BG Pulse Journal USA
ISSN:1947-2536 http://www.bgpulseusa.com/index.php/bg
BG PULSE JOURNAL

ENSURING BANKING SYSTEM SECURITY AMID THE DIGITALIZATION OF COMMERCIAL BANKS: EVIDENCE FROM UZBEKISTAN AND INTERNATIONAL PRACTICE

Parpiboyeva Lobar Abdikomilovna
Doctoral Researcher (PhD), Tashkent International University
Doi: https://doi.org/10.5281/zenodo.22642103

Abstract. The accelerated digitalization of commercial banks expands financial inclusion, reduces transaction costs, and improves service continuity, while simultaneously increasing exposure to cyberattacks, technology failures, fraud, data leakage, and third-party concentration. This study evaluates how banking-system security can be strengthened under rapid digital transformation, using Uzbekistan as the focal case and Estonia under the European Union framework, Singapore, and the United Kingdom as comparative benchmarks. The research applies institutional comparison, content analysis of regulatory documents, descriptive analysis of official banking statistics, and a risk-control mapping method. Central Bank data show that the value of mobile-banking transactions by individuals in Uzbekistan rose from UZS 397.0 trillion in 2024 to UZS 645.6 trillion in 2025, an increase of approximately 62.6 percent. During 2025, the regulator conducted 37 information-security and cybersecurity reviews, reduced the time required to analyse fraud cases from three working days to four hours through platform integration, and included more than 30 information systems of eight commercial banks in the register of critical information infrastructure. The comparative results indicate that Uzbekistan has developed important institutional foundations, including the Law on Cybersecurity and the CERT-CBU sectoral centre, but further progress is needed in harmonised incident reporting, threat-led penetration testing, third-party technology oversight, service-level impact tolerances, and sector-wide recovery exercises. The article proposes a Digital Banking Security and Resilience Framework based on six mutually reinforcing pillars: governance, preventive control, continuous detection, coordinated response, tested recovery, and systemic learning.

Keywords: banking digitalization; cybersecurity; operational resilience; cyber risk; payment systems; anti-fraud; critical information infrastructure; Uzbekistan.

INTRODUCTION

Digital transformation has changed the economic model of commercial banking. Mobile applications, instant payments, application programming interfaces (APIs), cloud services, biometric identification, artificial intelligence, and remote onboarding allow banks to serve customers at lower marginal cost and at any time. At the same time, the security perimeter is no longer limited to a bank's internal network. It now includes customers' mobile devices, telecommunications operators, payment organisations, fintech partners, cloud and software providers, outsourced service centres, and interconnected public databases. Consequently, a weakness in one participant can interrupt services or transmit losses across the entire financial system.

Cybersecurity in banking should therefore be interpreted more broadly than the prevention of unauthorised access. A secure banking system must preserve the confidentiality, integrity and availability of data; protect customer funds; maintain critical services during disruption; restore operations within acceptable time limits; and retain public confidence. The Basel Committee on Banking Supervision (BCBS, 2021) captures this broader objective through the concept of

operational resilience - the ability of a bank to deliver critical operations through disruption. The IMF (2024) similarly treats cyber risk as a macrofinancial concern because operational interruption, correlated technology dependence and a loss of trust can amplify an initially local incident.

The issue is particularly relevant for Uzbekistan, where the scale of remote financial services has increased rapidly. According to the Central Bank of the Republic of Uzbekistan (CBU, 2026a), mobile-banking transactions by individuals reached UZS 645.6 trillion in 2025, while bank cards in circulation rose to 68.2 million and electronic wallets to 24.8 million. This expansion increases the social and economic cost of any interruption and raises the attractiveness of the sector to fraudsters. The policy task is not to slow innovation, but to ensure that the marginal growth of digital services is accompanied by a corresponding increase in control capacity and recovery readiness.

The purpose of this article is to identify institutional and technological mechanisms for ensuring banking-system security during the digitalization of commercial banks. The study addresses three questions: (1) how does rapid digitalization alter the structure of banking-system risk; (2) which elements of international practice are transferable to Uzbekistan; and (3) what integrated framework can align innovation, cybersecurity and operational resilience? The contribution of the study is a six-pillar Digital Banking Security and Resilience Framework (DBSRF) that connects bank-level controls with sector-level supervision and continuous learning.

LITERATURE REVIEW

The literature has gradually shifted from a narrow information-security perspective to a systemic resilience perspective. Early approaches concentrated on technical controls and the expected loss of individual institutions. Kopp, Kaffenberger and Wilson (2017) argued that cyber risk combines operational, legal and reputational channels and that limited data complicate conventional risk quantification. Bouveret (2018) proposed a quantitative framework in which cyber losses depend not only on attack frequency but also on exposure, security investment and institutional interconnectedness. These studies established that cyber risk cannot be managed solely as an information-technology problem.

Later research focused on the network structure of finance. Aldasoro et al. (2020) showed that cyber costs are shaped by digital dependence and that the financial sector is exposed through common technologies and service providers. The IMF's Global Financial Stability Report (2024) reports that the number of cyberattacks has almost doubled compared with the pre-pandemic period; nearly one-fifth of recorded incidents affect financial firms, and extreme losses can be very large even though most direct losses are relatively small. Thus, low-frequency but high-impact events and the transmission of operational disruption deserve the same attention as average loss.

Regulatory scholarship and standards emphasise governance, mapping and testing. The CPMI-IOSCO (2016) guidance identifies governance, identification, protection, detection, response and recovery as the core of cyber resilience for financial market infrastructures. The BCBS (2021) adds mapping of critical operations and dependencies, business-continuity testing, third-party dependency management and lessons learned. NIST (2024) strengthens this logic by adding 'Govern' as a distinct function in the Cybersecurity Framework 2.0, making board accountability and risk appetite explicit.

International practice also highlights supervisory coordination. The EU Digital Operational Resilience Act (DORA) integrates ICT-risk management, incident classification and reporting, resilience testing, third-party oversight and information sharing within one legal framework.

Singapore's Monetary Authority uses technology-risk management guidelines, cyber-hygiene requirements and strong expectations for board responsibility, secure development, testing and vendor management (MAS, 2021). In the United Kingdom, the Bank of England, PRA and FCA require firms to identify important business services, set impact tolerances and demonstrate that services can remain within those tolerances under severe but plausible scenarios (Bank of England, 2021).

Despite a growing Uzbek literature on digital banking and payment expansion, fewer studies integrate cybersecurity, anti-fraud controls, critical infrastructure, third-party concentration and operational recovery in one system-level model. This study addresses that gap by linking official evidence from Uzbekistan to benchmark regulatory mechanisms and by distinguishing preventive security from resilience. Prevention seeks to reduce the probability of compromise; resilience seeks to limit the social and financial impact when preventive controls fail.

RESEARCH METHODOLOGY

The study uses a mixed qualitative-descriptive design. First, institutional content analysis is applied to Uzbekistan's Law No. LRU-764 'On Cybersecurity', the 2025 Annual Report of the Central Bank, BCBS operational-resilience principles, DORA, MAS technology-risk guidance, the UK operational-resilience framework, the FSB Format for Incident Reporting Exchange (FIRE), and NIST Cybersecurity Framework 2.0. Second, descriptive analysis is used to measure the growth of selected digital-banking indicators in Uzbekistan. Third, a structured benchmark compares four jurisdictions across six policy dimensions. Fourth, a likelihood-impact matrix links major digital threats to controls and supervisory responses.

The comparative units are Uzbekistan, Estonia as an EU member applying DORA, Singapore and the United Kingdom. These benchmarks were selected because they represent different but relevant models: a fast-digitising emerging economy; an advanced digital state operating under harmonised EU requirements; a highly connected Asian financial centre; and a mature principle-based supervisory system. Comparison is based on publicly documented requirements rather than self-reported cybersecurity effectiveness.

The main descriptive growth rate is calculated as $g = ((V2025 / V2024) - 1) \times 100$, where V denotes the annual value of mobile-banking transactions. Using CBU data, $g = ((645.6 / 397.0) - 1) \times 100 = 62.6$ percent. The benchmark assessment uses three transparent categories: established, developing and limited/not explicit in the reviewed public framework. These categories indicate the maturity of documented regulation and supervisory practice; they are not a ranking of actual national cyber defence.

Table 1.

Research design and analytical instruments[1]

Method	Evidence base	Analytical purpose
Document analysis	Laws, supervisory standards, annual reports	Identify formal responsibilities and control requirements
Descriptive statistics	CBU indicators for 2024-2025	Measure the scale and speed of digital-service expansion

[1] *Compiled by the author.*

Method	Evidence base	Analytical purpose
Comparative benchmark	Uzbekistan, Estonia/EU, Singapore, United Kingdom	Identify transferable institutional practices
Risk-control mapping	Threat, impact, control and supervisory response	Convert findings into a practical security architecture

RESULTS AND DISCUSSION

The CBU's 2025 results demonstrate that digital finance is becoming critical national infrastructure rather than an auxiliary delivery channel. Mobile-banking transactions by individuals rose from UZS 397.0 trillion to UZS 645.6 trillion. The number of bank cards in circulation reached 68.2 million, payments through 430,000 terminals totalled UZS 460.3 trillion, and the number of ATMs and self-service kiosks exceeded 40,000. Payment-organisation transactions reached UZS 412.4 trillion, while 24.8 million electronic wallets were active by 1 January 2026 (CBU, 2026a).

The growth of transaction value has two security consequences. First, the expected loss associated with account takeover, social engineering and fraudulent lending increases even if the probability of an individual event is unchanged. Second, the availability of payment and mobile-banking systems becomes systemically important: a short disruption can affect households, merchants, government payments and liquidity flows simultaneously. Security investment should therefore be linked to service criticality, transaction growth and recovery objectives rather than treated as a fixed administrative budget.

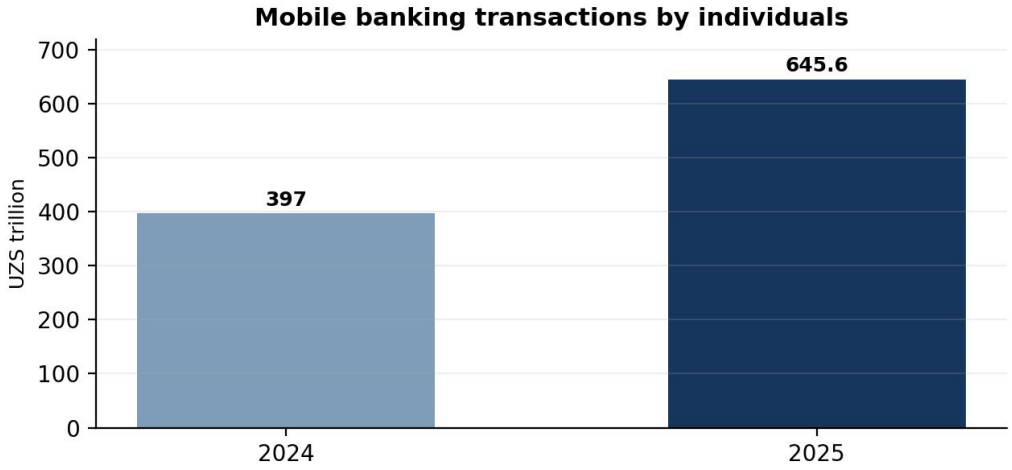


Figure 1. Growth of mobile-banking transactions by individuals in Uzbekistan[2]

[2] *CBU (2026a). The calculated annual increase is approximately 62.6 percent.*

Table 2.

Selected indicators of Uzbekistan's digital banking and security environment, 2025[3]

Indicator	2025 result	Security implication
Mobile-app transactions by individuals	UZS 645.6 tn; 1.6x increase	Higher exposure and systemic importance of mobile channels
Bank cards in circulation	68.2 million; +10%	Larger authentication and card-fraud perimeter
Electronic wallets	24.8 million; +20%	Need for wallet monitoring and identity controls
Cybersecurity reviews	37 reviews	Active supervisory verification of compliance
Fraud-case analysis time	Reduced from 3 working days to 4 hours	Faster cross-institution detection and response
Critical systems registered	30+ systems in 8 banks	Recognition of systemically important digital assets
Banks penalised for security deficiencies	3 banks; UZS 115 million	Enforcement exists, but deterrence should be risk-sensitive

Uzbekistan has also strengthened the protective layer. In 2025, controls included device-bound one-time passwords, session anti-fraud analysis, malware alerts and biometric identification for sensitive mobile-app events. Integration of banks, payment-system operators and credit bureaus with the CBU's unified platform reduced fraud-analysis time from three working days to four hours. The regulator conducted 37 reviews and imposed UZS 115 million in sanctions on three banks with identified deficiencies. More than 30 information systems belonging to eight banks were added to the critical-information-infrastructure register.

These measures are substantive, yet the evidence also suggests the need to move from institution-by-institution compliance toward system-wide resilience. A register of critical systems should be complemented by dependency mapping: which critical services rely on the same data centre, telecom operator, cloud provider, software component or identity service? Without such mapping, each bank may appear individually protected while the sector remains exposed to a common point of failure.

[3] *CBU (2026a).*

Table 3.

Comparative regulatory mechanisms for digital banking security[4]

Policy dimension	Uzbekistan	Estonia / EU	Singapore	United Kingdom
Integrated ICT-risk framework	Developing: general cyber law plus CBU requirements	Established under DORA	Established under MAS TRM	Established through PRA/FCA rules
Harmonised incident reporting	Developing; sectoral electronic collection exists	Established: classified major ICT incidents	Established supervisory notification	Established notification expectations
Threat-led penetration testing	Not yet explicit sector-wide	Established for designated entities	Advanced testing expected for critical systems	Established through CBEST
Critical third-party oversight	Developing through general and contractual controls	Established: registers and oversight of critical ICT providers	Established vendor and outsourcing controls	Established outsourcing and concentration focus
Impact tolerances for critical services	Limited/not explicit in reviewed public framework	Developing through resilience and recovery requirements	Embedded in continuity and recovery expectations	Established for important business services
Sector coordination and exercises	CERT-CBU and unified anti-fraud platform	EU/ECB coordination and stress testing	MAS-led sector coordination	Public-private exercises and CBEST ecosystem

Estonia benefits from DORA's harmonised structure. The regulation, applicable from 17 January 2025, integrates ICT governance, incident management, testing, third-party risk and information sharing. A particularly transferable feature is the register of contractual arrangements with ICT providers, because it makes concentration and substitutability visible to both banks and supervisors. The ECB's 2024 cyber-resilience stress test, covering 109 banks, further illustrates the value of testing response and recovery after a severe but plausible attack rather than assuming preventive controls will always succeed (ECB, 2024).

[4] Author's analysis based on CBU (2026a), DORA (EU, 2022), MAS (2021), Bank of England (2021), and ECB (2024). Categories describe public frameworks, not realised security outcomes.

Singapore's approach is notable for combining prescriptive cyber hygiene with risk-based governance. MAS guidance assigns responsibility to boards and senior management, requires inventory and protection of critical systems, secure software development, vulnerability management, monitoring, incident response and strong third-party controls. This approach is relevant to Uzbekistan because an expanding fintech ecosystem requires consistent minimum controls without eliminating proportionality for smaller institutions.

The United Kingdom contributes the concept of impact tolerance. Banks identify important business services and define the maximum tolerable level of disruption. They then map the people, processes, technology, facilities, data and third parties required to provide each service. This changes management attention from whether a server is running to whether customers can still make essential payments, access funds or receive time-critical services. For Uzbekistan, impact tolerances could be introduced first for instant payments, card authorisation, mobile-banking access, interbank settlement and customer identity services.

The comparison indicates that Uzbekistan's strongest features are sector-specific coordination through CERT-CBU, a unified anti-fraud platform, the registration of critical infrastructure, 24/7 monitoring and growing supervisory enforcement. The principal development opportunities are standardised incident data, sector-wide threat-led testing, explicit third-party concentration oversight, service-level impact tolerances and regular recovery exercises that include banks, payment operators, telecom providers and critical vendors.

Table 4.

Risk-control matrix for a digitalised banking system[5]

Threat	Likelihood / impact	Priority controls	System-level response
Phishing, social engineering and account takeover	High / High	Phishing-resistant MFA, device binding, behavioural analytics, transaction confirmation	Shared fraud intelligence; rapid blocking and customer reimbursement rules
Fraudulent digital lending and synthetic identity	High / High	Liveness checks, cross-bank credit-request checks, velocity rules, identity graph analytics	Real-time credit-bureau integration and telecom anti-fraud
Ransomware and destructive malware	Medium / Very high	Segmentation, privileged-access management, immutable backups, endpoint detection	Sector crisis protocol; offline recovery and liquidity contingency tests
API, cloud and software-supply-chain compromise	Medium / Very high	Secure SDLC, API gateways, secrets management, SBOM, vendor assurance	Critical-provider register, concentration limits and exit plans
DDoS and	High / High	Traffic scrubbing,	Coordinated telecom

[5] Compiled by the author using BCBS (2021), NIST (2024), IMF (2024), and CBU (2026a).

Threat	Likelihood / impact	Priority controls	System-level response
infrastructure outage		redundancy, capacity testing, multi-provider connectivity	response and alternative payment channels
Insider abuse and data leakage	Medium / High	Least privilege, segregation of duties, DLP, logging and user analytics	Common investigation protocol and accountable disclosure
AI-enabled fraud and deepfakes	Rising / High	Risk-based biometrics, challenge-response checks, model monitoring, human escalation	Shared detection models and public awareness campaigns

Table 4 demonstrates that no single technology can secure digital banking. Strong authentication is ineffective if customer devices are compromised; backups are insufficient if restoration is not tested; and bank-level controls cannot eliminate a common cloud or telecommunications failure. Security therefore requires defence in depth and coordinated recovery. A risk-based architecture should prioritise critical services and high-impact dependencies, because uniform control spending can leave systemically important processes underprotected.

Artificial intelligence creates both defensive and offensive effects. Banks can use machine learning to detect unusual device, session and transaction behaviour, but attackers can automate reconnaissance, personalise phishing and generate convincing synthetic identities or deepfake instructions. Model governance should therefore include data quality, explainability appropriate to the decision, false-positive monitoring, adversarial testing, human escalation and restrictions on autonomous high-risk actions.

Proposed digital banking security and resilience framework

Based on the empirical and comparative findings, the study proposes the DBSRF. Its central principle is that digital growth and control capacity must be managed as a coupled system. Each new product, API, outsourced service or automated decision should pass through six mutually reinforcing pillars:

- Govern: The board approves cyber-risk appetite, assigns accountable executives, links risk indicators to critical services and requires independent assurance. Security metrics should include service availability, fraud loss, detection time, recovery time, unresolved critical vulnerabilities, third-party concentration and exercise findings.
- Prevent: Banks apply secure-by-design architecture, zero-trust access, phishing-resistant multifactor authentication for high-risk actions, encryption, segmentation, privileged-access management, secure software development, vulnerability remediation and customer-protection controls.
- Detect: Continuous monitoring combines SIEM, endpoint and network detection, application telemetry, threat intelligence, behavioural analytics and cross-institution anti-fraud signals. Detection quality is measured by coverage and time-to-detect, not merely by the number of alerts.

- Respond: A harmonised incident taxonomy, severity thresholds and reporting template allow banks, CERT-CBU, payment operators and law-enforcement bodies to share essential information quickly. The FSB FIRE format can serve as a reference for common data fields and cross-border interoperability.
- Recover: Each critical service has an approved impact tolerance, recovery-time objective, recovery-point objective, tested backups, alternative communication channel and decision authority. Exercises must test loss of core data, unavailability of a major vendor and simultaneous fraud pressure.
- Learn: Post-incident reviews, red-team findings, supervisory observations and sector exercises feed into control changes, staff training and regulation. Anonymised sector loss and incident data support scenario calibration and investment decisions.

The framework should operate at three levels. At the bank level, it strengthens governance, engineering and recovery. At the ecosystem level, it covers payment organisations, fintech companies, telecommunications operators and technology vendors. At the supervisory level, it supports common reporting, thematic reviews, sector tests and concentration analysis. This layered approach reduces the risk that responsibility will fall between institutions.

Policy recommendations for Uzbekistan

First, the CBU should adopt a consolidated digital operational-resilience regulation for banks and payment institutions. The regulation should integrate ICT-risk governance, incident reporting, resilience testing, third-party risk, critical-service mapping and information sharing. Consolidation would reduce fragmented compliance and align management attention with customer and systemic outcomes.

Second, a unified incident-reporting taxonomy should be introduced and aligned, where practical, with the FSB FIRE format. Reporting thresholds should reflect service downtime, customers affected, financial loss, data sensitivity, geographic reach and potential systemic spillover. Initial notification should be rapid and followed by structured intermediate and final reports. The objective is not administrative volume, but a comparable dataset for early warning and sector learning.

Third, threat-led penetration testing should be introduced proportionally. Systemically important banks and payment infrastructures should undergo periodic intelligence-led red-team exercises with independent testers and controlled supervisory participation. Smaller institutions can use pooled exercises and standard scenarios. Remediation should be tracked to closure, while sensitive technical results remain protected.

Fourth, critical third-party risk should become a direct supervisory priority. Banks should maintain complete registers of ICT contracts, classify critical providers, assess substitutability, define exit plans, test data portability and report material concentration. The CBU should map common dependencies across the sector and coordinate with telecommunications and cybersecurity authorities. Contractual outsourcing must not outsource accountability.

Fifth, service-level impact tolerances should be established for essential banking functions. Instead of relying only on server recovery targets, institutions should determine how much disruption customers and the economy can tolerate. The CBU can issue common principles while allowing banks to calibrate thresholds to their scale and business model.

Sixth, customer protection should combine technology and behavioural intervention. Banks should use risk-based transaction friction, cooling-off periods for unusual high-value transfers, trusted-beneficiary controls, plain-language warnings, 24/7 emergency blocking and rapid

complaint channels. Shared campaigns should focus on social engineering, remote-access applications, OTP disclosure and fraudulent credit. Customer awareness is a control layer, but it must not replace bank responsibility for secure design.

Seventh, the effectiveness of supervision should be measured with outcome indicators. Recommended sector indicators include median time to detect and contain severe incidents; percentage of critical services tested under severe scenarios; share of critical providers with viable exit plans; ageing of critical vulnerabilities; fraud losses per unit of digital transaction value; and the percentage of exercise findings remediated on schedule. Risk-sensitive sanctions and remediation orders should reflect the potential impact of deficiencies rather than a uniform penalty scale.

CONCLUSION

Digitalization strengthens the efficiency and accessibility of commercial banking, but it also transforms operational weaknesses into potential threats to financial stability. Evidence from Uzbekistan shows rapid growth in mobile transactions, cards and electronic wallets alongside meaningful progress in anti-fraud integration, critical-infrastructure registration, monitoring and supervisory reviews. These measures create a strong foundation, yet digital scale requires a parallel transition from isolated technical compliance to measurable operational resilience.

International comparison shows that the most transferable mechanisms are an integrated ICT-risk framework, harmonised incident reporting, threat-led testing, critical third-party oversight, mapping of important business services, explicit impact tolerances and system-wide exercises. The proposed DBSRF unites these mechanisms through governance, prevention, detection, response, recovery and learning. Its implementation would allow Uzbekistan to expand digital banking without treating innovation and security as competing objectives.

The study is limited by reliance on public regulatory documents and aggregate statistics; confidential incident and loss data were unavailable. Future research should construct a bank-level panel dataset linking digital intensity, cybersecurity investment, service downtime, fraud losses and customer trust. Empirical testing could then estimate whether stronger resilience maturity reduces operational losses and improves the stability of digital financial intermediation.

A phased implementation sequence is recommended to convert these conclusions into measurable supervisory and institutional change.

Table 5. Proposed implementation roadmap for Uzbekistan[6]

Phase	Regulatory priority	Bank-level action	Measurable output
I: 2026-2027	Unified incident taxonomy; critical-service inventory; baseline third-party register	Map services, assets, data flows and key providers; approve impact tolerances	100% of critical services and material ICT contracts registered
II: 2027-2028	Threat-led testing standard; sector scenarios; harmonised recovery	Run severe-but-plausible exercises; remediate critical gaps; test immutable	All systemically important institutions tested and findings

[6] Source: Developed by the author on the basis of the DBSRF.

Phase	Regulatory priority	Bank-level action	Measurable output
	reporting	backups	tracked
III: 2028-2030	Sector concentration dashboard; cross-border FIRE interoperability; outcome-based supervision	Automate risk indicators and share anonymised threat intelligence	Lower detection/recovery times and fraud loss per unit of digital value

REFERENCES

1. Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T. (2020). The drivers of cyber risk. BIS Working Papers, No. 865. Bank for International Settlements. https://www.bis.org/publ/work865.htm
2. Bank of England (2021). Operational resilience: Impact tolerances for important business services. Policy Statement PS6/21. https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper
3. Basel Committee on Banking Supervision (BCBS) (2021). Principles for operational resilience. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.htm
4. Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. IMF Working Paper WP/18/143. https://doi.org/10.5089/9781484360750.001
5. Central Bank of the Republic of Uzbekistan (CBU) (2026a). Annual Report 2025. Tashkent. https://cbu.uz/en/publications/annual-report/
6. Central Bank of the Republic of Uzbekistan (CBU) (2026b). The Cybersecurity Center CERT-CBU. https://cbu.uz/uz/cert/
7. Committee on Payments and Market Infrastructures and IOSCO (CPMI-IOSCO) (2016). Guidance on cyber resilience for financial market infrastructures. BIS. https://www.bis.org/cpmi/publ/d146.htm
8. European Central Bank (ECB) (2024). ECB concludes cyber resilience stress test. 26 July 2024. https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240726~06d5776a02.en.html
9. European Union (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union, L 333, 1-79. https://eur-lex.europa.eu/eli/reg/2022/2554/oj
10. Financial Stability Board (FSB) (2025). Format for Incident Reporting Exchange (FIRE): Final report. https://www.fsb.org/2025/04/format-for-incident-reporting-exchange-fire-final-report/
11. International Monetary Fund (IMF) (2024). Cyber risk: A growing concern for macrofinancial stability. Global Financial Stability Report, Chapter 3. https://www.imf.org/-/media/files/publications/gfsr/2024/april/english/ch3.pdf
12. Kopp, E., Kaffenberger, L. and Wilson, C. (2017). Cyber risk, market failures, and financial stability. IMF Working Paper WP/17/185. https://doi.org/10.5089/9781484313787.001

13. Monetary Authority of Singapore (MAS) (2021). Technology Risk Management Guidelines. https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines
14. National Institute of Standards and Technology (NIST) (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29
15. Republic of Uzbekistan (2019). Law No. LRU-578 On Payments and Payment Systems. National Database of Legislation. https://lex.uz/
16. Republic of Uzbekistan (2022). Law No. LRU-764 On Cybersecurity, 15 April 2022. https://lex.uz/uz/docs/6997403