the ISO/IEC 27001 ISMS standard.

Keywords: *ISO/IEC 27001 ISMS standard, information security*

How to cite this article:
Haghighat A, Kalantari ., Kolahdoozi M .(2025). Providing a Framework to Support the Analysis and Implementation of Information Security Management Systems Based on the ISO/IEC 27001 ISMS Standard in Several Subsidiary Companies of the Ministry of Roads and Urban Development. Management Strategies and Engineering Sciences, 7(4), 23-32

1. Introduction

The analysis and implementation of information security management systems (ISMS) are among the most critical responsibilities of a professional programmer in the field of information security. This process involves analyzing security needs and risks, designing and implementing security systems, and continuously evaluating and improving these systems. One of the fundamental principles in the analysis and implementation of ISMS is risk analysis. In this phase, all security risks associated with the system must be identified and assessed, including the identification of threats, vulnerabilities, and potential impacts. Subsequently, appropriate security measures should be taken to mitigate the risks. After risk analysis, the security systems must be designed and implemented, which includes selecting and configuring security tools and technologies, establishing policies and guidelines, and creating control and monitoring mechanisms [1, 2].

The ISO/IEC 27001 standard is an international standard for information security management. This standard was initially published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005 [3] and later revised in 2013 [4], with the most recent revision occurring in 2022 [5]. Additionally, this standard has been recognized in various national standards. It outlines the requirements for establishing, implementing, maintaining, and continually improving an ISMS, aiming to help organizations secure their information assets [6]. Organizations that meet the standard’s requirements can receive certification from an accredited certification body upon the successful completion of an audit. The effectiveness of the ISO/IEC 27001 certification process and the overall standard was examined in a large-scale study conducted in 2020 [7].

Most organizations implement several information security controls. However, without an ISMS, these controls can be somewhat disorganized and fragmented, often implemented as point solutions for specific situations or merely as a contractual requirement [8]. Security controls in operations typically focus on specific aspects of IT or data security, while non-IT information assets (e.g., administrative work and proprietary knowledge) are generally less protected. Additionally, business continuity planning and physical security may be managed independently from IT or information security, while human resources practices may provide limited guidance on defining and assigning information security roles and responsibilities across the organization [9].

An IT solutions company specializing in compliance solutions for organizations conducted an annual survey [10] focused on the experience and challenges of ISO/IEC 27001 implementation across organizations from 2016 to 2020. The survey collected opinions from 250 information security professionals from 53 countries, all of whom were either certified in ISO/IEC 27001 or undergoing the certification process. These companies represented approximately 80% of the survey participants. The responses indicated that 71% of respondents received regular or occasional requests for ISO/IEC 27001 certification from clients or when bidding for new business opportunities.

A review of the literature suggests opportunities for evaluating the implementation and effectiveness of the standard within organizations. However, academic researchers have not fully embraced this challenge, as indicated by various studies [11]. Accordingly, the present study proposes a model-driven framework that enables organizations to adopt standard requirements using requirements engineering concepts. Many system designers may lack the necessary expertise in security and legal aspects to safeguard and deploy systems that meet an organization's security needs. Therefore, a framework will be proposed to guide them through the system development process [12]. Implementing ISMS requires a comprehensive and well-planned process for identifying assets and risks related to the organization's operations and well-being. Understanding the fundamental concepts of security is essential for defining security requirements effectively. One of the primary sources of information security deficiencies is the lack of attention to comprehensive system security requirements [13]. Organizations recognize that adhering to well-established reference frameworks for ISMS implementation is more beneficial than adopting temporary solutions [14].

From a business perspective, identifying the necessary resources for planning, implementing, and measuring ISMS management is a relatively costly and challenging endeavor. From an academic standpoint, ISMS frameworks have primarily originated from practitioners' perspectives [15], and literature reviews suggest a lack of research by scholars, indicating that these approaches may not be sufficiently attractive despite numerous organizations facing information security system deficiencies. Despite significant interest from organizations, ISMS has received minimal

attention from the academic community, particularly in the areas of IT audits, operations, and compliance [16].

After 15 years of scientific research on ISO/IEC 27001 and its growing popularity, we believe it is time for academics to assess how these fundamental concerns have been addressed with respect to this specific standard and to question related research perspectives in an increasingly connected and digitalized environment. ISO 27001 gap analysis is a professional assessment conducted between Stage 1 and Stage 2 of the ISO 27001 audit process. This evaluation helps bridge the gap between the two stages and ensures that any ISMS deficiencies identified in Stage 1 are adequately addressed. It assists companies in preparing for Stage 2 and the ISO 27001 certification process. It is important to note that gap analysis in ISO 27001 is mandatory only after the organization has prepared its Statement of Applicability, which details the security status of each of the 114 security controls specified in Annex A of ISO 27001. Thus, the ISO 27001 gap analysis should only be conducted for the Annex A controls and before initiating ISO 27001 implementation to gain insights into the organization's current state and the extent of work involved. There is a relative lack of scientific literature specifically focusing on standard requirements, with most studies being conducted on the pre-2013 version of the standard [16]. In response to real-world and academic challenges, this study proposes a model-driven approach to help organizations identify, analyze, and implement the standard's requirements.

2. Methodology

The strategy used in this study is a sequential exploratory mixed-methods approach. In mixed-method research designs, the researcher aims to investigate an "uncertain situation." In the present study, utilizing the results of this phase and through in-depth and semi-structured interviews with seven relevant managers from ten examined companies, the components related to the objectives and prerequisites for implementing information security management systems based on the ISO/IEC 27001 ISMS standard were identified. The collected data were then analyzed using thematic analysis, recognized as an efficient and flexible method, with the help of MAXQDA10 software.

In the next step, a focus group discussion was conducted within the domain of organizational standards to validate the obtained results, during which consensus and agreement were reached. Finally, to further validate and prioritize the identified components, a questionnaire was distributed among the employees of the ten companies, including deputies, managers, and operational staff, as another step of the research. The results obtained from this step contributed to presenting the final framework of objectives and prerequisites for the establishment of organizational security management based on the ISO/IEC 27001 ISMS standard in the intended dimensions, which can serve as the foundation for its implementation and development.

Furthermore, structural equation modeling (SEM) was employed to examine causal relationships between the variables using Smart PLS software. In the case study, the proposed framework was planned to be implemented in several subsidiary companies of the Ministry of Roads and Urban Development to evaluate its effectiveness, with the aim of confirming or rejecting the proposed framework's objectives. Therefore, 430 questionnaires derived from the qualitative research section were distributed among the statistical sample.

3. Findings and Results

In this research, the "Thematic Network Analysis" method was used. The criteria for including relevant texts encompassed having maximum necessary information about the connections between the specified keywords, while the exclusion criterion was a lack of relevance to the main subject and research problem. The thematic network, following a defined process, extracts the lowest-level themes (basic themes) from the text. These basic themes are then categorized and summarized into more abstract and conceptual principles (organizing themes). In the third step, these higher-level themes are incorporated into fundamental metaphors and become overarching themes governing the entire text (global themes).

In simpler terms, thematic network analysis can generally be divided into three main sections: first, text decomposition; second, text exploration; and third, integrating the findings. After reviewing 69 sources, the study reached theoretical saturation. Based on the analysis of various studies, the researcher identified the themes related to information security based on the ISO/IEC 27001 ISMS standard, as presented in Table 1:

Table 1. Research Themes

Global Themes	Organizing Themes	Basic Themes
Relationship with Other Standards	Comparison/integration with similar standards	Standards with a strong technology scope
		Information/document management standards
		Information security system standards
	Comparison/integration with other management standards	Combination with other management standards
		Implementation of multiple management standards
		ISO management standards with national-level indicators
Organizational Motivation	Functionalist	Support in achieving higher levels of IS security
		Increased efficiency in information management processes
	Institutional	Improving expected corporate image
		Governmental oversight and promotional activities
		Market demands
		ISO brand strength
Implementation	Tools and Methods	Flexible guidelines
		Evaluation/implementation of security controls
		Assessment of external dependencies
		Integration of legal requirements
		General Data Protection Regulation (GDPR)
		Cultural and psychological factors
	Project Governance	Senior management commitment
		Support from external consultants
		Organizational learning through implementation
		Significant time/cost for implementation
	Practical Adoption	Symbolic/informal implementation of the standard
		Low employee compliance with standards
Outcomes and Results	Specific Standard Outcomes	Effective risk prevention
		Higher business continuity
		Better stakeholder communication
		Reduced partner opportunism
		Sufficient return on investment
		Lower risk of profit loss
		High competitive advantage
		Reduced insurance costs
	National-level Indicators	Correlation with intellectual property indicators
		Correlation with security and trust indicators
Information Management Context	Country	Adoption by regulatory/promotional activities
		Higher adoption in export-driven countries
		Implementation/adaptation influenced by cultural factors
	Organization Size	Low awareness of SMEs regarding standards
		Various implementation challenges related to organization size
	Industry	High adoption rates in data-intensive industries
		Applicability in digital organizations
		Certification as a source of competitive differentiation

In a dedicated session, selected members were asked to provide feedback on the primary research problem following the anticipated steps. The Delphi method was utilized in two rounds for this purpose. The Delphi panel members were purposefully selected through non-probability sampling based on criteria such as theoretical expertise, practical experience, willingness, and ability to participate in the research. The statistical population of this section consisted of 18 experts, but due to their professional commitments, only accessible individuals were included. The participants included nine experienced members (with a minimum of 10 years of experience, holding at least a master's degree, and

active in the specialized field with experience in Delphi sessions).

In the second round, a semi-structured questionnaire was presented, and the participants were asked to provide their opinions regarding information security based on the ISO/IEC 27001 ISMS standard, derived from the thematic analysis. The identified components were presented for expert consultation in the form of a survey. The results from the first round showed that all identified themes were part of the ISO/IEC 27001 ISMS framework, with over 60% of participants rating these themes as significant. Additionally, in the second-round questionnaire, ranking of the ISO/IEC 27001 ISMS standard was conducted based on the collected data.

Regarding demographic data, the highest frequency in terms of gender was male participants at 57.4%. In terms of age, individuals between 31 and 50 years constituted 50.9%. Regarding marital status, 62.5% were married, and in terms of education, 52.0% held a bachelor's degree.

Descriptive statistics were used to analyze the respondents' answers to the research variables. The findings indicated that the mean scores of all variables were within the range of 3.75 to 4.24, suggesting an overall moderate level among the respondents.

Table 2. Descriptive Statistics of Research Variables

Variable	Mean	Standard Deviation	Skewness	Kurtosis
Relationship with Other Standards	4.24	0.451	-0.397	0.324
Organizational Motivation	4.22	0.468	-0.221	0.014
Implementation	4.008	0.697	-0.445	0.266
Outcomes and Results	3.75	0.763	-0.571	0.412
Context	4.21	0.62	-0.473	0.42

Structural equation modeling (SEM) was employed using the PLS software to analyze the relationships between the variables. This study aimed to investigate the impacts of the variables. To achieve this, after collecting data related to the research variables, the Kolmogorov-Smirnov test was conducted to determine whether the obtained data (from the questionnaire) followed a normal distribution. If the data were found to be normally distributed, parametric tests were used for hypothesis testing; otherwise, non-parametric statistics were applied.

Table 3. Kolmogorov-Smirnov Test Results

Research Variables	Kolmogorov-Smirnov Test	Sig Value	Significance Level
Relationship with Other Standards	0.300	0.00	Not Normal
Organizational Motivation	0.233	0.00	Not Normal
Implementation	0.247	0.00	Not Normal
Outcomes and Results	0.254	0.00	Not Normal
Context	0.231	0.00	Not Normal

As shown in Table 4, the research variables were not normally distributed; thus, non-parametric tests were used for analysis. Inferential analysis was conducted using the PLS-SEM (Partial Least Squares Structural Equation Modeling) approach.

The Kaiser-Meyer-Olkin (KMO) measure was utilized to assess the adequacy of sampling, which evaluates the correlation among variables and determines whether the variance in the research constructs is influenced by the common variance of underlying latent factors. The KMO index ranges from 0 to 1, with values closer to 1 indicating that the data are suitable for factor analysis and hypothesis testing. If the index is below 0.60, the factor analysis and results derived from it are considered unsuitable.

Table 4. KMO and Bartlett's Test Results

Test	Value
KMO	0.901
Bartlett's Test of Sphericity (Sig)	0.000

To ensure the reliability of the study, three main indicators were used: factor loadings, Cronbach's alpha, and composite reliability (CR). Factor loadings were calculated by measuring the correlation between the indicators and their corresponding constructs. If the factor loading value was equal to or greater than 0.40, it confirmed that the variance explained by the construct exceeded the measurement error, thus ensuring acceptable reliability for the measurement model.

Table 5. Cronbach's Alpha and Composite Reliability (CR) Values of Variables

Variable	Cronbach's Alpha (α)	Composite Reliability (CR)
Relationship with Other Standards	0.961	0.81
Organizational Motivation	0.971	0.87
Implementation	0.937	0.79
Outcomes and Results	0.974	0.88
Context	0.922	0.81

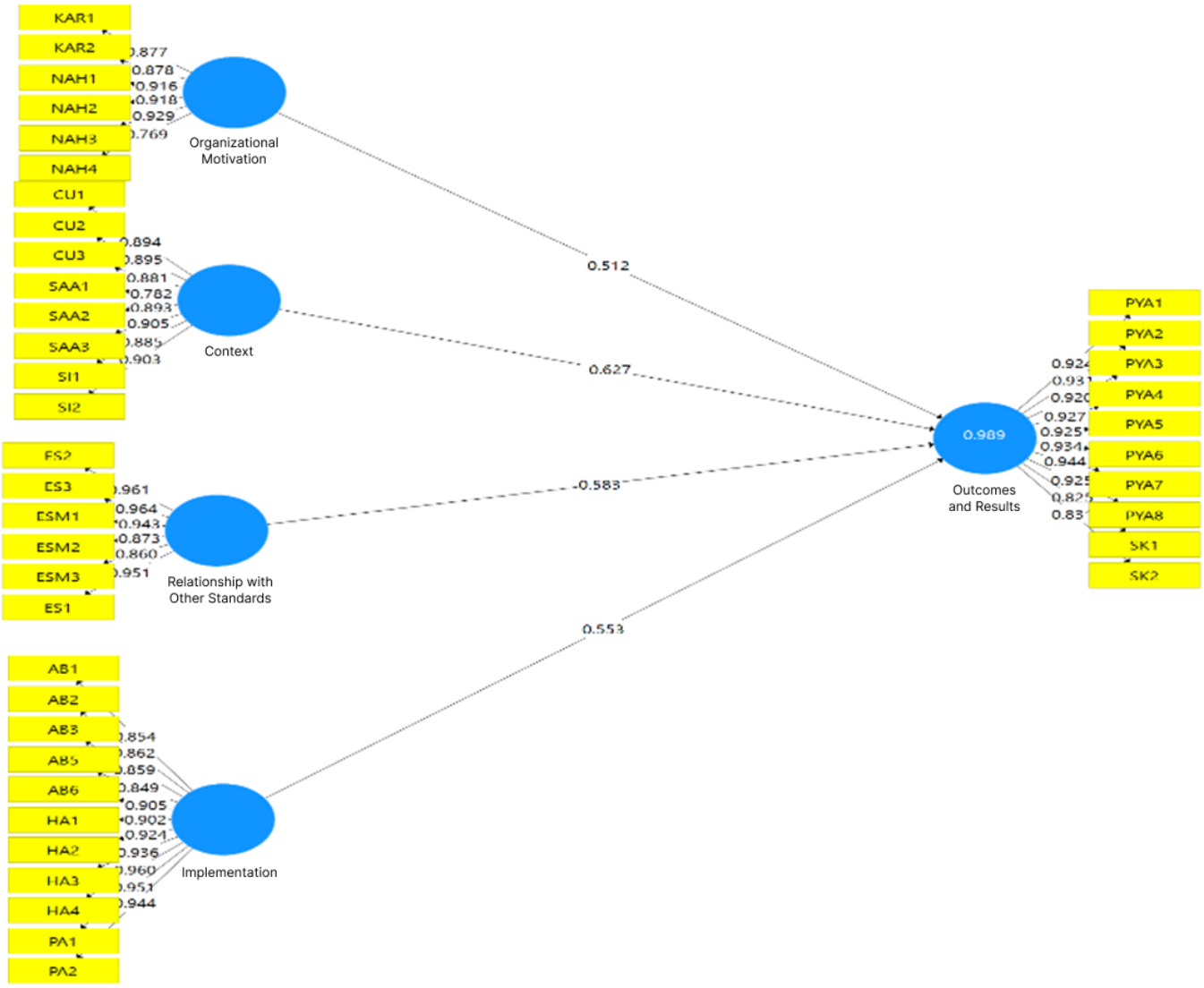

Figure 1. Factor Analysis Model of Variables

The above results indicate that all research variables have acceptable reliability, as their Cronbach's alpha and composite reliability values are above the recommended threshold of 0.70.

To assess the validity of the research, both convergent and divergent validity were examined and tested. In the convergent validity section, the Average Variance Extracted (AVE) index was used. This index should be greater than 0.70 for each variable and its related dimensions to confirm convergent validity. It is noteworthy that the values of this index for the variables and their dimensions in the present study were above 0.50, thus confirming convergent validity. For divergent validity, the Heterotrait-Monotrait Ratio (HTMT) index was utilized. If the values of this index for each research variable are below 0.90, divergent validity is confirmed. According to the values obtained from this index, as presented in Table 6, the divergent validity of the research instrument is also confirmed, indicating that the research instrument possesses comprehensive validity.

Table 6. Convergent Validity (AVE Index)

Variable	AVE
Relationship with Other Standards	0.896
Organizational Motivation	0.919
Implementation	0.844
Outcomes and Results	0.927
Context	0.881

After assessing the fit of the measurement models, the next step is evaluating the fit of the structural model. Unlike the measurement model, the structural model does not address observed variables but focuses only on the latent variables and their relationships. Two key predictive indicators in the structural analysis section using the Partial Least Squares (PLS) approach are the R^2 and Q^2 indices.

Table 7. R^2 and Q^2 Values

Variable (Construct)	R^2	Q^2
Relationship with Other Standards	0.86	0.81
Organizational Motivation	0.776	0.92
Implementation	0.761	0.89
Outcomes and Results	0.91	0.81
Context	0.87	0.86

Based on the obtained values, the predictive capability of the model is confirmed. These values indicate that the model possesses a suitable predictive ability.

To evaluate the overall model fit, the Goodness of Fit (GOF) index was employed. Since the PLS software does not provide a model fit index in the analysis, this index is used to assess model fit. If the value of this index exceeds 0.35, it indicates that the research model has acceptable validity. The obtained GOF value in the present study (GOF = 0.741) suggests that the model has a strong fit.

Using the Partial Least Squares (PLS) approach and path analysis, the study examined both the significance of the relationships and the estimation of standardized coefficients. Regarding significance, if the significance values of the conceptual model relationships exceed 1.96, it can be concluded with 95% confidence that the relationships between the variables are significant and the hypothesis is confirmed.

Table 8. Path Coefficients and Hypothesis Significance for the First Hypothesis

Variable	Path	β	t	p	Result
Context	→ Outcomes	0.625	7.96	**	Confirmed
Implementation	→ Outcomes	0.553	20.32	**	Confirmed
Integration with Standards	→ Outcomes	0.583	20.76	**	Confirmed
Organizational Motivation	→ Outcomes	0.512	6.25	**	Confirmed

Note: ** $p < 0.00$

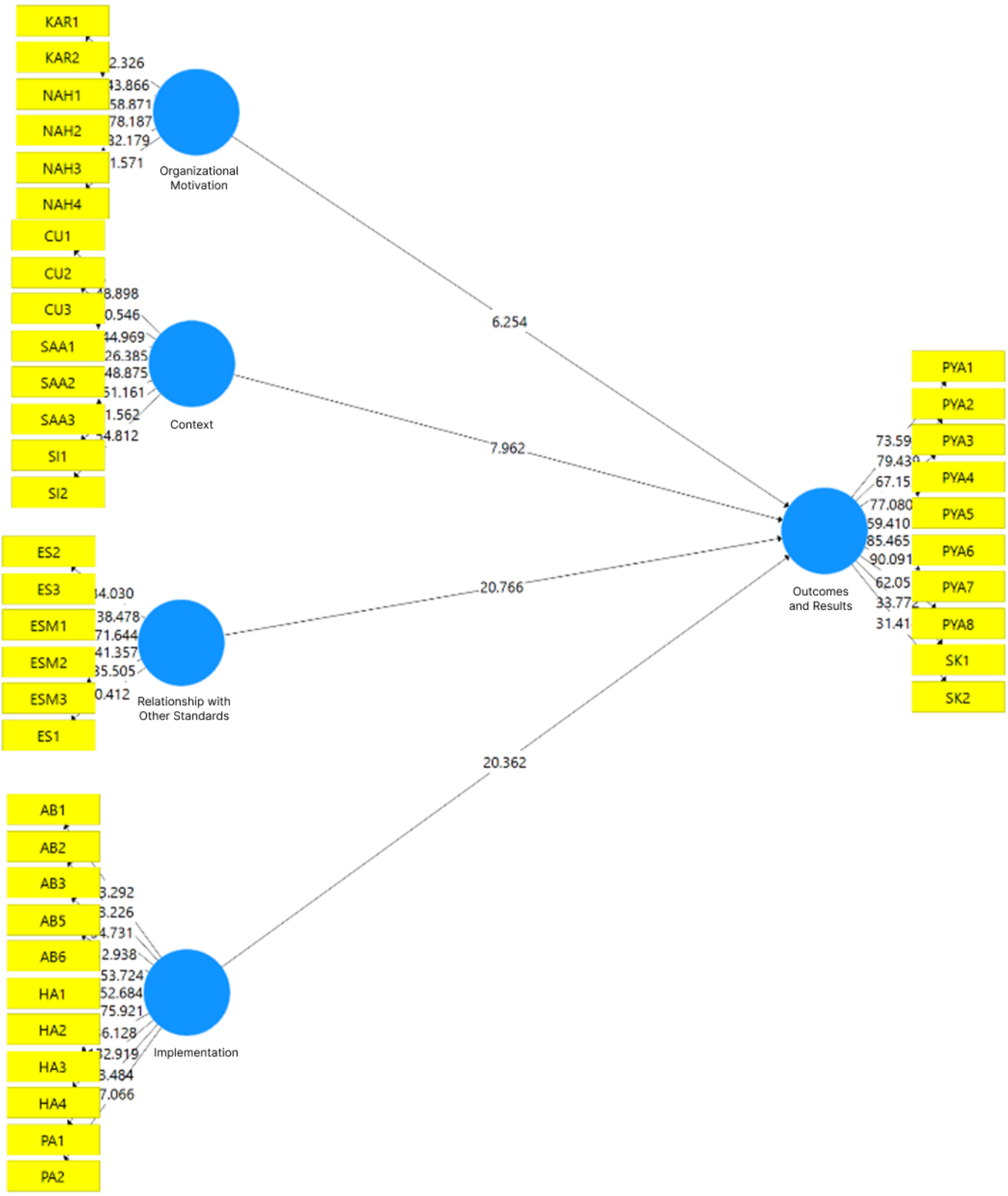

Figure 2. Model with T-values

Based on the results presented in Table 8, it can be concluded that context, implementation, integration with other standards, and organizational motivation significantly influence the outcomes and results of implementing information security management systems based on the ISO/IEC 27001 ISMS standard. Furthermore, as indicated in Table 8, integration with other standards has the greatest impact on the outcomes and results of standardization.

4. Discussion and Conclusion

A system is a set of interrelated elements, such that a change in one element affects the others within the system. A system is characterized by a common goal, operates as a whole, and adapts to changes in environmental conditions. The implementation of standards, both formal and informal—such as ISO/IEC 27001—by organizations aims to manage Information Security Systems (ISS) and cybersecurity. Additionally, it involves a network of relationships in which organizations are embedded, including supply chains, platform-based ecosystems, or industries. This study provides an overview of the current knowledge on the standard, highlights emerging issues and unresolved questions, and thus lays a solid foundation for future research on this subject. Furthermore, it explicitly presents a set of research opportunities by considering ISO/IEC 27001 as part of a standard system and its practices within the framework of business relationship networks.

Upon reviewing the research literature, several overarching, organizing, and sub-themes were identified. The relationship with other standards was highlighted as a key aspect in some studies, emphasizing that information security in compliance with ISO/IEC 27001 should be integrated or combined with other standards. These were categorized into two groups: comparison/integration with standards of similar scope, which includes sub-themes such as strong technology-based standards, information/document management standards, and information security system standards; and comparison/integration with other management system standards, which encompasses sub-themes such as integration with other management standards, implementation of multiple management systems, and ISO management system standards with national-level indicators.

Organizational motivation for adopting these standards was categorized into two groups: functionalist and institutional. The functionalist motivation includes components such as supporting the attainment of higher levels of information security and improving efficiency in information management processes. Institutional motivation includes elements such as enhancing the expected corporate image, governmental oversight and promotional activities, market demands, and the strength of the ISO brand.

In functionalist motivation, organizations expect the standard to improve processes and documentation, while institutional motivation sees certification as a tool for gaining credibility with external stakeholders, including competitors, customers, and regulatory bodies. Most studies reporting functionalist motivations highlight expectations for achieving higher levels of ISS, which are clearly aligned with the scope of the standard and the underlying logic of continuous improvement in ISMS and the acquisition of new skills and competencies. In institutional motivation, the focus is on enhancing the corporate image. Achieving certification demonstrates to stakeholders—including employees, suppliers, financial institutions, and customers—that the organization is a trustworthy partner. This, in turn, serves as an indirect goal for attracting more customers and strengthening customer relationships.

Implementation of standards includes the following components: tools and methods (flexible guidelines, assessment/execution of security controls, evaluation of external interdependencies, integration of legal requirements, General Data Protection Regulation (GDPR), and related cultural and psychological elements); project governance (commitment of senior management, support from external consultants, organizational learning through implementation, significant time/cost for execution); and actual adoption (symbolic/informal implementation of the standard and low employee compliance with standards).

Regarding the outcomes and results, information security management systems based on ISO/IEC 27001 fall into two categories: specific standardization outcomes (effective risk prevention, higher business continuity, improved stakeholder communication, reduced partner opportunism, return on investment, lower risk of profit loss, competitive advantage, and reduced insurance costs) and outcomes aligned with national-level indicators (correlation with intellectual property indices and correlation with security and trust indices). Therefore, based on the conducted analysis, the results of ISO/IEC 27001-based information security management systems can be divided into two levels: organizational and national. At the organizational level, the outcomes include effective risk prevention, higher business continuity, better stakeholder communication, reduced partner opportunism, return on investment, lower risk of profit loss, higher market advantage, and reduced insurance costs.

Finally, the contextual and environmental factors influencing the implementation of information security management systems based on ISO/IEC 27001 were categorized into three groups: the country in which information security management is implemented, the industry in which security management is conducted, and the

size of the company, which affects the adoption and implementation of the standard.

Authors' Contributions

Authors equally contributed to this article.

Data Availability Statement

The datasets generated during and/or analysed during the current study are available in http://promise.site.uottawa.ca/SERepository/datasets-page.html

Acknowledgments

Authors thank all participants who participate in this study.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

References

[1] P.-Y. Chen, "Information Security and Artificial Intelligence–Assisted Diagnosis in an Internet of Medical Thing System (IoMTS)," *Ieee Access*, vol. 12, pp. 9757-9775, 2024, doi: 10.1109/access.2024.3351373.

[2] O. Layode, "Data Privacy and Security Challenges in Environmental Research: Approaches to Safeguarding Sensitive Information," *International Journal of Applied Research in Social Sciences*, vol. 6, no. 6, pp. 1193-1214, 2024, doi: 10.51594/ijarss.v6i6.1210.

[3] T. D. Breaux and A. I. Anton, "Analyzing regulatory rules for privacy and security requirements," *IEEE Transactions on Software Engineering*, vol. 34, no. 1, pp. 5-20, 2008, doi: 10.1109/TSE.2007.70746.

[4] E. Targett. "6 months, 945 data breaches, 4.5 billion records." https://www.cbronline.com/news/global-data-breaches-2018 (accessed.

[5] "Data breach database." The Breach Level Index. https://breachlevelindex.com/data-breach-database (accessed.

[6] S. Moore. "Gartner says worldwide information security spending will grow 7 percent to reach $86.4 billion in 2017." https://www.gartner.com/newsroom/id/3784965 (accessed.

[7] J. P. Laudon and K. C. Laudon, *Essentials of MIS, global edition*. Pearson Higher Education & Professional Group, 2016.

[8] y. lu, "Research on Data Privacy Protection and Information Security Algorithm Technology in the Standard Digitalization Background," p. 38, 2024, doi: 10.1117/12.3034787.

[9] "The New Trend of the Integration of Artificial Intelligence and Blockchain in Network Security," *Academic Journal of Computing & Information Science*, vol. 7, no. 3, 2024, doi: 10.25236/ajcis.2024.070305.

[10] "ISO 27001 global report," IT Governance, 2016.

[11] L. Compagna, P. El Khoury, F. Massacci, R. Thomas, and N. Zannone, "How to capture, model, and verify the knowledge of legal, security, and privacy experts: a pattern-based approach," in *11th international conference on Artificial intelligence and law*, 2007, pp. 149-153, doi: 10.1145/1276318.1276346.

[12] C. B. Haley, R. Laney, J. D. Moffett, and B. Nuseibeh, "Security requirements engineering: a framework for representation and analysis," *IEEE Transactions on Software Engineering*, vol. 34, no. 1, pp. 133-153, 2008, doi: 10.1109/TSE.2007.70754.

[13] B. Von Solms, "Information Security governance: COBIT or ISO 17799 or both?," *Computers and Security*, vol. 24, no. 2, pp. 99-104, 2005, doi: 10.1016/j.cose.2005.02.002.

[14] E. Coles-Kemp, "The anatomy of an information security management system," King's College London, University of London, 2008.

[15] E. W. N. Bernroider and M. Ivanov, "IT project management control and the Control Objectives for IT and related Technology (CobiT) framework," *International Journal of Project Management*, vol. 29, no. 3, pp. 325-336, 2011, doi: 10.1016/j.ijproman.2010.03.002.

[16] D. Ganji, C. Kalloniatis, H. Mouratidis, and S. M. Gheytassi, "Approaches to develop and implement ISO/IEC 27001 standard - information security management systems: a systematic literature review," *International Journal On Advances in Software*, vol. 12, no. 3-4, pp. 228-238, 2019.