iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.81230

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Implementation of Cyber Security Framework in Financial Organizations of Bangladesh: A Comprehensive Study

Md. Abu Nahee Ibna Zahid[1], Halima Akter Beli[2]
[1]*IT Professional, Private Commercial Bank, Bangladesh*
[2]*ICT Tutor, Private College, Bangladesh*

Abstract: ***The expansion of digital financial services has reshaped Bangladesh's financial sector by improving service delivery, accessibility, and inclusion. At the same time, this transformation has increased exposure to sophisticated cyber threats, making cybersecurity a strategic necessity for financial institutions. In response, the central bank has introduced regulatory measures such as ICT Security Guidelines and a national Cybersecurity Framework to enhance institutional resilience.***
This study explores how cybersecurity frameworks are being implemented across financial organizations in Bangladesh, with particular attention to governance practices, technological integration, regulatory alignment, and operational preparedness. Based on qualitative analysis of secondary data, including policy documents and global standards, the study identifies both progress and persistent gaps. While regulatory awareness and structural frameworks have improved, limitations remain in areas such as skilled workforce availability, modernization of infrastructure, and uniform execution across institutions. The paper recommends strengthening governance mechanisms, investing in advanced security capabilities, and aligning with internationally recognized standards to ensure long-term sectoral resilience.
Keywords-Cybersecurity Framework, Financial Institutions, Bangladesh, ICT Security, Risk Management, Digital Banking, Information Security.

I. INTRODUCTION

The financial sector plays a fundamental role in economic development, acting as the backbone of financial intermediation, investment, and economic growth. In Bangladesh, the financial sector has undergone significant digital transformation over the past decade. The adoption of digital technologies such as online banking, mobile financial services, electronic fund transfers, and real-time payment systems has revolutionized financial service delivery.

This transformation has been driven by increased internet penetration, smartphone usage, and government initiatives promoting digital financial inclusion. Mobile financial service platforms such as bKash, Nagad, Rocket, etc. have enabled millions of individuals to access financial services, particularly in rural and underserved areas.

However, the rapid digitalization of financial services has also introduced new risks, particularly in the form of cyber threats. Financial institutions are prime targets for cybercriminals due to the high value of financial transactions and the sensitive nature of customer data they handle. Cyberattacks such as phishing, ransomware, malware, and distributed denial-of-service (DDoS) attacks have become increasingly common in the financial sector.

The significance of cybersecurity in Bangladesh became globally recognized following the Bangladesh Bank cyber heist in 2016, where hackers exploited vulnerabilities in the SWIFT network to transfer $81 million from the central bank's account [1]. This incident exposed critical weaknesses in cybersecurity infrastructure and governance, highlighting the need for a comprehensive cybersecurity framework.

In response, Bangladesh Bank introduced several regulatory initiatives, including the ICT Security Guidelines and the recently updated Cybersecurity Framework. These frameworks aim to standardize cybersecurity practices, enhance risk management, and improve resilience across financial institutions.

This study aims to analyse the implementation of cybersecurity frameworks in financial organizations in Bangladesh and evaluate their effectiveness in mitigating cyber risks.

II. LITERATURE REVIEW

A. Concept of Cybersecurity Framework

Cybersecurity frameworks provide structured approaches for managing cyber risks and protecting information systems. Frameworks such as the NIST Cybersecurity Framework, ISO 27001, and COBIT provide comprehensive guidelines for managing cybersecurity risks [2]. These frameworks emphasize key functions such as identification, protection, detection, response, and recovery.

B. Cybersecurity in Financial Institutions

Financial institutions are among the most targeted sectors for cyberattacks. According to the Verizon Data Breach Investigations Report, the financial sector consistently ranks among the top industries affected by cyber incidents [3].Cybercriminals use various techniques such as phishing, malware, ransomware, and social engineering to exploit vulnerabilities in financial systems. The increasing use of digital banking platforms has expanded the attack surface, making cybersecurity more complex.

C. Cybersecurity in Developing Countries

Developing countries face unique challenges in implementing cybersecurity frameworks. Limited technological infrastructure, shortage of skilled professionals, and weak regulatory enforcement contribute to increased cyber risks.In many cases, financial institutions in developing countries prioritize regulatory compliance over proactive cybersecurity strategies, resulting in reactive rather than preventive approaches.

D. Cybersecurity in Bangladesh

In Bangladesh, cybersecurity has become a major concern for financial institutions. Studies indicate that many banks lack comprehensive cybersecurity governance frameworks and rely on basic security controls.The Bangladesh Bank cyber heist has been extensively studied as a case of cybersecurity failure. Reports indicate that the attack exploited vulnerabilities such as outdated systems, lack of firewall protection, and inadequate monitoring mechanisms.Recent regulatory initiatives, including the Cybersecurity Framework, aim to address these challenges by introducing standardized cybersecurity practices across the financial sector.

III. RESEARCH METHODOLOGY

This study adopts a qualitative research approach based on secondary data analysis.

A. Data Sources

The research uses data from:

1) Bangladesh Bank ICT Security Guidelines
2) Cybersecurity Framework
3) Academic journals and research papers
4) Industry reports and cybersecurity studies
5) News articles on cyber incidents

B. Data Analysis

The collected data were analysed using descriptive and thematic analysis techniques to identify key trends, challenges, and implementation practices.

IV. CYBERSECURITY FRAMEWORK IN BANGLADESH

A. ICT Security Guidelines

The ICT Security Guidelines issued by Bangladesh Bank provide a comprehensive framework for managing cybersecurity risks [4]. These guidelines include:

1) Information security governance
2) Risk management processes
3) Network and system security
4) Incident management
5) Business continuity planning

B.Cybersecurity Framework

The Cybersecurity Framework represents a significant advancement in cybersecurity regulation [5]. Key components are:

1) Governance and risk management
2) Asset management
3) Threat detection and monitoring
4) Incident response
5) Recovery and resilience

The framework aligns with international standards such as NIST and ISO 27001 and mandates compliance by financial institutions.

V. IMPLEMENTATION OF CYBERSECURITY FRAMEWORK

A. Governance and Organizational Structure

Effective implementation requires strong governance structures. Financial institutions must establish cybersecurity committees, define roles and responsibilities, and integrate cybersecurity into enterprise risk management.

B. Technology Deployment

Implementation involves deploying advanced security technologies, including:

1) Firewalls
2) Intrusion detection systems
3) SIEM systems
4) Multi-factor authentication
5) Encryption technologies

C. Human Resource Development

Cybersecurity awareness and training programs are essential for employees. Skilled professionals are required to manage cybersecurity systems effectively.

D. Incident Response and Business Continuity

Organizations must establish incident response teams and disaster recovery plans to ensure operational continuity.

VI. CHALLENGES IN IMPLEMENTATION

A. Shortage of Skilled Professionals

There is a significant shortage of cybersecurity experts in Bangladesh.

B. Limited Budget Allocation

Many financial institutions allocate insufficient budgets for cybersecurity.

C. Legacy Systems

Outdated IT systems increase vulnerability to cyber threats.

D. Inconsistent Implementation

Differences in implementation practices across institutions create systemic risks.

E. Evolving Cyber Threat Landscape

Cyber threats continue to evolve rapidly, requiring continuous adaptation.

VII. DISCUSSION

Recent developments indicate that cybersecurity awareness within Bangladesh's financial sector has improved, largely due to regulatory pressure and increased exposure to cyber risks. Institutions are gradually adopting structured frameworks and implementing baseline security controls. However, in many cases, cybersecurity initiatives remain compliance-driven rather than strategy-driven.

A key limitation is the lack of consistency in implementation across organizations. While some institutions have advanced capabilities, others continue to operate with outdated systems and limited expertise. This uneven maturity creates systemic vulnerabilities within the sector.

To move forward, financial institutions must shift from reactive security practices to proactive risk management approaches that emphasize continuous monitoring, threat intelligence, and resilience planning.

VIII. RECOMMENDATIONS

Recommendations are given below:

1) Strengthen regulatory enforcement mechanisms
2) Increase cybersecurity investment
3) Develop skilled cybersecurity workforce
4) Adopt international standards
5) Enhance collaboration and information sharing

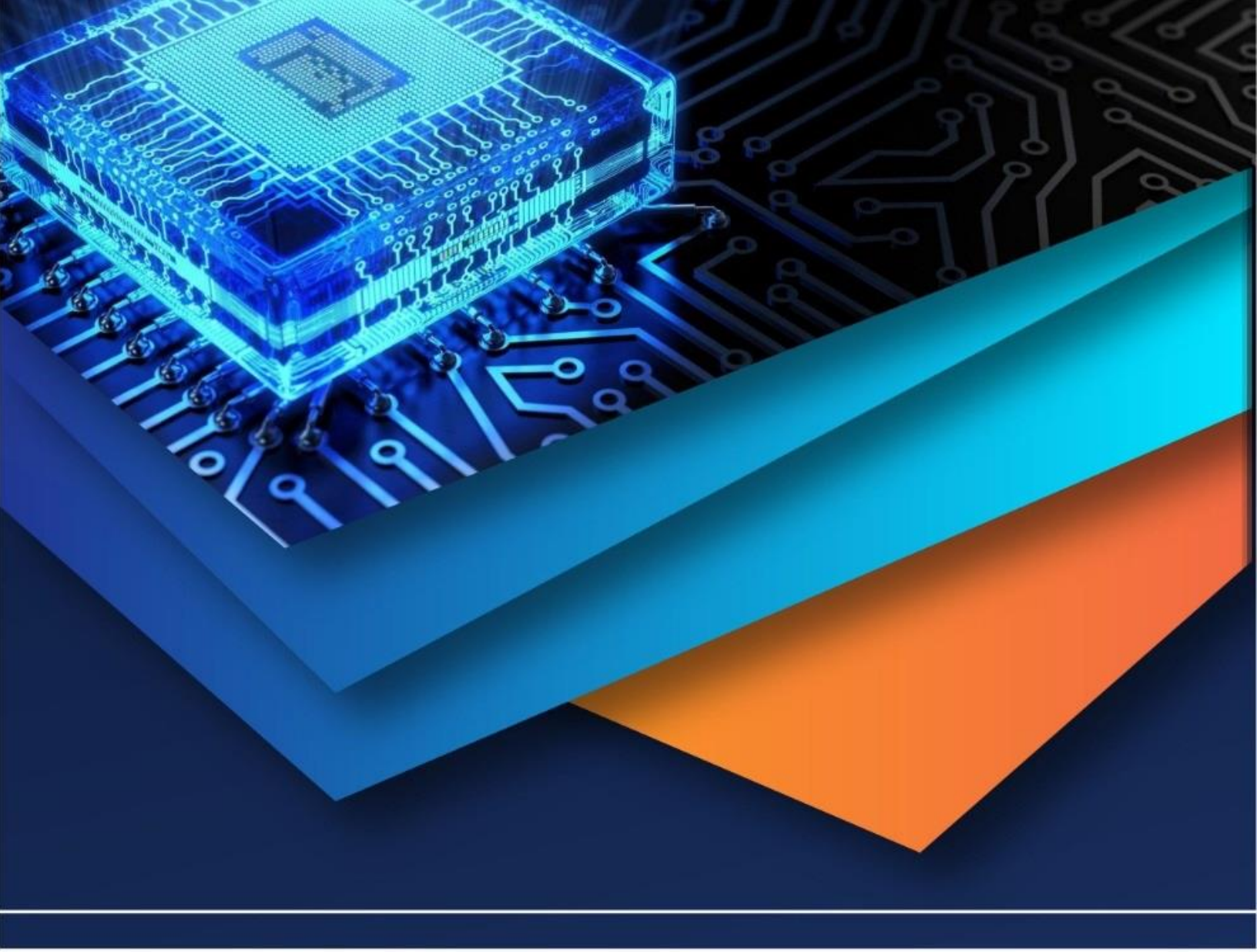
IX. CONCLUSION

The integration of cybersecurity frameworks is vital for protecting the integrity and stability of financial institutions in Bangladesh. Although regulatory interventions have contributed to measurable improvements, several structural and operational challenges continue to hinder full-scale effectiveness. These challenges include technological limitations, shortages of skilled professionals, and gaps in coordination among stakeholders.

Strengthening the sector's resilience requires a holistic approach that combines effective governance, modern technological solutions, and sustained investment in human capital. Rather than focusing solely on compliance, institutions must embed cybersecurity into their core strategic planning. Future research should prioritize data-driven assessments of framework implementation and critically examine how existing policies perform in real-world scenarios.

REFERENCES

[1] M. Rahman, "A Forensic View of Bangladesh Bank Reserve Heist," Sep. 2016.
[2] National Institute of Standards and Technology (NIST). *Cybersecurity Framework*, 2018.
[3] Verizon. *Data Breach Investigations Report*, 2025.
[4] Bangladesh Bank. ICT Security Guidelines for Banks and Non-Bank Financial Institutions, 2023.
[5] Bangladesh Bank. Cybersecurity Framework, 2026.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY