ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct257

Bridging IT Risk Governance in Bangladesh: A Comparative Gap Analysis of Bangladesh Bank's Guideline on ICT Security v4.0 and ISACA's Risk IT Framework

Sujit Kumar Sarker

Senior Engineer (IT), Sonali Bank PLC.
Head Office, 35-42, 44, Motijheel C/A, Dhaka, Bangladesh.

Publication Date: 2025/10/14

Abstract: IT risk governance describes the overall oversight of strategies, policies, controls, and accountability structures that aim to ensure security, resilience, and regulatory compliance related to system and technology assets in an organization. IT risk is an integral part of financial risk. Considering the growing cyber risk and systemic risk, Bangladesh Bank released Guideline on ICT Security – Version 4.0, 2023 to mitigate escalating cyber threats and systemic vulnerabilities of the financial sector. This paper conducts a cross-reference gap analysis between ICT Security Guideline, 2023 issued by Bangladesh Bank and ISACA's Risk IT Framework, identifying governance gaps, strengths, and opportunities for alignment. Based on a gap and maturity assessment structured around the 14 ISO/IEC 27001 controls and relevant international standards, this study highlights shortcomings in risk quantification, qualitative and quantitative assessments, integrating IT governance into corporate governance, and strategic alignment with enterprise and regulatory entities. Suggestions for enhancing governance maturity, compliance, and organizational resilience are presented.

Keywords: *IT Risk Governance, Bangladesh Bank, Guideline on ICT Security – Version 4.0, ISACA Risk IT Framework, Gap Analysis, Governance Maturity, ISO/IEC 27001 Controls, Cybersecurity in Financial Sector, Regulatory Compliance.*

How to Cite: Sujit Kumar Sarker (2025) Bridging IT Risk Governance in Bangladesh: A Comparative Gap Analysis of Bangladesh Bank's Guideline on ICT Security v4.0 and ISACA's Risk IT Framework. *International Journal of Innovative Science and Research Technology*, 10(10), 626-630. https://doi.org/10.38124/ijisrt/25oct257

I. INTRODUCTION

Stakeholders continually face stark challenges to the banks from escalating cyber-attacks, aligning with operational risk management, and complying with regulatory requirements that address cyber threats, losses, and resilience shortcomings in the financial institution [1][4]. In response, Bangladesh Bank has released Guideline on ICT Security – Version 4.0, 2023 [2] to mitigate the operational and systemic risk that has stemmed from previous high-profile cyber theft exploits. The term IT risk incurs losses due to the failure of key technology-focused elements, including systems, networks, and compliance with technology standards and regulations. The implication of the losses extends beyond the primary stakeholders to impact on the data and hardware firms involved and may involve government agencies [1][4][19].

As a guideline and framework, ISACA's Risk IT Framework [3] provides a comprehensive methodology establishing a direct link to corporate governance through focusing on three high-level domains of risk governance, risk evaluation, and risk response. Notable governance issues, gaps, and weaknesses are commonly observed in emerging markets in integrating IT strategy with enterprise strategy and corporate governance and in not measuring or poorly quantifying IT risk [8]-[11]. Notably, core elements refer to addressing key stakeholder concerns, which should include at least reporting measures and strong IT key risk indicators to support IT decision making. These issues are pertinent and important in assessing and achieving the best practice application of the ISACA Risk IT governance framework, particularly in the financial sector of Bangladesh, such as what is outlined in the ICT Security – Version 4.0, 2023.

Therefore, in the context of Bangladesh's emerging market, this study intent to cross-reference and compare ICT Security Guideline, 2023 against ISACA's Risk IT Framework to identify opportunities and gaps between both frameworks and guidelines in bridging the IT risk governance gap in the financial institution of Bangladesh.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct257

II. LITERATURE REVIEW

A. IT Risk Governance Frameworks

Frameworks for managing IT risk involve structured approaches adopted by organizations to identify, assess, and respond to risks associated with IT. Kaplan and Mikes [6] describe mapping each risk to its key drivers and triggers and asserts IT risks require direct and measurable connections to stakeholder value. Whitman and Mattord [7] argue a successful information security program is dependent upon the organizational structure of the program and how well its components, such as policies, procedures, technical controls, and personnel are governed. ISACA's Risk IT Framework [3] delineates three high-level categories of risk associated with IT: risk governance, risk evaluation, and risk response. The ISACA IT Risk Framework also includes a maturity assessment framework in the form of metrics.

B. IT Governance in Financial Institutions

IT governance has a positive effect on a firm's strategic flexibility, operational performance, and compliance with laws and regulations [8]-[12]. Poor governance has led to an enormous loss of funds or a critical threat to the entire organization as well as bad press for several important banking institutions [1][4][18]. Information and technology risk management and corporate governance are practiced together in the best interest of an organization to improve managerial capabilities and enhance enterprise goals and performance [11]-[13].

C. Bangladesh Context

Since 2000, the Bangladesh banking sector has been digitized and continues to digitalize rapidly; hence, cyberspace and cyber risk in the banking sector of Bangladesh are increasing [17][24]. The incident of the Bangladesh Bank cyber heist incident of 2016 has raised the awareness of the importance of governance capability, risk management framework, and technical countermeasures among corporate stakeholders [4][19][23][25]. ICT Security Guideline, 2023 released by Bangladesh Bank [2] regulates and prescribes a specific set of operational, technical, risk-specific, and strategic measures that financial institutions must take to align and improve IT risk governance, which includes but is not limited to cyber risk within organizational limits.

III. METHODOLOGY

This study involves qualitative comparative analysis to identify how well the current policy aligns with the ISACA Risk IT Framework description and best practices. The following steps were undertaken:

A. Document Analysis

Analysis of ICT Security Guideline, 2023 (v4.0) and ISACA Risk IT Framework.

B. Categorization and Mapping

Identify three high-level domain areas of the ISACA framework and the key elements of its best practice description and map it to the relevant sections and provisions of the policy.

C. Gap Analysis

Assess the degree of alignment or nonalignment between the ISACA description and the policy.

D. Maturity Assessment

A gap and maturity assessment based on 14 ISO/IEC 27001 control subsets, ISO standards, and metrics.

E. Synthesis of Recommendations

Identify opportunities to address the gaps and nonalignment, both strengthening the requirements of the policy or other actions on the part of organizations that should be taken [6]-[18]. Table 1 can map ICT Security Guideline provisions in guidelines to the ISACA Risk IT Framework to four primary ICT Security Guideline domains.

Table 1 – Mapping of Bangladesh Bank ICT Security Guideline, v4.0 to ISACA Risk IT Domains

ISACA Risk IT Domain	Key Components	Bangladesh Bank ICT Security Guideline (v4.0, 2023)	Alignment / Gap Notes
Risk Governance (Strongest Alignment)	Strategic alignment, board oversight, roles & responsibilities	**Sections 3.1 – 3.5:** Governance Structure, Roles, Oversight Committees	**Strong Alignment:** Provides clear operational governance structure and defines committees. **Gap:** Limited explicit formal integration with the Board of Directors for ultimate risk oversight.
Risk Evaluation (Partial Alignment)	Risk identification, assessment, quantification, prioritization	**Sections 4.1 – 4.4:** Risk Assessment Procedures, Reporting Mechanisms	**Alignment:** Covers qualitative risk identification and basic assessment procedures. **Significant Gap:** Lacks detailed guidance on quantitative risk metrics, economic impact analysis, and formal scenario analysis.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct257

ISACA Risk IT Domain	Key Components	Bangladesh Bank ICT Security Guideline (v4.0, 2023)	Alignment / Gap Notes
Risk Response (Moderate Alignment)	Mitigation, monitoring, escalation, risk acceptance	**Sections 5.1 – 5.6:** Incident Response, Contingency Planning, Compliance	**Strong Alignment:** Operational mitigation (IRP, BCP), monitoring, and compliance are well-covered. **Gap:** Enterprise-level escalation paths and formal processes for risk acceptance by business owners are less explicit.

Note: Table 1 demonstrates where Bangladesh Bank's ICT Security Guideline v4.0, 2023 aligns with ISACA's framework and highlights areas for improvement.

IV. COMPARATIVE ANALYSIS

A. Risk Governance

ICT Security Policy is a good high-level and prescriptive guide on an overall governance structure, roles, and responsibility groups, committees, etc., to be established – see sections: [2]. However, there are missing aspects of board-level integration with enterprise risk over time, specified engagement with the board itself and/or BCPSC, and limited provisions for articulating the key risk categories of the institution's appetite in relation to IT risk [3].

B. Risk Evaluation

There is an emphasis in the ISACA Framework and description that the risk evaluation process must be iterative and continuous and that risk must be expressed in both qualitative and quantitative formats for consistent engagement with key stakeholders [3]. The nature of the prescribed risk assessment process in the policy is much more prescriptive and refers only to the process of identifying risks, classifying them internally, and informing external agencies and stakeholders. There are no specified use cases and no prescriptive methods of conducting quantitative risk assessments, scenario assessments, vulnerability assessments, or consequence assessments [2][6][10][14].

C. Risk Response

The policy and the framework and description cover requirements for all the response strategies of mitigation, acceptance, avoidance, and transference in the use cases. However, not all are covered in detail. ISACA places emphasis on having a strategy for escalation that occurs outside the defined risk appetite and the roles and response strategies in these cases outside the remit of the parameters defined in the risk categories for the day-to-day operations staff and the BCP committee [3]. The policy strongly emphasizes operational mitigation strategies and has only a minimal reference to escalation and transference strategies further down in section [2].

Figure 1 can illustrate a visual representation of the mapping of provisions in the ICT Security Guideline to the ISACA Risk IT Framework domains. Figure 2 illustrates a detailed visual representation of the mapping of provisions in the ICT Security Guideline to the ISACA Risk IT Framework domains.

Bangladesh Bank ICT Security Guideline vs. ISACA Risk IT domains: Alignment Heat Map

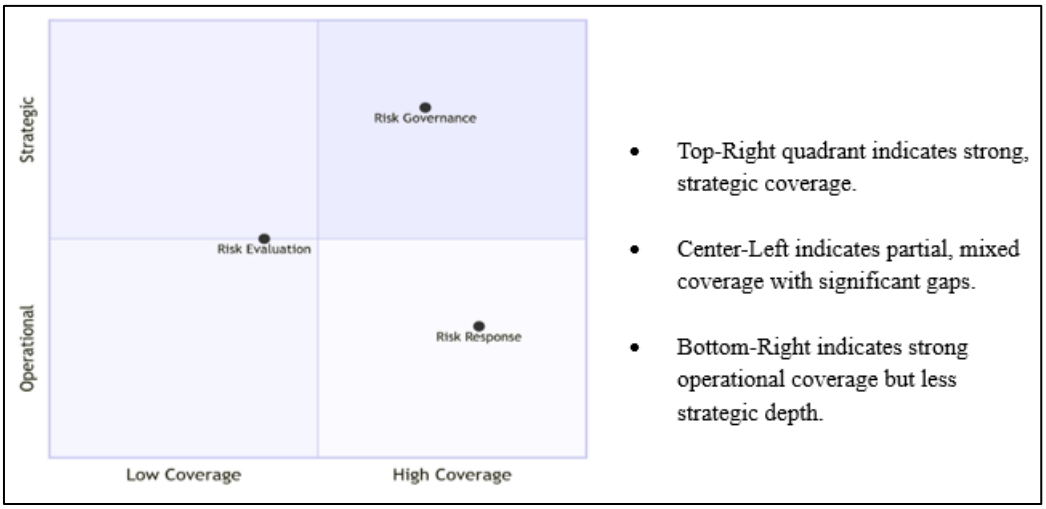

Fig 1 Illustrates the Mapping of ICT Security Guideline, v4.0 Provisions to ISACA's Risk IT Domains.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct257

Bangladesh Bank ICT Security Guideline vs. ISACA Risk IT domains: Detailed Alignment Diagram.

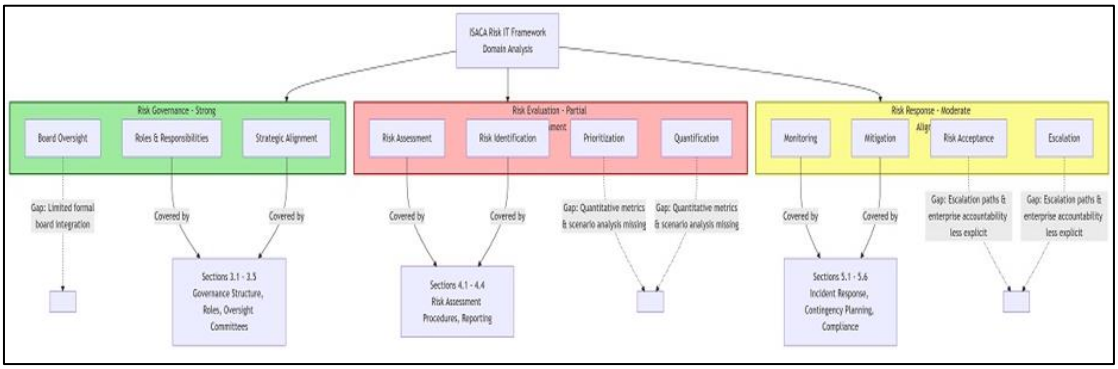

Fig 2 Illustrates a Detailed Visual Representation of the Mapping of Provisions in the ICT Security Guideline, v4.0 to the ISACA Risk IT Framework Domains.

V. DISCUSSION

The cross-reference analysis indicates that while there is an ICT Security Guideline addressing operational and technical mechanisms, there is limited detailed guidance on other areas of governance integration, consistency of alignment between the IT and enterprise strategies, and desired IT risk quantification approaches. Priority improvement areas that have emerged are:

A. Board and Enterprise Integration

Ensure that time-integrated reporting and accountability for enterprise integration occurs at board level with BCP committee stretch and formal board audit involvement and signoffs [6][12].

B. Quantification

Prescribe the preferred risk quantification formats, the use of methods such as scenario, vulnerability, and consequence assessments, and where to apply heat maps for purposes ahead of stakeholder engagement and accountability choices such as threshold limits beyond escalation/board committee levels and key risk indicator levels [10][14].

C. Engagement

Policies should ensure mechanisms are established for BI reporting and engaging with external parties such as media, Malaysian authorities, and regulatory authorities, as well as for updating the strategy and training staff as required [11][16].

D. Continuous Process

The ICT Security Guideline should ensure a prescribed process of regular updating based on changes in the threat landscape, lessons learned from vulnerabilities and threats, regular audit reviews, and the incorporation of international best practices [7][17][18]. Adoption and implementation of these areas of improvement will facilitate increased cyber risk resilience, regulatory compliance, and enterprise performance in the banking sector of Bangladesh.

VI. CONCLUSION

Bangladesh Bank's ICT Security Guideline issued in 2023 represents a major step in improving Bangladesh's IT risk governance further. An assessment against ISACA's Risk IT Framework description and associated project materials indicates that while it is an important step, offering a great deal in the way of improving individual projects, processes, departmental policy, and operational-level controls in silos, ICT Security Guideline has weaknesses in terms of lack of engagement at the board and enterprise level, lack of provisions for key quantitative/KRI engagement formats and levels both operationally and at the BCP committee level, lack of specified threat landscape, international best practices, continuous updating processes, and specified escalation processes. Addressing these shortcomings as follows is likely to produce more resilient consequences, comply more with international norms, and foster greater stakeholder confidence in enterprise governance.

Further research could involve an empirical confirmatory assessment of IT risk governance performance across the banks, for example, using the dimensions above with key stakeholders, and perhaps assessing the impact on overcoming each bank's key vulnerabilities or significant risk events.

REFERENCES

[1]. J. Newman, "The Billion-Dollar Bank Job," IEEE Spectrum, vol. 55, no. 6, pp. 32-37, June 2018.
[2]. Bangladesh Bank, "Guideline on ICT Security – Version 4.0", Dhaka, Bangladesh, BRPD Circular No. 10, 2023.
[3]. ISACA, The Risk IT Framework, Rolling Meadows, IL, USA, 2009.
[4]. P. S. Debreceny, "The Bangladesh Bank Heist: Lessons for the Central Banking Community," J. Payments Strategy & Systems, vol. 11, no. 3, pp. 226-237, 2017.
[5]. ISO/IEC, ISO/IEC 27001:2022 Information Security Management Systems — Requirements, Geneva, Switzerland, 2022.
[6]. R. S. Kaplan and A. Mikes, "Managing Risks: A New Framework," Harvard Bus. Rev., vol. 90, no. 6, pp. 48-60, 2012.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct257

[7]. M. E. Whitman and H. J. Mattord, Principles of Information Security, 7th ed., Boston, MA, USA: Cengage Learning, 2021.
[8]. P. Beng Sim, "The Impact of IT Risk Management on Strategic Agility and Organizational Performance: A Study on SMEs in Penang, Malaysia," 2014. [Online]. Available: https://core.ac.uk/download/200764279.pdf
[9]. S. M. Faizi and S. Rahman, "Securing Cloud Computing Through IT Governance," 2019.
[10]. A. Hemanidhi and S. Chimmanee, "Military-based cyber risk assessment framework for supporting cyber warfare in Thailand," 2017.
[11]. F. Jamba et al., "IT Governance Practices and Enterprise Effectiveness in Zimbabwe," 2013.
[12]. D. S. Kala Sethupathy and D. Preston, "Impact of corporate governance on information security practices in UK financial industry," 2010.
[13]. N. Sasongko and F. Lussie B, "IT Audit Performance for Accounting Transaction Security on Rural Banking in West Java Indonesia," 2013.
[14]. S. H. W. E. T. A. Singh et al., "Optimization of Different Objective Function in Risk Assessment System," 2013.
[15]. N. Che Pa et al., "A review on risk mitigation of IT governance," 2015.
[16]. D. Rios Insua et al., "An Adversarial Risk Analysis Framework for Cybersecurity," 2019.
[17]. A. K. M. Bahalul Haque, "Need for Critical Cyber Defence, Security Strategy and Privacy Policy in Bangladesh," 2019.
[18]. M. Asgarkhani et al., "Failed IT projects: is poor IT governance to blame?" 2017.
[19]. S. Nakashima, "The $81 million Bangladesh bank heist: How hackers targeted the federal reserve and got away with it," The Washington Post, 2016.