Reserve Bank of India guidelines for NEFT and RTGS payment systems

KPMG. Make the Difference.

March 2025

kpmg.com/in

About the Reserve Bank of India guidelines

Reserve Bank of India (RBI) had issued guidelines for Real-time Gross Settlement (RTGS) System Regulation Version 1.0 (dated 21 October 2024) and National Electronics Funds Transfer (NEFT) System Procedural Guidelines Version 1.1 (dated 25 October 2024) for enhancing efficiency, security, and reliability of these systems.

Applicability

RTGS	NEFT
Real-Time settlement	Deferred settlement in half hourly batches
High Value Transactions	Small to medium sized transactions
Gross Settlement	Deferred Net Settlement (DNS)
Minimum transaction amount is INR 2 lakhs	No minimum or maximum transaction limit

Key Stakeholders

RBI

Sending Participant

Receiving Participant

Objectives

RTGS Guidelines

1. Facilitate real-time settlement
2. Establish governance and management framework
3. Define membership review processes and access criteria
4. Enforce baseline cyber security guidelines
5. Ensure customer transaction efficiency and compliance
6. Lay focus on RBI guidelines for Digital Payment Security Controls.

NEFT Guidelines

1. Enhancing efficiency and security
2. Improve customer protection and service
3. Structured governance and framework
4. Define dispute resolution and compliance mechanisms
5. Gather feedback from industry for improvements in system
6. Define settlement and default handling processes.

As part of circular requirements, participants are required to submit annual compliance reports to RBI comprising of status of review of:

1. **Access criteria for members**
2. **Technology requirements.**

Access criteria for members

Access criteria means a set of norms issued by RBI from time to time to allow a member to access the payment systems. The criteria is defined as part of the RTGS guidelines. In case of NEFT, the payment participant has to be an existing member of the RTGS system or apply for both RTGS and NEFT systems. The membership needs to be reviewed on an annual basis.

Eligibility

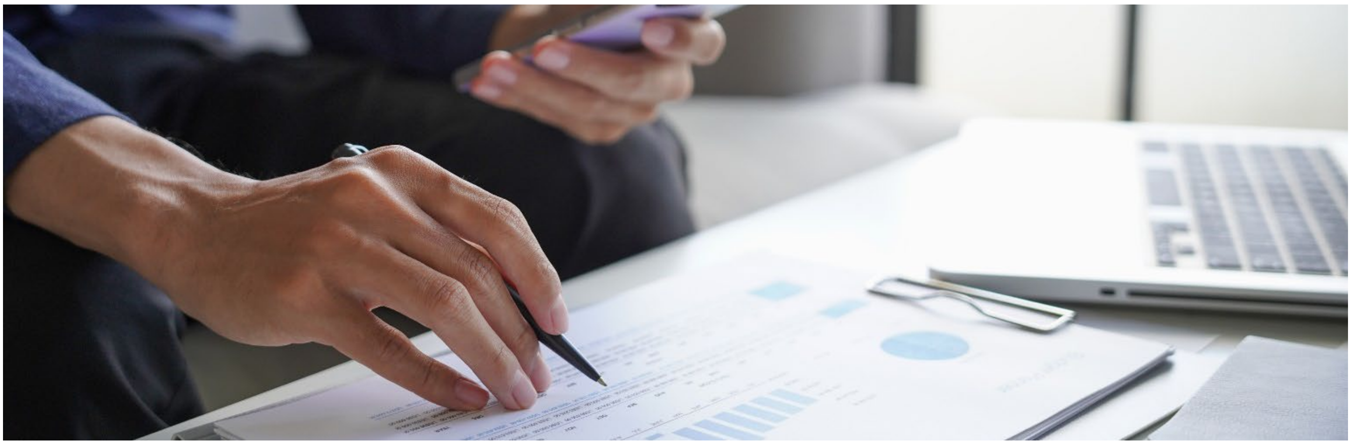
- **Open** to scheduled/licensed banks, standalone primary dealers, Prepaid Payment Instruments (PPI) issuers, white label Automated Teller Machine (ATM) operators, and card networks
- **Exclusions** include cooperative societies and unlicensed banks. RBI may permit other entities on case-to-case basis
- **Eligible** participants need to submit an application form to the RBI and the approval is subject to favorable supervisory/regulatory recommendation
- **Unique primary Indian Financial System Code** is granted to every approved participant which is to be used for RTGS and NEFT.

Membership

- The participant must hold **valid license/authorisation/registration** from relevant financial regulator, operate on a Core Banking System setup, and achieve cyber resilience requirements
- Compliance with RBI guidelines on **Storage of Payment Systems Data (Data Localisation)** and with the **cyber security baseline standards** mentioned in circular Annexure is mandated
- **Other specific requirements** also include membership with INFINET and SFMS, maintenance of current account, settlement account, and Subsidiary General Ledger with RBI and other specific requirements as required by RBI.

Financial Criteria

- **Scheduled/Licensed Banks** – compliance with CRAR requirements of RBI, Net Non-performing Assets (NPA) below 5 per cent (as per latest audited balance sheet), and minimum net worth prescribed by RBI or INR25 crore (whichever is greater)
- **Authorised Non-bank PSPs** - minimum net worth prescribed by RBI or INR25 crore (whichever is greater)
- **Standalone Primary Dealers** - minimum net worth prescribed by RBI or INR25 crore (whichever is greater) and compliance with CRAR requirements of RBI.



Source: Real-time Gross Settlement System Regulation, RBI, Version 1.0 (dated 21 October 2024) and National Electronics Funds Transfer System Procedural Guidelines, RBI, Version 1.1 (dated 25 October 2024)

Technology requirements

Cyber Security Baseline Standard

Areas	Requirements		
Inventory Management	Up-to-date asset inventory	Tracking of end-of-support systems	Availability of annual maintenance contracts
Network Security	Use of firewalls and intrusion detection systems	Perimeter security and network segmentation	Disabling of Remote Desktop Protocol
Unauthorised Software	Identification of unauthorised software	Continuous monitoring	Blocking or prevention on all systems
Change and Patch Management	Change approval matrix	Periodic patch updates	Change and patch testing
Access Management	Usage of least privilege principle	Multi-factor authentication	Segregation of duties
Email Security	Prevent email spoofing	Secure email gateway	Configuration of DMARC
Fraud Monitoring	Configuration and review of rules	Preventive and detective types of controls	Customer alerting
Disaster Recovery (DR)	Setup of DR site	Periodic DR Drill testing	Documentation of learnings and results
Backup Management	Periodic backups	Data security configurations for backups	Restoration testing processes
Application Security Life Cycle	‘Secure by design’ approach	Source code reviews	Static and Dynamic Application Security Testing
Use of Digital Certificates	Adherence to IDRBT CA guidelines	Availability of documentation	Monitoring for expiration of Digital Certificates
Logging and Monitoring	Setup of Security Operations Centre	Identification of log sources	Periodic review of log readiness
Cryptography Controls	Encryption for data at-rest and in-transit	Secure key length, algorithms, and cipher suites	Periodic review of configurations
Vulnerability Management	Bi-annual Vulnerability Assessment	Annual Penetration Testing	Tracking of finding closures

SAR

For continued adherence to the access criteria and cyber security guidelines, members are mandated to submit an annual system audit report (SAR) to RBI. The review is required to be conducted by a CERT-In empanelled information security auditor for NEFT and RTGS systems.

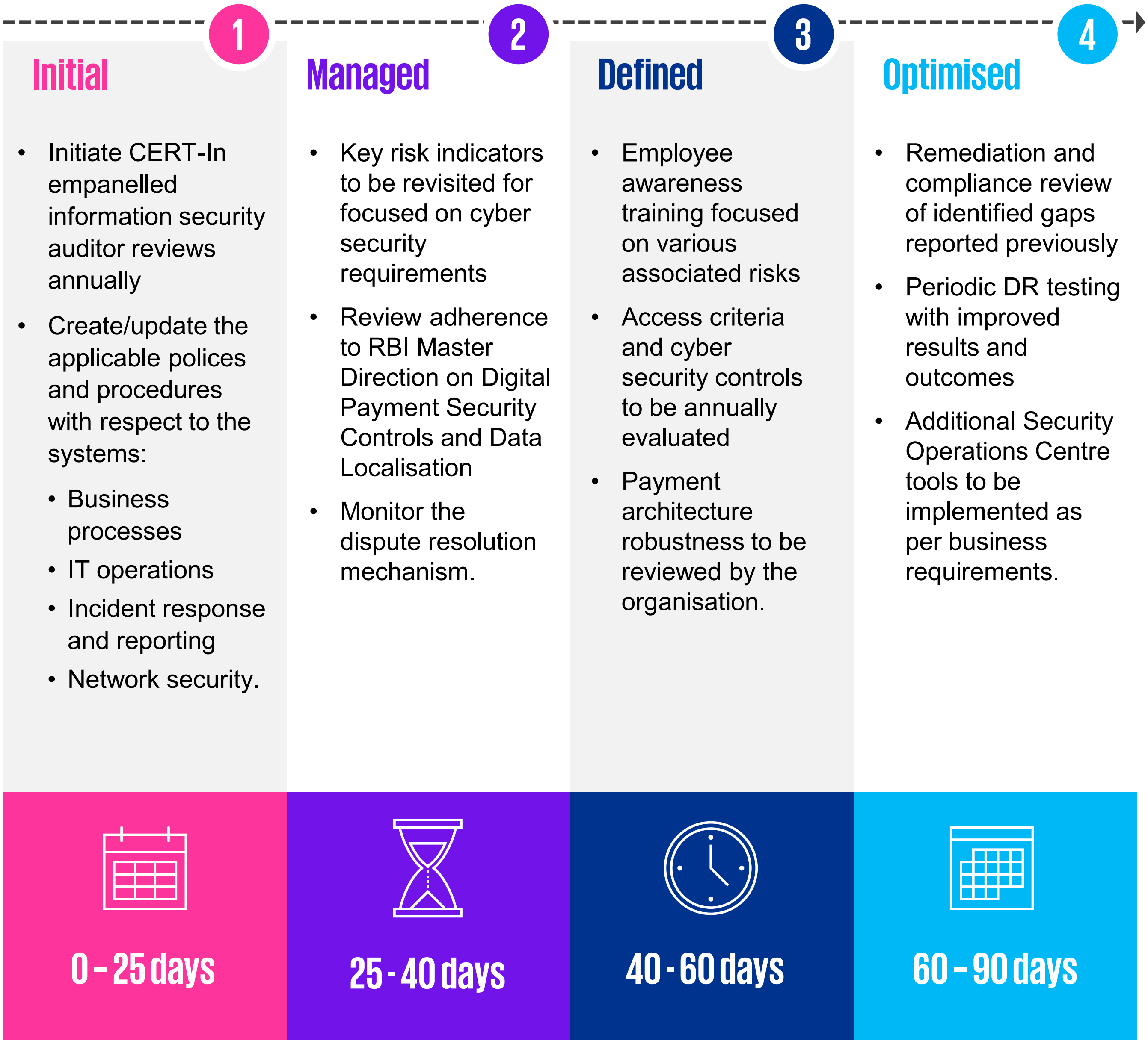
Rules

Circular recommends adherence to rules and guidelines of INFINET, INFINET framework, SFMS, Digital Payment Security Controls, and Storage of Payment System Data as updated from time-to-time.

Source: Real-time Gross Settlement System Regulation, RBI, Version 1.0 (dated 21 October 2024) and National Electronics Funds Transfer System Procedural Guidelines, RBI, Version 1.1 (dated 25 October 2024)

Way forward for organisations to comply with NEFT and RTGS cyber security guidelines

Aligned to CMMI model



1 Initial

- Initiate CERT-In empanelled information security auditor reviews annually
- Create/update the applicable polices and procedures with respect to the systems:
  - Business processes
  - IT operations
  - Incident response and reporting
  - Network security.

0 – 25 days

2 Managed

- Key risk indicators to be revisited for focused on cyber security requirements
- Review adherence to RBI Master Direction on Digital Payment Security Controls and Data Localisation
- Monitor the dispute resolution mechanism.

25 - 40 days

3 Defined

- Employee awareness training focused on various associated risks
- Access criteria and cyber security controls to be annually evaluated
- Payment architecture robustness to be reviewed by the organisation.

40 - 60 days

4 Optimised

- Remediation and compliance review of identified gaps reported previously
- Periodic DR testing with improved results and outcomes
- Additional Security Operations Centre tools to be implemented as per business requirements.

60 – 90 days

Source: Real-time Gross Settlement System Regulation, RBI, Version 1.0 (dated 21 October 2024) and National Electronics Funds Transfer System Procedural Guidelines, RBI, Version 1.1 (dated 25 October 2024)

About KPMG in India

Our digital payments security portfolio offers a diverse range of services to assist businesses in meeting regulatory requirements and generate value. Drawing on our extensive global and Indian expertise, we help businesses create customised, structured, and adaptable strategies to build and maintain robust payment systems. This approach not only helps with regulatory compliance but also unlocks economic potential.

KPMG in India has assisted multiple regulators and financial organizations with documenting various information security guidelines and circulars.

Wide range of cyber service line offerings

- Cyber strategy and governance
- Cyber transformation
- Cyber defence
- Cyber response
- Cyber managed services

Sector Focus

- Financial sector is a **focused** sector in India
- Working with leading **Public and Private sector Banks** in India
- Working with leading **FinTech's** and **NBFCs**
- Working with number of **Regulators** and **Government Bodies**
- Working with leading **Insurance** companies
- Working with large **multinational investment banks.**

KPMG in India has vast experience in helping clients to **meet regulatory obligations** and assess their current **cyber security risk posture.**

Clients are also **advised** on how to improve payment systems to help with **secure, efficient, and reliable transactions**, hence fostering **stability.**

Global Industry Recognition

KPMG in India has received multiple global awards and recognition in the field of consulting, cyber security risk management, data intelligence, and data management.

Our Values

We are committed to quality and service excellence in services we provide, helping our clients to earn public trust through our actions and behaviors both professionally and personally.

Integrity

We do what is right

Courage

We think and act boldly

For Better

We do what matters

Excellence

We never stop learning and improving

Together

We respect each other and draw strength from our differences

Cyber Centers and Labs with dedicated resources in Mumbai, Delhi, and Bengaluru.

KPMG in India team is a mix of Engineers, MBAs, Charted Accountants who work together to deliver innovative solutions to our clients.

Robust team with different certifications like ITIL, PMP, CSM, CBE, COBIT, SSCP, CCSP, CISA, CISM, CRISC, CISSP, and ISO LA/LI.

Acknowledgements

Contributors:

- Aakansha Gupta
- Madhuri Gangaramani

Design and Compliance:

- Angeeta Baweja

KPMG in India contacts:

Akhilesh Tuteja
Global Head
Cyber Security
E: atuteja@kpmg.com

Atul Gupta
Partner, Head of Function
Digital Trust and Cyber
E: atulgupta@kpmg.com

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

Rohan Padhi
Partner and Co-Lead
Digital Risk and Cloud Security
E: rohanpadhi@kpmg.com

Romharsh Razdan
Partner, Lead Payment Risk and
Co-Lead Cloud Security
E: romharsh@kpmg.com

Divya Poojari
Director, Digital Risk and
Cloud Security
E: divyap@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.