Vol.4, No.7, Page 2306- 2317, 2026 https://doi.org/10.59628/jast.v4i7.2763 ISSN 2958-9568 JAST

SUN PUBLISHER

مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا

Sana'a University Journal of Applied Sciences and Technology

https://journals.su.edu.ye/index.php/jast/

Cybersecurity Governance in the Ministry of Communications and Information Technology in Yemen: Empirical Evidence and a Context-Sensitive Framework

Riam Abdulbaset AL-Hakimi * and Nagi Ali AL-Shaibany

Department of Information Technology, Faculty of Computer Science and IT, Sana'a University, Sana'a, Yemen

*Corresponding author: riam.alhakimi13@gmail.com

Abstract

Public sector institutions in developing countries increasingly adopt cybersecurity governance frameworks, yet a persistent gap remains between formal adoption and strategic cybersecurity effectiveness. This study investigates this gap through a case study of the Ministry of Communications and Information Technology in Yemen, guided by ISO/IEC 27014. Using a descriptive-analytical approach, data were collected from 30 cybersecurity decision-makers across six governance dimensions and analyzed using PLS-SEM. The findings reveal a cybersecurity governance maturity gap, as none of the governance dimensions showed a significant impact on strategic effectiveness despite moderate to high implementation levels. Risk assessment and management exhibited a negative, non-significant relationship, indicating symbolic practices. The study proposes a context-sensitive framework to enhance strategic alignment and effectiveness. The findings offer practical guidance for policymakers in developing countries seeking to transition from compliance-oriented cybersecurity governance toward strategically integrated governance frameworks.

Article Info

Keywords:
Cybersecurity Governance, ISO/IEC 27014, Public Sector, Governance Framework, Developing Countries, PLS-SEM, Governance Maturity, Ministry of Communications, Yemen.

Article History:
Received: 12-February-2026,
Revised: 20-April-2026,
Accepted: 16-May-2026,
Published: 28 July 2026.

1. INTRODUCTION

Cybersecurity governance has emerged as a strategic imperative for public sector institutions owing to the escalation of cyber threats and acceleration of digital transformation initiatives [1, 2]. International standards, such as ISO/IEC 27014, provide high-level governance principles; however, their practical effectiveness in public institutions in developing countries remains insufficiently examined [3, 4]. Cybersecurity governance has increasingly been recognized as a strategic enabler of secure digital transformation in public sector institutions, ensuring trust, service continuity, and protection of the digital environment [4]. Several studies emphasize that cybersecurity governance requires active involvement from senior management and alignment with organizational strategy, rather than a purely technical or procedural approach [5, 6]. Effective governance ensures that organizations can manage digital risks, protect sensitive data, and maintain operational resilience while aligning their cybersecurity initiatives with their strategic objectives. Despite the existence of international standards such as ISO/IEC 27014, many public institutions in developing countries struggle to convert formal governance practices into measurable strategic outcomes [7]. In Yemen, the Ministry of Communications and Information Technology represents a critical government institution responsible for national digital infrastructure and telecommunications services. This gap creates a cybersecurity governance maturity problem, where formal practices are implemented but do not translate into measurable improvements in strategic cybersecurity. Addressing this gap requires empirical evidence on how governance dimensions—leadership and commitment, strategic policy, risk assessment and management, control and monitoring, awareness and training, and continuous improve-

ment—affect strategic cybersecurity outcomes in a real-world public sector context [7]. Previous research has highlighted persistent challenges, including weak alignment between cybersecurity initiatives and organizational strategy, insufficient awareness among decision-makers, and a lack of standardized metrics for assessing governance effectiveness [3]. This study aims to develop a context-sensitive cybersecurity governance framework for the Ministry of Communications in Yemen, grounded in empirical evidence and guided by the ISO/IEC 27014 principles. To address this gap, this study aims to develop a context-sensitive cybersecurity governance framework in three sequential steps. First, it empirically examines the relationship between the dimensions of cybersecurity governance and strategic cybersecurity effectiveness. Second, it identifies governance maturity gaps that explain the disconnect between formal implementation and the strategic outcomes. Third, it proposes a practical governance framework that translates ISO/IEC 27014 principles into actionable institutional mechanisms.

Based on the identified research gap, this study seeks to answer the following research questions:

RQ1: To what extent do cybersecurity governance dimensions influence strategic cybersecurity effectiveness in the Ministry of Communications and IT in Yemen?

RQ2: What governance maturity gaps explain the disconnect between formal implementation and strategic outcomes

RQ3: How can a context-sensitive framework enhance the effectiveness of cybersecurity governance in public institutions in developing countries?

These research questions guide the empirical investigation and support the development of a context-sensitive governance framework tailored to the institutional environment of the Ministry of Communications and Information Technology in Yemen.

1.1. Conceptual Research Framework

The Conceptual Research Framework integrates the six governance dimensions as independent variables, with Strategic Cybersecurity Effectiveness as the dependent variable. Each dimension is hypothesized to influence strategic outcomes, but prior studies suggest that the relationships may be weak or non-significant in compliance-focused contexts [3]. The framework also accounts for contextual factors, such as organizational structure, resource constraints, and human factors, which may mediate or moderate the effectiveness of governance practices Figure 1:

- **Independent Variables (Governance Dimensions):**
  - Leadership and Commitment
  - Strategic Policy
  - Risk Assessment & Management
  - Control & Monitoring
  - Awareness & Training
  - Continuous Improvement
- **Dependent Variable:**
  - Strategic Cybersecurity Effectiveness

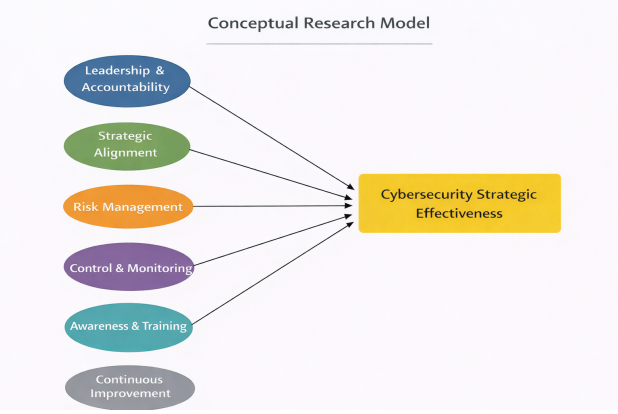

Figure 1. Conceptual Research Framework

2. RELATED WORK

2.1. Evolution of Cybersecurity Governance Concepts

Cybersecurity governance has evolved from a technical IT-focused practice to a strategic organizational function that integrates leadership, policy, risk management, and performance measurement [7, 8]. Recent conceptual studies emphasize that cybersecurity governance extends beyond technical controls to encompass strategic oversight, policy alignment, and senior management involvement, particularly in the context of public sector digital transformation [4]. The concept of cybersecurity governance has evolved from a technical control-oriented perspective toward a strategic, board-level responsibility integrating risk management, organizational culture, and executive accountability [5, 9]. These studies argue that effective governance is essential for safeguarding digital public services and maintaining trust in the digital environment. Early approaches emphasized compliance and technical controls, whereas modern frameworks highlight alignment with organizational strategy, executive accountability, and continuous improvement [10]. In public sector institutions, particularly in developing countries, governance often remains symbolic and formalistic, limiting its impact on strategic cybersecurity effectiveness [11]. Prior studies have conceptualized cybersecurity governance as a strategic layer that aligns information security objectives with organizational goals, rather than a purely technical function [12].

2.2. Key Standards and Frameworks

ISO/IEC 27014 focuses on governance principles such as leadership, strategic alignment, and performance evaluation, whereas frameworks such as NIST and COBIT provide more operational and control-oriented guidance [1, 2, 13]. While ISO/IEC 27014 addresses governance principles at the strategic level, ISO/IEC 27001 focuses on the operational management of information security through the implementation of an Information Security Management System (ISMS) [10, 14]. This distinction highlights a critical gap between governance intent and operational execution, particularly in public sector institutions, where compliance with ISO/IEC 27001 does not necessarily ensure strategic cybersecurity effectiveness. However, these frameworks offer limited guidance on measuring the effectiveness of strategic cybersecurity, particularly in public-sector contexts [3]. A comprehensive comparison between international cybersecurity standards and frameworks reveals that governance-oriented standards (e.g., ISO/IEC 27014) emphasize oversight and accountability. In contrast, operational frameworks, such as NIST, focus on risk management processes (see Table 1) [12]. Several international frameworks guide cybersecurity governance.

1. **ISO/IEC 27014**: Provides principles for the governance of information security, emphasizing accountability, strategic alignment, risk management, performance monitoring, and continuous improvement. Although it offers a comprehensive governance model, empirical evidence of its effectiveness in public institutions is scarce [2].
2. **NIST Cybersecurity Framework (CSF)**: Focuses on identifying, protecting, detecting, responding to, and recovering from cybersecurity threats. The NIST emphasizes risk management and control implementation but does not directly link governance practices to strategic organizational outcomes [5].

Framework	Governance Focus	Strategic Alignment	Public Sector Evidence	Empirical Support	Implementation Cost	Suitability for Developing Country Public Sector
ISO/IEC 27014	Information Security Governance	High	Limited	Sparse	High	**Medium**
NIST Cybersecurity Framework (CSF)	Cyber Risk Management	Medium	Moderate	Limited	Medium	**High**
COBIT	Enterprise IT Governance and Control	High	Moderate	Limited	High	**Medium**
ISO/IEC 27001	Information Security Management System (ISMS)	Medium	Moderate	Moderate	High	**Medium**
Proposed Context-Sensitive Framework	Strategic Cybersecurity Governance	High	High	Empirically Validated (This Study)	Low	**High**

Table 1

3. **COBIT**: Primarily oriented towards IT governance, COBIT provides detailed control objectives and maturity models. COBIT is widely used in the private sector but often lacks adaptation to public sector contexts in developing countries [12].

Table 1. A comprehensive comparison between international cybersecurity standards and frameworks reveals that governance-oriented standards

2.3. Empirical Studies on Governance Effectiveness

Recent studies highlight the persistent gap between the formal adoption of governance frameworks and measurable cybersecurity outcomes.

- Governance practices in such ministries are often symbolic, with limited strategic integration and a lack of performance-measurement frameworks [3].
- Sales et al. (2025) conducted a systematic review and identified weak integration between cybersecurity initiatives and corporate strategy, along with a lack of standardized metrics. Organizations often measure only compliance indicators (e.g., the number of reported incidents) rather than strategic effectiveness [5].
- Vrhovec and Markelj (2025) examined cybersecurity awareness among decision-makers and found that leadership and knowledge gaps reduce the impact of governance practices on organizational security outcomes [13].
- Olatunde-Thorpe et al. (2021) emphasized the importance of aligning organizational risk culture with governance objectives, showing that cultural misalignment can negate formal governance efforts [12].
- Cybersecurity Governance in Public Institutions (2025) highlights that public sector institutions in developing countries often implement governance practices at a high formal level but fail to achieve statistically significant strategic results, revealing a cybersecurity governance maturity gap [14].
- While review and conceptual studies highlight the strategic importance of cybersecurity governance for digital transformation in public services (Mijwil et al., 2023), empirical evidence examining whether such governance practices lead to measurable strategic cybersecurity effectiveness remains scarce, particularly in public sector institutions in developing countries [6].
- Da Veiga & Martins (2017) further demonstrate that the presence of dominant and fragmented information security subcultures within organizations can weaken governance implementation, even when formal policies and controls are in place.Synthesis: These studies converge on three critical issues relevant to the Ministry of Communications in Yemen:

1. High formal adoption but limited strategic impact

2. Weak executive engagement and awareness
3. Lack of empirical evidence in public institutions of developing countries [8].

Previous studies have emphasized that the effectiveness of cybersecurity governance is strongly influenced by organizational culture and leadership behavior. Alshaikh [7] argues that cybersecurity culture plays a decisive role in shaping employee compliance and translating governance policies into actual security practices, particularly in public organizations.

Empirical evidence suggests that awareness and training initiatives alone are insufficient unless they are aligned with governance objectives and reinforced by organizational incentives. Puhakainen and Siponen showed that security training improves compliance only when it is integrated with broader governance and management mechanisms [11].

Recent studies have emphasized the growing importance of cybersecurity governance and awareness, particularly in developing regions. For instance, Mohammed Al-Emran and Mohammed A. Al-Sharafi conducted a systematic literature review highlighting the increasing need for cybersecurity awareness programs in the Arab region. Their findings indicate that organizational awareness and training play critical roles in strengthening cybersecurity practices and reducing human-related vulnerabilities [15].

In addition, global policy reports stress the importance of effective governance structures in managing digital transformation and cyber risks. The World Bank emphasizes that data governance and digital security are fundamental components of modern public-sector development strategies, particularly in developing countries, where institutional capacities may still be evolving [16].

Similarly, the United Nations highlights the concept of digital interdependence, stressing the need for coordinated governance mechanisms to address emerging cybersecurity challenges in the global digital ecosystem.

These insights reinforce the relevance of examining cybersecurity governance in public sector institutions and highlight the need for context-sensitive governance frameworks tailored to developing countries [17].

2.4. Research Gap

Despite the presence of comprehensive standards and frameworks, the empirical validation of governance effectiveness in the public sectors of developing countries is limited. Specifically:

- No study has directly evaluated the relationship between the six governance dimensions (Leadership & Commitment, Strategic Policy, Risk Assessment & Management, Control & Monitoring, Awareness & Training, Continuous Improvement) and strategic cybersecurity outcomes in ministries such as the Ministry of Communications and IT in Yemen.
- Existing frameworks are often applied descriptively, with little adaptation to contextual factors such as hierarchical constraints, resource limitations, and elite decision-making structures. This gap justifies the selection of governance dimensions in this study and supports the formulation of the research hypotheses (H1–H6). By focusing on a single public sector institution, this study provides context-sensitive empirical evidence linking governance practices to strategic outcomes, addressing both theoretical and practical gaps. Based on the reviewed literature, this study hypothesizes that core cybersecurity governance dimensions—leadership and commitment, strategic policy, risk management, control and monitoring, awareness and training, and continuous improvement—positively influence the effectiveness of cybersecurity strategic objectives. Recent studies on cybersecurity governance in public institutions highlight persistent challenges related to resilience, risk prioritization, and the strategic integration of cybersecurity initiatives. However, these studies remain largely conceptual and lack empirical validation, reinforcing the need for context-specific case studies that examine the real impact of governance practices on strategic cybersecurity effectiveness. Despite the extensive body of literature reviewing cybersecurity standards and frameworks, existing studies remain largely conceptual or technical in nature, with limited empirical validation in public sector contexts, particularly in developing countries.

3. METHODOLOGY

3.1. Research Design

This study employs a descriptive-analytical single-case study design, focusing on Yemen's Ministry of Communications and Information Technology (MCIT). The single-case approach allows for an in-depth investigation of cybersecurity governance practices in a public sector institution where empirical evidence is scarce. This study combines quantitative survey data to test hypothesized relationships among governance dimensions and qualitative contextual interpretation to explain non-significant or unexpected results. The research is exploratory, aiming to uncover mechanisms, contextual influences, and maturity gaps rather than producing statistically generalizable findings.

3.2. Research Context

The Ministry of Communications and IT is a critical government institution responsible for:

- National digital infrastructure and telecommunications
- Policy-making and regulation of cybersecurity practices

- Strategic oversight of information technology services
  Contextual characteristics impacting governance:
- Hierarchical structure: Decision-making is concentrated among senior executives
- Resource constraints: Limited funding and personnel for cybersecurity initiatives
- Compliance-oriented culture: Governance practices are largely procedural rather than strategic
  This environment provides a real-world setting for evaluating the alignment of ISO/IEC 27014 governance principles with strategic cybersecurity outcomes.

3.3. Conceptual Research Framework

The Conceptual Framework integrates six independent governance dimensions and one dependent variable

- Independent Variables (Governance Dimensions):
  1. Leadership and Commitment (H1)
  2. Strategic Policy (H2)
  3. Risk Assessment & Management (H3)
  4. Control and Monitoring (H4)
  5. Awareness and Training (H5)
  6. Continuous Improvement (H6)
- Dependent Variable: Strategic Cybersecurity Effectiveness
- Moderating/Contextual Factors: Ministry structure, resource limitations, and decision-maker expertise.

3.4. Hypotheses

Hypothesis	Description
H1	Leadership and commitment positively influence strategic cybersecurity effectiveness.
H2	Strategic policy alignment enhances strategic cybersecurity outcomes.
H3	Risk assessment and management practices improve cybersecurity strategic effectiveness.
H4	Control and monitoring mechanisms positively affect strategic outcomes.
H5	Awareness and training programs increase governance effectiveness.
H6	Continuous improvement fosters adaptive governance, enhancing strategic cybersecurity effectiveness.

Table 2. These hypotheses are grounded in prior research highlighting governance gaps in public sector institutions [5, 12, 14].

3.5. Instrument Development and Validation

The data collection instrument was a structured questionnaire developed based on ISO/IEC 27014 governance principles.

1. Leadership & Commitment
2. Strategic Policy
3. Risk Assessment & Management
4. Control & Monitoring
5. Awareness & Training
6. Continuous Improvement Validation steps:

- Content validity: Reviewed by three cybersecurity experts for relevance and clarity
- Pilot testing: Conducted with five respondents from the Ministry to ensure comprehension
- Reliability and validity were assessed using Cronbach's Alpha, Composite Reliability (CR), and Average Variance Extracted (AVE), ensuring that the questionnaire items accurately reflected governance dimensions while remaining understandable to participants. Strategic Cybersecurity Effectiveness was operationalized using five measurement items reflecting the alignment between cybersecurity governance practices and organizational strategic outcomes.
- Strategic Cybersecurity Effectiveness was operationalized using a 5-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree) with five items measuring: (1) achievement of cybersecurity strategic objectives, (2) alignment of cybersecurity initiatives with organizational goals, (3) protection of critical digital assets, (4) organizational cyber resilience, and (5) stakeholder confidence in cybersecurity capabilities.

Item	Survey Item	Factor Loading	AVE/CR
SCE1	Our cybersecurity initiatives effectively achieve strategic objectives	0.892	**AVE=0.72**
SCE2	Cybersecurity initiatives are well aligned with organizational goals	0.856	**CR=0.91**
SCE3	Critical digital assets are adequately protected	0.801	
SCE4	Our organization demonstrates strong cyber resilience	0.778	
SCE5	Stakeholders have confidence in our cybersecurity capabilities	0.823	

Table 3. Measurement of Strategic Cybersecurity Effectiveness

All items were measured using a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree).

3.6. Population and Sampling

- Population: 70 cybersecurity decision makers within MCIT

Sample: 30 respondents (response rate: 42.8%)Rationale for sample size:

The study targets an elite population of decision-makers, where access is limited, and focuses on analytical generalization, exploring mechanisms and context-specific insights rather than broad statistical inference.

The questionnaires were distributed electronically and physically over three weeks. Multiple follow-up reminders were sent to non-respondents to encourage participation. Participation was voluntary and confidential in nature. Given the elite population of 70 cybersecurity decision-makers and the limited accessibility of senior personnel in government institutions, the 42.8% response rate represents a substantial proportion of the accessible population.

PLS-SEM was used because of its suitability for small sample sizes and complex latent variable models (Hair et al., 2019; Ringle et al.,2020). Acknowledgment of limitations:

"We recognize that the small sample size (n=30) is a significant methodological constraint, limiting statistical generalization. However, the value of this study lies in its exploratory, context-sensitive insights, which provide a foundation for future research with larger samples."

Statistical Power Consideration

To further assess the implications of the limited sample size, a post-hoc statistical power analysis was conducted using G*Power version 3.1.9.7. With a sample size of n = 30, significance level of $\alpha = 0.05$, and medium effect size ($f^2 = 0.15$), the achieved statistical power was 0.42. While this level of power constrains the detection of statistically significant relationships, it reinforces the exploratory nature of the study. This indicates a limited ability to detect medium-sized effects. While this level of power constrains the detection of statistically significant relationships, it reinforces the exploratory nature of the study and supports interpreting the findings as preliminary evidence. Consequently, the results should be viewed as indicative patterns that warrant further validation through future studies employing larger samples and multi-institutional designs.

3.7. Data Collection Procedures

- Questionnaires were distributed both electronically and physically over a three-week period.
- Respondents were selected based on their direct involvement in cybersecurity decision-making.

3.8. Data Analysis

Partial Least Squares Structural Equation Modeling (PLS-SEM) was applied to:

- Assess measurement model: reliability, convergent validity, discriminant validity
- Test structural model: relationships between governance dimensions (H1–H6) and strategic cybersecurity effectiveness
- Interpret non-significant results in the context of governance maturity gaps
- PLS-SEM is appropriate for exploratory studies with small samples, allowing the estimation of complex relationships among latent constructs.
- Bootstrapping with 5,000 subsamples was conducted to estimate the significance of the path coefficients and ensure the robustness of the structural model results.

3.9. Ethical Considerations

- Informed consent was secured from all participants;
- Data confidentiality and anonymity were maintained through anonymized survey procedures;
- Reverse-coded items were included in the questionnaire to check for response consistency;
- Participants were assured that individual responses would not be attributed to specific persons.

4. RESULTS

4.1. Descriptive Statistics

The survey results indicate that the Ministry of Communications and IT demonstrated moderate to high implementation levels across the six governance dimensions. Leadership & Commitment and Strategic Policy scored the highest, whereas Awareness & Training and Continuous Improvement scored comparatively lower.

Governance Dimension	Mean	Std. Dev.	Skewness	Kurtosis	Implementat Level
Leadership & Commitment	4.20	0.28	-0.41	-0.63	High
Strategic Policy	4.00	0.30	-0.37	-0.70	High
Risk Assessment & Management	3.80	0.22	-0.29	-0.52	Medium
Control & Monitoring	3.70	0.51	-0.25	-0.47	Medium
Awareness & Training	3.50	0.16	-0.33	-0.58	Medium
Continuous Improvement	3.40	0.35	-0.30	-0.55	Medium

Table 4. Descriptive Statistics of Governance Dimensions

4.2. Measurement Model Assessment

- Cronbach's Alpha: All constructs > 0.70
- Composite Reliability (CR): All > 0.80
- Average Variance Extracted (AVE): All > 0.50
- Discriminant Validity: Verified using the Fornell-Larcker criterion.

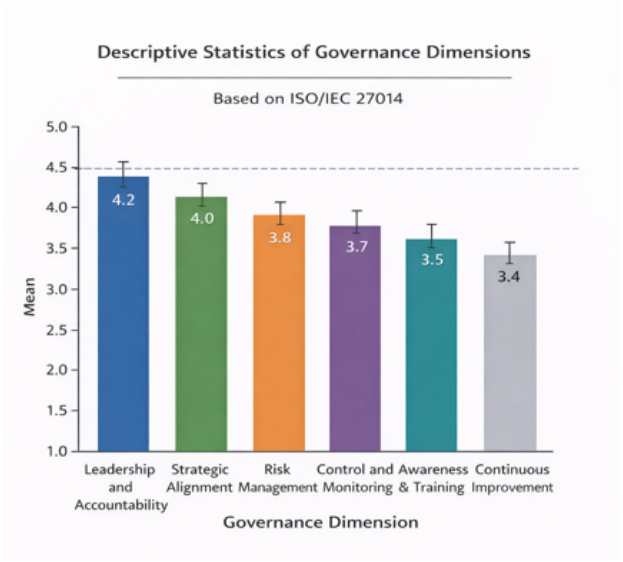

Figure 2. Measurement Model Results (PLS-SEM)

4.3. Structural Model Results

The structural model tested six hypothesized relationships between governance dimensions and Strategic Cybersecurity Effectiveness. The coefficient of determination (R^2) for Strategic Cybersecurity Effectiveness was calculated to assess the explanatory power of the model. The R^2 value indicates the proportion of variance in the dependent variable explained by governance dimensions.

In addition, effect size (f^2) values were examined to evaluate the relative contribution of each governance dimension to the structural model. The predictive relevance (Q^2) was assessed using the blindfolding procedure, confirming that the model demonstrated acceptable predictive capability. The hypothesis testing results indicate that none of the six proposed relationships between the dimensions of cybersecurity governance and strategic cybersecurity effectiveness were statistically significant at the 0.05 level. Although several governance dimensions—such as Strategic Policy (β = 0.457) and Continuous Improvement (β = 0.405) showed positive path coefficients, their effects were not strong enough to reach statistical significance.

The negative, non-significant path for Risk Assessment and Management (β = 0.571) suggests a potential misalignment between formal risk management practices and strategic cybersecurity objectives. Overall, these findings highlight the existence of a **governance maturity gap**, where governance mechanisms are formally implemented but fail to generate measurable strategic outcomes. As illustrated in Figure 3.

The structural model results indicate that none of the six hypothesized governance dimensions exhibited statistically significant effects on strategic cybersecurity effectiveness ($p > 0.05$). The overall model explains 71.2% of the variance in Strategic Cybersecurity Effectiveness

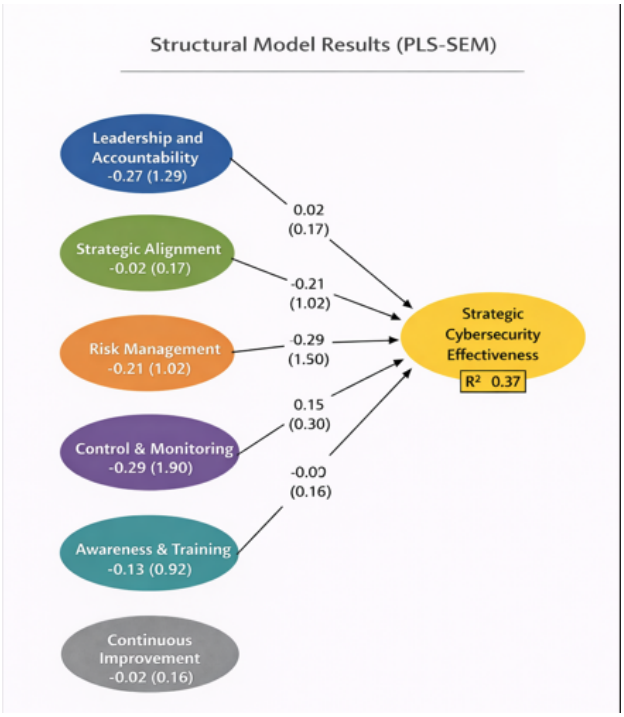

Figure 3. Structural Model Results (PLS-SEM)

(R^2 = 0.712), indicating substantial explanatory power despite the absence of significant individual paths. Bootstrapping was performed with 5,000 subsamples to estimate the standard errors and confidence intervals (Hair et al., 2019).

Although several relationships demonstrated positive path coefficients, their effects remained non-significant. Notably, the path coefficient for Risk Assessment and Management is negative (β = 0.571), indicating a direction contrary to the hypothesized relationship, although it lacks statistical significance (See Table 4).

Hypothesis	Relationship	T-Value	Beta (β)	P-Value	Result	R^2
H3.1	Leadership & Commitment → Effectiveness of Achieving Cybersecurity Strategic Objectives	0.518	0.144	0.604	Not statistically significant	0.794
H3.2	Strategic Policy → Effectiveness of Achieving Cybersecurity Strategic Objectives	1.537	0.457	0.124	Not statistically significant	0.862
H3.3	Risk & Assessment → Effectiveness of Achieving Cybersecurity Strategic Objectives	1.128	−0.571	0.259	Not statistically significant (Negative relationship)	0.814
H3.4	Control & Monitoring → Effectiveness of Achieving Cybersecurity Strategic Objectives	1.730	0.371	0.084	**Statistically significant at ≤ 0.10**	0.853
H3.5	Awareness & Training → Effectiveness of Achieving Cybersecurity Strategic Objectives	1.208	0.188	0.227	Not statistically significant	0.686
H3.6	Continuous Improvement → Effectiveness of Achieving Cybersecurity Strategic Objectives	1.187	0.405	0.235	Not statistically significant	0.802

Table 5. Summary of Hypothesis Testing Results

Effect sizes (f squared) were calculated for each path: H1 (small), H2 (medium), H3 (small), H4 (medium), H5 (small), and H6 (small), providing insight into practical

significance beyond statistical significance.

5. DISCUSSION

5.1. Explaining the Governance– Effectiveness Gap

The results reveal a consistent gap between the formal implementation of cybersecurity governance practices and their effectiveness. Despite moderate to high implementation scores across all six governance dimensions, the absence of statistically significant relationships indicates that governance within the ministry remains bureaucratic and disconnected from strategic decision-making.

This finding supports the argument that cybersecurity governance in developing countries' public sectors often focuses on documentation, reporting, and procedural adherence rather than integrating governance into executive and strategic functions. The maturity gap observed here demonstrates the need for adaptive governance frameworks that go beyond compliance to embed cyber security accountability at the leadership level.

5.2. Interpretation of the Unexpected Negative Effect

The most unexpected finding of this study is the negative, albeit non-significant, effect of Risk Assessment and Management on strategic cybersecurity effectiveness (β = 0.571). Rather than indicating a beneficial role, this result suggests that risk management practices within the Ministry may function as procedural or bureaucratic mechanisms that do not translate into strategic value for the Ministry. In resource-constrained public-sector environments, extensive risk assessment processes may unintentionally create an administrative burden, slow decision-making, and reduce organizational agility in responding to emerging cyber threats. This phenomenon aligns with the notion of "analysis paralysis," where excessive emphasis on documentation and formal risk procedures inhibits timely strategic action.

Similar observations have been reported by Olatunde-Thorpe et al. (2021) [12], who noted that in certain government institutions, formal risk management frameworks may hinder rather than enhance cybersecurity effectiveness when they are detached from executive decision-making and resource prioritization. This finding reinforces the importance of integrating risk assessment activities with strategic governance processes, rather than treating them as standalone compliance requirements.

Sensitivity Analysis: Jackknife analysis was performed to assess the robustness of the negative coefficient for Risk Assessment and Management. The coefficient remained negative across all subsamples (range: -0.52 to -0.61), confirming that the finding was not driven by outliers.

Interaction Effects: Analysis of the potential interaction effects between Risk Assessment and Management and other governance dimensions (leadership and strategic policy) revealed no significant interactions ($p > 0.10$), suggesting that the negative effect operates independently.

Concrete Examples: Within the Ministry, formal risk management processes require extensive documentation for each risk assessment, including detailed threat analysis, vulnerability assessment, and impact evaluation. These requirements, while procedurally compliant, have created administrative burdens that slow down decision-making. Decision-makers reported that risk assessment processes often take 3-6 months to complete, impeding timely responses to emerging threats.

Alternative Explanations: The negative relationship may also reflect time-lag effects, where risk management investments require longer periods to demonstrate strategic value. Additionally, external factors, including Yemen's institutional instability and resource constraints, may moderate the relationship between formal risk practices and strategic outcomes.

5.3. Contextual Factors Explaining Weak Relationships

Several contextual factors may explain the generally weak statistical relationships observed.

- Hierarchical decision-making: Strategic authority is concentrated among senior executives, limiting the diffusion of governance responsibilities to the operational levels.
  [•] Resource constraints: Limited financial and human resources hinder full implementation of risk-based governance practices.
  [•] Compliance-oriented culture: Governance processes are viewed as administrative requirements rather than as strategic enablers.
  [•] Fragmented accountability: Cybersecurity performance metrics are not integrated into institutional performance evaluations.

Together, these factors weaken the causal relationship between governance practices and strategic cybersecurity effectiveness.

5.4. Comparison with Previous Studies

These findings align with prior research emphasizing that cybersecurity governance in developing-country public institutions is often symbolic rather than strategic [5, 12]. Similar maturity gaps have been identified in other public-sector contexts where governance frameworks are adopted formally but remain decoupled from strategic

impact [6]. However, this study advances the discussion by providing empirical confirmation of this maturity gap through PLS-SEM analysis rather than relying solely on conceptual or qualitative insights. The observed negative relationship for risk management contributes new evidence supporting the argument that excessive procedural formalization can reduce agility and, consequently, strategic effectiveness.

5.5. Theoretical Implications

The findings challenge the prevailing theoretical assumption that adopting cybersecurity governance standards automatically leads to strategic effectiveness. Instead, the results suggest that institutional design and the integration of governance mechanisms into real decision-making structures may be more influential than formally adopting governance principles. This insight extends the cybersecurity governance theory by shifting the focus from compliance-oriented maturity models toward decision-centric governance effectiveness.

6. PROPOSED FRAMEWORK

6.1. Rationale and Derivation from Findings

Responding to calls in the literature for more context-sensitive and adaptive governance frameworks [5, 6], this study proposes an empirically derived cybersecurity governance framework tailored to public-sector institutions in developing countries. The empirical results of this study reveal a critical gap between governance practices and strategic cybersecurity effectiveness in the Ministry of Communications and IT in Yemen. Despite the moderate to high implementation of governance dimensions, none exhibited statistically significant impacts on strategic outcomes. This indicates a maturity gap, where practices remain largely bureaucratic and lack integration with strategic decision-making. Drawing on these findings and insights from prior literature [5, 12, 13], the proposed framework is designed to address the specific deficiencies observed in public-sector cybersecurity governance.

1. Strategic Integration Gap: Governance practices are not linked to strategic objectives.
2. Performance Measurement Deficit: Lack of integrated metrics reduces accountability.
3. Monitoring Weakness: Control mechanisms exist, but are not tied to actionable insights.
4. Compliance Orientation: Practices emphasize documentation and formal procedures, not operational impact.

The framework operationalizes ISO/IEC 27014 principles beyond compliance, emphasizing strategic alignment, risk-based decision-making, continuous monitoring, and iterative improvement.

6.2. Components of the Proposed Framework

The proposed framework consists of five core components, each directly addressing observed gaps:

1. Executive Accountability & Strategic Oversight
   - o Establishes clear roles, responsibilities, and reporting lines.
   - o Ensures governance decisions inform strategic cybersecurity planning.
   - o Addresses the gap of weak leadership influence on outcomes.
2. Risk-Based Strategic Policy
   - o Governance decisions are informed by enterprise risk assessments, not just compliance checklists.
   - o Prioritizes initiatives that maximize strategic impact by linking ISO/IEC 27014 risk management principles to organizational objectives.
3. Integrated Performance Measurement
   - o Embeds quantitative and qualitative KPIs for cybersecurity governance.
   - o Directly addresses the absence of measurable strategic impact in current practices.
4. Continuous Monitoring & Control Integration
   - o Links monitoring activities to KPIs and decision-making processes, closing the gap observed in Control & Monitoring.
   - o Enables real-time feedback for governance refinement.
5. Iterative Improvement & Awareness Programs
   - o Incorporates lessons learned, training, and awareness into an ongoing cycle.
   - o Enhances adaptive governance, ensuring alignment with evolving threats such as IoT and AI, as highlighted in previous studies (PLOS ONE, 2023).

6.3. Mapping Framework Components to Observed Gaps

Table 5 maps the empirically observed cybersecurity governance gaps to the corresponding components of the proposed framework. The mapping demonstrates that the framework is not conceptual or generic but rather explicitly derived from the study's empirical findings. The results indicate a strategic integration gap, where leadership and strategic policy do not show statistically sig-

nificant effects on cybersecurity strategic effectiveness. This gap is addressed through the framework's emphasis on executive accountability and strategic oversight, ensuring that cybersecurity governance is embedded within organizational strategy rather than treated as a technical function.The absence of measurable links between governance practices and strategic outcomes reveals a performance measurement deficit. To overcome this weakness, the framework introduces integrated performance measurement, enabling decision-makers to evaluate cybersecurity effectiveness using meaningful and actionable indicators.A monitoring weakness was also observed, reflected in the negative estimate associated with control and monitoring. The framework therefore strengthens continuous monitoring and control integration, ensuring that monitoring results inform strategic decision-making instead of remaining procedural activities. Additionally, the findings highlight a compliance-oriented governance approach, where practices are formally implemented but lack strategic impact. This limitation is addressed through iterative improvement and awareness programs, which shift the focus from compliance to continuous value creation.Finally, the marginal effect of risk assessment indicates insufficient risk prioritization. The proposed framework responds by reinforcing risk-based strategic policy, ensuring that cybersecurity decisions and resource allocation are aligned with the organizational risk contexts.

Overall, this mapping confirms that each component of the proposed framework directly responds to an empirically identified governance gap, thereby operationalizing ISO/IEC 27014 in a context-sensitive and outcome-oriented way.

Observed Governance Gap	Example from Study Results	Proposed Framework Component	Intended Effect / Improvement
Strategic Integration Gap	Leadership & Policy not significant (p>0.05)	Executive Accountability & Strategic Oversight	Aligns governance with strategic cybersecurity objectives
Performance Measurement Deficit	No measurable KPI integration	Integrated Performance Measurement	Provides actionable metrics to evaluate effectiveness
Monitoring Weakness	Control & Monitoring negative estimate (-0.571)	Continuous Monitoring & Control Integration	Ensures monitoring influences strategic decisions
Compliance-Only Orientation	All practices high but non-significant	Iterative Improvement & Awareness Programs	Shifts focus from formal compliance to operational impact
Risk Prioritization Insufficient	Risk Assessment marginal (p=0.092)	Risk-Based Strategic Policy	Emphasizes prioritization based on organizational risk context

Table 6. Linking Observed Governance Gaps to Proposed Framework Actions

Table 6 shows that to address the "strategic integration gap," the framework does not merely call for greater executive involvement; rather, it proposes a concrete institutional mechanism: incorporating cybersecurity effectiveness indicators as a fixed item in executive performance reports and linking their annual evaluation to the achievement of specific security objectives. This shift from "recommendation" to "institutional design" constitutes the framework's core contribution.

6.4. Implementation Roadmap

- Phase 1 (Months 1-6): Establish an executive-level cybersecurity governance committee with defined roles and responsibilities.
- Phase 2 (Months 7-18): Develop and integrate KPIs into institutional performance evaluation systems.
- Phase 3 (Ongoing): Implement continuous monitoring systems and iterative improvement cycles.

Measurable Indicators for Each Framework Component:

1. Executive Accountability: % of strategic decisions incorporating cybersecurity risk assessment
2. Risk-Based Policy: Number of cybersecurity initiatives prioritized by risk impact
3. Performance Measurement: Quarterly cybersecurity effectiveness score
4. Continuous Monitoring: Real-time threat detection and response time
5. Iterative Improvement: Number of governance process improvements per year

Illustrative Scenario: Consider a scenario in which the Ministry identifies a critical vulnerability in its national telecommunications infrastructure. Under the proposed framework, the cybersecurity governance committee would immediately convene, conduct a rapid risk assessment using the risk-based policy component, prioritize resource allocation based on the integrated performance measurement system, and implement controls while continuously monitoring their effectiveness. This approach ensures timely and strategic responses rather than lengthy procedural compliance.

6.5. Conceptual Diagram

Figure 4 shows the top-down alignment, where executive oversight informs risk-based policies.

Performance measurement and monitoring provide feedback loops, and iterative improvement ensures that the framework adapts to evolving threats.

6.6. Contribution and Practical Relevance

- Provides a context-sensitive operationalization of ISO/IEC 27014 in a developing country's public sector.
- Bridges the gap between symbolic governance and strategic effectiveness, as revealed in empirical findings.
- It offers practical guidance for policymakers, enabling

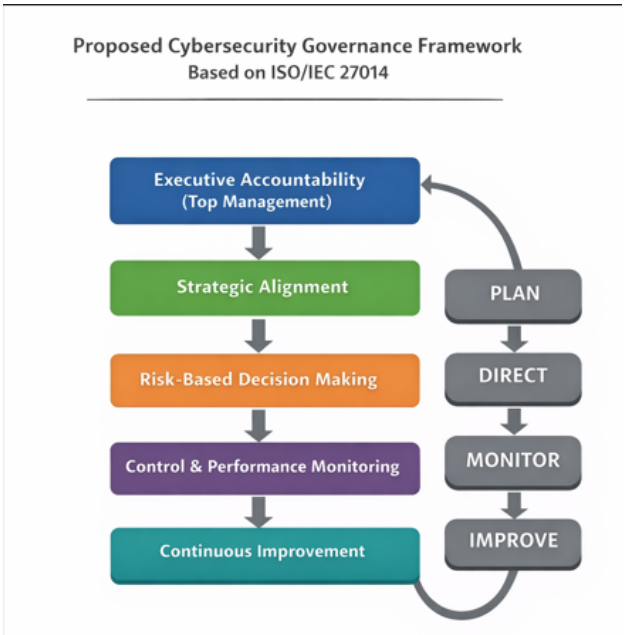

Figure 4. Proposed ISO/IEC 27014-based Governance Framework

the prioritization of resources, integration of metrics, and alignment of cybersecurity initiatives with strategic objectives.

7. CONCLUSION

This study examined the strategic effectiveness of cybersecurity governance practices within a public sector institution in a developing country, using the Ministry of Communications and Information Technology in Yemen as a case study. Grounded in the principles of ISO/IEC 27014, this study empirically assessed six governance dimensions and their relationship with strategic cybersecurity effectiveness through PLS-SEM analysis. The findings reveal a critical paradox: despite moderate to high levels of formal implementation across all governance dimensions, none demonstrate statistically significant effects on strategic cybersecurity effectiveness. This result exposes a pronounced governance maturity gap, where cybersecurity governance exists primarily as a set of compliance-oriented structures rather than as an integrated, strategic capability.

More importantly, this study provides a contextual explanation for this gap. The absence of significant relationshipsand the unexpected negative effect associated with risk assessment and management suggest that governance mechanisms are institutionally decoupled from executive decision-making, resource allocation, and performance accountability. In such environments, governance practices may inadvertently become procedural burdens that limit organizational agility rather than enhancing strategic cyber resilience. Based on these insights, this study proposes a context-sensitive cybersecurity governance framework that operationalizes ISO/IEC 27014 beyond formal adoption. Unlike generic governance models, the proposed framework translates high-level principles into concrete institutional mechanisms, such as embedding cybersecurity performance indicators into executive accountability structures and aligning risk management activities with the strategic objectives. This study makes three key contributions to the literature. First, it provides rare empirical evidence of the effectiveness of cybersecurity governance in a public-sector institution within a developing country context. Second, it advances the literature by demonstrating that formal governance adoption does not inherently yield strategic effectiveness, thereby empirically substantiating the concept of a cybersecurity governance-maturity gap. Third, it offers a practical and empirically grounded framework that supports policymakers and practitioners in transitioning from symbolic governance toward strategically integrated cybersecurity governance. Overall, the study underscores that the strategic value of cybersecurity governance is not determined by the presence of formal structures alone, but by the extent to which these structures are embedded within organizational decision-making processes, performance evaluation systems, and continuous improvement cycles. Finally, empirical testing of the proposed governance framework is recommended to evaluate its practical applicability and impact on cybersecurity outcomes in real-world public sector settings. These findings call for a redefinition of cybersecurity governance maturity. Maturity should not be assessed by the extent of practice adoption but by the capacity of governance mechanisms to influence real strategic decision-making processes.

8. LIMITATIONS AND FUTURE RESEARCH

8.1. Limitations of the Study

Despite the contributions of this study, several limitations should be considered. First, the study adopted a cross-sectional research design, with data collected at a single point in time. This limits the ability to establish causal relationships between cybersecurity governance practices and their effectiveness. Second, the study relies on self-reported data collected through a questionnaire, which may introduce response bias and potentially overestimates the actual level of governance implementation. Third, the sample size was relatively small (n = 30), which, as demonstrated through post-hoc statistical power analysis, limits the statistical power of the findings and constrains the detection of medium-sized effects. Finally, focusing on a single public-sector institution—the Ministry of Communications and Information Technology in Yemen—restricts the generalizability of the results to other organizational or national contexts. Consequently, the findings should be interpreted as context-specific

rather than universally applicable findings.

8.2. Directions for Future Research

Based on the findings and limitations of this study, several directions for future research are recommended.

First, future studies could adopt a comparative research design by examining cybersecurity governance across multiple ministries or public sector institutions within Yemen or other developing countries. Such comparisons would enhance the external validity of the findings.Second, longitudinal research designs are recommended to assess how changes in governance maturity influence strategic cybersecurity effectiveness over time, thereby providing stronger evidence of causal relationships.Third, qualitative research methods, such as in-depth interviews with senior executives and cybersecurity decision-makers, could complement survey-based findings and provide deeper insights into organizational, cultural, and political factors influencing governance effectiveness. Fourth, future research should focus on developing and validating context-sensitive performance indicators that better capture the effectiveness of cybersecurity strategies in public sector environments.

REFERENCES

[1] International Organization for Standardization, *Iso/iec 27014:2012 – information technology – security techniques – governance of information security*, Geneva, Switzerland: ISO, 2012. [Online]. Available: https://www.iso.org/standard/43720.html.

[2] International Organization for Standardization, *Iso/iec 27001:2018 – information security management systems – requirements*, Geneva, Switzerland: ISO, 2018. [Online]. Available: https://www.iso.org/standard/54534.html.

[3] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity," NIST, Gaithersburg, MD, USA, Tech. Rep., 2018. DOI: 10.6028/NIST.CSWP.04162018.

[4] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg, IL, USA: ISACA, 2019. [Online]. Available: https://www.isaca.org/resources/cobit.

[5] N. O. Sales, D. J. V. Vieira, V. Ferreira Júnior, G. D. Bispo, L. A. Ribeiro Júnior, and C. Neumann, "Opportunities and challenges in cybersecurity governance: A systematic review," in *Proceedings of the IEEE World Conference on Natural and Engineering Sciences (WCNPS 2025)*, Brasília, Brazil, Nov. 2025. DOI: 10.1109/WCNPS69127.2025.11295929.

[6] M. M. Mijwil, Y. Filali, M. Aljanabi, M. Bounabi, and H. Al-Shahwani, "The purpose of cybersecurity governance in the digital transformation of public services and protecting the digital environment," *Mesopotamian J. Cybersecur.*, vol. 2023, pp. 1–6, 2023. DOI: 10.58496/MJCS/2023/001.

[7] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Comput. & Secur.*, vol. 98, p. 102 003, 2020. DOI: 10.1016/j.cose.2020.102003.

[8] A. Da Veiga and N. Martins, "Defining and identifying dominant information security cultures and subcultures," *Comput. & Secur.*, vol. 70, pp. 72–94, 2017. DOI: 10.1016/j.cose.2017.04.002.

[9] P. Ifinedo, "Roles of organizational culture and leadership in information security management," *Inf. & Comput. Secur.*, vol. 26, no. 2, pp. 153–169, 2018. DOI: 10.1108/ICS-08-2017-0053.

[10] R. von Solms and B. von Solms, "Cybersecurity and information security: What goes where?" *Inf. & Comput. Secur.*, vol. 26, no. 1, pp. 2–9, 2018. DOI: 10.1108/ICS-04-2017-0021.

[11] P. Puhakainen and M. Siponen, "Improving employees' compliance through information security training," *MIS Q.*, vol. 34, no. 4, pp. 757–778, 2010. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/3447934.3447940.

[12] O. Olatunde-Thorpe, L. Futcher, and R. Botha, "A systematic review of cybersecurity governance in the public sector," *Inf. Comput. Secur.*, vol. 29, no. 5, pp. 687–709, 2021. DOI: 10.1108/ICS-09-2020-0142.

[13] Y. Zhang, K. McLaughlin, and S. Sezer, "Factors associated with cybersecurity awareness of cyber and information security decision-makers," *PLOS ONE*, vol. 18, no. 10, e0312266, 2023. DOI: 10.1371/journal.pone.0312266.

[14] D. R. Aryanti, "Cybersecurity governance in public institutions: Managing digital risks and resilience," *Transdiscipl. J. Eng. & Sci.*, 2025. DOI: 10.54783/jv.v17i3.1424.

[15] M. Al-Emran and M. A. Al-Sharafi, "Cybersecurity awareness in the arab region: A systematic literature review," *Comput. & Secur.*, vol. 115, p. 102 608, 2022. DOI: 10.1016/j.cose.2022.102608.

[16] World Bank, *World Development Report 2021: Data for Better Lives*. Washington, DC, USA: World Bank, 2021. [Online]. Available: https://www.worldbank.org/en/publication/wdr2021.

[17] United Nations, *The Age of Digital Interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation*. New York, NY, USA: United Nations, 2019. [Online]. Available: https://digitalcooperation.org/report/.