Technology Risk Management Framework for Payment Institutions

Payment Systems Policy & Oversight Department

Table of Contents

1. Objective

The objective of this Technology Risk Management (TRM) framework, hereinafter referred to as 'Framework' is to provide baseline requirements for the management of technology risks in proportion to the relevant risk exposure of Payment Institutions (PIs).

2. Scope & Applicability

The requirements of this framework shall be applicable on Payment Systems Operators/Payment Service Providers (PSOs/PSPs), Electronic Money Institutions (EMI) and any other entity licensed/authorized by State Bank of Pakistan (SBP) under Payment System & Electronic Fund Transfers (PS&EFT) Act, 2007 (hereinafter collectively referred to as PIs). The framework is not "one-size-fits-all" and implementation needs to be risk-based and commensurate with size, nature, types of products, services and complexity of technology operations of the individual PI in the following manner:

a) At the In-Principle Approval (IPA) stage, PI shall provide written assurances including detailed plans regarding their intent and ability to comply with the requirements of this framework.
b) For Pilot Operations stage, PI shall be able to demonstrate reasonable operational readiness in terms of technology operations. Baseline technology readiness requirements for pilot stage operations are available at **Annexure-I.**
c) For Commercial Operations, PI shall, at all times, be able to demonstrate compliance with the requirements of this framework.

3. Definitions

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

- **Audit Firms**: Audit firms on SBP's panel of auditors and Pakistan Telecommunication Authority (PTA)'s approved Security Audit Firms available at their respective websites.
- **Commercial Operations:** As stated in the Regulations for EMIs and referred to as "Final Approval" in the Rules for PSOs and PSPs.
- **Designated Payment System**: Means a Payment System designated by the State Bank of Pakistan (SBP) under section 4 of PS&EFT Act of 2007.
- **EMIs:** As defined in Section 24 of PS&EFT Act of 2007.
- **IPA:** As stated in Regulations for EMIs and in the Rules for PSOs and PSPs.
- **Material Outsourcing** – Shall have the same meaning as defined in SBP's Framework for Risk Management in Outsourcing Arrangements by Financial Institutions as amended from time to time.
- **Personally Identifiable Information (PII)**: As defined in SBP's Framework for Risk Management in Outsourcing Arrangements by Financial Institutions as amended from time to time.
- **Pilot Operations**: As stated in the Regulations for EMIs and in the Rules for PSOs and PSPs.
- **PSOs/PSPs:** As defined in the Rules for PSOs and PSPs.
- **Technology Audit**: An independent, systematic review of a PI's information system and its controls to verify that the controls whether technical, operational, or managerial are properly designed, implemented, and operating effectively to ensure that the system maintains the confidentiality, integrity and availability of information.

4. Status of Previous Regulations

The instructions contained in this framework shall supersede the following:

a) Section 19 titled 'Outsourcing of Function(s) to the Third Party(ies)', Section 21 titled 'Security and Confidentiality' and Section 23 titled 'Risk Management Mechanism' of the Regulations for EMIs issued vide PSP&OD Circular No. 03 of 2023 (as amended from time to time).

b) Clause No. 9 of Section 6 titled 'Operations of PSOs and PSPs', Section 8 titled 'Risk Management Mechanism', Section 9 titled 'Security and Confidentiality' of the Rules for PSOs and PSPs issued vide PSD Circular No. 03 of 2014 (as amended from time to time).

5. Governance and Oversight

Principle: PIs shall ensure that use of technology and its associated risks are governed appropriately and proportionate with the size and complexity of their operations.

A. Role of the Board of Directors (BoDs) and Senior Management

a) The BoDs shall have sufficient number of members with requisite technology experience to oversee and manage enterprise technology risks including cybersecurity risks.

b) The BoDs or any of its designated committees, shall be responsible for:
   i) Ensuring that relevant policies, procedures and controls are in place.
   ii) Assessing relevant senior management competencies for managing technology risks.
   iii) Ensuring an independent audit function to assess the effectiveness of the internal controls for technology risk management.

c) Senior management shall be responsible for:
   i) Developing and implementing technology risk policy (strategy, procedures and controls) and updating the same at least once in 3 years or as and when necessitated
   ii) Clearly delineating the roles and responsibilities of staff in managing technology risks.
   iii) Promptly informing BoDs about the developments in technology risk including cyber incidences and events that are likely to have a major impact on the PI.

b) PIs shall have Head of IT and Head of Information Security (or equivalent), possessing the requisite expertise and experience.

B. Policies and Procedures

PI(s) shall preferably incorporate industry standards and best practices in their policies and procedure to manage technology risks and safeguard information assets covering functionality, security and performance aspects including but not limited to:

a) Necessary controls to protect confidentiality, integrity of the customer data and processes associated with the digital product/ services offered.

b) Comprehensive policies to address all potential vulnerabilities and threats.

c) High availability of systems/ channels to minimize service disruptions.

d) Efficient dispute resolution mechanism and handling of customer grievances.

e) Cyber-incident response and management plan, duly approved by the BoDs to swiftly isolate and neutralize a cyber-threat and securely resume affected services

f) Outsourcing policy, duly approved by the BoDs, shall, at a minimum, include roles & responsibilities of all stakeholders, materiality assessment criteria, vendor management, risk assessment & mitigation measures for all types of outsourcing risks, contingency planning and an exit strategy from the outsourcing arrangement.

C. Technology Audit:

PIs shall ensure that:

a) Technology audits provide the BoDs and senior management with an independent and objective opinion on the adequacy and effectiveness of technology risk management, governance, and internal controls.
b) The scope and frequency of technology audits are commensurate with the complexity, sophistication and criticality of technology systems and applications.
c) Independent technology audits shall be conducted by external audit firms[1], which possess the necessary expertise to assess the adequacy of IT policies, procedures, processes, and controls.

6. Technology and Cyber Risk Management

Principle: PIs shall put in place appropriate controls to safeguard against the risks to confidentiality, integrity, availability, authenticity and non-repudiation of customers' data, systems, services and applications. Accordingly, PIs shall adhere to the following:

A. Inventory Management

PIs shall:

a) Maintain a record of key roles, information technology assets, critical functions, processes and third-party service providers and classify them based on their levels of usage, criticality and business value.
b) Maintain a complete data flow diagram of network resources, inter-connections and dependencies.
c) Conduct risk assessment of any hardware/software reaching their end-of-life or end-of-support.

B. Identity and Access Management

PIs shall ensure that:

a) Policies, procedures, and controls are implemented to define and administer access privileges.
b) Default authentication settings in systems / software / services are deactivated and changed before rolling out to live environment.
c) Access to all systems and environments (development, testing, production, etc.) is granted in accordance with the principle of least privilege.
d) Mechanism is in place to limit, lock and terminate systems and remote sessions after a pre-defined period of inactivity.
e) Privileged access is granted strictly on a need-to-use basis for the minimum required duration and shall require multi-factor authentication. All account activity of privileged accounts must be logged and reviewed as part of ongoing monitoring.
f) User access are reviewed at regular intervals to validate privilege assignments, detect inactive or redundant accounts.
g) Necessary security controls, including a centralized whitelist/blacklist mechanism, are implemented to secure removable media and portable devices (e.g., smartphones, laptops).
h) In case of remote / work from home scenarios, adequate precautions, including Multi Factor Authentication (MFA) are put in place.

[1] For a list of audit firms for technology audit, PIs in addition to SBP's panel of auditors may also consult PTA's approved Security Audit Firms list available at: https://www.pta.gov.pk/category/security-audit-firms-categorization-1547609365-2023-05-30

C. Network Security

PIs shall ensure that:

a) Network devices are configured and checked periodically for security rules.
b) Network segmentation is made based on role, location and environment (production, testing, development, etc.) to segregate systems and data of varying criticality ensuring that most critical communications occur in the most secure and reliable segment.
c) Multi-layered security model is incorporated to efficiently monitor the network traffic and filter the flow of data in and out of the PIs' environment.
d) Comprehensive network and system logs are monitored proactively and centrally, with tools in place for detection, escalation, and rapid incident response.
e) Automated security monitoring mechanisms (e.g., Security Information and Event Management (SIEM) systems and Security Operations Center (SOC)) are established to correlate network and system alerts and detect anomalous activity.
f) Anti-malware solutions are implemented to prevent, detect and contain malware attacks by scanning all incoming data.
g) Whitelisting solutions are in place to ensure that only permitted applications and services with validated needs are running. Prevent users from accessing malicious websites by implementing URL blacklists and/or allow lists.
h) Only allowed devices (such as laptop, desktop, mobile, etc.) are connected to network after verification of meeting PIs' security requirements.
i) Open and listening ports of network are scanned and unnecessary ports are closed.

D. Security Testing

PIs shall ensure that:

a) Risk-based information security assessments, including vulnerability assessments and penetration testing, are conducted regularly to identify and mitigate vulnerabilities affecting confidentiality, integrity, and availability of systems and applications.
b) A process is established for regular vulnerability scanning to identify and remediate security risks promptly, with scanning frequency aligned to system/application criticality and exposure.
c) Externally facing digital services are subject to penetration tests at regular intervals, at least on a yearly basis and after any significant changes to underlying systems.
d) Security testing deficiencies are remediated within defined timeframes. Any recurring issues must be reported to the BoDs or relevant committee, accompanied by a detailed analysis of recurrence and corrective actions.

E. Data Security

PIs shall ensure to:

a) Put in place a comprehensive data leak prevention mechanism for protection of critical business and customer information.
b) Put in place controls for application and database security with a focus on secure handling, processing, storage and protection of data, in particular, handling of the PII.
c) Adhere to Payment Card Industry Data Security Standard (PCI-DSS) guidelines when storing payment cards data.

d) Maintain offline, encrypted backups of data and regularly test backups. Backup procedures shall be conducted on regular basis and ensure recovery without loss of transactions or audit-trails.

F. Patch and Change Management Life Cycle

PIs shall ensure to:

a) Put in place a documented mechanism to identify and implement patches to technology and software assets released by Original Equipment Manufacturers (OEMs) / others.
b) Apply security patches to the relevant systems and applications within a defined timeframe upon release. Critical patches addressing known threats must be deployed immediately.
c) Implement patches and changes in production environment after testing and validating the same in non-production environments.
d) Prioritize timely patching of internet-facing servers, as well as software processing internet data.
e) Consider using a centralized, virtual patch management system.
f) Automatically update antivirus and anti-malware solutions and conduct regular virus and malware scans.

G. Incident Response & Reporting

PIs shall ensure to:

a) Create, maintain, and exercise a cyber-incident response plan that includes:
    i) Procedures for response and notification in a ransomware incident.
    ii) Plans for the possibility of critical systems being inaccessible for a period of time.
b) Establish a process to identify and investigate the security control deficiencies that led to the security incident.
c) Conduct post-incident analysis to determine the impact and root cause of incidents. Adequate measures shall be taken to avoid recurrence of similar incidents.
d) Report all technology incidents like cyber-attacks, outage of critical system / infrastructure immediately to SBP as per the incident reporting template provided in **Annexure II** or as per the regulatory instructions on incident reporting issued and amended from time to time.

H. Application Programming Interfaces (APIs)

PIs shall ensure to:

a) Perform risk assessment of Third-party API integrations, with security controls tailored to the sensitivity and business criticality of the exchanged data.
b) Establish security mechanism to secure APIs that shall include:
    i) Measures to protect the API keys or access tokens, which are used to authorize access to APIs to exchange confidential data.
    ii) A reasonable timeframe for access token expiry to reduce the risk of unauthorized access.
c) Adopt strong encryption standards and key management controls to secure transmission of sensitive data through APIs.
d) Conduct security testing of the API between the PI and its third parties prior to its deployment in the production environment.
e) Log the sessions involving third parties by the PI. Logs shall include details such as the identity of the party making the API connection, date and time, as well as the transactions executed and data accessed. These logs shall be available for audit purposes as and when needed.

I. Cyber Threat Intelligence and Information Sharing

PIs shall ensure to:

a) Establish a process to collect, process, and analyze cybersecurity-related information for its relevance and potential impact on its business and IT environment.

b) Establish cyber intelligence monitoring services and actively participate in cyber threat information-sharing arrangements.

J. Cyber Event Monitoring and Detection

PIs shall ensure to:

a) Establish a process to collect, process, review and retain system logs to facilitate the PI's security monitoring operations. The baseline of minimum logging requirements (e.g., logging successful and unsuccessful logon events, privilege changes, etc.) shall be established. These logs shall be protected against unauthorized access.

b) Establish a baseline profile of each IT system's routine activities and analyze the system activities against the baseline profiles. The profiles shall be regularly reviewed and updated.

c) Escalate suspicious or anomalous system activities or user behavior to relevant stakeholders.

7. Managing Digital Financial Frauds

Principle: PIs shall design end-to-end processes of digital fraud risk management and customer complaint management to continuously monitor, prevent, detect, respond and remediate incidents of digital financial fraud.

A. Governance of Fraud Risks

PIs shall:

a) Establish digital fraud risk management function with an effective control by management and oversight of the BoDs or its designated committee.

b) Allocate necessary resources, systems and people, to build the necessary capacity.

c) Enforce security mechanisms commensurate with the risks in respective areas of digital payments products and services.

d) Perform comprehensive fraud investigations, identifying root causes, taking corrective actions and documenting the entire process.

B. Fraud Prevention Measures

PIs shall ensure that:

a) NADRA biometric verification of customers is conducted at the time of digital channels activation/sign–up, new device registration, and modification of customer email address and phone numbers.

b) Customer devices are registered using device finger-printing/device binding[2] for authenticating customer access.

c) The functionality of managing (adding/removing) the registered devices is provided in the mobile app.

[2] Device Finger-Printing / Device Binding: Using unique set of identification features such as Device ID, Universal Unique Identifier (UUID), Integrated Circuit Card Identifier (ICCID), International Mobile Equipment Identity (IMEI) Number or International Mobile Subscriber Identity (IMSI) Number.

d) 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 after switching devices must be enforced.
e) A limit is placed on number of devices allowed to access a single account/wallet. Similarly, a limit shall be placed on number of accounts/wallets activated/used on one device.
f) Credential reset (such as change in user ID/password) is only implemented after MFA using customer's registered device.
g) Enforce One Time Password (OTP) auto-fetch with sender binding control to prevent phishing attacks or require other forms of MFA when OTP entry is not feasible.
h) Set reasonable default transaction limits on the digital channels and enable the customers to enhance or reduce these limits after due authentication.

C. Fraud Detection, Response & Recovery

PIs shall be liable for any loss of customer funds' resulting from the PIs' delayed remedial actions or control failure (e.g., blocking digital channels, initiating dispute requests) and must fully compensate customers for such losses. Following liability structure shall be applicable subsequent to a fraudulent transaction/social engineering scam:

a) Liability to make good of all customer losses shall lie with originating institution (sender PI) in case dispute is not lodged within the stipulated time (within 30 minutes of customer complaint).
b) The originating institution(s) shall be fully liable if customers are unable to lodge a dispute due to unavailability of their complaint channel(s).
c) Liability to make good of all customer loss shall lie with beneficiary institution (receiving PI) in case funds were withdrawn because disputed amount was not blocked in the beneficiary account within the stipulated time (within 30 minutes after a case is lodged by the sender PI) after receiving the dispute.
d) In cases of false customer registration, the responsible PI shall bear full liability if required registration controls were absent or improperly implemented.
e) PIs shall be liable to compensate the customers, in case where they are unable to establish that the transactions were executed through the customers' registered device.
f) PIs shall be fully liable for customer losses if transaction alerts are delayed and not received in a timely manner.

8. Outsourcing and Technology Service Provider Management

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

A. Outsourcing Oversight

PIs shall ensure to:

a) Establish an outsourcing function or designate a senior staff member responsible for managing and overseeing the risks of outsourcing arrangements as part of the institution's internal control framework.

b) 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.

B. Outsourcing Arrangements

a) Outsourcing arrangement with Cloud Service Providers (CSPs) shall continue to be governed under SBP's Framework on Outsourcing to Cloud Service Providers issued vide BPRD Circular No. 01 of 2023 and as updated from time to time.
b) For outsourcing arrangements other than those involving cloud services, PIs shall inform PSP&OD-SBP in writing seven (07) business days, in advance before entering into any new material outsourcing arrangement.
c) For offshore outsourcing arrangements, PIs shall take written approval from SBP prior to the arrangement.
d) PIs shall ensure that any outsourcing arrangements with third parties and group companies shall be entered into at arm's length basis.

C. Outsourcing Agreement

PIs shall ensure that outsourcing arrangement is governed by a written agreement that is legally enforceable and shall necessarily include the following minimum requirements, among others:

a) SBP's right to have direct, timely and unrestricted access to the systems and any information or documents relating to the outsourced activity.
b) SBP's right to conduct on-site assessment of the service provider where it deems necessary.
c) SBP's right to appoint an independent party to perform a review of the relevant systems, information or documents of the service provider relating to the outsourced activity, where it deems necessary.

D. Third Party Risk Management

PI(s) shall identify their critical third-party service provider(s) and ensure that they:

a) Possess the ability to identify and manage relevant operational and financial risks to their critical services and ensure the effectiveness of their risk-management processes.
b) Implement appropriate policies and procedures, and provide sufficient resources to ensure the confidentiality and integrity of information and the availability of its critical services in order to fulfil the terms of its relationship with the PIs.
c) Have adequate business continuity management and disaster recovery plans to support the timely resumption of critical services in the event of an outage.

Further, designated PI(s) shall regularly evaluate their critical service providers as per the template provided in **Annexure-III**.

9. Disaster Recovery and Business Continuity

Principle: PIs shall serve their customers with minimal disruptions, minimize financial losses to the institution, and mitigate the negative effects of disruptions on business operations.

A. System Availability

PIs shall ensure that IT systems are designed and implemented to achieve the level of system availability commensurate with its business needs and recorded in internal or external service level agreements.

B. Business Continuity Management and Disaster Recovery

PIs shall ensure to:

a) Establish a sound business continuity management process to maximize their ability to provide services on an ongoing basis, reach their availability goals defined in their Service Level Agreements, and minimize losses in the event of severe business disruption.
b) Conduct business impact analysis (BIA) by analyzing their exposure to, and impact from, business disruptions including severe but plausible range of scenarios.
c) Establish system Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) which are aligned with the results of the BIA. However, designated PI(s) shall make arrangements to minimize their RTO to 02 hours.
d) Set up a Disaster Recovery (DR) facility, preferably, in a geographically diverse zone than the Primary Data Centre (PDC).
e) Establish scalable capacity adequate to handle increasing stress volumes and to service level objectives

C. Testing of Disaster Recovery Plan

PIs shall ensure to:

a) Conduct DR drills at least annually and update them as and when changes to business operations, systems and networks occur. Any divergence from the RTO and RPO shall be analyzed and the deficiencies shall be rectified on urgent basis.
b) The results of such drills shall be recorded in a formal report and be shared with SBP as and when required.
c) 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 level.

Annexures

Annexure – I

Baseline Technology Readiness Requirements

A. For pilot stage operations, Payment Institutions shall ensure smooth and intended functioning of the following systems/applications and processes:

Systems/Applications/Processes*		
1	Wallet Management System / Payment Service Solution	A customer wallet management system / payment service solution including customer on-boarding application and/or ledger of wallets
2	Transaction Monitoring System	A functional transaction monitoring system with the ability to continuously monitor and screen transactions and generate alerts
3	Security Apparatus	Basic network, application, database security tools.
4	Fraud Management System	A comprehensive set of tools, technologies designed to detect, prevent, and mitigate fraudulent activities within an organization by analyzing data, identifying patterns, and triggering alerts for suspicious activity
5	Customer Complaint Management System	A platform designed to streamline the process of handling customer complaints, feedback, and concerns
6	Fraud Risk Management process	A systematic approach to identify, assess, and mitigate the risks of fraudulent activities within an organization, encompassing prevention, detection, and response strategies
7	Customer Complaint Management process	A structured approach to handling, resolving, and analyzing customer complaints to improve service quality and customer satisfaction, encompassing receiving feedback, logging issues, investigating concerns, communicating solutions, and implementing preventative measures

B. For starting Commercial Operations, in addition to the requirements at (A) above, Payment Institutions shall inter alia ensure the availability of the following systems/applications and processes:

Processes		
1	DR/BC process	Processes that ensure an organization can continue operating during and after a disruption, with business continuity focusing on maintaining operations and disaster recovery on restoring IT systems and data
2	Cybersecurity plan	A strategic blueprint that outlines how an organization will protect itself from cyber threats and vulnerabilities, encompassing various aspects like network security, data protection, risk management, and incident response
3	Incident Response plan	A formal document outlining the procedures for responding to and managing security incidents, including detection, analysis, containment, eradication, recovery, and post-incident activities
4	VA/PT process	A cybersecurity process that combines automated vulnerability scanning with manual penetration testing to identify and assess security weaknesses in systems, networks, and applications

** All software tools/application, operating systems, hardware appliances shall have valid licenses and shall not have reached End of Life (EoL). Open source software applications, libraries, frameworks etc. shall be up-to-date and have valid support, where applicable.*

Annexure – II

Technology Incident Reporting Template*

#	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

***All IT and cyber incidents shall be reported to SBP via email at RE-IT.incidents@sbp.org.pk**

Annexure-III

Tools for Onboarding and Ongoing Monitoring of Critical Third Party Service Providers	
1	Information on the service provider's business continuity planning
2	Documentation on the service provider's controls
3	Performance-related information (e.g. key performance indicators (KPIs) and scorecards)
4	Financial condition information such as audited financial reports and credit rating reports
5	Other relevant information such as data breaches and service disruption reports, risk assessment report on cyber security, details of key nth-party service providers and other components of the service provider's supply chain
6	Questionnaires (e.g. on cyber-risk and business continuity), which might be standardized or tailored to the service provider
7	Inspections of the service provider's technology assets and infrastructure (e.g. the premises where the relevant service(s) are provided)
8	Customized assessments (non-critical) (e.g. assessment of the service provider's cyber and technology vulnerabilities)
9	Incident reports, root cause analysis and remediation actions completed by independent parties
10	Technology platforms for the management of workflows associated with the lifecycle of a third-party service relationship and monitoring the financial institution's internal controls