www.asa.in

ASA Going The Extra Mile | bakertilly NETWORK MEMBER

UPI Information Security & Compliance Framework 2025: Key Highlights for Stakeholders

The Unified Payments Interface (UPI), developed by the National Payments Corporation of India (NPCI), has transformed the way India transacts, offering a seamless and inclusive digital payments platform. With its ability to link multiple bank accounts through a single mobile interface, UPI has made digital payments fast, convenient, and accessible across the nation.

As the platform continues to scale, handling millions of transactions daily, ensuring its security, resilience, and reliability has become more critical than ever. In response to the growing complexity of cyber threats and operational risks, NPCI has introduced the UPI Information Security and Compliance Framework 2025. This updated framework outlines robust security protocols, compliance mandates, and audit mechanisms to safeguard the UPI ecosystem.

Key Compliance Requirements

1. **Annual Security Audits**

   All participating entities must undergo comprehensive security audits by a CERT-IN empanelled auditor both prior to onboarding and annually thereafter.

2. **Full Remediation of Vulnerabilities**

   Entities are required to address and resolve all identified security gaps before submitting their final compliance reports.

3. **End-to-End Audit Scope**

   Audits must encompass all components—mobile applications, infrastructure, backend systems, and frontend interfaces.

4. **Strict Reporting Timeline**

   Final compliance reports, with zero pending issues, must be submitted to NPCI by December 31 each year.

Objectives of the Framework

1. Uniform Security Standards

The framework mandates a consistent set of security protocols across banks, payment service providers (PSPs), and third-party applications. This includes encryption standards, access control mechanisms, API security, and proactive vulnerability management. All audit findings must be transparently reported to NPCI.

2. Ensuring System Integrity, Availability, and Confidentiality

Built on the CIA (Confidentiality, Integrity, Availability) triad, the framework calls for:

- Confidentiality: Use of encryption and tokenization to protect sensitive data.
- Integrity: Safeguarding data through hashing, digital signatures, and secure protocols.
- Availability: Designing high-resilience systems with disaster recovery, load balancing, and failover capabilities.

3. Proactive Threat Management

Entities must implement regular security testing, real-time monitoring, and advanced AI-based fraud detection to counter threats such as phishing, deepfake manipulation, and API exploitation.

4. Alignment with Global Standards

The framework aligns with international benchmarks such as Zero Trust Architecture, ISO 27001, PCI DSS, NIST Cybersecurity Framework (CSF), and complies with RBI guidelines and the Digital Personal Data Protection Act.

Applicability

The framework is mandatory for the following stakeholders:

- Issuing and acquiring Banks
- Payment Service Provider Banks and entities
- Third-party application providers (TPAPs)
- Technology service providers
- IVR and voice-based payment platforms

It further emphasizes the active involvement of senior leadership, including CISOs and system owners, in driving governance and compliance initiatives.

Implementation in Practice

Security Measures:

- Robust encryption standards
- Multi-factor authentication
- Secure API/SDK integration
- Continuous vulnerability assessments

Operational Resilience:

- Regular business continuity planning (BCP) and disaster recovery (DR) drills
- Real-time system monitoring
- Automated compliance tracking tools

Building a Security-First Culture

Cybersecurity is not solely a technological concern—it requires a strong cultural foundation. The framework advocates structured training and awareness programs to promote a security-first mindset among employees, developers, and partners within the UPI ecosystem.

Why It Matters

The UPI Information Security and Compliance Framework 2025 is more than a regulatory requirement—it is a strategic imperative. By adhering to its guidelines, stakeholders can reduce compliance risks, mitigate fraud, enhance operational stability, and, most importantly, build and sustain user trust in India's leading digital payment infrastructure.

In a digital economy that's constantly evolving, staying ahead of security threats is not optional. It's essential.

Authorised by

Rachit Shukla
Baker Tilly ASA India