KPMG

RBI's technology focused Master Directions

Issued on 31 July 2026

1. Cybersecurity, Technology: Risk, Resilience and Assurance Framework
2. Digital Payment Security Controls Directions



Cyber Risk & Compliance, Financial Services

September 2026

KPMG. Make the Difference.



01

Introduction

RBI's supervisory consolidation

RBI has moved from fragmented regulatory instructions to an entity-centric regulatory architecture, creating a new technology compliance framework across regulated entities.

Key message

- RBI has consolidated regulatory expectations across regulated entities through **entity-wise Master Directions issued** on **31 July 2026**, accompanied by the **repeal of existing circulars**.
- Technology oversight is now anchored around two interconnected domains that collectively address cybersecurity and digital payments security.
- All directions became effective immediately, requiring institutions to align existing controls and governance structures with the new regulatory architecture.

Entity types covered

- Commercial Banks
- Small Finance Banks
- Payments Banks
- Urban Co-operative Banks
- All India Financial Institutions
- Non-Banking Financial Companies (NBFCs)
- Credit Information Companies (CIC)

Master Directions

- Cybersecurity, Technology: Risk, Resilience and Assurance Framework
- Digital Payment Security Controls Directions

Key implications

- Technology risk is a regulatory priority, with expectations spanning governance, cybersecurity, resilience, and digital payment security
- Responsibility extends beyond technology teams, requiring active oversight from Boards, senior management, risk, compliance and security functions
- Supervisory focus is being placed on resilience, emphasising the ability to prevent, detect, respond to and recover from cyber and operational disruptions
- Cybersecurity and digital payments are increasingly interconnected, driving the need for integrated monitoring, reporting and assurance capabilities
- Organisations may need to reassess and realign existing controls, governance structures and operating models to demonstrate alignment with the new Directions and support supervisory readiness.

KPMG

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

02

RBI's technology focused Master Directions



RBI's Cybersecurity, Technology: Risk, Resilience and Assurance Framework Directions

RBI issued the Cybersecurity, Technology: Risk, Resilience and Assurance Framework Directions on 31 July 2026, consolidating regulatory expectations related to technology governance, cybersecurity, operational resilience and information systems assurance across seven regulated entities.

Overview

Establishes a unified framework for technology governance, cybersecurity, operational resilience and assurance across regulated entities.

Applicability

- Commercial Banks
- Small Finance Banks
- Payments Banks
- Urban Co-operative Banks
- Credit Information Companies
- All India Financial Institutions
- NBFCs

Key themes

Governance: Two of eight chapters - Role of the Board and IT Governance and Oversight carries details on roles and responsibilities.

Baseline controls: Chapter V sets 31 baseline control domains, labelled A to EE. These form the minimum requirements for regulated entities.

Resilience: Business continuity, disaster recovery, cyber incident response and recovery, and forensics sit together are areas in focus.

Continuous monitoring: Continuous surveillance, real-time threat defence, risk-based transaction monitoring and a dedicated Cyber Security Operations Centre chapter.

Third party risk: Third-party arrangements is the longest sub-section of Chapter V and sits inside the set of baseline requirements.

Information systems (IS) Audit: A standalone IS Audit chapter, plus metrics and audit committee oversight, make assurance a structural requirement.

Major changes introduced

Consolidates earlier cybersecurity and IT governance requirements	A Cyber Security Operations Centre chapter	Incident reporting	Red teaming
Combines multiple technology risk, governance and cybersecurity instructions into a single supervisory framework.	The Cyber Security Operations Centre which was previously covered in annexes, is now a standalone chapter (VI).	Reporting is to the RBI DAKSH platform, within six hours of detection.	The direction states the bank 'may' conduct red teaming exercises

KPMG

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

RBI's Digital Payments Security Controls Directions

RBI issued the Digital Payment Security Controls Directions on 31 July 2026, establishing a comprehensive security framework for digital payment channels, customer authentication, application security and fraud prevention controls across five regulated entities.

Overview

Establishes security expectations across digital payment ecosystems through governance, authentication, application security and fraud prevention controls.

Applicability

- Commercial Banks
- Small Finance Banks
- Payments Banks
- Urban Co-operative Banks
- Credit Card Issuing NBFCs

Key themes

Channel architecture

Three channel-specific chapters are present - internet banking, mobile payments and cards for banks; web application, mobile application and cards for NBFCs.

Authentication framework

Authentication is treated as a framework that is designed and governed, in addition to specific controls to be implemented.

Product-based applicability

The direction covers any digital payment product or service offered for financial or non-financial transactions, expressly including balance enquiry, PIN set and change and OTP generation.

Fraud and reconciliation

Fraud risk management and reconciliation mechanism are covered as chapters of the general controls.

Major changes introduced

Role of the Board

Chapter II now requires board-approved policies including for digital payment products and services.

NBFC scope

Applicability is limited to credit-card-issuing NBFCs, stated in the applicability clause of a dedicated NBFC direction.

Entity-specific Directions

Replaces one common direction with five entity-specific directions aligned to individual business models and channels.

KPMG

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



03

Way forward

Key takeaways from the Directions

01

A six-hour cyber incident reporting obligation

Cyber incidents must be reported within six hours of detection on the DAKSH platform, along with an obligation to proactively notify CERT-In regarding these cyber incidents.

02

Vulnerability assessment and penetration testing cadences

For critical information systems and those in the demilitarized zone carrying a customer interface, vulnerability assessment must be conducted at least **once every six months** and penetration testing at least **once every twelve months.** For non-critical systems a risk-based approach determines the requirement.

03

Disaster recovery (DR) drill periodicity is fixed for critical systems, with a re-test requirement

DR drills for critical information systems must be **conducted at least half-yearly**. Any major issue observed during a drill must be resolved and re-tested successfully before the next cycle.

04

Third-party technology arrangements are covered in the Cybersecurity Master Directions

Third-party arrangements is the longest sub-section of Chapter V and covers all third-party **arrangements not within the scope of the RBI Managing Risks in Outsourcing Directions**.

05

Digital payment obligations apply to products, including non-financial uses

The Digital Payment Security Controls Directions covers any digital payment product or service offered **for financial or non-financial transactions**, expressly including balance enquiry, PIN set and change, mobile banking registration and one-time password generation

06

A policy for digital payment products is mandated

A **board approved policy** covering digital payment products and services is to be formulated with details on product parameters, risk management, regulatory compliance, customer experience, and payment security requirements.

KPMG

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

What regulated entities should do next



- Identify applicable Directions based on entity type
- Assess security and payment-related applicability requirements
- Establish a documented applicability register

- Map existing policies and standards to the new Directions
- Update references to repealed circulars
- Align governance, risk and control frameworks

Output: Control-to-regulation mapping

- Evaluate governance arrangements
- Assess cybersecurity and payment security controls
- Identify capability and operating model gaps

Output: Prioritised gap assessment

- Address identified control gaps
- Address gaps in monitoring, reporting and resilience capabilities.
- Update procedures and technology enablement mechanisms

Output: Remediation roadmap

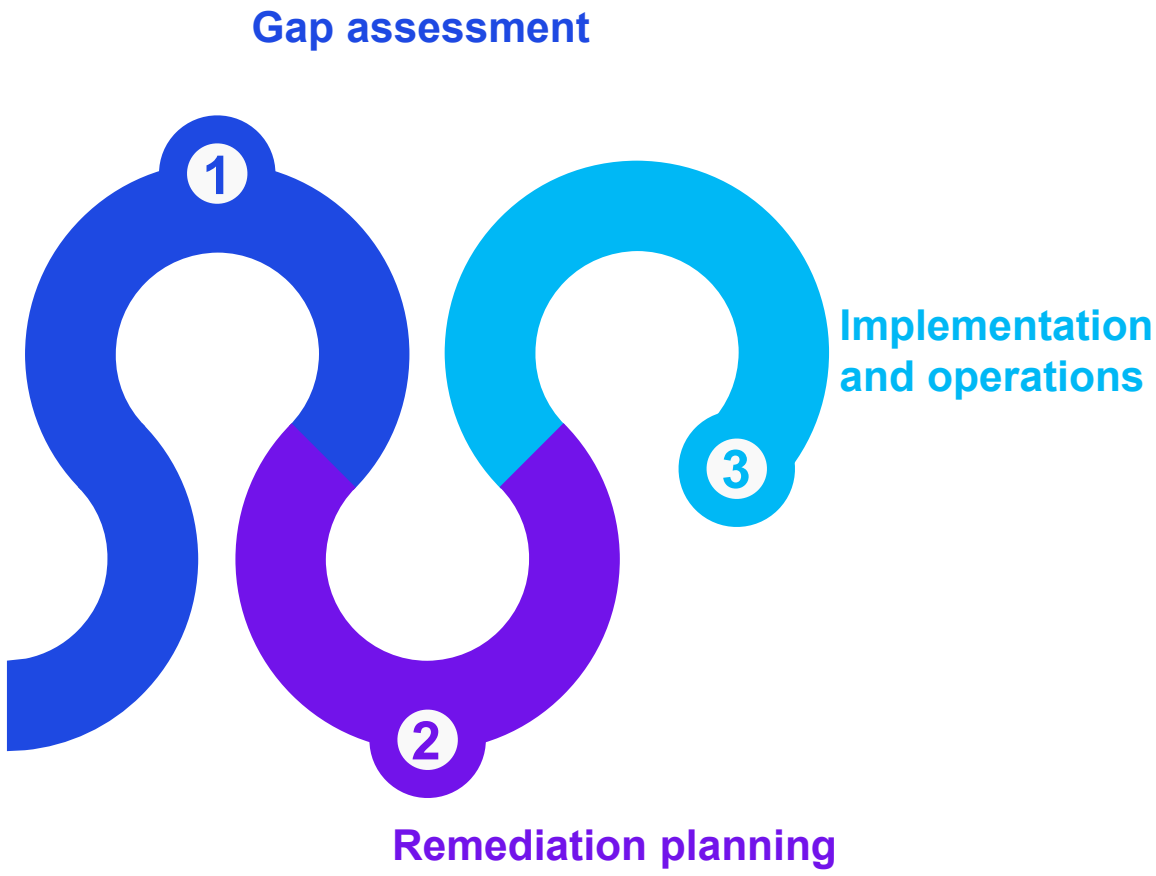
- Align audit and review programs
- Align regulatory reporting and evidence management processes with the new Directions.
- Establish ongoing governance and oversight mechanisms

Output: Supervisory readiness and assurance framework

The immediate priority is not the implementation of new controls, but the ability to demonstrate that existing governance, security and digital payment security practices are aligned to the new RBI Directions.

KPMG
© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
Document Classification: KPMG Public

How KPMG in India can help



Gap assessment

- Determine applicable Directions based on entity type and business activities
- Assess impact across governance, cybersecurity, payment security and fraud management
- Identify regulatory obligations and expectations
- Review readiness against the new framework

Remediation planning

- Map existing policies, standards and controls to the new Directions
- Prioritise remediation based on risk and supervisory exposure
- Update operating procedures and reporting mechanisms

Implementation and operations

- Implement prioritised remediation actions and control enhancements
- Update processes, procedures and technology configurations to meet the new Directions
- Operationalise monitoring, reporting and issue-management mechanisms
- Support continuous compliance and supervisory readiness

KPMG
© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Acknowledgements

Contributors:

- Aakansha Gupta
- Allan Dev
- Darrian Bharucha

Source: RBI's Cybersecurity, Technology: Risk, Resilience and Assurance Framework and Digital Payment Security Controls Directions issued on 31st July 2026



© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG in India contacts:

Akhilesh Tuteja
Partner & National Leader,
Clients and Markets
KPMG in India
E: atuteja@kpmg.com

Kunal Pande
National Leader – Cyber, Risk
and Compliance Services
KPMG in India
E: kpande@kpmg.com

Sundar Ramaswamy
Partner, Cyber, Risk and
Compliance Services
National Co-Leader- Cyber
Risk & Control Services
E: sr@kpmg.com

Rahul Singhal
Partner, Cyber, Risk and
Compliance Services
National Co-Leader- Cyber
Risk & Control Services
E: rahulsinghal@kpmg.com

Rohan Padhi
Partner, Cyber, Risk and
Compliance Services
Lead Responsible AI
E: rohanpadhi@kpmg.com

Romharsh Razdan
Partner, Cyber, Risk and
Compliance Services
Lead RegTech Compliance
E: romharsh@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

Access our latest insights
on KPMG Insights Edge

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. This document is for informational purposes only and does not promote or endorse any company, product, or service.

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.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.