Unified Payments Interface (UPI) Information Security Compliance Framework 2025

National Payments Corporation of India (NPCI)

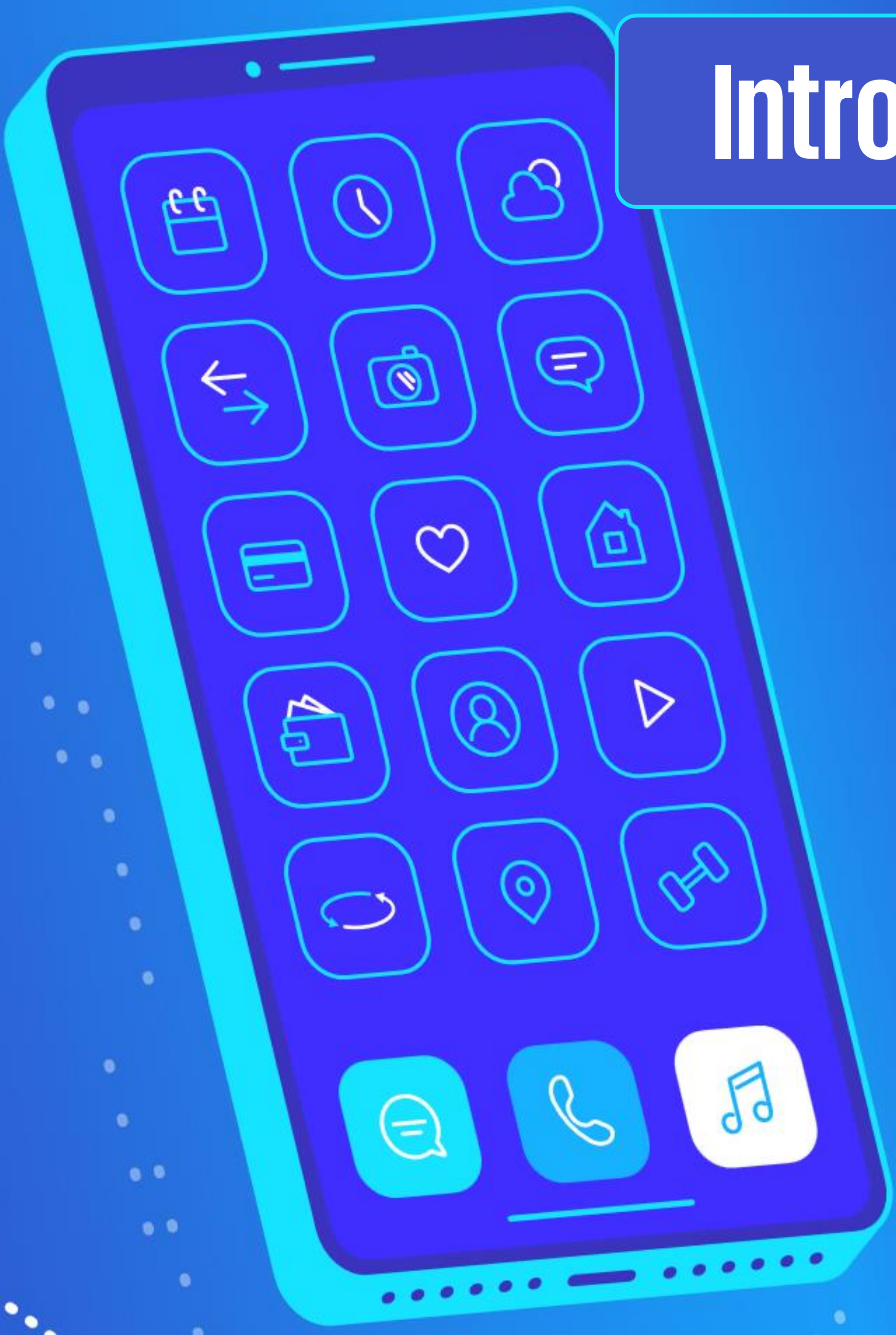
July 2025

kpmg.com/in

KPMG. Make the Difference.

Table of contents

Introduction



Introduction

Unified Payments Interface (UPI), introduced by the National Payments Corporation of India (NPCI), allows users to link several bank accounts to a single mobile application offered by any member bank. It simplifies digital banking by combining multiple services, including money transfers, merchant transactions, and account features into one secure and easy-to-use platform. Recognizing the importance of UPI security standardization across participants, NPCI has issued UPI Information Security Compliance Framework - 2025 (hereinafter also referred to as ***'UPI InfoSec Compliance Framework 2025'*****).**

Applicability				Key Stakeholders Impacted
Remitter/ Issuer Bank	PPI's/ PSP Bank	Beneficiary/ Acquiring Bank	Third Party App Provider (TPAP)	Board of Directors Senior Management (CEO, IT Head, CRO, etc.)
Technology Service Provider (TSP)	Voice-Based Service Provider (VSP)	Interactive Voice Response (IVR)	Application Service Provider (ASP)	CISO Application Owner

Objective

- To outline the information security compliance requirements and standards for entities seeking to onboard or onboarded on NPCI's Unified Payment Interface.
- To help build a secure and resilient UPI ecosystem.
- To help comply with key cybersecurity principles, including confidentiality, integrity, availability, privacy and resilience of payment applications.
- To proactively recognize, track, mitigate, and oversee risks associated with cybersecurity and emerging technologies.

Audit and Compliance Obligations

- All UPI entities must undergo a comprehensive security audit based on guidelines outlined in the framework.
- This audit is a pre-onboarding activity and annual thereafter, that must be conducted by a CERT-IN empaneled auditor. Entities need to bear the cost of audit.
- In case of non-compliance during initial audit, entities must close all open findings and submit final compliance report to NPCI with no open findings.
- Once final compliance report with no open findings is submitted to NPCI, entities can be onboarded to the UPI ecosystem.
- Once onboarded, entities must submit an annual compliance report with no open findings on or before December 31st of every year.
- The audit scope must cover the entire UPI infrastructure and UPI application, including frontend and backend.

Overview of UPI InfoSec Compliance Framework 2025

Overview of UPI InfoSec Compliance Framework 2025

Governance Controls

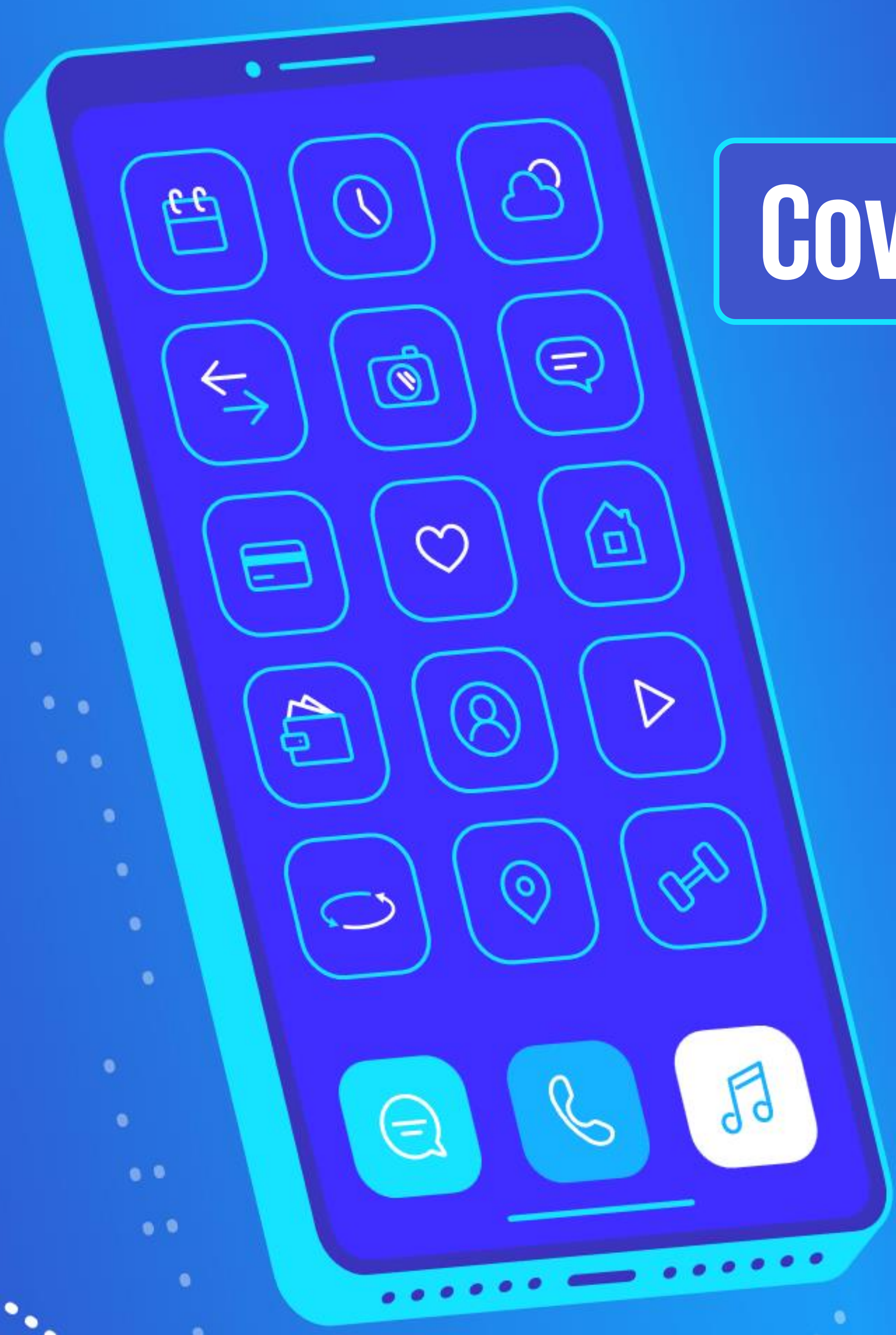
- Policy
- Compliance
- Roles
- Audit
- Legal
- Risk

Security Measures / Controls

- Data Security
- Identity and Access Management
- Network Security
- Application Security Life Cycle
- Incident Response
- Fraud Risk
- Data Privacy
- Infrastructure Security
- Other Security Measures
- Application Programming Interfaces (APIs)

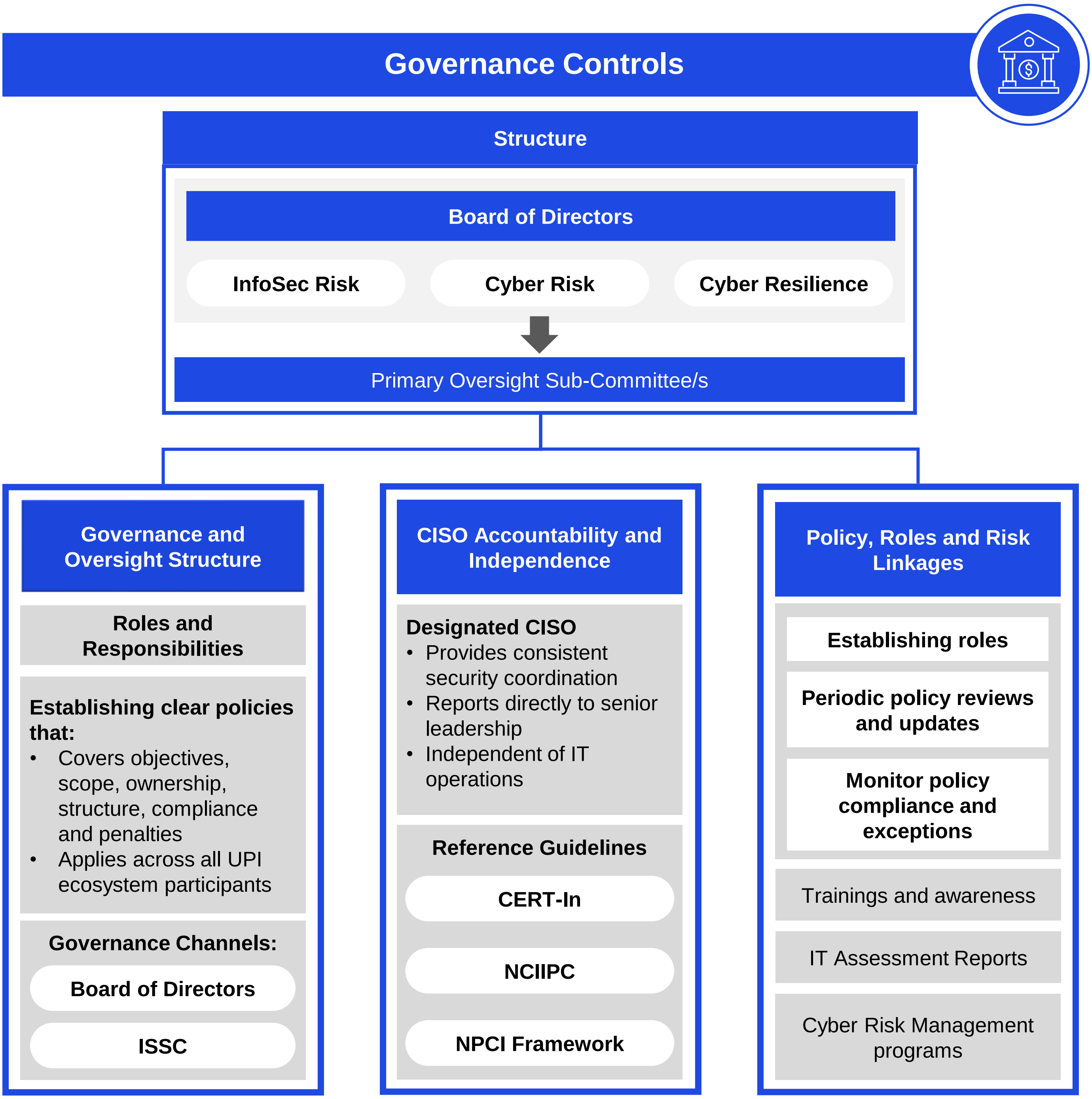
Operational Review

- Business Continuity Plan (BCP)
- Infrastructure Resiliency
- VAPT Testing and Re - assessment
- Logging and Monitoring
- Architecture Review



Coverage

Coverage: Governance controls



Governance Controls

Structure

Board of Directors

InfoSec Risk | Cyber Risk | Cyber Resilience

Primary Oversight Sub-Committee/s

Governance and Oversight Structure

Roles and Responsibilities

Establishing clear policies that:

- Covers objectives, scope, ownership, structure, compliance and penalties
- Applies across all UPI ecosystem participants

Governance Channels:

- Board of Directors
- ISSC

CISO Accountability and Independence

Designated CISO

- Provides consistent security coordination
- Reports directly to senior leadership
- Independent of IT operations

Reference Guidelines

- CERT-In
- NCIIPC
- NPCI Framework

Policy, Roles and Risk Linkages

Establishing roles

Periodic policy reviews and updates

Monitor policy compliance and exceptions

Trainings and awareness

IT Assessment Reports

Cyber Risk Management programs

Security Measures / Controls

Operational Review

Coverage: Security measures / controls

Governance Controls

Security Measures / Controls

Data	Encryption	Storage	Protection	Masking	Deletion	
Identity and Access Management	Privileged Identity Management	Authorization	Multifactor Authentication	Whitelist Mechanism	Roles	Access Mechanism
Network Security	Firewall	VPN	Anti-Malware Solutions	Network Segmentation	TLS	Routing
Application Security	SDK Handling and Device Binding	API and POS Security	Hardening and Patching			
Fraud Management	Detection	Prevention	Reporting			
Incident Management	Logging	Investigating	Reporting			
Infrastructure	Resilience	Testing	Scalability	Redundancy	Monitoring	

Operational Review

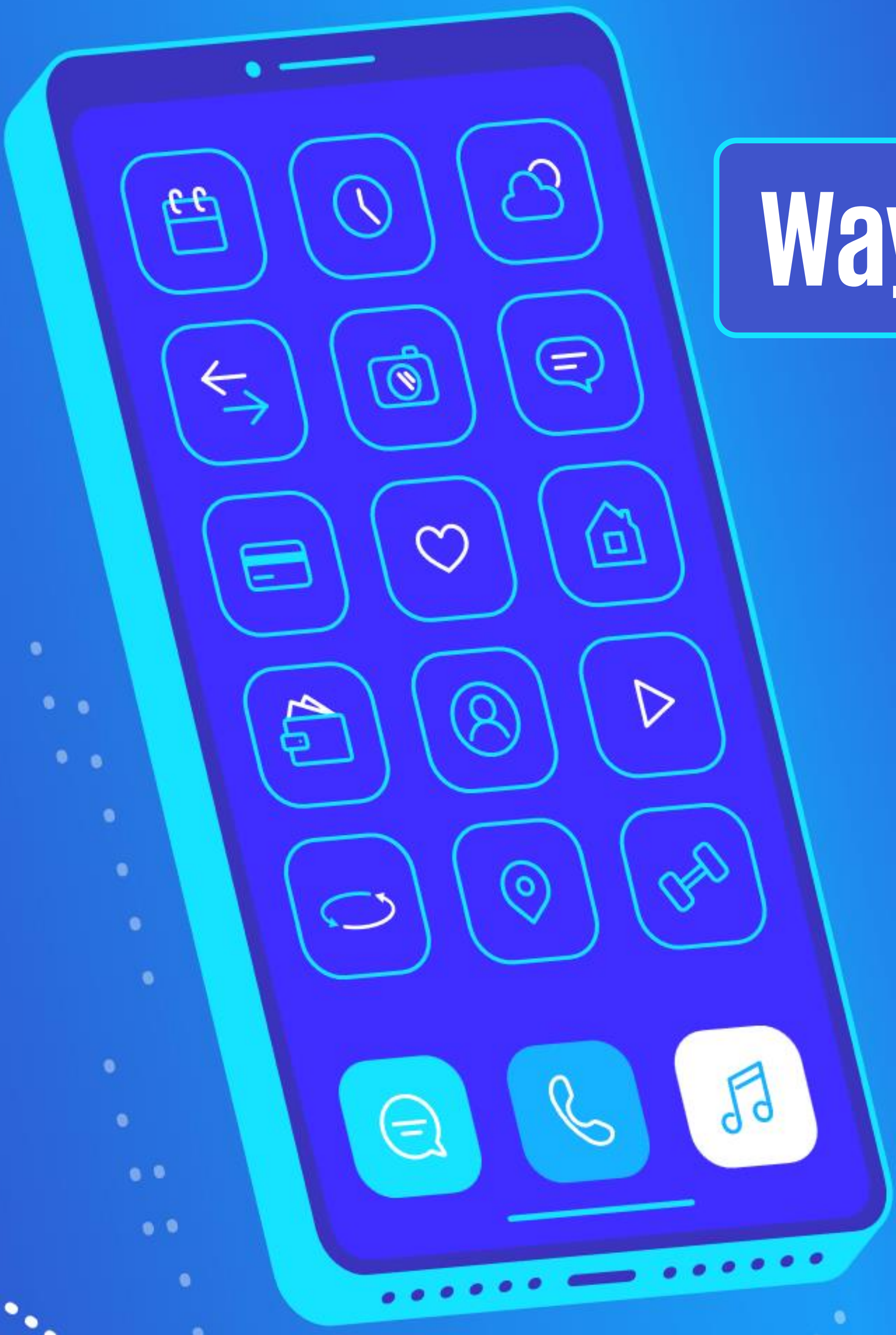
Coverage: Operational review

Governance Controls

Security Measures / Controls

Operational Review

Business Continuity Plan	Data Leak Prevention Policy	High Availability	Disaster Recovery (DR)	DR Drills	Recovery Time Objective Recovery Point Objective
Infrastructure Resiliency	Capacity	Performance	Reliability		
Testing	VAPT	Validation and Benchmarking	Re-assessment and Closure	Source Code Review	Application Security Assessment
Logging and Monitoring	Alerts and Tracking	Oversight and Retention	Reporting to Regulators		
Review	Architectural Review	ISO 27001 and PCI DSS	Timely Closure of Audit Findings		



Way Forward

Way Forward for organisations to comply with UPI InfoSec Compliance Framework 2025 - aligned with CMMI model

1 Initial

- Initiate CERT-In empaneled information security auditor reviews annually.
- Review and update Information Security and Cyber Security Policy.
- Establish foundational security controls adhering to industry-best practices.

2 Managed

- Identify and revisit key risk indicators focusing on cybersecurity.
- Review adherence to RBI and NPCI directives on Payment Security and Data Localization.
- Establish periodic technical assessments across critical systems and applications.

.

3 Defined

- Conduct structured employee awareness programs on cybersecurity and fraud vectors.
- Review robustness of UPI ecosystem and architecture.
- Align technical reviews with evolving regulatory and operational needs.

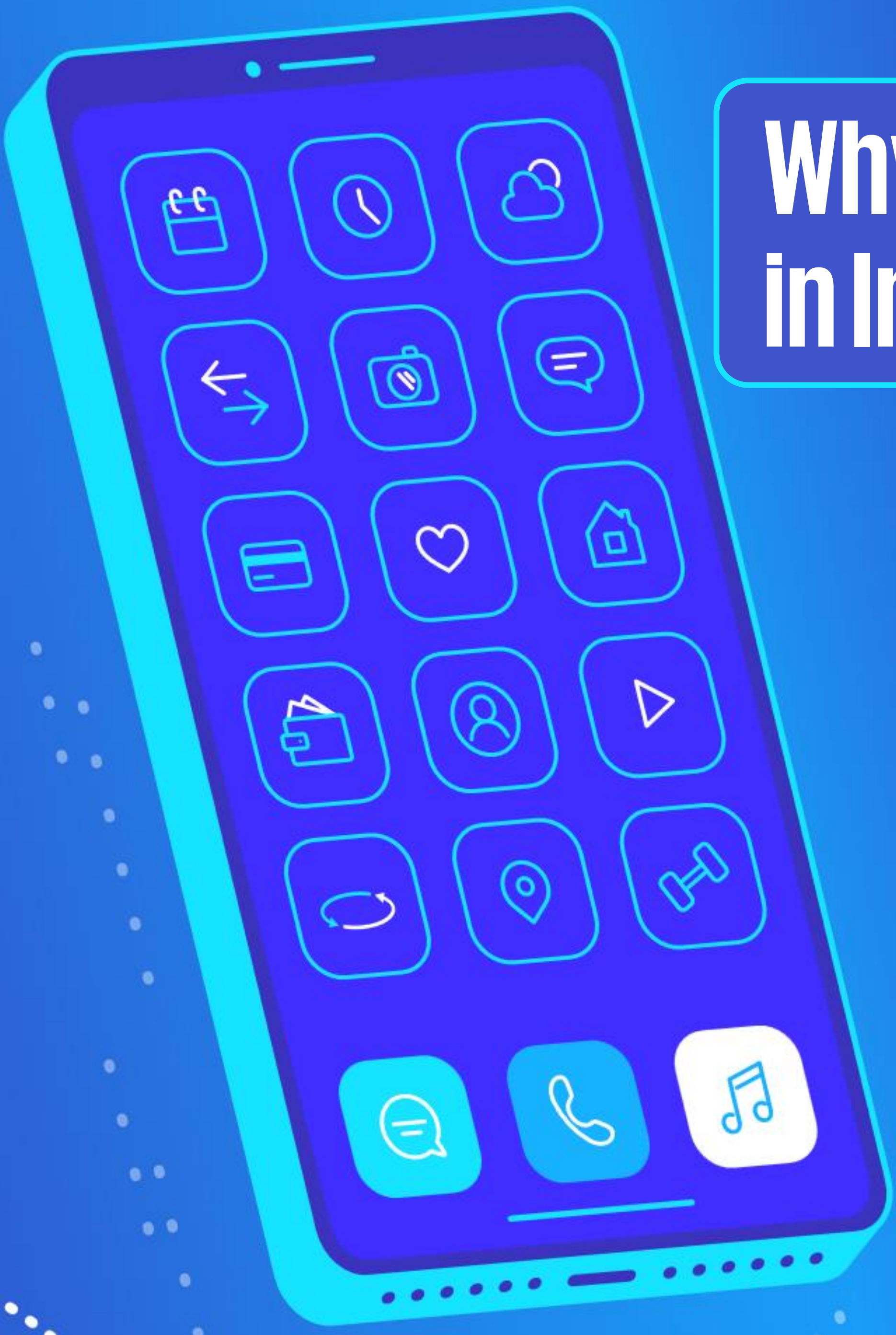
4 Optimizing

- Integrate automated security tools within IT operations for real-time insights.
- Conduct periodic disaster recovery and simulation exercises with improved outcomes.
- Continuously review compliance posture and remediate previously identified gaps.

0 – 10 days

60 - 90 days

90 - 100 days



Why KPMG in India

Why KPMG in India

Regulatory Alignment

Helping businesses align UPI security standards with RBI, NPCI, and global regulations to avoid penalties.

Strengthening Cybersecurity and Risk Management

Assisting in fraud risk mitigation, VAPT execution, and secure encryption protocols to protect UPI transactions.

Enhancing Business Continuity and Disaster Recovery

Guiding businesses in resilient infrastructure planning, DR site placement, and failover strategies to prevent hindrances in operations.

Financial Sector Focus

Engaged with key players in India's UPI ecosystem including banks, third party application providers and aggregators.

Streamlining Audit Requirements

Assisting in audit readiness and NPCI-mandated submissions for financial institutions.

We have served our clients in their endeavor to achieve regulatory compliance in digital payments. A representative list of selected credentials is illustrated below:

Large multinational bank	Indian public sector client	Large Indian bank	Global card payment network
Global TPAP	Large payment aggregator	Indian private sector bank	Indian TPAP

Contributors:

- Pranay Mahaldar
- Jay Goyal
- Madhuri Gangaramani
- Aakansha Gupta

KPMG in India contacts:

Akhilesh Tuteja
Head – Clients & Markets
T: +91 124 254 9191
E: Atuteja@kpmg.com

Atul Gupta
Partner and Head of Function,
Digital Trust and Cyber
T: +91 98100 81050
E: atulgupta@kpmg.com

Kunal Pande
Partner, Co-Head - Digital Risk and
Cyber, Leader - Digital Trust for FS
T: +91 98926 00676
E: kpande@kpmg.com

Romharsh Razdan
Partner, Digital Trust
T: +91 99755 96366
E: romharsh@kpmg.com

kpmg.com/in

Access our latest insights on
KPMG Insights Edge

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai – 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.