|  |
| --- |
|  |
| Technology & Operations Risk Management Framework for Payment Institutions |
|  |

|  |
| --- |
| Payment Systems Policy & Oversight Department |



**Table of Contents**

Contents

[1. Introduction 3](#_Toc191565401)

[2. Objective 3](#_Toc191565402)

[3. Authority 3](#_Toc191565403)

[4. Applicability 3](#_Toc191565404)

[5. Definitions 4](#_Toc191565405)

[6. Technology Policy & Governance 4](#_Toc191565406)

[7. Information/ Cybersecurity 5](#_Toc191565407)

[8. Fraud Risk Management 8](#_Toc191565408)

[9. Outsourcing of Technology 9](#_Toc191565409)

[10. Disaster Recovery and Business Continuity 10](#_Toc191565410)

[11. Technology Audit 11](#_Toc191565411)

## Introduction

The evolving role of technology and automation in the payment services has become increasingly complex. A growing number of payment institutions are leveraging technological advancements to offer innovative products, deliver fast and efficient service at affordable prices and venture into new markets. Moreover, technology drives the efficiency of operations and financial soundness of these institutions by improving overall decision-making process. As technology becomes integral to PIs’ operations, inadequate management of technology risk can heighten operational vulnerabilities that this Framework seeks to mitigate.

The framework is aimed to enable PIs to keep abreast with the rapid and widespread adoption in the financial services industry and consequently strengthen existing regulatory framework for technology risk supervision. This framework shall be integrated with the PI(s)' overall enterprise risk management program. SBP expects PI(s) to have the knowledge and skills necessary to understand and effectively manage technology risks. The framework is broadly based on international standards and recognized principles of international best practices.

## Objective

The objective of the *Technology and Operations Risk Management Framework*, hereinafter referred to as the ‘Framework’ is to provide baseline requirements for Payment Institutions (PIs) to govern and manage risks related to the (i) use of technology in their operations, (ii) outsourcing of technology services to third parties (other than cloud outsourcing) and (iii) digital financial frauds.

## Authority

This Framework is being issued in exercise of the powers conferred upon SBP under Payment Systems and Electronic Fund Transfers Act, 2007.

## Applicability

1. The requirements of this ‘Framework’ shall be applicable on all authorized Payment Systems Operators/Payment Service Providers (PSOs/PSPs), Electronic Money Institutions (EMI) and any other entity regulated/licensed/authorized by SBP under Payment System & Electronic Fund Transfers Act, 2007 (hereinafter collectively referred to as ‘**Payment Institution(s) (PIs)**’).
2. At the In-Principle Approval (IPA) stage, PI(s) shall provide written assurances including detailed plans regarding their intent and ability to comply with the requirements of this framework.
3. For Pilot Operations stage, PI(s) shall be able to demonstrate reasonable operational readiness in terms of technology operations.
4. For Commercial Operations, PI(s) shall, at all times, be able to demonstrate compliance with the requirements of this framework.
5. PI(s) shall be responsible to ensure that their technology stack including people, processes and technology operations and associated infrastructure are aligned with this framework latest by December 31, 2025.

## Definitions

Wherever used in this Framework, the following terms shall have the following meanings:

* **Electronic Money Institutions (EMI):** as defined in Section 24 of PS&EFT Act of 2007.
* **Payment Systems Operators/Payment Service Providers (PSOs/PSPs):** As defined in the “Rules for Payment System Operators and Payment Service Providers”.
* **In-Principle Approval (IPA):** As defined in Section 8, sub-section I, of Regulations for Electronic Money Institutions (EMIs).
* **Pilot Operations**: As defined in Section 8, Sub-Section I, of Regulations for Electronic Money Institutions (EMIs).
* **Commercial operations:** As defined in Section 8, Sub-Section I, of Regulations for Electronic Money Institutions (EMIs)
* **Technology Risk**: Technology risk, also known as IT risk, encompasses any risk to information technology, data, or applications that negatively impact business operations. This includes cybersecurity risks that may be incurred by an institution as a consequence of connecting its IT infrastructure to the internet
* **FTDH**: 1LINK introduced 1IBFT Fraudulent Transaction Dispute Handling to provide enhanced monitoring and 24×7 dispute lodgment for fraudulent transactions between banks for end to end dispute resolution.

## Technology Policy & Governance

PI(s) shall ensure that use of technology and its associated risks are governed appropriately commensurate with the size and complexity of their operations. Using this Framework as a guiding principle, Payment Institution(s) shall:

1. Establish a Technology Risk Management Framework (TRMF) with the objective to safeguard their information infrastructure, integrity and availability of their systems and services and protection of customer data. The TRMF shall include following Board-approved policies:
   1. Outsourcing policy, fraud risk management policy including digital frauds, Disaster recovery and business continuity policy, Technology assurance/audit policy, Incidence Response Policy, Vendor and Third-Party Risk Management, Information Security Policy, Change Management Policy, Customer Protection & Complaint Management Policy, Data Protection and Governance Policy, AI/ML Risk Management policy
2. Establish an entity-wide technology risk management function which shall be responsible for:
   1. implementing the technology risk management and cyber resilience framework;
   2. advising on material technology projects and ensuring critical issues that may have an impact on the PI’s risk tolerance; and
   3. providing independent views to the board and senior management on third party assessments, where necessary.
3. Constitute a Board IT Committee for advising and reporting to the board on the status of technology activities, cybersecurity and digital risk posture and digital initiatives.
4. Designate a Chief Information Security Officer (CISO), or equivalent, to be responsible for the technology and cyber risk management function
5. Ensure that the CISO has sufficient authority, independence and resources and shall be independent from day-to-day technology operations.
6. The CISO may directly report to the Board of Directors or a Senior Committee for Independence.

## Information/ Cybersecurity

PI(s) shall ensure that appropriate controls covering people, process and technology are in place to safeguard against the risks to confidentiality, integrity, availability, authenticity and non-repudiation of customers’ data, systems, services and applications. Accordingly, PI(s) shall adhere to the following:

**7.1. Inventory Management**

*A Payment Institution shall:*

1. Maintain a record of all the key roles, information assets (applications, data, infrastructure, personnel, services, etc.), critical functions, processes and third-party service providers, and classify and document their levels of usage, criticality and business value.
2. Create and maintain a complete process flow diagram of network resources, inter-connections and dependencies, and data flows with other information assets, including any other third-party systems.
3. Asset information shall necessarily include an identifier, network address, asset location, asset owner name and End of Life Support (EoLS). All assets (hardware or software) approaching EoLS shall be assessed to evaluate risks associated with the continued use of the unsupported asset.

**7.2. Identity and Access Management**

*A Payment Institution shall ensure that:*

1. Policies, procedures and controls are in place to address access privileges as well as administration of access rights.
2. All individuals having access to the IT environment of the PI shall be assigned a digital identity, which shall be maintained and monitored till termination.
3. Default authentication settings in systems / software / services shall be deactivated and changed before they are rolled out to live environment.
4. Access to systems and different environments (development, test, production, etc.) shall be based on need-to-have, need-to-know and based on the principle of least privilege.
5. The use of privileged accounts shall be with Multi-Factor Authentication (MFA) and tightly monitored. Appropriate controls, including rotation policy, shall be implemented.
6. Necessary security controls, including centralized mechanism to whitelist / blacklist, shall be put in place to ensure secure use of removable media and portable devices (eg. smartphones, laptops, etc.).
7. In case of remote / work from home situations, adequate precautions, including Multi-Factor Authentication mechanism, shall be in place.
8. Define and implement procedures that limit, lock and terminate system and remote sessions after a pre-defined period of inactivity.

**7.3. Network Security**

*Payment Institution(s) shall put in place the following measures to protect its network and systems from external threats:*

1. Network devices shall be configured and checked periodically for security rules;
2. A Security Operations Centre (SOC) shall ensure proactive and centralized monitoring of comprehensive network and system logs collected and management of security incidents with effective tools for detection, escalation and quick response;
3. Automated mechanisms (eg. Security Information and Event Management (SIEM) system), which correlate all network and system alerts and any other anomalous activity across its business units to detect multi-faceted attacks, shall be established;
4. Anti-malware solutions shall be implemented so as to prevent, detect and contain malware attacks by scanning all incoming data to prevent malware from being installed and infecting a system;
5. Multi-layered boundary defenses shall be incorporated into IS systems to efficiently monitor the network traffic and filter the flow of data in and out of the PIs’ environment. There shall be adequate measures to detect and remedy unusual activities / events;
6. Network segmentation shall be made based on role, location and environment (production, testing, development, etc.) to segregate systems and data of varying criticality; Whitelisting solutions shall be in place to ensure that only permitted applications and services with validated needs are running. Whitelisting of ports may also be ensured with constant monitoring; and
7. Allow devices (such as laptop, desktop, mobile, etc.) to be connected to its network only after ensuring that they meet the prescribed security measures / requirements.

**7.4. Security Testing**

*A Payment Institution shall ensure that:*

1. All its applications are subjected to rigorous security testing, such as source code review, VA, PT, etc., through qualified professionals at adequate frequency (at least on annual basis) in authenticated mode.
2. If the source code is not owned by the PI, it shall obtain a certificate from the application developer stating that the application is free of vulnerabilities, malwares and any covert channels in the code. Fresh certificate shall be obtained for any changes to source code.
3. Deficiencies reported in the security testing shall be resolved in a time bound manner. Any recurring observation shall necessarily be reported to the Board sub-committee responsible for IT oversight along with detailed analysis for recurrence and resolution.
4. Any deployment or redeployment of new or existing services supporting critical functions, applications and infrastructure components must be done only after conducting security audits, including VA / PT, and addressing the resultant observations.
5. Regular information security assessments including VA/PT are conducted on a risk-based approach to identify and rectify any vulnerabilities which can an impact on the security, confidentiality, integrity and availability of services, along with risk-based mitigation

**7.5. Data Security**

*A Payment Institution shall ensure to:*

1. Put in place a comprehensive data leak prevention policy for confidentiality, integrity, availability and protection of business and customer information (both in transit and at rest) in respect of data available with it or at vendor managed facilities, commensurate with the criticality and sensitivity of the information held / transmitted.
2. Employ suitable mechanism to ensure traceability and visibility of data assets.
3. Develop and implement an Information Security Management System (ISMS) based on applicable standards.
4. Application and database security controls shall focus on secure handling, processing, storage and protection of data, in particular, Personally Identifiable Information (PII). Data in transit and rest shall be secured through either data or channel encryption or both.
5. Shall adhere to PCI-DSS guidelines when storing card (debit / credit / prepaid) data
6. Test the backed-up data, periodically (at least on a half-yearly basis) to ensure recovery without loss of transactions or audit-trails.

**7.6. Patch and Change Management Life Cycle**

*A Payment Institution shall ensure to:*

1. Put in place a documented policy and process to identify and implement patches to technology and software assets released by OEMs / others.
2. Apply security patches to the relevant systems and applications within an appropriate time frame from their release. In case of critical patches released to tackle well-known / reported attacks, the PI(s) shall have a mechanism to apply them immediately.
3. Patches and changes shall be implemented in production environment after testing and validating the same in other environments (e.g. development, testing, etc.).

**7.7. Incident Response**

*A Payment Institution shall ensure to:*

1. Put in place a Board approved incident response mechanism, which shall include provisions to promptly notify its senior management, relevant employees and regulatory, supervisory and relevant public authorities, of cyber incidents.
2. Response strategies shall incorporate readiness to meet various incident scenarios based on situational awareness and potential impact, consistent communication and co-ordination with stakeholders.
3. Post-incident analysis, including forensic analysis (wherever necessary), shall be conducted to determine the impact and root cause of incidents. Adequate measures shall be taken to avoid recurrence of similar incidents.
4. All unusual incidents like cyber-attacks, outage of critical system / infrastructure shall immediately be reported to relevant stakeholders including PSP&OD, SBP as per the incident reporting template provided in Annexure A.

**7.8. Application Programming Interfaces (APIs)**

*A Payment Institution shall ensure to:*

1. To safeguard applications against risks emanating from insecure APIs. Accordingly, PIs shall put in place, inter-alia, the following measures:
   1. Authentication and Authorization – Establish identity of the communicating applications;
   2. Confidentiality – Ensure that the message content is not tampered with;
   3. Integrity – Resources are reliably transferred; and
   4. Availability and Threat Protection – APIs are available when needed; anomalous activities identified and mitigate action taken.
2. Adhere to relevant standards and globally recognized frameworks on API security.

## Fraud Risk Management

Design, review and continuously improve end-to-end processes of digital fraud risk management and customer complaint management in order to continuously monitor, prevent, detect, respond and remediate incidents of digital financial fraud. Accordingly, PIs shall:

1. Ensure that risk management processes, procedures, systems and controls are in place to enable effective fraud risk mitigation and management.
2. Conduct comprehensive information security reviews of new digital products and services and for any modification in their existing digital products and services.
3. Ensure that the overall product and service design, development and operations shall strictly follow the core principles of information security i.e., confidentiality, availability and integrity.
4. Effective procedures on fraud detection, analysis, investigation and reporting, which among others, shall ensure that:
   1. Customer devices are registered using device finger-printing / device binding for authenticating customer access.
   2. The functionality of managing (adding/removing) the registered devices is provided in the mobile app.
   3. Any new device registered shall be notified to the customer immediately on their registered contact (email or phone number). Additionally, a cool-off period of at least 2 hours before switching devices must be enforced.
   4. fraud detection and transaction monitoring that can facilitate timely identification and mitigation of suspicious transactions
   5. regular analysis to understand fraud trends and modus operandi
   6. reporting of fraud incidents to senior management and the board on a regular basis.
   7. Put a limit on number of devices accessed per account is in place, and implement additional authentication controls for devices exceeding the defined limit.
   8. Credential reset (such as change in user ID/password) is only performed after multi-factor authentication using customers’ registered device.
   9. Enforce OTP auto-fetch with sender binding control to prevent phishing attacks or require Robo Call Back (RCB) when OTP entry is not feasible.
5. In the event of fraud occurrences, the EMI shall take appropriate and immediate corrective in accordance with BPRD Circular No. 4 of 2023.

*In addition to Requirements outlined above, the PIs, shall:*

1. Design the process and application in such a way that the chances of disclosure of customer information - in whole or partially in a manner that makes it possible to be collated to reconstruct - are eliminated or minimized.
2. Ensure that information of customers, individual or in bulk, shall never be in the personal possession or personal access of the PIs’ staff or transportable by the staff, third parties and any other service provider to prevent its possible misuse.
3. Ensure sufficient controls and measures to safeguard the confidentiality of customer’s PII under their outsourcing arrangements, and where such data is stored and processed outside the PIs software/ applications (i.e. in office productivity software/tools).

## Outsourcing of Technology

PI(s) shall ensure that outsourcing of any function, activity or process shall (i) not cause disruption ***to*** and deterioration ***in*** the quality of services provided to customers, (ii) not reduce the protection and security available to customers, and (iii) not be used as a way of avoiding compliance with regulatory requirements. Accordingly, PI(s) shall:

1. conduct a thorough risk-based analysis of the functions and related data and systems that are being considered for outsourcing or have been outsourced and address any potential risks which may arise due to outsourcing.
2. Obtain SBP’s prior written approval before entering into a new material outsourcing arrangement or making material changes to an existing material outsourcing arrangement as amended from time to time.
3. Consider specific measures, for data in transit, data in memory and data at rest, such as the use of encryption technologies.
4. Assess materiality of an outsourcing arrangement taking into consideration the following factors:
5. significance of the outsourcing activity in facilitating the PI to achieve its strategic and business objectives;
6. impact on the PI’s continuing ability to meet its obligations to its customers and counterparties in the event the service provider fails to provide the service or encounters a breach of data confidentiality or security;
7. aggregate exposure to a particular service provider in cases where the PI, including any affiliates, outsources multiple activities to the same service provider; or
8. complexity of the outsourcing arrangement and number of parties involved, in particular where the service is sub-contracted or where more than one service provider collaborates to deliver an end-to-end outsourcing solution.
9. Assess the service provider’s ability to maintain continuity of service during disruptions, including their disaster recovery and business continuity capabilities. Further, regularly assess the risks associated with third-party service providers and dependencies. Ensure that contingency measures are in place for critical third-party services to reduce the risk of disruptions due to external factors.

PI(s) shall assess the potential impact of outsourcing arrangements on their operational risk and should take into account the assessment results when deciding if the function should be outsourced. Accordingly, PI(s) shall:

1. Take appropriate steps to avoid undue additional operational risks.
2. Undertake assessments that include high-severity operational risk events.
3. Take into account concentration risks rising from:
   1. outsourcing to a dominant service provider that is not easily substitutable
   2. multiple outsourcing arrangements with the same service provider or closely connected service providers, creating a potential single point of failure.
4. Ensure that all contractual terms are clearly defined, including service levels, performance metrics, confidentially of data, penalties for non-compliance, and exit clauses that detail how the institution can transition services if necessary.

The regulated entity should conduct appropriate due diligence in selecting third-party service providers. In accordance to this, PI(s) shall:

1. Develop criteria to assess the third-party service provider’s capacity and ability to perform the outsourced activities effectively, reliably and to a high standard
2. Conduct appropriate due diligence taking into account the following:
   1. The selection of service providers qualified and with adequate resources to perform the outsourcing work;
   2. Ensuring that the service provider understands and can meet the objectives of the regulated entity in the specified activity.
   3. Recognition of the service provider’s financial soundness to fulfil its obligations.
   4. The reputation and experience of the service provider in the industry.
3. Ensure that the service provider implements appropriate technical and organizational measures to protect the data

## Disaster Recovery and Business Continuity

PI(s) shall serve their customers with minimal disruptions, minimize financial losses to the institution, and mitigate the negative effects of disruptions on business operations. Accordingly, PI(s) shall ensure that:

1. To develop a BCP based on different cyber threat scenarios, including extreme but plausible events to which it may be exposed. It shall be reviewed at least once a year and include a comprehensive cyber incident response, resumption and recovery plan, to manage cyber security events or incidents.
2. The BCP shall be designed to enable rapid recovery from any adverse event and facilitate safe resumption of critical operations aligned with Recovery Time Objective (RTO) and Recovery Point Objective (RPO) while ensuring the security of processes and data.
3. The PSO shall set up a Disaster Recovery (DR) facility in a different seismic zone than the Primary Data Centre (PDC). There shall be a defined methodology for reconciliation of data so as to ensure that there is no data loss while resuming operations from the DR.
4. DR drills shall be conducted on a half-yearly or more frequent basis. Any divergence from the RTO and RPO shall be analyzed and the deficiency be rectified on urgent basis.
5. Periodically review and update the contingency plan, taking into account developments which may affect their feasibility
6. Tier-1 PSOs are expected to minimize their RTO to 2 hours.
7. Perform a "gap analysis" and shall implement a BCP based on disruptions identified and their resulting impact on the PSO.
8. Evaluate the recovery plan and incident response procedures at least annually and update them as and when changes to business operations, systems and networks occur.
9. BCP and DR drills shall be conducted half yearly in presence of independent reviewers and results should be recorded in a formal report and be shared with SBP as and when required.
10. Test and validate, at least annually, the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures.
11. Participate in disaster recovery tests that are conducted by its service provider(s).
12. BCP and DR plans shall cover various scenarios such as total shutdown, complete switchover of the primary site and/or component failure at the individual system or application cluster level.
13. BCP/DR drills planned with third parties shall be performed annually.
14. Any BCP/DR drill conducted by the third-party of functions that would affect the ability of the PSO to conduct its business activities must be reviewed by PSP&OD.
15. The PSO must participate in annual BCP/DR drills planned with third parties.

## Technology Audit

*A Payment Institution shall:*

1. Establish a risk-based audit plan that provides appropriate coverage of critical technology services, technology service providers, material external system interfaces, delayed or prematurely terminated material technology projects and post-implementation reviews of new or material enhancements of technology services.
2. That the scope, frequency and intensity of technology audits are proportionate with the complexity, sophistication and criticality of technology systems and applications.
3. Get their systems, applications and processes audited from reputable technology audit firms after commencement of their pilot operations and thereafter on annual basis.

Annexure 1

|  |  |  |
| --- | --- | --- |
| # | Data Field | Data Value Type |
| 1 | Regulated Entity Name | Text |
| 2 | Type | Cyber-attack, IT Incident |
| 3 | Category | Ransomware, Data Breach, DDoS,  Website Defacement, Upgradation Failure, Hardware Failure, Patch Upgrade Issue, Connectivity Issues, Power,  Data Center Hazards, Others (please specify) |
| 4 | Severity / Classification | (e.g. High, Medium, Low, etc.) |
| 5 | Impact | Unavailability, Service Degradation  Financial Loss, Data Breach  Data Integrity Compromise,  Others (please specify) |
| 6 | Detection Date & Time | DD-MM-YYYY HH:MM |
| 7 | Initial Response Date & Time | DD-MM-YYYY HH:MM |
| 8 | Impacted Customer Facing Services | Text |
| 9 | Impacted Non-Customer Facing Services | Text |
| 10 | Mitigation & Containment Milestones with Tentative Timelines | Text |
| 11 | Vendor Dependency for Mitigation & Containment | YES / NO |
| 12 | Name of Vendor Engaged for Mitigation & Containment (if any) | Text |
| 13 | Recovery Milestones with Tentative Timelines | Text |
| 14 | Vendor Dependency for Recovery | YES / NO |
| 15 | Name of Vendor Engaged for Recovery (if any) | Text |
| 16 | External Security Firm Engaged | YES / NO |
| 17 | Name of External Security Firm (if any) | Text |