MSI Journal of Multidisciplinary Research (MSIJMR)

Volume: 1, Issue: 2 (December-2024)
Published by *MSI Publishers*
ISSN 3049-0669 (Online)

Received: 02-11-2024
Accepted: 19-11-2024
Published: 30-12-2024

Financial Risk Management in the Digital Era: Cybersecurity, FinTech Innovation, and Banking Sector Resilience

Authors Details

Md. Ruhul Amin[1*]
Associated Professor, Department of Business Administration, Dhaka International University.

Corresponding Author: *Md. Ruhul Amin*

ABSTRACT: The financial services industry has experienced a rapid digital revolution that has transformed the nature of financial risk management. The adoption of financial technology (FinTech), artificial intelligence (AI), cloud computing, mobile banking, digital payment systems and data-driven financial services has boosted operational efficiency, financial inclusion and the capacity of financial institutions to create innovative products. But these developments also present complicated risks ranging from cyberattacks, data breaches, and digital fraud to third-party technological dependencies, algorithmic bias, operational disruptions, and systemic vulnerabilities. As such, the challenges of modern banking cannot be addressed by traditional risk management systems. This research analyzes the relationship between cyber security, FinTech innovation and resilience in the banking sector in the digital era. This research adopts qualitative analytical method, based on secondary sources such current literature, regulations, and institutional risk management principles. The importance of cybersecurity governance, regulatory compliance, technological innovation and organizational resilience is addressed, and how digital technology transforms credit, market, liquidity, operational and systemic risks is investigated. The analysis reveals that digital transformation can assist financial stability if underpinned by coordinated regulatory supervision, responsible innovation, solid cyber-

DOI: *10.5281/zenodo.23553304*

risk controls and robust governance. The study recommends establishment of robust risk management frameworks, continuous threat monitoring, scenario-based stress testing, evaluation of third-party risks, employee education and international collaboration in regulation. The conclusion is that financial institutions should balance innovation with security, accountability and resilience to develop sustainable digital finance.

Keywords: *Financial Risk Management, Cybersecurity, FinTech Innovation, Banking Resilience, Digital Transformation, Operational Risk, Artificial Intelligence, Financial Stability.*

1. Introduction

Digital technology has become an intrinsic part of banking operations, payment systems, lending activities, investment services and customer relationship management, which has resulted in a major transformation in the financial services industry. Increasingly, conventional financial models rely on the infrastructure of digital technology to support the processing of transactions, the appraisal of creditworthiness, the administration of financial portfolios and the provision of services that go beyond territorial limits. Artificial intelligence, blockchain, cloud computing, automated decision-making systems, mobile financial services and internet banking have brought great prospects for financial organizations and their clients.

But despite these positives, digital transformation has transformed the character and distribution of financial risks. Traditional risks like credit, market and liquidity risks are now joined by a host of other risks faced by financial institutions, including cyber-attacks, identity theft, ransomware, payment fraud, technology failures, manipulation of data, and disruptions caused by external service providers. The aggregation of various threats may lead to effects not within the remit of particular institutions. Thus, cyber security has become a more significant component of financial risk management. If a cyberattack is effective and clients quickly get their money out, the following can happen customer information is compromised, payment processing is complicated, consumer confidence in a bank is eroded and liquidity difficulties arise. Similarly, the failure of a popular technology vendor could result in the simultaneous downfall of several different types of financial institutions. These interdependencies prove that digital risk is not only an IT issue, but also a strategic one that spans governance, financial stability, regulatory compliance and

 DOI: *10.5281/zenodo.23553304*

organizational continuity. Another related problem is FinTech innovation. Real-time payments, algorithmic credit scoring, digital financing, and computerized financial advising can expand access to financial services. But these technologies also create model risk, data privacy concerns, operational complexity and new types of deception.

Financial vulnerability can undermine technological efficiency when innovation exceeds the ability of institutions to manage risk. Consequently, the ability of financial institutions to foresee, absorb, respond and recover from disruptions and continue to provide important financial services is a key characteristic of resilience in the banking sector. Resilience is not simply about preventing certain things from happening. This involves the identification of important processes, the preparation of contingency plans, the maintenance of adequate cash reserves, the management of external dependencies and the learning from operational failures. These problems are particularly pronounced in developing economies where there is the opportunity for digital financial services to enhance financial inclusion. But there may be major gaps in levels of cybersecurity awareness, institutional resources, digital infrastructure and supervisory capacity. This essay discusses the influence of financial risk management, cybersecurity, FinTech innovation, and resilience of the banking industry. Its fundamental objective is to support a holistic understanding of how financial institutions should support digital innovation, while preserving security and stability.

The study addresses three research questions:

1. 1.What is the impact of digital transformation on the nature of financial risks in the banking sector?
2. What is the influence of cybersecurity and FinTech innovations on institutional resilience and financial stability?

2. Literature Review

2.1 The evolution of financial risk management

Traditionally, financial risk management has been concerned with the identification, measurement, monitoring and control of hazards that may degrade institutional performance. The main forms of risk are; interest rate risk, liquidity risk, operational risk, market risk and credit risk. Established methods are based on quantitative modeling,

 DOI: *10.5281/zenodo.23553304*

regulatory monitoring, capital adequacy, portfolio diversification and internal controls. Modern risk management is less about hazard as a separate category, and more about enterprise-wide integration. The Basel Committee on Banking Supervision has developed international standards on capital sufficiency, supervisory review, market discipline and operational risk. Digital interdependence creates further issues. But these frameworks are an important basis to control financial risks. Digitalization enhances on operational side of risk management. A technology failure could also impair transaction processing, regulatory reporting, liquidity management, and consumer access in a negative way. A cyber event, similarly, can lead to financial losses, legal duties and damage to reputation and future funding challenges. So, modern financial risk management requires financial analysis to be linked with strategic planning, business continuity, technology governance and information security.

2.2 Cybersecurity and financial risks

Cybersecurity is the defense of digital infrastructure, networks, information systems and data against illegal access, tampering, interruption and destruction. Financial firms are attractive targets because they can process sensitive client data, have significant financial holdings, and run vital payment infrastructure. Bouveret (2018) stresses the importance of understanding cyber risk within the framework of financial stability. Cyber incidents may generate immediate losses, operational stoppage, uncertainty, reputational damage and related institutional weaknesses. The most prominent risks on the internet involve malware, ransomware, phishing, distributed denial-of-service (DDoS) attacks, insider threats, and software security flaws. Social engineering tactics are becoming more and more sophisticated and can overcome good technical security by deceiving staff or customers. Thus, cybersecurity risk is inherent in the governance and conduct of an organization. Technical measures are not enough to eliminate the risks if people are not trained properly, privileged access management is not implemented, or top management is not focusing on security investment.

2.3 Financial Services and FinTech Innovation

The phrase “FinTech” is a comprehensive term for the integration of digital technologies into financial goods, services and operations. This includes mobile banking, digital

 DOI: *10.5281/zenodo.23553304*

payments, P2P lending, automated investment services, blockchain applications, digital identification systems and AI-enabled credit evaluation. According to Arner, Barberis, & Buckley (2016), FinTech is one of the key milestones in the growth of financial services, as it signifies the integration of technology with innovative business models and regulatory structures. FinTech can reduce transaction costs, speed up the delivery of services, improve data analysis and provide financial access to neglected people. Alternative data can support lenders in assessing borrowers with little traditional credit history and digital payment platforms can help small enterprises access formal financial institutions. However, technological advances may pose new threats. Automated credit models can reproduce historical biases, digital lending platforms can underestimate borrower vulnerability, and highly interconnected payment systems can rapidly convey operational problems. Reliance on a small number of technology providers could potentially give rise to concentration danger.

2.4 Resilience of the banking system and financial stability

"Banking resilience" is the ability of banks and the financial system as a whole to recover successfully from disruptions and to continue to perform essential operations under stress. It comprises operational, financial, technological, organizational and institutional factors. According to the Financial Stability Board (2020), operational resilience is important to maintain crucial financial services amid disruptions. Similarly, the operational resilience principles of the Basel Committee focus on governance, operational risk management, business continuity, third-party dependency management and mapping of important operations. "Traditional risk avoidance is different from resilience in the sense that there are some disruptions that cannot be completely eliminated. So a resilient organization has to be able to get back to normal in acceptable periods, keep key services going, communicate efficiently and contain harm. The literature indicates that cybersecurity, technology governance, and resilience planning should be included inside the complete risk management framework rather than as stand-alone administrative operations.

3. Research Methodology

This research is a qualitative descriptive analytical research design of secondary data. The analytical method is based on the review of academic literature, global regulatory

 DOI: *10.5281/zenodo.23553304*

standards, policy publications and institutional frameworks in the area of financial risk management, cybersecurity, FinTech innovation and banking resilience. Key sources include peer-reviewed scholarly literature, the International Monetary Fund, the Financial Stability Board and the Basel Committee on Banking Supervision. The articles offer conceptual frameworks and practical support to analysis of digital financial threats. The analysis considers four themes: the changing architecture of financial risk, governance of cybersecurity, the pros and cons of FinTech and the tools that can be utilized to improve resilience in the banking system. The paper did not use any original survey data, interviews or econometric estimate. Accordingly, its results are analytical instead of causal in the statistical sense. The results should be seen as a combination of institutional advice and proven wisdom, not as definitive proof that any one technology or approach in isolation would lead to a more stable financial system.

Cyber events and institutional vulnerabilities may be underreported. Technological settings and regulatory policies may evolve rapidly. That is a disadvantage of secondary research. Future study can address these constraints using comparative nation studies, institutional case studies, surveys, and quantitative assessments of financial performance and cyber incidents.

4. Digital Transformation and the Changing Nature of Financial Risk

4.1 Digital Banking Credit Risk

Credit risk is the chance that a borrower may default on its financial obligations. Automated scoring methods, machine learning, transaction analytics and alternative data have reshaped credit assessment in the digital banking space. The technologies could boost the consistency and speed of lending decisions. However, the reliability of automated assessments can be influenced by discriminatory characteristics, model instability, faulty training data, and insufficient explainability. Rapid digital lending can potentially result in over-borrowing when institutions do not appropriately analyze repayment capabilities. Besides building internal monitoring capabilities, more streamlined application processes could boost loan volumes in competitive digital markets. Hence, financial institutions are recommended to combine automated credit assessment with model validation, independent review, borrower affordability analysis and continuing portfolio quality monitoring.

 DOI: *10.5281/zenodo.23553304*

4.2 Liquidity and Market Risk

In the digital world, information and transactions of a financial nature can be sent across marketplaces at a quick pace. This can improve operational efficiency and price discovery but can also accelerate market reactions during times of uncertainty. When algorithms all react at the same time to similar signals, automated trading systems can exacerbate price swings. Digital communication and mobile transfers in banking could expedite deposit withdrawals and worsen liquidity constraints in a lack of confidence. Thus, liquidity risk management needs to examine how online communication may drastically affect depositors' expectations, consumer behavior, concentrated sources of funding, and the speed of digital transactions. Stress testing should be focused on scenarios with sudden deposit withdrawals, payment disruptions, cyber events, and short-term loss of access to vital systems.

4.3 Third Party and Operational Risks

Operational risk comprises losses due to external events, errors of people, system failures and inadequate processes. Digital banking means more reliance on software, telecommunications, cloud infrastructure, digital identity systems and outsourced service providers. A failure of one essential service might impact other banking services simultaneously. Institutions may also encounter challenges if they cannot readily transfer workloads across providers or where contractual arrangements do not sufficiently disclose security and recovery capabilities. Due diligence must therefore be supplemented by contractual safeguards, monitoring of service levels, control of access, incident notification requirements, contingency planning and exit strategies, as well as third-party risk management. However, financial institutions are accountable for monitoring the risks of outsourced critical activities, even where the underlying infrastructure is maintained by external providers.

5. Cybersecurity as a Core Component of Financial Risk Management

5.1 Key Cyber Risks to Financial Institutions

Essential services and financial information confidentiality is becoming increasingly impacted by Cyber-attacks. Ransomware can have a significant impact on operating systems and customer services; plus phishing attacks could lead to the capture of employee

 DOI: *10.5281/zenodo.23553304*

information. Potential attackers can also raise a third-party provider as a source for accessing a financial institution, exploit flaws in its application programming interfaces or alter payment orders. There is another danger which is when there are also insider threats. Employees or contractors who have access to resources may be persuaded to intentionally manipulate information or unintentionally leave the systems open. The risks may be exacerbated by aspects of identity management and lack of role separation. Thus, cyber risk assessment needs to take into account the systemic relevance of the services concerned, the sensitivity of the data, the legal exposure, the business interruption, the potential financial loss and the probability of the threat.

5.2 Cybersecurity Governance and Accountability

Good cyber security is the basis for clear responsibilities at executive and board level. Senior management must articulate the risk appetite, provide necessary resources, assess material vulnerabilities and ensure that cyber risk is included in the institutional plan. The NIST Cybersecurity Framework 2.0 is a framework that organizes cybersecurity activities around six tasks Govern, Identify, Protect, Detect, Respond and Recover (NIST, 2024). The paradigm offers a practical starting point for building security requirements into organizational risk management. “The Govern function is critically important because cybersecurity decisions involve strategic trade-offs, regulatory needs, organizational accountabilities and third-party interactions. The other components assist with asset identification, prevention, continual monitoring, and incident management and recovery. Institutions should have independent assurance methods as well, such as internal audits, penetration testing, vulnerability assessments, and frequent reviews of security policy.

5.3 Identity Security and Data Protection

Financial organizations acquire a lot of personal and transactional data. A disclosure without authorization could lead to financial loss, identity theft, regulatory fines and damage to reputation. Good data protection processes should include encryption, data minimization, secure storage, access control, data retention policies and secure destruction. Mitigating compromised credentials includes privileged-access control, multi-factor authentication and continuous identity-monitoring. The customers are equally important to protect. Financial firms also need to offer easy means for people to report fraud,

 DOI: *10.5281/zenodo.23553304*

immediately notify people about transactions and provide simple ways to dispute any payments that are not authorized. Security is there to protect clients, not to deny them because they don't have enough knowledge of technology or access to the latest gear.

5.4 Incident Response & Cyber Recovery

There is no cybersecurity solution that can promise that all threats will be averted. Therefore, well-defined processes for event preparation response and recovery systems are critical for financial organizations. A good incident response plan will clearly define the decision makers, the escalation time, the technical response teams, the person accountable for communications, the legal requirements and the manner of storing evidence. The recovery plans shall identify important services and specify acceptable recovery time and recovery point objectives. Routine simulations can be used to test how institutions communicate with clients, restore service, liaise with authorities and operate through alternative channels. Think of ransomware, a breach of one of your payment systems, an outage of your cloud services or the double whammy of more than one supplier going down at the same time. The real measure of cyber resilience is learning from incidents and strengthening controls so that the same vulnerabilities are not exploited again.

6. FinTech Innovation: Opportunities and Emerging Vulnerabilities

6.1 Machine Learning and Artificial Intelligence

Artificial Intelligence can assist with better fraud detection, credit assessment, transaction monitoring, customer service and financial forecasting. Machine-learning algorithms can evaluate huge quantities of data and detect patterns that rule-based systems would overlook. But AI also has the danger of algorithm bias, privacy, model drift and data quality. When economic conditions change, or when their training data are not representative of the population analyzed, automated systems can produce false results. Other generative AI problems include poor management of systems that could lead to the disclosure of personal information, convincing phishing messages and synthetic identity fraud. Good governance of AI requires documentation of the purpose of the model, custody of the data, independent validation of the model, oversight by humans of significant or high-risk decisions, monitoring performance, and providing ways to challenge incorrect results.

 DOI: *10.5281/zenodo.23553304*

6.2 Distributed Ledger Technology and Blockchain

Blockchain and distributed ledger technologies can provide transaction traceability, reconciliation, programmable financial contracts and customized cross-border payment applications. Some of the potential benefits include reduced reliance on certain reconciliation processes and exchange of records. But solutions built on blockchain are not without risk. These exposures can be significant and result from governance failures, operational complexity, legal uncertainty, smart contract vulnerabilities and theft of private keys. The adoption of electronic assets could lead to market instability, liquidity mismatch, custody difficulty and regulatory issues. Financial institutions need to evaluate uses of distributed ledger technology on a case-by-case basis rather than assuming that it will necessarily result in improved security or efficiency.

6.3 Mobile Banking and Digital Payments

Mobile banking and digital payment systems can increase access to financial services and cut transaction costs. They can also help areas with little access to normal bank branches, small companies and remittances in developing economies. However, the fast uptake can also elevate the risk of account takeovers, fraudulent transfers, SIM-related attacks, social engineering and gaps in client verification. To create a safe digital payment ecosystem all these need to be in place: interoperability of reporting systems, consumer education, speedy dispute-resolution procedures, proper authentication, trustworthy identity verification and monitoring of transactions. Innovation, too, must be accessible. Excessive security can keep legitimate customers away, and insufficient security might cause consumers to suffer avoidable losses.

6.4 Cloud computing and technological focus

With cloud computing you could potentially have better recovery capabilities, flexible storage and scalable infrastructure. But the delivery of key services through a limited number of technology suppliers could generate pockets of community failure. Institutions should consider the potential for shifting operations to different locations, provider security, service continuity, portability and data-location demands, and contractual rights. A multi-provider approach may alleviate some concentration concerns but can also increase operational complexity and cost. The right strategy will depend on whether alternate

 DOI: *10.5281/zenodo.23553304*

arrangements, regulatory expectations, critical-service requirements and institutional scale can be maintained.

7. Banking Sector Resilience and Systemic Risk

In the banking system, institutions need to be able to show resilience, withstand financial obligations that are important for public confidence and for the provision of critical services in times of crisis. It is influenced by a combination of capital, liquidity, governance, technology, manpower and external infrastructure. The operational resilience principles of the Basel Committee (BCBS, 2021) promote financial institutions to identify critical activities, establish disruption tolerances, map dependencies and assess their ability to continue provision of essential services. Systemic risk is especially critical when banks share technology providers, payment networks, cloud platforms or financial market infrastructure. The failure of multiple institutions at the same time may lead to operational losses associated with the failure of one common shared service. Cyber events can also be indirectly transmitted. If the institution is compromised it can impact the operations of its counterparties. Ambiguity over the breadth of an assault can sap confidence in the financial system. So, resilience planning has to go beyond the gates of certain institutions. Central banks, financial institutions, communications companies, payment operators and regulators must be able to exchange information and to react to crises in an effective manner. Capital and liquidity buffers are necessary because operational failures can lead to financial losses and funding difficulties. But fixing a faulty payment system or restoring lost data can be costly. Financial robustness and operational resilience are two objectives that reinforce each other.

8. Regulatory Frameworks and International Best Practices

8.1 Operational Risk and Basel Norms

The Basel standards are a globally accepted framework for risk management, capital adequacy and banking regulation. But their importance in the digital world is not only about managing dependencies that could endanger key services. It also touches upon operational risk, governance and internal controls. Institutions need to tie regulatory compliance to actual risk identification, monitoring, testing and remediation, to make compliance more than paperwork exercise.

 DOI: *10.5281/zenodo.23553304*

8.2 Recommendations from the Financial Stability Board

The Financial Stability Board has identified the implications for financial stability of third-party dependencies and cyber incidents. The cooperation is reinforced by the activity of the financial authorities and institutions in responding to and recovering from cyber incidents. The FSB toolbox on management and oversight of third-party risks (from 2023) describes strategies to mitigate the risks from financial institutions' use of third-party service providers.

This advice is particularly relevant where there are a number of systemically important institutions backed by common providers.

8.3 New Regulatory Strategies

Topics including data protection, technology outsourcing, incident reporting and digital operational resilience are attracting increased attention from regulators. One of the major examples of a framework that includes ICT risk management, incident reporting, resilience testing and governance of essential ICT third-party providers is the Digital Operational Resilience Act (DORA) of the European Union, which will come into effect on 17 January 2025. International cooperation is still vital as technological supply chains, digital payment transfers and cyber risks do not stop at national borders. Coordinated responses may be hindered by differences in supervisory capacity and reporting requirements. Therefore, authorities should encourage risk-based and appropriate oversight, harmonized incident classification, information exchange and cross-border cooperation, while minimizing needless hurdles to positive innovation.

9. Financial Risk Management in Emerging Economies: The Bangladesh Context

Developing countries have a particular mix of opportunities and constraints. "Digital financial services can promote financial inclusion, lower the cost of remittances, empower small businesses and eliminate geographical barriers to banking. However, they may also be more exposed due to lack of digital expertise, inadequate cybersecurity resources, fragmented data systems, and reliance on external technology vendors.

In Bangladesh, the emergence of mobile financial services, digital payments, agent banking and internet-based banking has broadened the range of financial goods. Their

 DOI: *10.5281/zenodo.23553304*

impact on financial inclusion is sustainable if clients trust the products, they have the right infrastructure, regulators are effective, and they can avoid fraud.

Financial institutions need to strengthen such areas as authentication, transaction monitoring, secure software development, data governance, incident tracking and client awareness. Special attention is paid to phishing, fraudulent mobile transactions, account hijacking and exploitation of personal data.

Bangladesh Bank and other relevant authorities should develop proportionate cybersecurity regulations, undertake regular supervisory assessments, coordinate incident response, and develop appropriate stress-testing standards to strengthen resilience. Commercial banks, mobile financial services providers, telecommunications carriers and technology suppliers may combine to improve threat intelligence and response capability. Less complex security systems may be limited by the technological and budgetary constraints of smaller institutions. Such shortfalls can be resolved by supervisory advice, consistent documenting of events, industry-wide training and collaboration in security services. Financial inclusion projects should realize that financial stability is not the same as digital access. Customers want to see that fraud prevention is visible and clear, that there are clear complaint channels in place and that processes are fair when dealing with disputed transactions.

10. Findings and Discussion

The study showed five noteworthy conclusions.

First, we are transforming the architecture of financial risk. In contrast, digital transformation results in the increased interconnectivity of financial institutions, technology infrastructure and external service providers. So, we need to estimate credit, liquidity, operational and cyber risk in one framework.

Second, cybersecurity is a strategic concern for financial stability rather than a technical requirement as such. The fallout might damage consumer confidence, company image, market stability and business continuity.

Third, FinTech innovations can enhance efficiency and inclusivity, but these gains are conditional on good governance. The usage of electronic payment systems, blockchain

 DOI: *10.5281/zenodo.23553304*

technology, cloud computing services and artificial intelligence models should be controlled to the extent that is appropriate to their complexity and relevance.

Fourth, banking resilience means not only avoiding failure but also being ready for it. Some of the major features which aid in the long-term process of risk management are these. Incident response. Assessment of recovery procedures. Critical services identification. Contingency Operations Procedures. Good communication.

5. Regulation and information sharing has to be harmonized, especially where institutions operate across borders or share common technology providers. Developing countries can increase resilience through enhancing monitoring, knowledge exchange, consumer education and setting acceptable norms. The results suggest a comprehensive view on risk management that considers financial, technological, operational and strategic challenges at the same time. The method has the potential to enhance organizational readiness and diminish ad hoc decision making. Money invested in technology does not always ensure the stability of the system. Within the institution data quality is important for effective risk management, continual assessment of controls, accountability of leadership, people competency and company culture.

11. Recommendations

Based on the analysis, the following recommendations are made:

1. Establish a robust digital risk governance structure. Banks should integrate cyber, technological, model, operational and third-party risk into their enterprise-wide risk management frameworks. “Senior management and boards should receive regular updates on their risk appetite, recovery readiness, key vulnerabilities and events.
2. Improve cybersecurity. Institutions should employ multi-factor authentication, encryption, secure software development, vulnerability management, network segmentation, and constant threat monitoring. They should also enforce least privilege of access.
3. Adopt risk-based AI governance. AI applications should be independently validated and assessed for bias and explainability and monitored continuously for performance.” But humans should still be making some big decisions.

 DOI: *10.5281/zenodo.23553304*

4. Strengthen third party risk management. Banks should assess the durability of critical vendors, identify service dependencies, put in place clear contractual obligations and develop practical exit and substitution plans.

5. Continuous Testing of Resilience. Scenario-based exercises to evaluate the impact of cyber-attacks, payment failures, cloud outages, data loss and unplanned deposit outflows. Testing will include evaluation of institutional decision making and technology recovery.

6. Create operational and financial reserves. Institutions should have access to critical systems, backup facilities and recovery resources in the event of disruptions and hold adequate capital and liquidity positions.

7. Raise customer and employee awareness. Ongoing training should include phishing, social engineering, data security, incident escalation and safe digital habits. The customer education should be appropriate and available to all levels of digital proficiency.

8. Strengthen regulatory cooperation. “Financial institutions and supervisors need to have consistent processes for incident reporting, encourage cross-border information sharing and coordinate their response to incidents that affect more than one business.

9. Focus on capacity building in developing countries. Policymakers should also encourage affordable security infrastructure, shared technological skills, literacy and supervisory training, with sufficient safeguards for consumer protection and financial stability.

10. Resilience is a process. Institutions should have measures of performance in recovery, frequency of incidents, effectiveness of controls, concentration of vendors and remediation progress. Progress should continue to be guided by lessons learned from actual incidents and exercises.

12. Conclusion

In the digital era, financial risk management requires a paradigm shift from traditional, siloed risk categories to an integrated approach that recognizes the interdependence of

 DOI: *10.5281/zenodo.23553304*

technology infrastructure and monetary systems. The way banks feel and transmit risk has changed substantially, due to cyber risks, FinTech innovation, third party dependencies and digital transaction networks. The use of new digital technology has tremendous benefits in terms of better fraud detection, faster transactions, more financial inclusion and improved efficiency. These benefits are short lived without institutional preparedness, appropriate use of data, adequate control and excellent governance. Cybersecurity should be considered as an important component of financial stability, and the evaluation of FinTech applications should be based on their potential benefits, operational complexity and exposure to developing vulnerabilities. Banking resilience is a continual learning, identifying, responding, recovering and preventing. In emerging economies like Bangladesh, the challenge is to scale up consumer protection, supervisory capacity, cybersecurity awareness and operational reliability while developing digital financial services. Financial institutions, regulators, technology providers and consumers might join forces to build a more inclusive and secure financial system. "Financial risk management in the digital era is not about killing innovation or getting rid of risk entirely. The purpose is to absorb shocks, to build resilience that allows financial institutions to continue to provide critical services, to protect public confidence and to innovate prudently in a changing economic and technological environment.

References

1. Arner, D.W., Barberis, J. and Buckley, R.P. (2016) 'The evolution of FinTech: A new post-crisis paradigm?', Georgetown Journal of International Law, 47(4), pp. 1271–1319.

2. Basel Committee on Banking Supervision (BCBS) (2021) Principles for Operational Resilience. Basel: Bank for International Settlements.

3. Basel Committee on Banking Supervision (BCBS) (2021) Revisions to the Principles for the Sound Management of Operational Risk. Basel: Bank for International Settlements.

4. Basel Committee on Banking Supervision (BCBS) (2023) The Basel Framework. Basel: Bank for International Settlements.

 DOI: *10.5281/zenodo.23553304*

5. Bouveret, A. (2018) ‘Cyber risk for the financial sector: A framework for quantitative assessment’, IMF Working Paper, WP/18/143. Washington, DC: International Monetary Fund.

6. European Parliament and Council of the European Union (2022) Regulation (EU) 2022/2554 on digital operational resilience for the financial sector. Official Journal of the European Union.

7. Financial Stability Board (FSB) (2020) Enhancing Third-Party Risk Management and Oversight: A Toolkit for Financial Institutions and Financial Authorities. Basel: Financial Stability Board.

8. Financial Stability Board (FSB) (2023) Enhancing Third-Party Risk Management and Oversight: A Toolkit for Financial Institutions and Financial Authorities. Basel: Financial Stability Board.

9. Financial Stability Board (FSB) (2023) Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence. Basel: Financial Stability Board.

10. International Monetary Fund (IMF) (2024) Global Financial Stability Report: The Last Mile—Financial Vulnerabilities and Risks. Washington, DC: International Monetary Fund.

11. National Institute of Standards and Technology (NIST) (2024) The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: U.S. Department of Commerce.

12. Organisation for Economic Co-operation and Development (OECD) (2021) G20/OECD Report on Financial Consumer Protection. Paris: OECD.

13. World Bank (2022) The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19. Washington, DC: World Bank.

14. World Economic Forum (2024) The Global Risks Report 2024. Geneva: World Economic Forum.

 DOI: *10.5281/zenodo.23553304*