

COMPLIANCE PLAYBOOK · BFSI · MARCH 2026

RBI, CERT-In & DPDPA Compliance Playbook:

MFA as the Foundation of BFSI Security

A practical guide for CISOs, IT heads, and compliance officers at Indian banks, NBFCs, insurance companies, and payment system providers

Table of Contents

<u>1. Up Front</u>	3
<u>2. The Regulatory Landscape</u>	4
• 2.1 RBI Authentication Mechanisms Directions 2025	5
• 2.2 CERT-In Comprehensive Cyber Security Audit Policy Guidelines 2025	6
• 2.3 Digital Personal Data Protection Act 2023	7
• 2.4 SEBI Cybersecurity and Cyber Resilience Framework	8
<u>3. The Control Gaps</u>	8
• 3.1 The Authentication Coverage Gap	8
• 3.2 The SMS OTP Dependency	9
• 3.3 The Vendor and Third-Party Access Gap	10
• 3.4 The Compliance Documentation Gap	11
<u>4. The MFA Implementation Framework for BFSI</u>	11
• 4.1 Regulatory-to-Technical Requirements Map	11
• 4.2 Factor Selection by User Population	13
• 4.3 Deployment Sequencing	15
<u>5. Cisco Duo for BFSI — The Architecture Case</u>	18
• 5.1 The Mixed-Environment Reality of Indian BFSI	18
• 5.2 Data Residency	18
• 5.3 Phishing-Resistant MFA for Privileged Accounts	19
• 5.4 The Audit Trail	20
<u>6. The BFSI Compliance Calendar</u>	21
<u>7. Frequently Asked Questions</u>	22
<u>8. About the Authors</u>	25

1. Up Front

Three regulators. Four frameworks. Overlapping deadlines. All pointing at the same control gap.

The Reserve Bank of India's Authentication Mechanisms Directions 2025, in force from 1 April 2026, mandate flexible two-factor authentication across all digital payment transactions. CERT-In's Comprehensive Cyber Security Audit Policy Guidelines, effective 25 July 2025, make annual cybersecurity audits mandatory for every private sector organisation in India and explicitly require MFA for all remote access. The Digital Personal Data Protection Act 2023, with full enforcement deadline of 13 May 2027, requires "reasonable security safeguards" for personal data — a standard that no credible legal interpretation in 2026 excludes MFA for systems handling financial and customer data.

For Indian BFSI organisations, these three frameworks are not three separate compliance workstreams. They are three angles of examination of the same underlying question: does your organisation know, with evidence, who accessed what system, when, and from where?

Why MFA is the foundation — not just a component

MFA is foundational in a precise operational sense: every downstream control depends on knowing who is accessing the system, and MFA is the only control that establishes that fact. Access logging proves nothing if you cannot establish that the logged user was actually the person who authenticated. Privileged access management fails if a privileged account was accessed by an attacker holding stolen credentials. Threat detection cannot identify anomalous behaviour if there is no authenticated identity baseline to deviate from.

This playbook maps each framework to specific operational requirements, identifies the control gaps most commonly found in Indian BFSI environments, and provides a structured implementation roadmap. It is written for organisations that have already decided MFA is necessary and need to understand exactly what "necessary" means under each regulatory lens — and what it looks like in practice for a bank branch network, an NBFC treasury system, or a fintech platform processing millions of daily transactions.

2. The Regulatory Landscape

Visual 1 — The BFSI Compliance Deadline Map

Four regulatory frameworks, four deadlines. Two already in force. One now effective. One thirteen months away.

Framework	Core MFA Requirement	Status	Evidence Required
SEBI CSCRf	MFA for privileged access to all trading, risk management, and back-office systems	ALREADY IN FORCE Jan–Apr 2025	Annual SEBI-recognised audit 90-day log retention
CERT-In CISO-2025-02	MFA for ALL remote access; named individual accounts; 180-day logs in India	ALREADY IN FORCE 25 July 2025	Annual third-party audit; 180-day log archive; access review records
RBI Authentication Directions 2025	2FA mandatory for all digital payment transactions; at least one dynamic factor; factor independence	NOW EFFECTIVE 1 April 2026	Granular auth logs per transaction; RBI examination readiness
DPDPA 2023	Reasonable security safeguards for all systems handling personal data (MFA is baseline standard)	APPROACHING 13 May 2027	Breach investigation evidence; access governance documentation; penalty: up to ₹250 crore

RBI IT Governance Master Direction (ongoing): Separately requires MFA for all employee access to critical banking systems including core banking, treasury, and internet banking back-end.

2.1 RBI Authentication Mechanisms Directions 2025

On 25 September 2025, the Reserve Bank of India issued the Authentication Mechanisms for Digital Payment Transactions Directions, 2025. These came into force on 1 April 2026. They apply to all Payment System Providers, Payment System Participants — including every bank and non-bank entity in India's payment ecosystem — and cover all domestic digital payment transactions unless specifically exempted.

Visual 2 — RBI Directions 2025: Factor Classification and Independence Principle

The three factor categories and the principle that makes them work. Both factors must operate through independent channels.

SOMETHING YOU KNOW	SOMETHING YOU HAVE	SOMETHING YOU ARE
Password or PIN Secret question response Transaction PIN	Hardware token (TOTP) Authenticator app (TOTP) SMS OTP on registered device Physical payment card	Fingerprint biometric Facial recognition Voice recognition Iris scan

FACTOR INDEPENDENCE PRINCIPLE

The reliability of one factor must not affect the other. A mobile device cannot be both the payment initiation channel AND the sole MFA delivery channel for the same transaction.

Practical implication: For mobile banking transactions, SMS OTP delivered to the same phone initiating the transaction may not satisfy the independence requirement for higher-risk transactions.

The shift away from SMS OTP dependency is deliberate and documented. The RBI's own regulatory statements cite a consistent rise in phishing, SIM-swap, and device-spoofing attacks - patterns that specifically exploit SMS-based authentication. The Directions do not prohibit SMS OTP but signal clearly that it is insufficient as the sole dynamic factor for higher-risk transactions. Banks and payment providers are expected to implement risk-based authentication that assesses transaction amount, device recognition, user location, and behavioural patterns.

KEY POINT

The RBI Directions 2025 cover payment transactions. Internal employee access to core banking, treasury, and internet banking back-end systems is governed by the RBI IT Governance Master Direction, which independently requires MFA for all employee access to critical information systems, formal privileged access management, and documented access reviews. Together, the two frameworks create a comprehensive MFA obligation covering both customer-facing payment authentication and internal system access.

DATA

₹54.78 crore in penalties were issued by RBI to 353 regulated entities in FY 2024-25 for cybersecurity non-compliance. (RBI Annual Report / RBI press releases, FY 2024-25)

2.2 CERT-In Comprehensive Cyber Security Audit Policy Guidelines 2025

On 25 July 2025, CERT-In published the Comprehensive Cyber Security Audit Policy Guidelines (CISG-2025-02), issued under Section 70B of the Information Technology Act, 2000. These are the most consequential cybersecurity compliance development for Indian private sector organisations in over a decade.

Annual cybersecurity audits are now mandatory for all organisations in India - public and private - that own or operate information technology systems. The previous mandate was limited primarily to government entities and critical infrastructure. That limitation no longer exists. Sectoral regulators including RBI and SEBI retain discretion to mandate more frequent audits based on risk profile.

What CERT-In auditors will specifically examine in a BFSI environment:

- MFA for all remote access - including VPN, remote desktop, and all third-party and contractor access. Auditors will examine whether MFA is enforced, not merely available, and whether documented exceptions exist with compensating controls.
- Named individual accounts for all critical system access. Shared accounts - the shared treasury workstation credential, the generic admin login - will be flagged as control deficiencies regardless of whether MFA is deployed on top of them.

- Principle of least privilege applied across all users and systems, with documented role definitions and evidence of access removals when roles change.
- 180-day authentication logs retained in India, available for export during the audit window, demonstrating individual accountability for every access event.

KEY POINT

CERT-In's 180-day log retention requirement applies to: identity provider and authentication logs; remote access session logs; VPN gateway logs; and privileged access event logs. Logs must be stored in India. The audit examines whether logs are retained and accessible, not merely whether MFA is deployed.

2.3 Digital Personal Data Protection Act 2023

The DPDPA 2023 and its 2025 Rules do not mention MFA by name. The Act requires data fiduciaries to implement "reasonable security safeguards" to protect personal data. This formulation is deliberate — it avoids prescribing specific technologies and allows the standard to evolve with the threat landscape.

Any system that stores, processes, or transmits personal data of Indian residents — which includes every core banking system, loan origination platform, insurance policy database, payment transaction record, and customer onboarding system in the BFSI sector — must be protected by controls a reasonable examiner in 2026 would consider adequate. Given that CERT-In explicitly mandates MFA for remote access, RBI requires two-factor authentication for payment transactions, and SEBI CSCRf mandates MFA for privileged access, the absence of MFA from systems handling personal data is not defensible as "reasonable" in a post-breach proceeding.

PENALTY

The Data Protection Board of India, once constituted — a process that was ongoing as of early 2026 — will adjudicate breach-related complaints and assess whether data fiduciaries met their obligations. The penalty for failure to implement security safeguards is up to ₹250 crore per instance (DPDPA 2023, Schedule 1 Item 4). Unlike RBI penalties, DPDPA penalties are triggered by breach events, not scheduled examination cycles.

2.4 SEBI Cybersecurity and Cyber Resilience Framework

The SEBI CSCRF compliance window is closed. Compliance deadlines for registered market participants ran from January to April 2025 by entity category. Stock brokers, depository participants, asset management companies, portfolio managers, KYC registration agencies, and market infrastructure institutions are all in scope.

The CSCRF explicitly mandates MFA for privileged access to all trading systems, risk management systems, and back-office infrastructure. It requires annual cybersecurity audits by SEBI-recognised auditors, 90-day log retention, and incident reporting within prescribed timelines. For SEBI-regulated entities that have not yet deployed MFA for privileged access: the question is not whether to deploy, but how to close the existing compliance gap as quickly as possible.

3. The Control Gaps

The following scenarios are composite illustrations drawn from Proactive's BFSI deployment experience. They are not descriptions of specific client environments. The patterns they represent are consistent with findings from DSCI's Cyber Security Maturity Survey (Data Security Council of India, India Cyber Threat Report 2025), which found that 57% of Indian organisations lack basic cyber hygiene practices and 73% are unaware of whether they have ever been attacked.

3.1 The Authentication Coverage Gap

Most Indian banks and NBFCs have deployed some form of MFA — typically for internet banking customer-facing authentication and, in more mature organisations, for corporate email and M365 access. The coverage gap sits in the systems that carry the highest internal risk.

Visual 3 — The Authentication Coverage Gap

What MFA typically covers in Indian BFSI environments versus what it typically misses. The gap on the right is where breaches happen.

TYPICALLY COVERED	TYPICALLY MISSING
• Microsoft 365 / email access • Internet banking portal (customer-facing) • Corporate VPN (sometimes) • Executive / senior management accounts <i>These are covered by most basic MFA deployments</i>	• Core banking terminal (branch staff) • Treasury and ALM platforms • Vendor and third-party remote access • Legacy ERP and back-office applications • Shared branch workstations • Domain, database, and infrastructure admins <i>These are covered by most basic MFA deployments</i>

A relationship manager at a branch accesses the core banking system — often a Finacle, Temenos, or Flexcube deployment — from a shared workstation using a username and password. The VPN used for inter-branch communication requires only a password. The same credential is known to colleagues who covered the workstation during leave. There is no second factor on the core banking logon. This describes a significant portion of Indian mid-tier banking operations.

3.2 The SMS OTP Dependency

The Indian financial sector built its authentication architecture on SMS OTP. It is ubiquitous, understood by customers, supported by every device, and deeply embedded in both customer-facing and employee-facing authentication flows. It is also the specific vulnerability that India's cybercrime statistics reflect.

DATA	Financial cyber fraud losses reported on India's National Cyber Crime Reporting Portal reached ₹36,450 crore as of February 2025, largely driven by phishing-led UPI fraud, SIM-swap attacks, and AI-assisted social engineering. (National Cyber Crime Reporting Portal, February 2025)
DATA	UPI fraud recorded 632,000 incidents in FY 2023-24, many facilitated by OTP interception through SIM-swap fraud. (NPCI / RBI Annual Report FY 2023-24)

For BFSI organisations planning MFA deployments, the SMS OTP transition plan is a required component of compliance architecture, not an optional upgrade. The RBI's 2025 Directions do not ban SMS OTP but signal clearly that it is insufficient as the sole dynamic factor for higher-risk transactions. The direction of travel is toward authenticator apps, hardware tokens, and FIDO2 cryptographic methods.

3.3 The Vendor and Third-Party Access Gap

Indian BFSI organisations maintain extensive third-party access ecosystems: technology vendors maintaining core banking systems, payment switch operators, cloud service providers, business correspondents, and fintech partners. Each of these relationships involves remote access to internal systems, and in most cases, that access is managed through a VPN with shared credentials that have been in place since the original onboarding.

CERT-In audit requirements create direct exposure here. Auditors examining vendor and third-party access will look for named individual credentials, time-limited access with formal renewal processes, session logs, and MFA on all remote sessions. The 180-day log retention requirement means that access by a vendor who completed a project months ago must be auditable — and if their credentials were never deactivated, those logs will show ongoing access to systems that should no longer be accessible.

3.4 The Compliance Documentation Gap

Regulatory examiners in 2026 are not satisfied by policy documents and architecture diagrams. They ask for evidence: logs, access records, policy enforcement screenshots, exception registers, review documentation.

An institution that deployed MFA several years ago may find that authentication logs from early periods were not retained; the exception register for bypasses was never formally maintained; the user access review committed to quarterly was last conducted over a year ago; and the vendor access register has not been updated since the last major digital banking project. Each of these is an audit finding. Collectively, they represent a compliance posture that looks secure on paper and is demonstrably incomplete on examination.

4. The MFA Implementation Framework for BFSI

4.1 Regulatory-to-Technical Requirements Map

Before selecting a platform or designing a deployment, translate each regulatory requirement into a specific technical control. This is the map a CISO presents to their board.

Regulation	Specific Requirement	Technical Control	Evidence Required
RBI Authentication Directions 2025	Minimum 2FA for all digital payment transactions	MFA on all customer payment channels (internet banking, mobile, UPI, gateway)	Auth logs per transaction; RBI examination evidence package
RBI Authentication Directions 2025	At least 1 dynamic factor for non-card-present transactions	TOTP, hardware token, or biometric as minimum one factor	Factor type logged per transaction
RBI Authentication Directions 2025	Factor independence — reliability of one must not affect the other	Separate channels for 2 factors; mobile cannot be sole channel for mobile-initiated transactions	Architecture documentation demonstrating channel separation
RBI IT Governance Master Direction	MFA for all employee access to critical information systems	MFA enforced on core banking, treasury, internet banking back-end, payment switch	Named user access logs; enrolment register
RBI IT Governance Master Direction	Privileged access management; access reviews with evidence	Phishing-resistant MFA (Verified Push or FIDO2) for admin accounts; documented quarterly access reviews	Access review records; de-provisioning logs
CERT-In CISO-2025-02	MFA mandatory for ALL remote access connections	MFA on all VPN, RDP, and third-party remote sessions - no exceptions without documented compensating controls	VPN auth logs; remote session logs; 180 days, stored in India

Regulation	Specific Requirement	Technical Control	Evidence Required
CERT-In CISG-2025-02	Principle of least privilege; no shared accounts on critical systems	Role-based access control; named individual accounts; deactivation process for leavers	Auth logs per transaction; RBI examination evidence package
DPDPA 2023	Reasonable security safeguards for all systems handling personal data	MFA on all systems storing, processing, or transmitting personal data of Indian residents	Breach investigation evidence; access governance documentation
SEBI CSCRF	MFA for privileged access to market infrastructure systems	Phishing-resistant MFA for all trading, risk management, and back-office privileged accounts	Annual SEBI-recognised audit; 90-day log retention

4.2 Factor Selection by User Population

Deploying a single factor type across all populations is the most common implementation mistake. This matrix maps the right factor to each population.

User Population	Recommended Factor	Enrolment Method	Session Model	Key Constraint
Retail banking customers	Tiered: SMS OTP (low-value) → Authenticator app (step-up) → Biometric (high-risk)	Self-enrolment via mobile banking app; bank staff-assisted for low-digital-literacy segments	Per transaction; risk engine determines step-up requirement	Factor independence for mobile-initiated transactions
Branch employees	Duo Mobile push (with corporate smartphone) Hardware TOTP token (without smartphone or device-prohibited environments)	IT-assisted bulk enrolment by branch; hardware tokens pre-provisioned	Shift-based: authenticate at shift start, session maintained, auto-terminate at shift end	Named individual accounts mandatory; no shared workstation credentials
Back-office and operations staff	Duo Mobile push notification	Self-enrolment with helpdesk support; bulk rollout by department	Per-session; re-authenticate on new session or after inactivity timeout	Ensure contractor accounts are in same enrolment scope
Privileged & administrator accounts	Verified Duo Push (minimum) FIDO2 hardware security key (highest-privilege accounts)	Admin-verified individual enrolment; no self-enrolment for privileged tier	Per-session with step-up for sensitive actions; no persistent admin sessions	Standard push notification INSUFFICIENT - push fatigue attack risk
Vendor and third-party accounts	Duo Mobile push or hardware TOTP token provided by organisation	IT-provisioned per engagement; credentials time-limited with 30-day expiry and formal renewal	Per-session; all sessions logged and attributed to named individual	Deactivation on engagement end is mandatory; vendor access register required

4.3 Deployment Sequencing

Sequence by regulatory risk, not by size or convenience. Close the CERT-In and SEBI exposure first; the largest operational deployment comes later.

Visual 2 — RBI Directions 2025: Factor Classification and Independence Principle

Phase 1 Credential Audit & Stale Account Remediation

Weeks 1–2 • Complete before any MFA configuration

- Inventory every account with access to critical systems: VPN, remote access, core banking, privileged administrator, third-party vendor
- For each account: named individual? last active session? engagement still live? access scope justified?
- Deactivate accounts whose associated engagements have ended; deactivate dormant accounts
- Output: clean credential register that establishes the authentication surface at deployment start

Phase 2 Privileged Access MFA

Weeks 2–6 • Highest regulatory risk, smallest population

- Deploy MFA for all administrator and privileged accounts - domain admins, DBAs, core banking app admins, infrastructure engineers
- Configure Verified Duo Push as mandatory factor for all admin accounts; disable standard push notification for this policy group
- Enrol all accounts individually with admin verification; no self-enrolment for this tier
- Generate break-glass bypass codes; store in physical envelope in CISO's safe; log every issuance in bypass code register
- Outcome: closes the CERT-In and SEBI CSCRf privileged access requirement

Phase 3 VPN and Remote Access

Weeks 4–8 • Closes CERT-In mandatory remote access requirement

- Deploy MFA for all VPN connections via RADIUS integration with existing VPN concentrator (Cisco ASA/Firepower, Palo Alto, Fortinet)
- Configure MFA for all remote desktop and third-party remote access sessions
- Build vendor access register: named individual, company, engagement scope, access scope, 30-day expiry, renewal date
- Configure time-limited vendor credentials with defined expiry and formal renewal requirement
- Outcome: closes the CERT-In mandatory MFA-for-remote-access requirement

Phase 4 Employee Access to Critical Systems

Weeks 6–12 • Operationally complex; branch-by-branch rollout

- Deploy MFA for all employee access to core banking systems, treasury platforms, internet banking back-end, customer data repositories
- Named account migration for shared workstations; coordinate with core banking system user administration
- Configure shift-based sessions: authenticate at shift start, session maintained for shift duration, auto-terminate at shift end
- Hardware TOTP tokens for branch staff without corporate smartphones; allow 2–3 weeks lead time for procurement
- Critical: send branch communication BEFORE rollout — prevents Day 1 phishing-false-positive flood

Phase 5 Customer-Facing Payment Authentication Review

Weeks 8– variable • Parallel workstream; timeline depends on platform

- Review authentication flows in internet banking platform, mobile banking app, UPI stack, and payment gateway
- Assess whether existing flows satisfy RBI Directions: minimum 2FA, at least one dynamic factor, factor independence for mobile
- Banks on proprietary or highly customised platforms: plan for 6–8 months — requires vendor coordination, release cycles, UAT
- Banks on modern third-party platforms with API-accessible authentication flows may achieve this faster
- Risk engine capability (most Indian mid-tier banks do not have this in production): separate planning project

Phase 6 Evidence Package Compilation

Ongoing from Phase 1 • Build the audit pack as you deploy, not the week before

- Deployment architecture document: systems protected, integration method per system, user populations covered
- Access control policy signed by CISO/equivalent: MFA requirements by role and system classification, effective date
- User population register: named user, enrolled factor, assigned group, applications accessible, last access review date
- Break-glass procedure document: failmode setting, bypass code holders, device loss procedure, tabletop test record
- Authentication log exports: enforcement date per system, retained independently of MFA platform Admin Panel
- Vendor access register: current as of audit date, with expiry dates and last renewal
- Bypass code log: every code issued, reason, issue date, expiry, and whether used — specific CERT-In audit request item

5. Cisco Duo for BFSI — The Architecture Case

This section examines Cisco Duo's architecture specifically, as the platform Proactive deploys. For a multi-vendor comparison of MFA platforms for Indian enterprises, see our companion piece: "What is the Best MFA Solution for Enterprises in India?"

5.1 The Mixed-Environment Reality of Indian BFSI

Indian banks and NBFCs are not cloud-native. Core banking systems - Finacle, Temenos T24, Flexcube - are predominantly on-premises or private cloud deployments, authenticating against Active Directory via LDAP or against their own user stores via proprietary interfaces. Treasury and ALM platforms have similar characteristics. Internet banking back-ends may be on public cloud, but the integration with core banking typically runs through an on-premises middleware layer.

This environment requires an MFA platform that can reach legacy applications via RADIUS and LDAP without requiring those applications to be modernised or replaced. The Duo Authentication Proxy - a lightweight software service installed on a Windows or Linux server in the bank's environment - provides an on-premises bridge that handles authentication requests from RADIUS-dependent VPNs, LDAP-dependent core banking systems, and legacy applications that predate modern authentication protocols, while connecting outbound to Duo's cloud over TCP port 443 only.

ARCHITECTURE

The Duo Authentication Proxy requires no inbound firewall rules, no DMZ modifications, and no changes to the applications it protects. A bank running a core banking system deployed in 2008 and a VPN concentrator deployed in 2016 can deploy MFA on both systems without touching either system's software.

5.2 Data Residency

Cisco operates a Duo data centre in Mumbai for Indian tenants. Indian customer identity data - user records, device enrolment information, authentication event logs - is processed and stored in India. The Mumbai instance has been operational since May 2022, holds ISO 27001 and SOC 2 certifications, and carries a 99.999% availability SLA.

When evaluating any MFA platform for BFSI deployment, obtain written confirmation of where authentication data is processed and stored, in a form that will satisfy an RBI examiner. This is not a documentation formality — it is a baseline compliance requirement for cloud-delivered authentication services deployed in Indian BFSI environments.

5.3 Phishing-Resistant MFA for Privileged Accounts

Privileged accounts in BFSI environments require phishing-resistant MFA. Standard push notification is inadequate for this population. Push fatigue attacks — in which an attacker with stolen credentials sends repeated push approval requests until the user approves one — have been the mechanism in several high-profile financial sector breaches globally.

Visual 7 — How Push Fatigue Attacks Work — and Why Verified Push Stops Them

The attack that compromised Uber in 2022 and MGM Resorts in 2023. The fix is architectural, not procedural.

STANDARD PUSH NOTIFICATION	VERIFIED DUO PUSH
1. Attacker obtains stolen password 2. Attacker triggers push approval request 3. User receives push on their phone 4. Attacker sends 10, 20 more requests... 5. User approves one to make it stop 6. ATTACKER IS IN MFA log shows: approved. Everything looks clean.	1. Attacker obtains stolen password 2. Attacker triggers push approval request 3. A 3-digit code appears on the user's LOGIN SCREEN 4. User must type that code into the Duo app to approve 5. Attacker is remote. Cannot see the code. 6. ATTACK FAILS. Every time. Sending 100 push requests changes nothing. The attacker can never complete the match.

Cisco Duo's Verified Push is available from the Essentials tier — no premium upgrade required. It uses the same Duo Mobile app as standard push. The only change is a policy configuration that enables number matching. FIDO2 hardware security keys (YubiKey, Feitian) provide stronger phishing resistance and are appropriate for the highest-privilege accounts: domain administrators, database administrators, and core banking application administrators.

5.4 The Audit Trail

Cisco Duo's authentication logs provide a timestamped record of every authentication event: user, application, factor used, device type, operating system, location, and outcome. Logs are available for export from the Admin Panel in multiple formats and feed to a SIEM or log management platform for the 180-day CERT-In retention requirement.

The logs are granular enough to answer every examiner question that arises in a BFSI audit: who accessed the treasury system on the morning of a specific date; whether the vendor who logged in last week used MFA; whether the domain administrator account flagged in an incident report had MFA enrolled; what device a remote user was accessing the core banking system from.

IMPORTANT

For the 180-day CERT-In log retention requirement: export Duo authentication logs to an India-resident SIEM or log management platform. Duo's Admin Panel has a default retention period that may not cover the full 180-day window. The export must be configured from deployment Day 1, not retroactively.

6. The BFSI Compliance Calendar

Four frameworks, four status points. If your programme has not already addressed the first two rows, the compliance exposure is current and accumulating.

Framework	Specific MFA Obligation	Status	If Not Done
SEBI CSCRF	MFA for privileged access to all trading, risk management, and back-office systems. Annual SEBI-recognised audit. 90-day log retention.	COMPLIANCE WINDOW CLOSED Jan–Apr 2025	Current examination exposure. First post-deadline audit cycle is underway.
CERT-In CISG-2025-02	MFA for all remote access. Annual audit mandatory. 180-day logs in India. Named individual accounts. Least privilege.	IN FORCE 25 July 2025	First annual audit due. Finding of inadequate MFA is likely. Rectification timeline required.
RBI Authentication Directions 2025	2FA mandatory for all digital payment transactions. At least one dynamic factor for non-CNP transactions. Factor independence principle. Risk-based authentication.	EFFECTIVE NOW 1 April 2026	Non-compliance with a live regulatory direction. RBI examination cycle: 2–3 years for large banks, less frequent for smaller NBFCs.
RBI IT Governance Master Direction	MFA for all employee access to critical information systems: core banking, treasury, internet banking back-end. Privileged access management. Documented access reviews.	ONGOING REQUIREMENT	Cited deficiency in RBI inspection findings for banks without documented privileged access controls.
DPDPA 2023	Reasonable security safeguards for all systems handling personal data. MFA is baseline standard. Data Protection Board to adjudicate breach-related complaints.	FULL ENFORCEMENT 13 May 2027	Post-breach: penalty up to ₹250 crore (DPDPA 2023, Schedule 1 Item 4). Unlike RBI, triggered by breach event not examination cycle.

7. Frequently Asked Questions

Does the RBI Authentication Mechanisms Directions 2025 apply to NBFCs?

Yes. The Directions apply to all Payment System Providers and Payment System Participants, which includes non-bank entities operating within India's payment ecosystem. This covers NBFCs that issue prepaid payment instruments, operate as payment aggregators, or participate in the UPI ecosystem as PSPs. NBFCs not directly involved in payment transactions are subject to the RBI IT Governance Master Direction rather than the Authentication Directions 2025, but the IT Governance framework independently requires MFA for employee access to critical information systems.

What data localisation requirements apply to MFA platform selection for Indian BFSI organisations?

RBI's data localisation expectations for financial data and the DPDPA's "reasonable safeguards" obligation together require that authentication data — user records, device enrolment information, authentication event logs — be processed and stored in India. Cloud-delivered MFA platforms that do not operate India-resident infrastructure cannot satisfy this requirement. When evaluating any MFA platform, obtain written confirmation of data residency in a form that will satisfy an RBI examiner. Cisco Duo's Mumbai data centre, operational since May 2022 and certified to ISO 27001 and SOC 2, satisfies this requirement for Indian tenants.

What log requirements do RBI and CERT-In impose, and what should organisations require from their MFA platform?

CERT-In Directions 2022 require 180 days of log retention for security events, stored in India. For MFA compliance the relevant categories are: identity provider and authentication logs (every MFA event, factor used, outcome); remote access logs (VPN session logs, remote desktop logs, third-party access logs); and privileged access logs. These logs must be available for export during the audit window and should feed into a SIEM for correlation and alerting. Any MFA platform evaluated for BFSI deployment should provide granular, exportable logs at all tier levels without premium add-ons. Confirm that the platform's default log retention covers the full 180-day requirement — if not, configure export to an external log management system from Day 1.

Our bank uses SMS OTP for internet banking authentication. Does that satisfy RBI Directions 2025?

SMS OTP combined with a password satisfies the minimum two-factor requirement — it provides “something you have” and “something you know.” However, the RBI Directions’ factor independence principle creates a specific complication for mobile banking: where a transaction is initiated on the same device that receives the SMS, independence may not be satisfied for higher-value transactions. The direction of travel in the Directions is clearly away from SMS OTP as the primary dynamic factor — the framework explicitly acknowledges FIDO2 cryptographic methods and authenticator apps as preferred alternatives. Organisations relying primarily on SMS OTP should include a transition plan as part of their RBI Directions compliance programme.

Does deploying MFA satisfy the DPDPA “reasonable security safeguards” obligation?

MFA is a necessary component of reasonable security safeguards but not a sufficient one. For BFSI organisations, the “reasonable” standard in 2026 encompasses: encryption at rest and in transit; role-based access control; MFA for all systems handling personal data; access audit logs demonstrating individual accountability; incident response procedures meeting CERT-In reporting requirements; and data breach notification capabilities. MFA is the authentication layer — it must operate alongside access governance and monitoring controls to constitute a defensible compliance posture.

What is the correct break-glass procedure for a bank that deploys MFA on its core banking system?

Break-glass procedures for BFSI MFA deployments must be documented because undocumented bypasses are themselves a CERT-In audit finding. The standard configuration: the Authentication Proxy failmode is set to “safe” for operational systems (VPN, core banking access from branches) and “secure” for systems where a lockout during a Duo outage is preferable to unprotected access (treasury systems, privileged administrator consoles). Bypass codes for critical administrator accounts are generated, documented in a physical evidence register, stored in the CISO’s safe, and every issuance is logged in the bypass code register with date, reason, and expiry. This register is a specific CERT-In audit request item.

How long does a BFSI MFA deployment take?

For privileged access and remote access — the two highest-priority phases for regulatory compliance — typically four to six weeks from credential audit completion to acceptance sign-off for an organisation of 500 to 2,000 employees. The full enterprise deployment including branch employee access runs eight to twelve weeks, depending on branch locations and core banking integration complexity. Customer-facing payment authentication review is a parallel workstream with a variable timeline: six to eight months for banks on proprietary or highly customised platforms; potentially faster for banks on modern third-party platforms with API-accessible authentication flows. The binding constraint on timeline is almost never the technology — it is the credential audit at the start and the enrolment communication for branch employees.

Is MFA mandatory under India's DPDPA Act?

The DPDPA 2023 and its 2025 Rules do not mandate MFA by name. However, the Act requires data fiduciaries to implement "reasonable security safeguards" to protect personal data. Given the current threat environment and the explicit authentication requirements in parallel regulations (RBI, SEBI, CERT-In), any credible interpretation of "reasonable safeguards" in 2026 includes MFA for systems that store, process, or transmit personal data. Organisations that suffer a breach without MFA controls in place will face significant difficulty demonstrating compliance with this standard before the Data Protection Board.

8. About the Authors

Proactive Data Systems Pvt Ltd

Proactive Data Systems is an enterprise IT infrastructure and services company. For more than three decades, the company has designed, deployed, and operated the technology foundations behind some of India's most demanding enterprise environments, from regulated industries to large distributed operations.

Founded in 1991, Proactive serves more than 1,500 customers, from fast-growing businesses to Fortune 500 enterprises, across banking and financial services, manufacturing, healthcare, public sector, IT and ITES, retail, education, and global capability centres. Our work spans enterprise networking, cybersecurity, cloud and AI-ready data centres, collaboration platforms, structured cabling, and managed services.

A Cisco Preferred Partner under the Cisco 360 Partner Program, Proactive is recognised across the Networking, Security, Collaboration, Cloud & AI, and Services portfolios, and is a Cisco Advanced Customer Experience Specialised Partner. The company is ISO 9001:2015 and ISO/IEC 27001 certified, and engineers solutions in partnership with Dell, Nutanix, NetApp, Palo Alto Networks, Fortinet, VMware, Veeam, and CommScope.

If your organisation wants an honest assessment of its current authentication surface against the requirements mapped in this playbook - what is compliant, what is not, and what a sequenced deployment would look like - Proactive's security practice is available to provide that assessment. As a Cisco Preferred Security Partner we can also confirm when Cisco Duo is and is not the right answer for a specific environment, because getting the architecture right matters more than getting a particular product deployed.

Delhi (HQ) · Mumbai · Pune · Bengaluru · Hyderabad · Indore · Singapore

Note: All statistics in this document are cited at point of use. The 73% and 57% figures reference DSCI's Cyber Security Maturity Survey (Data Security Council of India, India Cyber Threat Report 2025). The ₹54.78 crore penalty figure references RBI Annual Report / RBI press releases, FY 2024-25. The ₹36,450 crore fraud figure references the National Cyber Crime Reporting Portal, February 2025. The UPI fraud figure references NPCI / RBI Annual Report FY 2023-24. The ₹250 crore penalty ceiling references DPDPA 2023, Schedule 1 Item 4.

© 2026 Proactive Data Systems Pvt Ltd. All rights reserved. This document is intended for informational purposes. It does not constitute legal or regulatory advice. Organisations should seek independent legal counsel on specific compliance matters.