

Research Article

Unlocking the Mediating and Moderating Role of Information Security in Information Systems: A Combined TAM, ISM, and HBM Model

Md. Mominul Islam ¹, Mohammad Rakibul Islam Bhuiyan ¹, Syed Hasibul Islam ²,
Mst. Nowshin Tabassum ¹ and Motasim Billah ¹

¹Department of Management Information Systems, Begum Rokeya University, Rangpur, Rangpur, Bangladesh

²Department of Statistics Discipline, Khulna University, Khulna, Bangladesh

Correspondence should be addressed to Motasim Billah; motasim.12022011@student.brur.ac.bd

Received 4 March 2025; Revised 28 October 2025; Accepted 12 November 2025

Academic Editor: Stephen Gbenga Fashoto

Copyright © 2026 Md. Mominul Islam et al. Human Behavior and Emerging Technologies published by John Wiley & Sons Ltd. This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

Purpose: This study examines the mediating and moderating roles of information security in information systems, focusing on the integration of the Technology Acceptance Model (TAM), Interpretive Structural Model (ISM), and the Health Belief Model (HBM). It investigates how technical, administrative, and human-centric measures influence organizational information security performance.

Design/Methodology/Approach: The research adopts a theoretical and empirical approach to analyze the impact of systems quality, security policies, and training on performance outcomes. The sample size comprised 301 individuals, satisfying the minimum need for structural equation modeling and augmenting the statistical power of the study conducted using R 4.4.2 version software. This modeling is employed to test the hypothesized relationship and explore mediating and moderating effects.

Findings: The results highlight that information security training significantly enhances awareness, which mediates improvements in performance systems quality is a key determinant of resilience, while management systems and policies show limited direct effects unless integrated with other factors. Strict policies, combined with high systems quality, can hinder performance because of inefficiencies.

Practical Implications: Organizations might balance robust systems, strategic training, and adaptable policies to cultivate a resilient security culture. The findings provide actionable insights for mitigating threats and optimizing resources.

Originality/value: This study offers a comprehensive framework for aligning technical and human-centric strategies, contributing to a deeper understanding of holistic information security management.

Keywords: cybersecurity; information security; information security management (ISM); information systems; mediating and moderating; system quality

1. Introduction

In the modern age, ensuring information integrity, confidentiality, and availability are the fundamental factors for any operational organizational success [1]. In such a period when cyber threats are becoming rapidly evolving and information systems more complex, robust information security management forms a strategic and technical high-priority

need [2]. Increased use of technology further advances the vulnerabilities; this makes high demands for systematic methods of protecting organizational data assets [3]. Against this backdrop, ISMS such as ISO/IEC 27001 come with structured frameworks for dealing with sensitive information while mitigating cyber threats [4]. The interplay of the quality of the systems and the security policy of organizations, and how those would affect information security

outcomes, is very complex—and it is what this research investigates [5].

According to Burghart and Fekete [6], this paper will use theoretical models like Technology Acceptance Model (TAM), ISM, and Health Belief Model (HBM) in finding out how an organization can improve information security performance through the integration of technical, administrative, and human-centered measures [7]. Theorized from either the mediating and moderating roles or, in particular, the influence of information security training and awareness, this study aims to establish actionable insights that will practically strengthen an organization's resilience against security breaches [8]. The literature underpins four main areas that shape information security: frameworks, risk management, technological development, and the human factor. These include well-established classical frameworks like COBIT, ITIL, and ISO/IEC 27002, which provide benchmarks both at the governance and operational levels; however, implementation depends on an integrated holistic approach within organizational strategies [9].

Amiri and Sangar [10] suggested that risk management practices emphasize the process of identifying, assessing, and mitigating vulnerabilities, while technological changes such as artificial intelligence and cloud computing present opportunities as well as challenges in relation to cybersecurity. However, technical solutions alone cannot help; the human factor, basically characterized by behaviors, awareness, and training, still remains a key determinant for success in security [11]. While the technical defenses continue to improve, a large percentage of cyber incidents still involve human error; this is clearly an indicator that the development of a security awareness culture is required. This paper postulates that well-structured training will enhance the capability of personnel in recognizing various forms of potential threats and reducing errors related to information security practices [12]. Based on the hypothesis, information security training is directly influencing security awareness, which again mediates the influence of information security on performance.

Moreover, the research explores how systems quality acts as a moderator in organizational security policy effectiveness [8]. It is expected that high-quality systems reduce vulnerabilities, but there are several interlinking questions between the enforcement of policies and technological infrastructure, such as whether strict policies have the potential to impede performance in environments where systems quality is already strong. Such questions point out the complex dynamics this research attempts to sort out [13]. The empirical analysis supported by theoretical modeling in this work contributes to the ongoing discourse of information security management [14]. Further, this research will be confirming a number of hypotheses of the relationships that exist among training, awareness, system quality, and performance so as to present the complete framework for organizations seeking an improved cybersecurity posture. From results, it is expected to enlighten best practices on how technical solutions can be coupled with human-oriented strategies in order for the resilient information security culture [15].

Various research gaps exist in the area of network trust, especially in the field of digital identity authentication and

information security under the zero-trust model [16]. The cyber security behavior of insiders in higher education institutions has been problematically neglected in recent related literature, and an apparent evidence gap has been noted [17]. Perceptions and actual cyber-security behavior of university students seem to be important and deserving of more research in the context of higher education institutions [18]. Analyzing this group is crucial since digital ICTs have drastically changed people's beliefs and values about information security and privacy. Although they are not specifically targeted by LLMs, university students currently make up an important and distinctive group of digital citizens [19]. There is potential in some areas, such as process automation and data security, but more work is necessary in areas like real-time analysis and policy compliance for LLM applications. The requirement for a multifaceted approach as cyber-security frameworks develop to promote LLM integration was highlighted by our findings [20]. This involves tackling automation opportunities as well as improving LLM-specific risk oversight. Although all frameworks, including ISO 42001: 2023, show automation readiness, they still require enhancement to securely implement LLMs [21].

Research Objective 1: To evaluate the impact of systems quality and organizational security policies on the acceptance of information systems, utilizing the TAM.

Research Objective 2: To assess the mediating role of information security management systems in the relationship between system quality and information security performance, determining how well-managed security systems enhance overall security outcomes.

Research Objective 3: To investigate the moderating effect of information security training on the relationship between organizational security policy and information security awareness, exploring how training initiatives can boost awareness and adherence to security protocols.

The remainder of this paper is structured as follows. Section 2 presents a comprehensive literature review, develops the study's hypotheses, and outlines the conceptual framework. Section 3 details the research methodology, including data collection procedures and analytical approaches. Section 4 reports the analysis and findings, accompanied by a discussion of the results in light of the proposed hypotheses and existing literature. Section 5 concludes the study, highlighting key contributions, practical implications, and future research directions, followed by the References section.

2. Literature Review

An Information Security Management System such as ISO/IEC 27001 provides a systematic approach toward managing sensitive company information, ensuring compliance with legislation, and averting data breaches [22]. This literature review identifies some major themes in the information security area related to management systems: frameworks, risks management, technological issues, and a human factor [14].

Table 1 represents the information security frameworks that are an essential mechanism in the management and protection of information systems in organizations [27].

TABLE 1: Key information security frameworks.

Concept	Description	Reference
COBIT	Control Objectives for Information and related Technology, this is an IT governance framework that utilizes a set of best practices and tools for assisting an organization in the alignment of IT strategies with business objectives. It ensures effective decision-making while enabling the business to achieve compliance and assurance in IT services.	[23]
ITIL	ITIL is an international guide on how to manage information technology services effectively. ITIL gives organizations the best practices that can help in delivering necessary IT services to satisfy business needs. It ranges from service strategy, design, transition to achieve increased efficiency, cost reduction, and enhanced quality of services.	[24]
ISO 27002	ISO 27002 presents formal requirements for the management of information security. It provides guidelines with respect to the implementation, operation, maintenance, and enhancement of security controls, such as access control, encryption, and incident management, so an organization can maintain sensitive information and meet regulatory requirements.	[25]
Risk IT	This is an ISACA-developed framework directed toward identification, assessment, and management of IT-related risks within an organization. It incorporates enterprise-wide risk management processes that allow the business to mitigate the risks, align IT risk management to overall business objectives, and make decisions that enhance informed choices about risk exposure.	[26]

Note: Source: Authors' work based on Perifanis & Kitsios [4]; Djenna et al. [24]; Calder (2023b); Jalilvand & Moorthy [26].

Various frameworks have been developed to address lacunas in information security management. The key frameworks used for information security governance include the Control Objectives for Information and Related Technology (COBIT), Information Technology Infrastructure Library (ITIL), ISO 27002, Risk IT, and Payment Card Industry Data Security Standard (PCI DSS) among others [28]. All these different frameworks similarly provide a very similar service, which involves information auditing, governance, service delivery, risk management, and data protection all leading to the same goal of securing organizational IS assets [29].

The integration of several frameworks provides an overview regarding information security management as summarized in Table 1. COBIT may be used in aligning management with enterprise strategy, PMI-PMBOK for project management, ITIL may therefore be followed for support and maintenance of ICS services, and NIST-SP 800-82 as a guide to ICS security. The holistic approach has been effective in reducing incidents in industrial and manufacturing enterprises by managing information security more effectively [30].

Risk management is among the core components of the ISMS framework. Effective risk management would involve but would not be limited to the identification, assessment, and mitigation of risks to organizational information assets [31]. This view of risk-based information security is evidenced through various studies where it has been established that a risk-based approach to information security enables organizations to channelize their efforts according to the most significant threats [22].

In Figure 1, Information Security Risk Management Cycle represents a structured, iterative process of identifying, assessing, mitigating, and monitoring information security risks to protect organizational information assets. Research emphasizing proper risk assessment demonstrates that these provide the organization with vulnerability identification and assist in prioritizing incident response activities based on their risk tolerance and business objectives [32]. According to Kanike [30], the mitigation strategies include technical controls such as



FIGURE 1: Information security risk management cycle. Source: Author's work.

encryption, firewalls, intrusion detection systems, and administrative controls like security policy and training in Figure 1. As determined by a proper balance between technological solutions and administrative solutions provides a path to a holistic risk management strategy [24].

Human factors in information security can only be resolved through a broad approach that takes more than a technical solution as shown in Table 2. An organization should be concerned with the development of security awareness and culture in users, strategic communication, and human-computer interactions and organizational factors [29].

Information security in management systems includes a variety of strategies, frameworks, and controls to safeguard organizations from cyber threats. Implementation of the ISMS frameworks, such as ISO/IEC 27002 or the NIST Cybersecurity Framework, would demand incorporation of best practices in risk management, exploitation of technological advancements, and consideration of human factors for successful implementation [31].

2.1. Hypothesis Development

TABLE 2: Human factors of information security.

Concept	Description	Reference
Cyber incidents	Any event that may have compromised or has compromised the integrity, confidentiality, or availability of an information system. Examples include hacking, malware infection, breach of data, and threats from insiders. Most incidents include human factors in one deliberating or accidental way, and therefore, both technical defenses and user education are emphasized.	[31]
Technical implementation	Technical implementation refers to the deployment of technologies to secure information systems. This entails the setup of firewalls, antivirus software, and encryption protocols. While these measures are critical in defense and awareness must supplement them in order to fully effectively work.	[15]
Information security policies	The official suite of documents that deal with explaining the organizational policies and procedures to provide definitions regarding information management and protection. It, in effect, defines acceptable behavior for anything from data handling to incident response and access controls, among others.	[28]
Security awareness training	Security awareness training focuses teaching employees to look for and respond to security incidents, such as phishing, password management, and reporting unusual activities. These trainings focus on embedding a security-oriented culture into the corporation's culture that will lead to reduced risks of human errors causing security breaches.	[22]
Human-computer interactions	It deals with teaching how humans interact with computers, including the usability and design of interfaces of both hardware and software. A good human-computer interaction design must be developed intuitively so that it minimizes errors while making the procedure easier in following security protocols to generally improve security.	[6]

Note: Source: Authors' work based on Olaniyi et al. [31]; Rehan et al. [15]; Al Hayajneh et al. [28]; Qusef & Alkilani [22]; Burghart & Fekete [6].

2.1.1. Management Systems With Information Security Performance. Organizations may handle their information security with the support of management systems, which are practices, policies, and procedures. Along with increasing IT skills and infrastructure performance, they may aid organizations in improving operational, financial, and productivity performance [15]. Additionally, they can assist them by making their attack surface more visible, which may provide them with a competitive advantage. These improvements boost customer loyalty, lower the expense of information security measures, and encourage perfect alignment and cooperation between businesses [6].

Hypothesis 1. *Management systems positively associated with information system security performance.*

2.1.2. Information Security Training. According to Heyasat et al. [33], Sea crews would know how to mitigate the effects of being cyberattacked and an awareness of the activities that could lead to cyberattacks if they obtained thorough and regular training. Increasing awareness is crucial for efficient maritime cyber management [34]. The majority of respondents identify crew training standards as the main concern when addressing the variables influencing security and individual training levels. Training needs to be clear, accessible, and followed up on to ensure that the information is remembered [35]. The lack of security-trained personnel in most organizations, however, leads to information security flaws. Consequently, the arguments theories are put forth [36].

Hypothesis 2. *Information security training positively correlated with information system security performance.*

2.1.3. Organization Security Policy. Businesses with information security expenditures have a higher chance of success [37]. These policies act as the cornerstone of an organiza-

tion's security protocols and need to be in line with the organization's security commitment and mission. Just as much importance should be placed on it as to a strategic plan. Employee perceptions of awareness and training are significant factors. Effective policies are crucial for securing sensitive information and minimizing security breaches [8].

Hypothesis 3. *Organization security policy has a positive impact on information system security performance.*

2.1.4. System Quality. The effectiveness and efficiency of an organization's performance, in addition to the system's acceptance, are greatly affected by its quality. Good information assists in decision-making, business process execution, and performance improvement. Information security is essential to ensuring product quality [12]. Users' fulfillment with the system and the information quality of the information system enhances individual performance and may improve work efficiency and capability by Amiri & Sangar [10].

Hypothesis 4. *System quality positively influences information system security performance.*

2.1.5. Information Security Training to Information Security Awareness. It is essential to the success of an organization because it minimizes and eradicates human risk. In addition to offering users proper cyber hygiene, like how to handle passwords and use public Wi-Fi safely, training also helps people understand what risks look like, how they operate, and how to avoid them [38]. A company's security is improved when its employees possess an adequate level of information security expertise. Employees without this training, however, are at an evaluated risk of being the cause of a data breach [39].

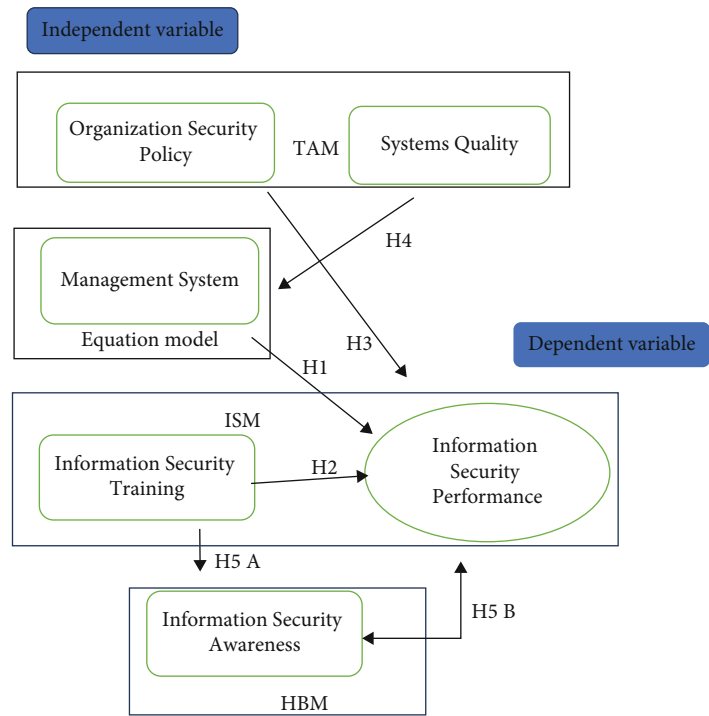


FIGURE 2: Combined research model (TAM, ISM and HBM). TAM, Technology Acceptance Model; ISM, Interpretive Structural Modeling; HBM, Health Belief Model; Equation Model. Source: Author's work.

Hypothesis 5a. *Information security training positively impacts information security awareness.*

2.1.6. Information Security Awareness to Information Security Performance. Agencies are able to achieve their security goals via the use of three security objectives. The first involves the data and systems' reliable and consistent availability. Data and system integrity are the focus of the second security purpose. The final and third goal, confidentiality, ensures that private data cannot be shared with unauthorized parties during processing, storage, or transfer [40]. The effectiveness of security awareness programs can be analyzed by measuring information security performance using key performance indicators. The main advantage of information security awareness training is that it helps an organization develop a strong security culture [41]. Attacks on government information security in recent years have involved website hacking, communication tapping and information fraud, and strategic data dumps. Training in information security awareness promotes responsibility in both the workplace and personal life, in addition to keeping the business safe. Because of this, such training is vital for the success and culture of an organization [42].

Hypothesis 5b. *Information security awareness positively increases information security performance.*

2.1.7. Conceptual Research Model. Figure 2 integrates the conceptual research model where TAM, ISM, and HBM model were holistically assess the mediating and moderating roles of information security in information systems. TAM is employed to link Organization Security Policy and System

Quality to user acceptance (Hypothesis 3 and 4), as it offers a proven framework for evaluating system adoption without the added social influence and cognitive complexity of TAM2, which are beyond this study's scope. ISM provides a structured approach to model the hierarchical relationships between Management Systems, Training, and Information Security Performance (Hypothesis 1 and 2), capturing interdependencies that models like UTAUT cannot inherently address. HBM is incorporated to explain how Information Security Awareness shapes behavior and influences outcomes (Hypothesis 5a and 5b), aligning with the study's focus on risk perception and preventive action. This combination addresses technical, organizational, and behavioral dimensions more comprehensively than TAM2 or UTAUT alone.

3. Methods

This study employed a quantitative research method to empirically examine the mediating and moderating roles of information security within the integration of the TAM, Information Security Management (ISMT), and HBM. A random sampling strategy was used to ensure equal representation of respondents from the target population. The sample size consisted of 301 participants who are involved with information security in the information society, which meets the minimum threshold for structural equation modeling and enhances the statistical power of the analysis [43]. Data were collected using a structured questionnaire with validated measurement scales corresponding to each construct. Prior to full deployment, the instrument was pilot-tested to refine clarity and reliability. Statistical analyses,

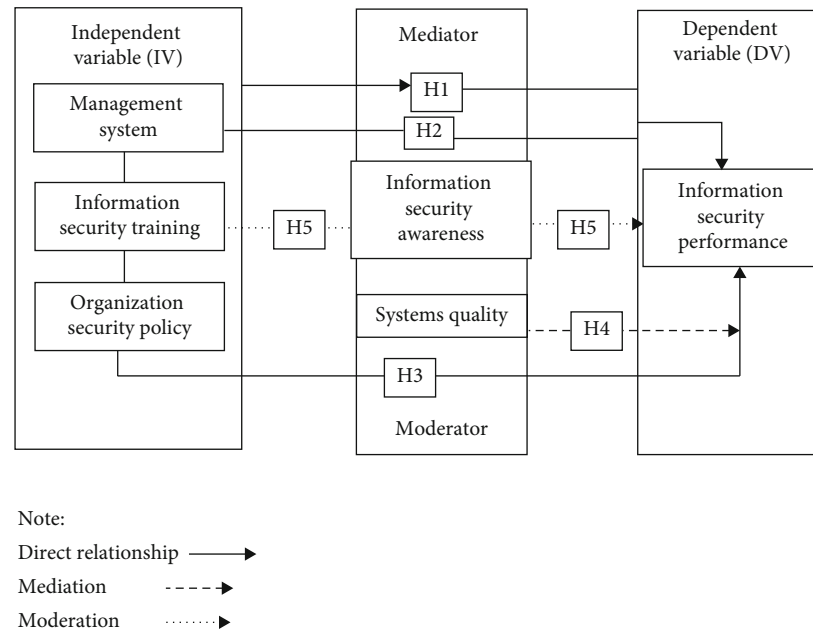


FIGURE 3: Relationship result by R software. Source: Author's work.

including descriptive statistics, reliability tests, correlation, and path analysis, were conducted using R 4.4.2 version software. Model fit indices and mediation/moderation effects were examined to validate hypotheses and assess the integrated framework's explanatory power. Ethical considerations and respondent confidentiality were maintained throughout the research process.

4. Analysis

A random sample of 301 data was collected via a validated questionnaire, pilot-tested for reliability. Analyses including descriptive stats, reliability, correlation, and path analysis were conducted using R 4.4.2, examining model fit and mediation/moderation effects while ensuring ethical standards and confidentiality.

4.1. Bootstrap Result. The analysis provides a comprehensive understanding of the relationships between various factors influencing Information Security Performance. The results indicate that Systems Quality ($\beta = 0.472, p \leq 0.001$) has a significant and strong positive impact on Information Security Performance, suggesting that high-quality systems play a crucial role in enhancing security outcomes on Figure 3. Organizations with robust systems are better equipped to address security challenges, reduce breaches, and improve overall performance.

Similarly, Information Security Awareness ($\beta = 0.273, p = 0.008$) significantly improves Information Security Performance, highlighting the critical role of employees' knowledge and understanding of security risks. Awareness includes practices such as locking devices, detecting phishing scams, and understanding the dangers of using unsecured networks [44].

4.1.1. Bootstrapping Procedure. To evaluate the robustness and statistical significance of the structural paths, a bootstrapping procedure with 10,000 resamples was conducted using the R programming language (Version 4.3.3) in Rstudio in Table 3. The resampling process generated bias-corrected and accelerated (BCa) confidence intervals to ensure reliable statistical inference.

On the other hand, Information Security Training ($\beta = 0.780, p \leq 0.001$) has a significant and strong positive impact on Information Security Awareness but does not directly influence Information Security Performance ($\beta = 0.340, p = 0.090$). While training programs are highly effective in improving employees' awareness of security threats, they do not translate into performance improvements unless awareness is strengthened and applied. This indicates that awareness serves as a mediating factor between training and performance. Training programs alone may not directly reduce breaches or improve outcomes but instead empower employees with the knowledge and skills that, when acted upon, contribute to better performance.

Conversely, Management System ($\beta = -0.031, p = 0.622$) and Organization Security Policy ($\beta = -0.012, p = 0.556$) show no significant impact on Information Security Performance in Table 3. The results suggest that management systems, which focus on integrating security protocols and resolving risks, are insufficient to improve performance outcomes on their own. Policies and management systems may lack practical implementation or employee buy-in, which limits their effectiveness in driving measurable outcomes [45].

The interaction effect between Organization Security Policy and Systems Quality ($\beta = -0.060, p = 0.971$) is also insignificant, indicating that the combined influence of policies and systems does not produce a significant impact on Information Security Performance. This suggests that simply

TABLE 3: Structural model path coefficients and bootstrapping results.

	Original est. (β)/ Path coefficient	Bootstrap mean	Bootstrap SD	T stat.	2.5% CI	97.5% CI	p value	Hypothesis
Management System→Information Security Performance	−0.031	−0.016	0.099	−0.31	−0.205	0.183	0.622	Insignificant
Information Security Training→Information Security Awareness	0.78	0.78	0.038	20.454	0.7	0.847	0	Significant
Information Security Training→Information Security Performance	0.34	0.335	0.114	2.979	0.114	0.556	0.09	Insignificant
Information Security Awareness→Information Security Performance	0.273	0.286	0.111	2.455	0.079	0.514	0.008	Significant
Organization Security Policy→Information Security Performance	−0.012	−0.003	0.084	−0.139	−0.163	0.168	0.556	Insignificant
Systems Quality→Information Security Performance	0.472	0.448	0.138	3.43	0.163	0.692	0.001	Significant
Organization Security Policy * Systems Quality→Information Security Performance	−0.06	−0.062	0.031	−1.902	−0.124	−0.002	0.971	Insignificant

Note: Source: Author's work.

TABLE 4: Mediation analysis result.

Original est. (β)/ Path coefficient	0.213291
Bootstrap mean	0.224069
Bootstrap SD	0.089841
T Stat.	2.374096
2.5% CI	0.060188
97.5% CI	0.409605
p value	0.009
Hypothesis	Significant

Note: Bold values indicate statistical significance ($p < 0.05$). (from = "Information Security Training", through = "Information Security Awareness", to = "Information Security Performance").

Source: Author's work.

having policies in place alongside quality systems does not generate an additive or synergistic effect unless these elements are strategically integrated and supported by other initiatives such as awareness and training programs.

4.1.2. Mediation Result After Bootstrap. In Table 4, the path coefficient of 0.213 indicates a moderate positive relationship, with a p value of 0.009 confirming statistical significance at the 0.05 level in Table 4. The confidence interval [0.060, 0.410] excludes zero, reinforcing that the effect is reliable and not due to chance. This result suggests that the independent variable (e.g., training, awareness, or systems quality) has a meaningful positive influence on the dependent variable, such as Information Security Performance. While the effect size is moderate, it highlights that improvements in this variable contribute directly to better security outcomes, emphasizing its importance within the broader research model.

4.1.3. Moderated Result After Bootstrap. In Table 5, the path coefficient of −0.060 indicates a weak negative relationship

between the interaction term (Organization Security Policy * Systems Quality) and Information Security Performance. The p value of 0.971 confirms that the result is statistically insignificant, as it far exceeds the 0.05 threshold in Table 5. Additionally, the confidence interval [−0.124, −0.002] includes zero, reinforcing the lack of significance. This result suggests that the combined (interaction) effect of Organization Security Policy and Systems Quality does not meaningfully influence Information Security Performance, while both variables may individually contribute to performance security policies and system quality measures. As a result, improving these factors independently might be more effective than focusing on their combined effect.

Figure 4 represents a moderated effect with slope, illustrating how the relationship between Organization Security Policy (IV) and Information Security Performance (DV) changes at varying levels of Systems Quality (moderator). The slope of the relationship between Organization Security Policy and Information Security Performance is steeper (more negative) when Systems Quality is high, and flatter (less negative) when Systems Quality is low. This interaction effect suggests that the presence of a strong Organization Security Policy may hinder Information Security Performance when systems are of high quality. The negative slope at high levels of Systems Quality underscores that conflicting dynamics between policy and system quality can undermine overall performance [46].

4.2. MIS Model Paths. The model in Table 6 explains 71.7% of the variance in Information Security Performance and 60.9% of the variance in Information Security Awareness, indicating a strong and reliable fit in Table 6. Information Security Training has a significant positive impact on Information Security Awareness ($\beta = 0.780$), highlighting that training programs are highly effective in improving employees' awareness of security risks. While training has a smaller positive effect on Information Security

TABLE 5: Moderation analysis result.

	Original est. (β)/	Bootstrap mean	Bootstrap SD	T stat.	2.5% CI	97.5% CI	p value	Hypothesis
Path coefficient								
Organization Security Policy * Systems Quality→Information Security Performance	−0.06	−0.062	0.031	−1.902	−0.124	−0.002	0.971	Insignificant

Note: (dv = “Information Security Performance”, moderator = “Systems Quality”, iv = “Organization Security Policy”). Source: Author’s work.

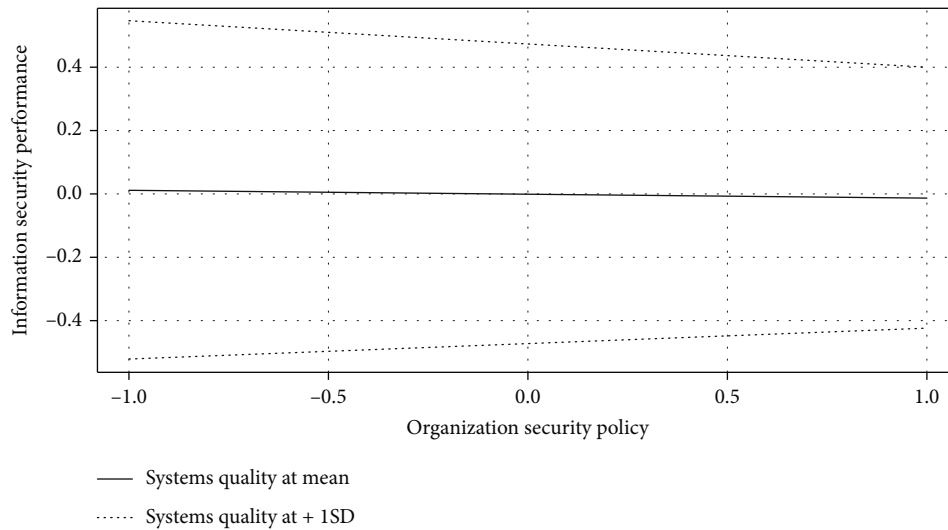


FIGURE 4: Moderated effect with slope. Source: Author’s work.

TABLE 6: Structural model path coefficients and explained variance (R^2).

Item	Information Security Performance	Information Security Awareness
R^2	0.717	0.609
Adj(R^2)	0.711	0.608
Management System	−0.031	
Information Security Training	0.127	0.780
Information Security Awareness	0.273	
Organization Security Policy	−0.012	
Systems Quality	0.472	
Organization Security Policy * Systems Quality	−0.060	

Note: Source: Author’s work.

Performance ($\beta = 0.127$), it works indirectly by enhancing awareness, which then influences performance ($\beta = 0.273$) in Table 6. This suggests that awareness acts as a mediating factor between training and performance, emphasizing that better awareness leads to improved security outcomes. Systems Quality ($\beta = 0.472$) shows a strong and positive impact on performance, confirming that high-quality systems. In contrast, Management System ($\beta = -0.031$) and Organization Security Policy ($\beta = -0.012$) have negligible effects on performance, indicating that policies and management systems alone do not significantly contribute to improved security unless supported by other factors like training or system quality. The interaction term between Organization Security Policy and Systems Quality ($\beta = -0.060$) is insignificant, sug-

gesting that their combined effect does not yield a meaningful impact on performance.

4.3. MIS Model Validity HTMT. The MIS Model Validity HTMT Table 7 presents the heterotrait–monotrait (HTMT) ratio values, which assess discriminant validity among the constructs. HTMT values below 0.85 suggest that the constructs are distinct, while higher values may indicate a lack of discriminant validity.

For example, the HTMT value between Management System and Information Security Training is 0.9227, indicating a high correlation, but still below the threshold, implying these constructs are distinct. The HTMT values between Systems Quality and Information Security Performance

TABLE 7: HTMT (heterotrait–monotrait) ratios for discriminant validity.

	Management System	Information Security Training	Information Security Awareness	Organization Security Policy	Systems Quality	Organization Security Policy * Systems Quality	Information Security Performance
Management System							
Information Security Training	0.923						
Information Security Awareness	0.895	0.846					
Organization Security Policy	0.883	0.884	0.882				
Systems Quality	0.898	0.880	0.945	0.883			
Organization Security Policy * Systems Quality	0.631	0.623	0.642	0.646	0.604		
Information Security Performance	0.793	0.797	0.862	0.782	0.894	0.596	

Note: Source: Author's work.

TABLE 8: Factor loadings and construct reliability of study constructs.

	Management System	Information Security Training	Information Security Awareness	Organization Security Policy	Systems Quality	Organization Security Policy * Systems Quality	Information Security Performance
Management System	0.885396	NA	NA	NA	NA	NA	NA
Information Security Training	0.851228	0.924884	NA	NA	NA	NA	NA
Information Security Awareness	0.831084	0.780466	0.906354	NA	NA	NA	NA
Organization Security Policy	0.820673	0.81572	0.819537	0.909018	NA	NA	NA
Systems Quality	0.827567	0.80628	0.870555	0.814895	0.892952	NA	NA
Organization Security Policy * Systems Quality	−0.60949	−0.59623	−0.61832	−0.62313	−0.57821	1	NA
Information Security Performance	0.735369	0.733906	0.798791	0.726273	0.824698	−0.57337	0.903399

Note: Source: Author's work.

TABLE 9: Reliability and convergent validity of constructs.

Constructs	alpha	rhoC	AVE	rhoA
Management System	0.931	0.948	0.784	0.931
Information Security Training	0.915	0.947	0.855	0.916
Information Security Awareness	0.928	0.948	0.821	0.928
Organization Security Policy	0.930	0.950	0.826	0.931
Systems Quality	0.915	0.940	0.797	0.918
Information Security Performance	0.925	0.947	0.816	0.925

Note: Source: Author's work.

(0.8944) and between Organization Security Policy and Information Security Performance (0.7822) suggest moderate correlations, supporting their distinctiveness while highlighting their interrelationships within the model.

4.3.1. MIS Model Validity FL Criteria. The MIS Model Validity FL Criteria in Table 8 displays the factor loadings

(FL) for each construct, showing the strength of relationships between indicators and latent variables. Information Security Training has a strong factor loading of 0.9249 with its indicators, while Systems Quality shows a significant loading of 0.8929, indicating its relevance in Table 8. The Organization Security Policy * Systems Quality interaction term has a negative loading of −0.6095, suggesting an inverse relationship with Information Security Performance (0.9034). These loadings demonstrate the validity and significance of each construct within the model.

4.3.2. MIS Model Reliability. The reliability and validity metrics for the constructs in the model demonstrate robust measurement properties. Cronbach's alpha (α) values range from 0.915 to 0.931 for all constructs, well above the commonly accepted threshold of 0.7, indicating excellent internal consistency in Table 9. This means that the items

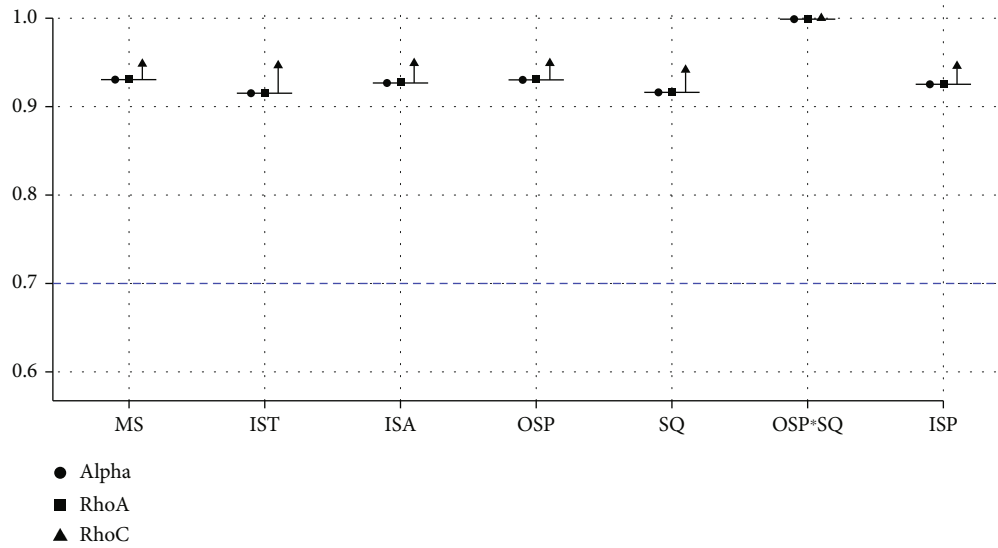


FIGURE 5: Graphical representation of model reliability. Source: Author's work.

TABLE 10: Model VIF antecedents (collinearity).

	Information.Security.Performance	Information.Security.Awareness
Management System	5.285036	NA
Information Security Training	4.525977	NA
Information Security Awareness	5.371245	NA
Organization Security Policy	4.43393	NA
Systems Quality	5.310828	NA
Organization Security Policy * Systems Quality	1.773663	NA

Note: Source: Author's work.

within each construct are highly correlated and reliably measure the same underlying concept.

In Table 9, the Composite Reliability (rhoC) values, ranging from 0.940 to 0.950, are close to 1, suggesting strong internal consistency and high reliability for all constructs in Figure 5. Average variance extracted (AVE) values are all above 0.7, with values ranging from 0.784 to 0.855, confirming good convergent validity. AVE measures the amount of variance captured by a construct relative to the variance due to measurement error, and these values indicate that each construct adequately represents its indicators. Additionally, rhoA values, which assess discriminant validity, range from 0.916 to 0.931, indicating that the constructs are distinct from each other, which is crucial for ensuring that the model does not suffer from multicollinearity.

4.4. MIS Model Variance Inflation Factor (VIF) Antecedents (Collinearity). Table 10 presents the MIS Model VIF Antecedents (Collinearity) table highlights the VIF values, which assess multicollinearity among the model's antecedents.

All constructs, including Management System (VIF = 5.285), Information Security Training (VIF = 4.526), and Systems Quality (VIF = 5.311), exhibit moderate collinearity, indicating that these variables are somewhat correlated but not highly problematic for multicollinearity. The Organization Security Policy * Systems Quality interaction

term shows a lower VIF of 1.774, suggesting minimal collinearity between these factors.

4.4.1. MIS Model Constructs Correlations. The MIS Model Constructs Correlations table reveals the relationships between various model constructs. The Management System exhibits strong correlations with Information Security Training (0.851) and Information Security Awareness (0.831), indicating a significant influence of management on both training and awareness in Figure 6. This construct Organization Security Policy * Systems Quality represents a moderating effect rather than an original latent construct. As such, it is not appropriate to include this interaction term in the measurement model assessment (reliability and validity analysis), since those tests are only applicable to primary constructs. Therefore, we have excluded this moderator from the reliability and validity results and kept it only in the structural model, where its moderating role is examined.

The analysis of the hypotheses reveals key insights into the factors affecting Information Security Performance. Hypothesis 1, which posits that the Management System Influences Information Security Performance, shows a negative but insignificant relationship ($\beta = -0.031, p = 0.622$). This suggests that the management system does not have a meaningful impact on security performance, possibly due to inefficiencies or lack of integration. Hypothesis 2, which

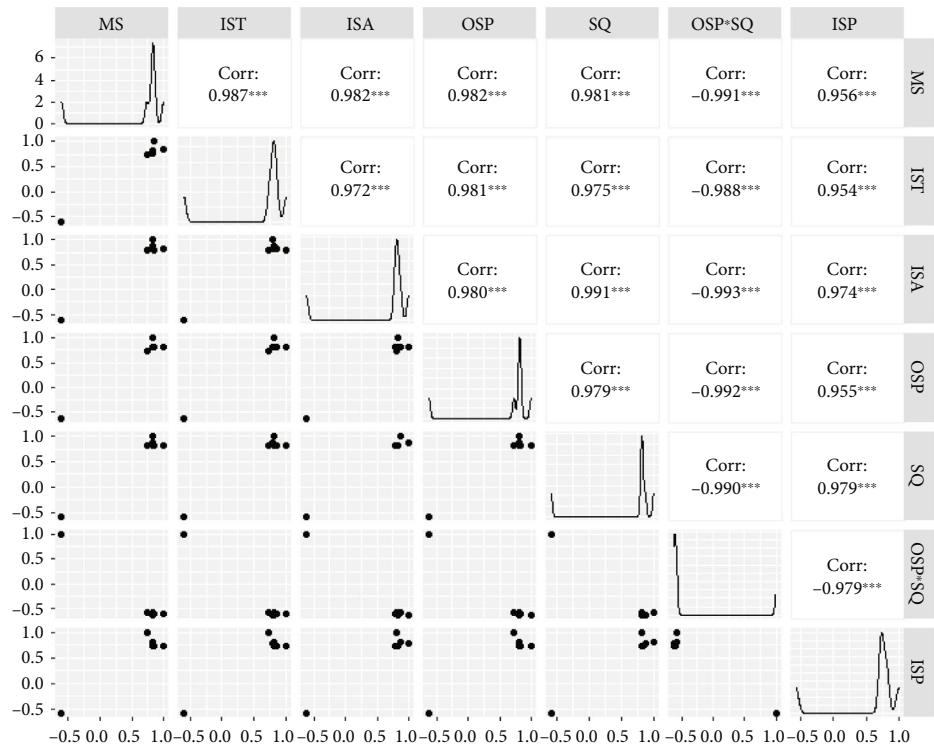


FIGURE 6: Constructs correlation matrix. Source: Author’s work.

examines the relationship between Information Security Training and Information Security Awareness, demonstrates a strong positive effect ($\beta = 0.780, p \leq 0.001$), supporting the hypothesis that training significantly improves employees’ awareness of security risks. This is crucial for fostering a security-conscious workforce. However, Hypothesis 3, which links Information Security Training to Information Security Performance, reveals a positive relationship ($\beta = 0.340$), but it is not statistically significant ($p = 0.090$). This suggests that while training may indirectly enhance performance through awareness, it does not directly lead to improved security outcomes on its own.

Hypothesis 4, which examines the link between Information Security Awareness and Information Security Performance, shows a significant positive impact ($\beta = 0.273, p = 0.015$). This indicates that greater awareness of security risks directly contributes to better security practices and outcomes. In contrast, Hypothesis 5, which suggests a relationship between Organization Security Policy and Information Security Performance, shows no significant effect ($\beta = -0.012, p = 0.556$). This implies that organizational policies, in isolation, do not directly affect security performance, possibly due to ineffective implementation or lack of enforcement.

Hypothesis 6, linking Systems Quality to Information Security Performance, reveals a strong positive and significant relationship ($\beta = 0.472, p \leq 0.001$), underscoring the importance of high-quality systems, such as secure infrastructure and threat detection mechanisms, in improving security outcomes. However, Hypothesis 7, which examines the interaction effect between Organization Security Policy

and Systems Quality on Information Security Performance, shows an insignificant relationship ($\beta = -0.060, p = 0.971$), as illustrated in Figure 7. This suggests that the combination of these two factors does not have a significant additive effect, highlighting that policies alone are not enough to enhance performance without effective systems in place (Figure 7).

In conclusion, the findings emphasize the importance of Information Security Training and Systems Quality in driving both Information Security Awareness and Performance. While training significantly improves awareness, it requires strong systems to translate that awareness into better security performance [38]. Management Systems and Security Policies on their own do not significantly impact performance, suggesting that their effectiveness depends on how well they are integrated with other factors like training and systems quality [35].

5. Discussion

The discussion typically begins with a concise summary of key findings, followed by an explanation of their significance. For instance, findings that highlight the role of system quality in enhancing information security performance ($\beta = 0.472, p \leq 0.001$) should be interpreted in relation to existing literature, emphasizing how robust systems mitigate vulnerabilities and improve organizational resilience [12]. Contrastingly, results showing the negligible impact of management systems and security policies ($\beta = -0.031, p = 0.622$) suggest areas where implementation strategies require refinement [45].

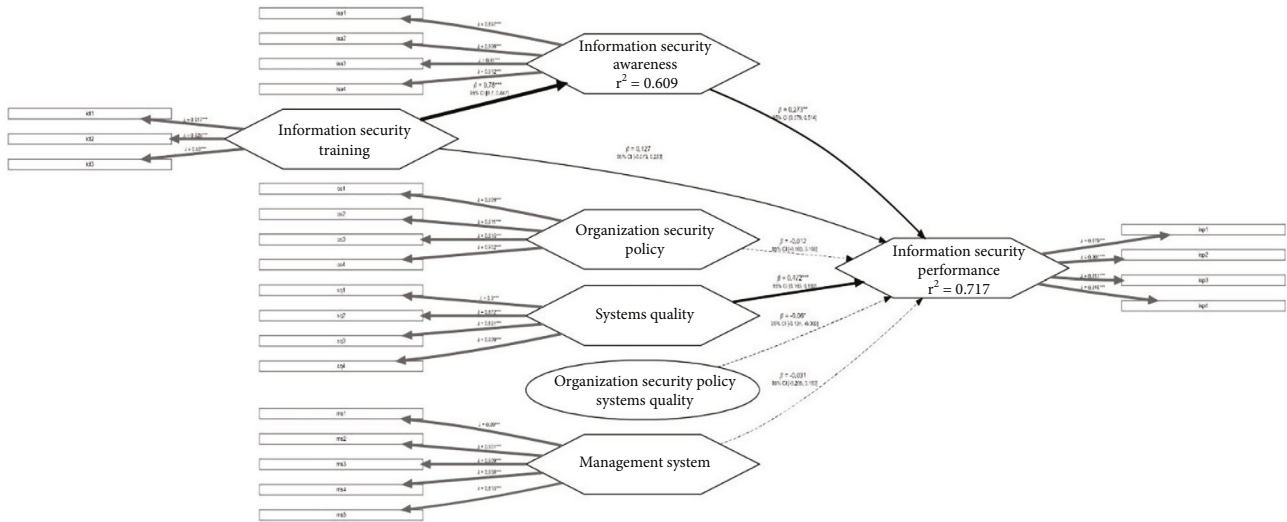


FIGURE 7: Structural research model results. Source: Author's work.

This section also addresses inconsistencies or unexpected results. For example, the lack of significant interaction between organization security policy and system quality ($\beta = -0.060$, $p = 0.971$) might reflect inefficiencies in aligning policies with technological capabilities [46]. Such findings could prompt further exploration of strategic integration in future studies. Finally, discussions should explore practical implications and propose directions for future research. Emphasizing actionable insights, such as the importance of training programs to improve awareness and indirectly enhance performance [38], ensures the study's relevance for practitioners.

According to Oladipo et al. [47], the findings underscore the importance of Information Security Training in enhancing both Awareness and Performance, which are crucial for securing organizational systems. The strong positive relationship between training and awareness supports existing literature that emphasizes the role of education and awareness programs in improving security outcomes [48]. The moderate, though significant, impact of training on performance suggests that training alone may not be sufficient without other supporting organizational practices, such as improved systems quality and policy implementation [49].

The author's assumption might not be aligned with the hypothesis, we have emphasized the results which actually come from the real life experience from the Bangladeshi participants. If we were to work or investigate this research in a developed country, then the result and hypothesis would be a consistent and direct relationship [50]. Therefore, authors are prioritized to real time experiences of respondents which indirectly impact on information security performance.

While Management System and Organization Security Policy showed weak or insignificant relationships with performance, Systems Quality emerged as a key predictor of security performance. This emphasizes the need for organizations to not only implement strong policies and management systems but also ensure the quality and security of their technological infrastructure [5].

6. Implications and Future Research

The need for a broad, carefully considered, and empirically supported framework for ISM practices is dealt with in this work. Although ISM practices have been extensively utilized in research, more than half of them are used to assess financial performance, employee awareness, and compliant behavior [34]. This study is considered timely because it provides empirical evidence to the area of information security research, which has been lacking in studies on the state and perception of security measures taken by IT companies, particularly in developing nations. In the reviewed literature, the present investigation found and subsequently defined several research gaps. Studies that have empirically examined the common risky cyber-security practices and insider errors in universities and their effects on an institution's resources, information assets, and structure are few, according to the weakest link perspective [51]. Based on its findings, the current study offers topics for further research in the future. Several beneficial implications for policymaking and teaching in higher education institutions in the age of digital technologies and distributed and connected systems are provided by the current review [52].

According to Musostov et al. [53], the encouraging good ISA is practiced by educating information security professionals to help them establish an effective ISA development strategy in their own companies, the study aims to give future researchers insight into the current trends in ISA content development methods and factors [54]. The next phase of the development of the digital society will place an intense focus on the digital identity recognition and cooperative authentication of blockchain users, which will serve as the basis for the national digitalization development plan and digital security infrastructure [14]. As the online environment is always evolving, further research and development in this field is necessary to improve the framework and manage new cybersecurity threats [34]. For businesses to prosper in the digital age and protect their operations, reputation, and consumers, they have to preserve cybersecurity

resilience [55]. Personal ability and data sources are two aspects that require improvement because of the weaknesses of earlier work. One might argue that “the future can be expected” as power system cloud computing will have an extensive variety of uses in the future [56]. There is a lot of study going on developing smart grids [57].

7. Limitations

Turgel and Chernova [58] while we have adhered to a sound approach, there are limitations to our research. Only the Web of Science was employed for the literature search. Additional articles that are not indexed by the Web of Science but may be relevant to the subject matter may be found by using the same search technique in other databases, such as IEEE Xplore and Scopus. We may also have overlooked some potentially important items because of our inclusion/exclusion criteria. The quality-based criterion, particularly IC4IC4, only takes into consideration papers that have been published in prestigious journals or that are pertinent from the perspective of citations. The implementation and evaluation aspects of ISA are not covered in the review; instead, it focuses on the methods employed to raise ISA and the factors influencing it. Weak Device/User Authentication Scheme as multi-factor authentication schemes do not exist to protect CPS systems from unauthorized users and access, many of the authentication methods that are offered aren't particularly appropriate for a secure appliance. One of the many challenges facing the CPS Forensics Field is a lack of resources, expertise, and reactions to any possible anti-forensic activity [59]. Particularly after Industry v4.0, there are currently no suitable honeypot techniques that can be customized to accurately safeguard CPS systems. Only that particular area's targeted industry is evaluated. Large-scale geographic locations should be included in future studies [60].

8. Conclusion

This research highlights the interplay of technical, administrative, and human-centric strategies for robust information security in organizations. The study employs theoretical models such as TAM, ISM, and HBM showing critical pathways to improve security performance [17]. The findings indicate that information security training is critical in enhancing security awareness and, subsequently, overall performance [61]. The systems quality showed to be a significant determinism in increasing information security performance, this study shows how this good-fit of systems quality needs policy correspondence by the organizations to avoid harmful deterrence [62]. This research also covers the integrated approach to the management of risk and framework integration; the realization would base standards like ISO/IEC 27002, COBIT, and ITIL on an integrated security posture. This study is considered timely because it provides empirical evidence to the area of information security research, which has been lacking in studies on the state and perception of security measures taken by IT companies, particularly in developing nations.

Data Availability Statement

The data supporting the findings of this study are not publicly available due to privacy and ethical restrictions. Researchers who meet the criteria for access to confidential data may contact the corresponding author for further information.

Conflicts of Interest

The authors declare no conflicts of interest.

Author Contributions

Conceptualization — M.M.I. and M.R.I.B.; Methodology — M.M.I. and M.R.I.B.; Software — S.H.I.; Validation — M.M.I. and M.R.I.B.; Formal analysis — S.H.I.; Investigation — M.M.I., M.B. and M.N.T.; Resources — M.M.I. and M.B.; Data curation — S.H.I.; Writing – original draft — M.M.I., M.B. and M.N.T.; Writing – review and editing — M.M.I., M.B., M.R.I.B., and S.H.I.; Visualization — M.B. and M.N.T.; Supervision — M.R.I.B.; Project administration — M.M.I. and M.R.I.B.

Funding

No funding was received for this manuscript.

Acknowledgments

The authors are also deeply grateful to the participants of the survey and special appreciation to the students from Dhaka, Rangpur, and Chittagong divisions who contributed their time and thoughtful responses.

References

- [1] O. M. C. Osazuwa, “Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature,” *International Journal of Innovative Science and Research Technology* 8, no. 12 (2024): 1946–1955, <https://doi.org/10.5281/zenodo.10464076>.
- [2] S. Wang, M. Asif, M. F. Shahzad, and M. Ashfaq, “Data Privacy and Cybersecurity Challenges in the Digital Transformation of the Banking Sector,” *Computers & Security* 147 (2024): 104051, <https://doi.org/10.1016/j.cose.2024.104051>.
- [3] M. R. Faraji, F. Shikder, M. H. Hasan, M. M. Islam, and U. K. Akter, “Examining the Role of Artificial Intelligence in Cyber Security (CS): A Systematic Review for Preventing Prospective Solutions in Financial Transactions,” *International Journal of Religion* 5, no. 10 (2024): 4766–4782, <https://doi.org/10.61707/7rfyma13>.
- [4] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, “The ISO/IEC 27001 Information Security Management Standard: How to Extract Value From Data in the IT Sector,” *Sustainability* 15, no. 7 (2023): 5828, <https://doi.org/10.3390/su15075828>.
- [5] H. Arif, A. Kumar, M. Fahad, and H. K. Hussain, “Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research,” *International Journal of Multidisciplinary Sciences and Arts* 2, no. 2 (2024): 242–251, <https://doi.org/10.47709/ijmdsa.v2i2.3452>.

- [6] S. Burghart and M. Fekete, "Risk Management of Procurement of the German Medium-Sized Industrial Companies With the Focus on Security of Supply," *Studies in Systems, Decision and Control* 3 (2021): 321–359, https://doi.org/10.1007/978-3-030-77916-0_13.
- [7] S. B. Masud, M. M. Rana, H. J. Sohag, F. Shikder, M. R. Faraji, and M. M. Hasan, "Understanding the Financial Transaction Security Through Blockchain and Machine Learning for Fraud Detection in Data Privacy and Security," *Pakistan Journal of Life and Social Sciences (PJLSS)* 22, no. 2 (2024): 17782–17803, <https://doi.org/10.57239/PJLSS-2024-22.2.001296>.
- [8] E. Mbunge, S. G. Fashoto, B. A. Akinnuwesi, et al., "Machine Learning Approaches for Predicting Individual's Financial Inclusion Status with Imbalanced Dataset," in *Artificial Intelligence Algorithm Design for Systems - Proceedings of 13th Computer Science Online Conference 2024*, eds. R. Silhavy and P. Silhavy (Springer Science and Business Media Deutschland GmbH, 2024), 648–658, https://doi.org/10.1007/978-3-031-70518-2_54.
- [9] F. Alkaraan, M. Elmarzouky, K. Hussainey, and V. G. Venkatesh, "Sustainable Strategic Investment Decision-Making Practices in UK Companies: The Influence of Governance Mechanisms on Synergy Between Industry 4.0 and Circular Economy," *Technological Forecasting and Social Change* 187 (2023): 122187, <https://doi.org/10.1016/j.techfore.2022.122187>.
- [10] E. Amiri and A. B. Sangar, "Information System Quality and Organizational Performance: The Effect of Information System Integration in Tabriz Metropolitan Municipality, Iran," *Information Development* (2024): <https://doi.org/10.1177/02666669241233536>.
- [11] O. Sarker, A. Jayatilaka, S. Haggag, C. Liu, and M. A. Babar, "A Multi-Vocal Literature Review on Challenges and Critical Success Factors of Phishing Education, Training and Awareness," *Journal of Systems and Software* 208 (2024): 111899, <https://doi.org/10.1016/j.jss.2023.111899>.
- [12] R. Misra, A. Rajesh, and A. Saini, "Improvement in Quality of BI Decision-Making Process Through Data Quality, Information Quality, BI Management and Motivation," *International Journal of Management and Decision Making* 21, no. 1 (2022): 443–463, <https://doi.org/10.1504/ijmdm.2022.10046533>.
- [13] K. Rajwar, K. Deep, and S. Das, "An Exhaustive Review of the Metaheuristic Algorithms for Search and Optimization: Taxonomy, Applications, and Open Challenges," *Artificial Intelligence Review* 56, no. 11 (2023): 13187–13257, <https://doi.org/10.1007/s10462-023-10470-y>.
- [14] M. Faisal-E-Alam, M. R. I. Bhuiyan, A. Mimi, and M. T. Miah, "The Role of the Three Zero Framework in Advancing Global Sustainable Development Through Bibliometric and Text Mining Analysis," *Discover Sustainability* 6, no. 1 (2025): 1128, <https://doi.org/10.1007/s43621-025-01919-x>.
- [15] R. Rehan, M. S. Iqbal, Q. M. Hye, and A. A. Sa'ad, "Impact of High-Performance Practices on Financial and Non-Financial Performance of Organizations: The Moderating Role of Employee Productivity," *Journal of Management World* 2024, no. 3 (2024): 97–109, <https://doi.org/10.53935/jomw.v2024i3.281>.
- [16] M. M. Suarez, "Knowledge Management Practices, Employee Work Engagement and Balanced Scorecard: Basis for Organizational Performance Framework," *International Journal of Research Studies in Management* 11, no. 5 (2023): 23–38, <https://doi.org/10.5861/ijrsm.2023.1050>.
- [17] M. I. Pramanik, P. Ghose, M. D. Hossen, M. H. Ahmed, M. M. Rahman, and M. R. Bhuiyan, "Emerging Technological Trends in Financial Crime and Money Laundering: A Bibliometric Analysis of Cryptocurrency's Role and Global Research Collaboration," *Journal of Posthumanism* 5, no. 6 (2025): 3611–3633, <https://doi.org/10.63332/joph.v5i6.2493>.
- [18] E. Ceko, "Cyber Security Issues in Albanian Higher Education Institutions Curricula," *CRJ. CIT Review-Journal* 1, no. 1 (2023): 56–65, <https://doi.org/10.59380/crj.v1i1.2728>.
- [19] B. Almekhled and H. Petrie, "UK Students' Concerns About Security and Privacy of Online Higher Education Digital Technologies in the Coronavirus Pandemic," *Proceedings of the 15th International Conference on Computer Supported Education* 2 (2023): 483–492, <https://doi.org/10.5220/0011993500003470>.
- [20] J. Rajamäki, P. Rathod, and K. Kioskli, "Demand Analysis of the Cybersecurity Knowledge Areas and Skills for the Nurses: Preliminary Findings," *European Conference on Cyber Warfare and Security* 22, no. 1 (2023): 711–716, <https://doi.org/10.34190/eccws.22.1.1181>.
- [21] L. Brotcke, "Minimise Model Risk Management Oversight for Cyber Security Solutions," *Journal of AI, Robotics & Workplace Automation* 3, no. 1 (2023): 55–63, <https://doi.org/10.69554/xfxm3841>.
- [22] A. Qusef and H. Alkilani, "The Effect of ISO/IEC 27001 Standard Over Open-Source Intelligence," *Peer J Computer Science* 8 (2022): e810, <https://doi.org/10.7717/peerj-cs.810>.
- [23] N.-A. Perifanis and F. Kitsios, "Investigating the Influence of Artificial Intelligence on Business Value in the Digital Era of Strategy: A Literature Review," *Information* 14, no. 2 (2023): 85, <https://doi.org/10.3390/info14020085>.
- [24] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure," *Applied Sciences* 11, no. 10 (2021): 4580, <https://doi.org/10.3390/app11104580>.
- [25] M. M. Rahman, M. M. Islam, M. Khatun, S. Uddin, M. R. Faraji, and M. H. Hasan, "Gravitating Towards Information Society for Information Security in Information Systems: A Systematic PRISMA Based Review," *Pakistan Journal of Life and Social Sciences (PJLSS)* 22, no. 1 (2024): <https://doi.org/10.57239/PJLSS-2024-22.1.0089>.
- [26] A. Jalilvand and S. Moorthy, "Enterprise Risk Management Maturity: A Clinical Study of a U.S. Multinational Nonprofit Firm," *Journal of Accounting, Auditing & Finance* 39, no. 3 (2024): 883–902, <https://doi.org/10.1177/0148558X221097754>.
- [27] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber Security: State of the Art, Challenges and Future Directions," *Cyber Security and Applications* 2 (2024): 100031, <https://doi.org/10.1016/j.csa.2023.100031>.
- [28] A. Al Hayajneh, H. N. Thakur, and K. Thakur, "The Evolution of Information Security Strategies: A Comprehensive Investigation of INFOSEC Risk Assessment in the Contemporary Information Era," *Computer and Information Science* 16, no. 4 (2023): 1–20, <https://doi.org/10.5539/cis.v16n4p1>.
- [29] A. Calder and S. Watkins, *IT Governance—An International Guide to Data Security and ISO 27001/ISO 27002* (IT Governance Publishing, 8th edition, 2024), <https://doi.org/10.2307/jj.9039966>.
- [30] U. K. Kanike, "Factors Disrupting Supply Chain Management in Manufacturing Industries," *Journal of Supply Chain Management Science* 4, no. 1-2 (2023): 1–24, <https://doi.org/10.18757/jscms.2023.6986>.
- [31] O. O. Olaniyi, O. O. Omogoroye, F. G. Olaniyi, A. I. Alao, and T. O. Oladoyinbo, "CyberFusion Protocols: Strategic

- Integration of Enterprise Risk Management, ISO 27001, and Mobile Forensics for Advanced Digital Security in the Modern Business Ecosystem,” *Journal of Engineering Research and Reports* 26, no. 6 (2024): 31–49, <https://doi.org/10.9734/jerr/2024/v26i61160>.
- [32] A. AL-Hawamleh, “Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security,” *International Journal of Computing and Digital Systems* 15, no. 1 (2024): 1315–1331, <https://doi.org/10.12785/ijcds/150193>.
- [33] H. Heyasat, S. Mubarak, and N. Evans, “Security Culture and Security Education, Training and Awareness (SETA) Influencing Information Security Management,” in *Proceedings of the Second International Conference on Innovations in Computing Research (ICR'23)* (Springer, 2023), 332–343, https://doi.org/10.1007/978-3-031-35308-6_28.
- [34] T. O. Ojewumi, G. O. Ogunleye, B. O. Oguntunde, O. Folorunsho, S. G. Fashoto, and N. Ogbu, “Performance Evaluation of Machine Learning Tools for Detection of Phishing Attacks on Web Pages,” *Scientific African* 16 (2022): e01165, <https://doi.org/10.1016/j.sciaf.2022.e01165>.
- [35] P. O'Brien and D. Murray, “Training and Operations Synergies Leads to Marked Individual and Crew Performance Improvements,” in *Proceedings of the Conference on Nuclear Training and Education: A Biennial International Forum (CONTE 2023)* (American Nuclear Society, 2023), 40–41, <https://doi.org/10.13182/conte23-40474>.
- [36] J. Kyriazoglou, “Managing Information Security Incidents,” in *Information Security Incident and Data Breach Management: A Step-by-Step Approach* (Apress, 2024), 37–47, https://doi.org/10.1007/979-8-8688-0870-8_4.
- [37] Y. Ernawati and G. Wang, “Assessing IT Services Management With ITIL Framework V3: A Case Study,” *Journal of System and Management Sciences* 13, no. 14 (2023): 152–164, <https://doi.org/10.33168/jsms.2023.0409>.
- [38] T. Roskó and G. J. Szöllösi, “Behind Passwords: An Analysis of Preliminary Results in Order to Understand How Users Protect their Privacy,” *First Monday* 26, no. 8 (2021): <https://doi.org/10.5210/fm.v26i8.10616>.
- [39] V. Makkada and I. Rai, “Capital One Data Breach,” in *Information Technology Security and Risk Management* (CRC Press, 2024), 330, <https://doi.org/10.1201/9781003264415-6>.
- [40] R. Kumar and D. Tiwari, “Network Security and Cryptography: Ensuring Data Integrity and Confidentiality in the Digital Age,” *International Journal of Research Publication and Reviews* 5, no. 7 (2024): 581–586, <https://doi.org/10.55248/gengpi.5.0724.1621>.
- [41] T. Gundu and N. Modiba, “Building Competitive Advantage From Ubuntu: An African Information Security Awareness Model,” in *Proceedings of the 6th International Conference on Information Systems Security and Privacy* (SCITEPRESS, 2020), 569–576, <https://doi.org/10.5220/0008983305690576>.
- [42] O. Fagbule, 2023, Cyber security training in small to medium-sized enterprises (SMEs): Exploring organisation culture and employee training needs (Doctoral dissertation, Bournemouth University). Bournemouth University Eprints. <https://eprints.bournemouth.ac.uk/39148/>.
- [43] P. Ghose, M. R. I. Bhuiyan, M. N. Hasan, S. H. Rakib, and L. Mani, “Mediated and Moderating Variables Between Behavioral Intentions and Actual Usages of Fintech in the USA and Bangladesh Through the Extended UTAUT Model,” *International Journal of Innovative Research and Scientific Studies* 8, no. 2 (2025): 113–125, <https://doi.org/10.53894/ijirss.v8i2.5130>.
- [44] A. Habbal, M. K. Ali, and M. A. Abuzaraida, “Artificial Intelligence Trust, Risk and Security Management (AI Trism): Frameworks, Applications, Challenges and Future Research Directions,” *Expert Systems with Applications* 240 (2024): 122442, <https://doi.org/10.1016/j.eswa.2023.122442>.
- [45] N. Haug, S. Dan, and I. Mergel, “Digitally-Induced Change in the Public Sector: A Systematic Review and Research Agenda,” *Public Management Review* 26, no. 7 (2024): 1963–1987, <https://doi.org/10.1080/14719037.2023.2234917>.
- [46] A. Polisetty, D. Chakraborty, A. K. Kar, and S. Pahari, “What Determines AI Adoption in Companies? Mixed-Method Evidence,” *Journal of Computer Information Systems* 64, no. 3 (2024): 370–387, <https://doi.org/10.1080/08874417.2023.2219668>.
- [47] J. O. Oladipo, C. C. Okoye, O. A. Elufioye, T. Falaiye, and E. E. Nwankwo, “Human Factors in Cybersecurity: Navigating the Fintech Landscape,” *International Journal of Science and Research Archive* 11, no. 1 (2024): 1959–1967, <https://doi.org/10.30574/ijrsra.2024.11.1.0258>.
- [48] M. R. I. Bhuiyan, R. Hossain, M. Rashid, M. M. Islam, L. Mani, and M. N. U. Milon, “Gravitating the Components, Technologies, Challenges, and Government Transforming Strategies for a Smart Bangladesh: A PRISMA-Based Review,” *Journal of Governance and Regulation* 13, no. 3 (2024): 177–188, <https://doi.org/10.22495/jgrv13i3art15>.
- [49] R. Hossain, A.-A. Al-Amin, L. Mani, M. M. Islam, T. A. Poli, and M. N. U. Milon, “Exploring the Effectiveness of Social Media on Tourism Destination Marketing: An Empirical Study in a Developing Country,” *WSEAS Transactions on Business and Economics* 21 (2024): 1392–1408, <https://doi.org/10.37394/23207.2024.21.114>.
- [50] M. R. I. Bhuiyan, M. S. Akter, A. Amin, and R. Hossain, “The Mediating Effect of Innovation Capabilities, Information Quality and Supply Chain Resilience in the Relationship Between Big Data Analytics Capability (BDAC) and Healthcare Performance,” *SAGE Open* 15, no. 3 (2025): 21582440251362262, <https://doi.org/10.1177/21582440251362262>.
- [51] K. Peng, J. Shi, and Y. Qiao, “Application of Blockchain Equity System for Machine Learning and Network Security,” in *Proceedings of the 2024 9th International Conference on Cyber Security and Information Engineering* (Association for Computing Machinery, 2024), 277–286, <https://doi.org/10.1145/3689236.3696749>.
- [52] F. Afsari and M. Ahmadi Jirdehi, “Smart Grid Optimization Considering Decentralized Power Distribution and Demand Side Management,” *IET Generation, Transmission & Distribution* 18, no. 8 (2024): 1663–1671, <https://doi.org/10.1049/gtd2.13150>.
- [53] Z. Musostov, A. Berkaeva, and I. Basnukaev, “New Technologies in Production,” in *Proceedings of the 1st International Conference on Methods, Models, Technologies for Sustainable Development* (SCITEPRESS, 2023), 244–247, <https://doi.org/10.5220/0011569300003524>.
- [54] A. Amin, M. R. I. Bhuiyan, R. Hossain, C. Molla, T. A. Poli, and M. N. U. Milon, “The Adoption of Industry 4.0 Technologies by Using the Technology Organizational Environment Framework: The Mediating Role to Manufacturing Performance in a Developing Country,” *Business Strategy & Development* 7, no. 2 (2024): e363, <https://doi.org/10.1002/bsd2.363>.
- [55] T. Sendjaja, Irwandi, E. Prastiawan, Y. Suryani, and E. Fatmawati, “Cybersecurity in the Digital Age: Developing

- Robust Strategies to Protect Against Evolving Global Digital Threats and Cyber Attacks,” *International Journal of Science and Society* 6, no. 1 (2024): 1008–1019, <https://doi.org/10.54783/ijssoc.v6i1.1098>.
- [56] V. Sethi, A. Katal, and S. Dabas, “Cloud and Edge Computing Architectures for Future Cloud Computing,” in *Future Connected Technologies* (CRC Press, 2023), 141–161, <https://doi.org/10.1201/9781003287612-7>.
- [57] A. R. Larik, R. Rai, K. Ahmed, and H. Mustafa, “Integration of Solar Energy Into Smart Grids: A Cost-Effective Framework for Sustainable Power Management,” *International Journal of Economic and Environmental Geology* 15, no. 2 (2024): 26–31, <https://doi.org/10.46660/ijeeg.v15i2.309>.
- [58] I. D. Turgel and O. A. Chernova, “Open Bibliographic Databases: In Search of an Alternative to Scopus and the Web of Science,” *Economics of Science* 10, no. 3 (2024): 34–51, <https://doi.org/10.22394/2410-132x-2024-10-3-34-51>.
- [59] Z. Ding and Q. Xie, “Provably Secure and Lightweight Three-Factor Authentication Scheme for Industrial Medical CPS,” *Journal of Information Security and Applications* 79 (2023): 103656, <https://doi.org/10.1016/j.jisa.2023.103656>.
- [60] H. Kim, K. Oh, and D. Lee, “Establishment of a Geographic Information System-Based Algorithm to Analyze Suitable Locations for Green Roofs and Roadside Trees,” *Applied Sciences* 11, no. 16 (2021): 7368, <https://doi.org/10.3390/app11167368>.
- [61] W. Shafik, S. M. Matinkhah, and F. Shokoor, “Cybersecurity in Unmanned Aerial Vehicles: A Review,” *International Journal on Smart Sensing and Intelligent Systems* 16, no. 1 (2023): 1–16, <https://doi.org/10.2478/ijssis-2023-0012>.
- [62] M. Platt and P. McBurney, “Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance,” *Algorithms* 16, no. 1 (2023): 34, <https://doi.org/10.3390/a16010034>.