PROACTIVE™
Enhancing Digital Experience

RBI Master Directions Compliance: A Field Guide for Indian BFSI CISOs.

The regulatory landscape, the applicable Master Directions, the evidence RBI inspectors ask for, and the implementation timeline that actually holds.

Version 1.1 · Updated August 2026.

Reflects DPDP Rules (notified 13 November 2025) and SEBI CSCRF (issued 20 August 2024).

Written by **Mitesh Pandya, Regional Head - West**

Proactive Data Systems Pvt Ltd

Cisco Preferred Partner across Networking, Security, Collaboration, Data Center, and Services · Cisco Advanced Customer Experience Specialised · Since 1991.

Preface

Every Indian BFSI CIO and CISO reading this already knows one thing: RBI does not write single-page rules. Between the Master Direction on IT Governance (November 2023, effective April 2024), the Cyber Security Framework in Banks (June 2016), the Master Direction on Cyber Resilience for non-bank Payment System Operators (July 2024), and the Master Direction on Outsourcing of IT Services (April 2023, effective October 2023), the current cyber-compliance surface for an Indian bank, NBFC, or payment operator spans hundreds of pages of primary text and a decade of accreted circulars.

This field guide is not a substitute for reading the Directions. It is a working reference for the CIO or CISO who has read them, has to run against them, and wants a single document that maps which requirement applies to which entity, what evidence an RBI inspector will ask for, where the common gaps sit, and how a typical implementation programme actually sequences.

It is written by the Proactive Data Systems Security Practice, from live implementations across Indian BFSI customers since 1991. It is deliberately opinionated on sequencing, hedged on interpretation, and free of legal advice. Consult your General Counsel and your Chief Compliance Officer before you act on any specific control decision.

Which RBI Master Directions Apply to Your BFSI Entity?

Entity classification determines which framework applies. Four Master Directions are currently central: IT Governance (2023) for governance backbone, Cyber Security Framework in Banks (2016) for bank-side cyber controls, Cyber Resilience for non-bank PSOs (2024) for payment operators, and Outsourcing of IT Services (2023) for every material vendor arrangement.

The Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, issued 7 November 2023 and effective 1 April 2024, applies to Scheduled Commercial Banks (excluding Regional Rural Banks), Small Finance Banks, Payment Banks, NBFCs classified in the Middle, Upper, or Top Layer under Scale Based Regulation, Credit Information Companies, and specified All-India Financial Institutions (EXIM Bank, NABARD, NHB, SIDBI, NaBFID). It is the current governance backbone.

The Cyber Security Framework in Banks, issued 2 June 2016, applies to all Scheduled Commercial Banks. It predates the 2023 Master Direction but has not been superseded. It defines the Cyber Crisis Management Plan (CCMP), the Cyber Security Operations Centre (C-SOC) expectations, and the incident-reporting flow that Indian banks operate against.

The Master Direction on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators, issued 30 July 2024, applies broadly to all authorised non-bank PSOs; payment aggregators, prepaid instrument issuers, cross-border money transfer operators, White Label ATM Operators, Bharat Bill Payment Operating Units (BBPOUs), card networks, ATM networks, TReDS operators, CCIL, NPCI, and instant money-transfer operators. Implementation is phased; large PSOs' compliance date passed in April 2025.
The Master Direction on Outsourcing of Information Technology Services, issued 10 April 2023 and effective 1 October 2023, applies broadly across banks, NBFCs, CICs, and All-India Financial Institutions. It governs how regulated entities engage IT service providers, including cloud.

For Base Layer NBFCs, the RBI Master Direction, Information Technology Framework for the NBFC Sector (June 2017), including its Information and Cyber Security chapter, remains the applicable framework. Middle Layer, Upper Layer, and Top Layer NBFCs now operate under the 2023 IT Governance Master Direction.

The mapping table below shows which Direction applies to which entity classification.

Regulated Entity	IT Governance Framework	Cyber Security Framework	Outsourcing Framework
Small Finance Bank	Master Direction on IT Governance (2023)	Cyber Security Framework in Banks (2016)	Master Direction on Outsourcing of IT Services (2023)
Payment Bank	Master Direction on IT Governance (2023)	Cyber Security Framework in Banks (2016)	Master Direction on Outsourcing of IT Services (2023)
NBFC-Top, Upper, or Middle Layer	Master Direction on IT Governance (2023)	Covered within the IT Governance MD; 2017 NBFC IT Framework superseded for these tiers	Master Direction on Outsourcing of IT Services (2023)
NBFC - Base Layer	IT Framework for NBFC Sector (2017)	IT Framework for NBFC Sector (2017), Information & Cyber Security chapter	Master Direction on Outsourcing of IT Services (2023)
Non-Bank Payment System Operator	Applicable governance framework per entity	Master Direction on Cyber Resilience for non-bank PSOs (2024)	Master Direction on Outsourcing of IT Services (2023)
Credit Information Company	Master Direction on IT Governance (2023)	As applicable	Master Direction on Outsourcing of IT Services (2023)
All-India Financial Institution (EXIM, NABARD, NHB, SIDBI, NaBFID)	Master Direction on IT Governance (2023)	As applicable	Master Direction on Outsourcing of IT Services (2023)

What Does the RBI Master Direction on IT Governance (2023) Require?

The 2023 Master Direction requires a governance architecture with a Board-level IT Strategy Committee (ITSC) chaired by an independent director with IT expertise, a senior-management-level IT Steering Committee, and a dedicated Head of Information Security Function (HIS) reporting into a defined governance line. It also requires an approved IT Strategy, an Information Security Policy, a Business Continuity Management framework, and an assurance regime with independent IT audit.

The four operational pillars of the Direction are: IT and information asset lifecycle governance, IT services management including a robust change and problem management regime, information and cyber security operations aligned to a risk-based framework, and business continuity plus disaster recovery for critical business functions. Each pillar has specified sub-controls.

The Direction requires an annual IT Strategy document approved by the Board, an Information Security Policy reviewed at least annually, an IT Operations Manual, a Business Continuity Management framework tested at least annually with defined RTO and RPO for critical systems, and a cyber-incident-response plan aligned to the Cyber Security Framework in Banks (or the applicable cyber framework for the entity type).

Third-party arrangements, cloud, managed services, and outsourced software, must be governed by contracts that include specific clauses on right to audit, business continuity, exit management, and information security obligations that mirror the entity's own obligations. This is where cloud and MSP engagements most often fail RBI scrutiny.

Assurance is a Board-level obligation. Independent IT audit is required, with findings tracked to closure through a documented remediation cycle. The CIO and HIS must report cyber-security posture to the Board at defined intervals, typically quarterly. For NBFCs newly brought under the Direction (Middle, Upper, and Top Layer), the compliance clock started on 1 April 2024. For banks and CICs already under prior frameworks, the 2023 Direction consolidates and updates but does not restart the clock.

What Is the RBI Cyber Security Framework in Banks (2016)?

Issued 2 June 2016 (circular RBI/2015-16/418), the Cyber Security Framework in Banks remains the operating cyber-security spine for Indian Scheduled Commercial Banks. It requires a Board-approved Cyber Security Policy distinct from the general IT or Information Security policy, an active Cyber Crisis Management Plan (CCMP) covering detection, response, recovery, and containment, and a Cyber Security Operations Centre (C-SOC) with baseline detection and response capabilities per the framework's Annex 3.

The Framework prescribes a Baseline Cyber Security and Resilience Requirements Annex with specific controls across network security, application security, endpoint security, data security, access management, and vendor security. Banks self-assess against this Annex on a defined cadence and report gaps to the Board.

The Framework requires reporting of cyber-security incidents to RBI within specified timelines through the appropriate channel. This is separate from CERT-In reporting under the Directions issued 28 April 2022, which continues to apply concurrently. Banks must be prepared to file both reports for a single incident.

Because the 2016 Framework and the 2023 IT Governance Master Direction address different layers (cyber-security controls vs. IT governance structure), the requirements intersect at specific control areas. The comparison table below shows where the two frameworks overlap and where each is authoritative.

Requirement Area	Cyber Security Framework in Banks (2016)	Master Direction on IT Governance (2023)
Cyber controls baseline	Baseline Cyber Security and Resilience Requirements Annex	References cyber controls; does not replace the 2016 baseline
Incident management	CCMP with scenario coverage; RBI incident reporting	Cyber-incident-response plan aligned to applicable cyber framework
Assurance and audit	Self-assessment against Annex; Board reporting	Independent IT audit; findings tracked to closure
Third-party risk	Vendor security controls within the Annex	Specific chapter on IT outsourcing (aligned to 2023 Outsourcing MD)
Business continuity	Covered within resilience baseline	Distinct BCM framework with defined RTO/RPO for critical systems

What Are the RBI Cyber Resilience Requirements for Non-Bank Payment System Operators?

The Master Direction on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators, issued 30 July 2024, brought all authorised non-bank PSOs under a formal cyber-resilience baseline for the first time. It requires a Board-approved cyber-security policy, a Cyber Crisis Management Plan proportionate to scale, cyber-security governance with a designated senior officer accountable, baseline controls across the payment technology stack, and mandatory reporting of cyber-security incidents to RBI.

The Direction applies to a broad set of non-bank PSOs authorised under the Payment and Settlement Systems Act, 2007: payment aggregators, prepaid payment instrument issuers, cross-border money transfer operators, White Label ATM Operators, Bharat Bill Payment Operating Units (BBPOUs), card networks, ATM networks, Trade Receivables Discounting System (TReDS) operators, Clearing Corporation of India Limited (CCIL), National Payments Corporation of India (NPCI), and instant money-transfer operators.

Implementation is phased by scale. Large PSOs (defined by transaction volume thresholds) had a compliance date in April 2025 and are already operating against the baseline. Medium and small PSOs have extended windows, with the full phase-in continuing through 2026.
The Direction is explicit about digital payment security controls - the customer authentication, transaction integrity, and fraud detection baseline for payment products. It is not a general IT security direction; it applies specifically to the payment operations of the regulated entity.

Non-bank PSOs preparing for compliance should read the Direction alongside the parent Payment and Settlement Systems Act, 2007, and any authorisation-specific conditions in their RBI licence. Circular reference should be verified against the RBI PDF on rbi.org.in before publication of internal implementation programmes.

What Does the RBI Master Direction on Outsourcing of IT Services Require?

The Master Direction on Outsourcing of Information Technology Services (issued 10 April 2023, effective 1 October 2023) governs how regulated entities engage external IT service providers. It requires a Board-approved Outsourcing Policy, a Materiality Framework, Board or Board-Committee approval for material arrangements, ongoing monitoring, an Exit Strategy for every material arrangement, and specific contract clauses on RBI's right of inspection, information security obligations, data localisation, and breach notification

The Direction applies to cloud services, managed services, application development and maintenance, IT operations, IT-enabled services, and any material outsourced IT function. It applies across banks, NBFCs, CICs, and All-India Financial Institutions.

Every material outsourcing contract must include: right of the RBI to inspect the service provider, right of the regulated entity to conduct or commission audits, obligations on the service provider to maintain information security controls at least equivalent to those of the regulated entity, data localisation obligations consistent with RBI's PSS Data Storage circular where applicable, breach notification within defined timeframes, and defined exit and transition provisions.

Cloud engagements are treated as a specific case. The Direction does not prohibit cloud, but requires that regulated entities using cloud services (including hyperscalers) satisfy the same governance, contractual, and monitoring requirements as any other material outsourcing. Data at rest is expected to be within India where RBI Payment Systems Data Storage rules apply, and cross-border data flows require documented authorisation and risk assessment.
For most Indian BFSI entities, the Outsourcing Direction is the framework that most directly affects the shape of their vendor relationships. Every material MSP contract signed since October 2023 has to meet these requirements. Contracts signed before that date should be reviewed on renewal.

How Does RBI Cyber Compliance Interact With CERT-In and DPDP?

RBI cyber compliance operates alongside two other pan-Indian frameworks that apply concurrently to every regulated BFSI entity. The CERT-In Directions issued on 28 April 2022 apply to all Indian entities regardless of RBI regulation, requiring cybersecurity incident notification within six hours, log retention for 180 days within India, and mandatory NTP synchronisation to NIC or NPL time servers. The DPDP Act 2023 with DPDP Rules notified 13 November 2025 applies to all data fiduciaries processing personal data of Indian residents.
The frameworks are complementary but not identical. Where they overlap, the strictest requirement typically prevails.

Incident reporting

CERT-In requires notification within six hours of a cybersecurity incident. RBI cybersecurity frameworks require reporting to RBI within timelines specified for the entity type. DPDP Rule 7 requires notification to the Data Protection Board of India within seventy-two hours of a Personal Data Breach. A single ransomware incident affecting an Indian bank's core banking system with customer data exposure triggers all three. Preparation should assume the shortest window (six hours) as the operational target, with separate reports filed to CERT-In, RBI, and the Data Protection Board in the applicable formats.

Log retention

CERT-In requires 180 days of log retention within India. RBI IT Governance framework requires retention consistent with the entity's information security policy, typically longer for material systems. DPDP requires retention consistent with the purpose of processing. Align to the longest applicable retention period per system.

Data localisation

RBI Payment Systems Data Storage circular (6 April 2018) requires end-to-end payment system data to be stored only in India, with a domestic copy retained even where cross-border components exist for cross-border transactions. DPDP Rules 2025 add a separate cross-border personal-data transfer regime with restricted-country provisions. RBI's expectation for BFSI generally is that customer data, payment, KYC, transaction remains within India. Cross-border flows for global group operations require documented authorisation.

The correct approach for a BFSI entity is to design controls once and satisfy each framework's evidence requirement from the same underlying control implementation. Duplicating controls to please multiple regulators is expensive and creates its own risk of inconsistency.

How Do RBI and SEBI Cyber Frameworks Interact for Diversified BFSI Groups?

Diversified BFSI groups with capital-market subsidiaries, asset management companies, brokerages, depository participants, and mutual funds face the SEBI Cybersecurity and Cyber Resilience Framework (CSCRF) alongside RBI's regime. SEBI's CSCRF, issued 20 August 2024 with subsequent clarifications in December 2024, applies to SEBI-regulated entities on a five-tier classification: Market Infrastructure Institutions, Qualified REs, Mid-size REs, Small-size REs, and Self-Certification REs.

Adoption deadlines under CSCRF are already live for most entities: 1 January 2025 for entities previously under a SEBI cyber circular, and 1 April 2025 for other REs. Diversified groups should therefore assume SEBI CSCRF is already in force for their capital-market operations.

For a group with a bank and an AMC in the same corporate family, this means two frameworks operating in parallel: RBI's IT Governance Master Direction for the bank and SEBI CSCRF for the AMC. Where control implementations can be shared (SIEM, identity, endpoint security), a common infrastructure design satisfies both. Where they cannot (governance committees, incident reporting channels, audit obligations), duplicate structures are required.

Boards of diversified groups often ask whether a single consolidated cyber-compliance programme can serve both subsidiaries. In practice, the answer is that infrastructure can be shared but governance, reporting, and evidence must be maintained per-entity.

What Is a Typical RBI IT Governance Implementation Timeline?

A mid-size Scheduled Commercial Bank implementing the 2023 Master Direction on IT Governance from a baseline compliance posture typically runs a 120 to 180-day programme end-to-end. The phases follow governance foundation, policy refresh, control implementation, testing and independent review, and Board reporting steady-state.

Days 0 to 30. Governance foundation.

IT Strategy Committee formalised at Board level, IT Steering Committee constituted at senior management level, Head of Information Security Function (HIS) role established with defined reporting line. Board-approved IT Strategy document drafted and approved.

Days 31 to 60. Policy and framework refresh.

Information Security Policy reviewed and updated to the 2023 Master Direction requirements. IT Operations Manual updated. Business Continuity Management framework aligned. Change and Problem Management processes documented and approved.

Days 61 to 90. Control implementation and evidence generation

Gap assessment against Master Direction requirements. Remediation of high-priority gaps. Evidence packs formatted and archived for each control area. Third-party outsourcing arrangements reviewed against the Outsourcing Master Direction requirements.

Days 91 to 120. Testing and independent review.

Cyber Crisis Management Plan tabletop exercise. Business Continuity Plan test. Independent IT audit against the Master Direction. Findings tracked to closure with defined remediation timelines.

Days 121 to 180. Board reporting and steady-state operationalisation.

CIO and HIS Board reports formalised. Ongoing quarterly reporting cadence established. Programme moves from project to steady-state operation.

For entities updating from prior frameworks (banks already under Cyber Security Framework 2016), the 2023 Master Direction adds specific IT governance structure requirements but preserves much of the existing cyber-security control base. A refresh runs 60 to 90 days.

For Middle Layer NBFCs newly brought under the Direction, the timeline can extend to 240 days for entities without a prior IT governance framework in place. The gap between the 2017 IT Framework for NBFCs and the 2023 IT Governance Master Direction is substantial for entities that have not previously invested in IT governance discipline.

What Evidence Do You Need for an RBI IT and Cyber Inspection?

RBI inspections of IT and cyber posture look for evidence, not for claims. Inspectors expect to see Board minutes evidencing ITSC and IT Steering Committee meetings at prescribed frequency, Board-approved policies (IT Strategy, Information Security, Cyber Security for banks, Outsourcing), the current Cyber Crisis Management Plan with tabletop testing evidence, and independent IT audit reports with findings tracked to closure.

Beyond the governance evidence, inspectors expect: CIO and HIS appointment letters, role charters, and Board reports covering IT operations, security posture, incidents, and third-party risk.

Asset inventory covering IT and information assets, with classification and ownership documented. Access review reports at prescribed frequency, particularly for privileged and administrative accounts. Change Management records for the inspection period, with approval trails.

Incident response evidence: the inspector will pick two or three past incidents and ask to see the full trail from detection through reporting to closure, including CERT-In notification where applicable. Business Continuity test evidence including declared RTO, RPO, actual test results, and remediation of any gaps identified.

For outsourcing arrangements: the register of material outsourcing, contract clauses evidencing RBI right of inspection and information security obligations, monitoring reports for service provider performance, and Exit Strategy documentation for each material arrangement.

For payment operators: transaction reconciliation evidence, fraud monitoring reports, customer authentication logs, and digital payment security control effectiveness reports.
RBI inspectors will also ask for evidence of the previous inspection's findings being closed. An inspection cycle is treated as continuous; unclosed findings from the previous cycle become the highest-priority observations of the current one.

What Are the Common Gaps RBI Inspectors Find?

The most common gaps observed across Proactive's Indian BFSI implementation and remediation engagements in the last four quarters - and predicted by gap assessments in advance of RBI inspection- cluster in seven areas: governance structure, third-party contracts, incident evidence, BCP closure, CCMP currency, cloud outsourcing governance, and log retention. Each is remediable, but each takes 30 to 90 days of focused work.

Governance structure separation.

Many entities operate a single committee covering both IT strategy and information security. The 2023 Master Direction requires an ITSC at Board level distinct from an IT Steering Committee at senior management level, with a defined HIS role. Remediation is a governance change, not a technology one.

Third-party outsourcing contracts predating October 2023.

Contracts signed before the Outsourcing Master Direction came into effect often lack the specific clauses now required. Remediation requires contract addenda or re-negotiation on renewal.

Incident response evidence trail.

Entities can typically produce incident tickets and closure summaries, but the full inspector-ready trail- detection, triage, escalation decision, containment steps, communication to affected parties, regulatory notification, root-cause analysis, remediation, and closure is often incomplete.

BCP test evidence.

Business continuity tests are conducted, but the after-action reports and remediation of test-identified gaps are often not tracked to closure. Inspectors ask to see closure evidence, not just test evidence.

Cyber Crisis Management Plan tabletop currency.

The CCMP exists, but the last tabletop was more than a year old, or covered only one scenario when the Framework expects multiple scenarios covered on a rotation.

Cloud governance under the Outsourcing framework.

Many BFSI entities use hyperscaler cloud services, but the cloud engagement is not treated as a material outsourcing arrangement with the required governance. Cloud is one of the fastest-changing areas of RBI inspection focus.

Log retention and forensic readiness.

Logs are captured, but retention or accessibility for forensic review during an incident is not always adequate. CERT-In's 180-day requirement is the floor; inspectors expect longer retention for material systems.

Most of these gaps are administrative or documentation-related, not control-effectiveness gaps. They are remediable but time-consuming. Preparation cycles of 60 to 90 days in advance of an inspection are typical.

What Comes Next in the RBI Regulatory Pipeline?

Two verifiable items sit in the immediate regulatory pipeline. First, further phased implementation of the Master Direction on Cyber Resilience for non-bank PSOs continues through 2026, with medium and small PSOs coming into scope on rolling deadlines. Second, RBI has publicly flagged cloud-specific guidance as an area of active consultation, aligned to global regulator practice (equivalent to FCA in the UK or MAS in Singapore); the 2023 Outsourcing Direction is the current framework, but a cloud-specific Direction is under discussion.

Beyond these two, RBI is expected to continue harmonising IT and cyber-security guidance across entity types, with further consolidation likely for Base Layer NBFCs on a longer horizon. CISOs and CIOs should build compliance programmes that can absorb incremental Direction updates without complete redesign. Controls-mapping frameworks that reference specific Direction clauses need to be updated as clauses change; controls themselves should be designed to be framework-neutral where possible.

Frequently Asked Questions

Does the 2023 Master Direction on IT Governance supersede the 2016 Cyber Security Framework in Banks?

No. The 2023 Master Direction on IT Governance addresses IT governance structure, risk management, and assurance. The 2016 Cyber Security Framework addresses cyber-security controls specifically. Both apply concurrently to Scheduled Commercial Banks. The 2023 Direction consolidates governance; the 2016 Framework continues to define cyber-security controls.

Are cloud engagements subject to the Outsourcing Master Direction?

Yes. Cloud services (including hyperscaler engagements such as AWS, Azure, and GCP) are treated as material outsourcing arrangements when they meet the entity's materiality threshold. Contract clauses, monitoring, exit strategy, and business continuity requirements apply as they would for any material outsourced IT service. Some hyperscaler contracts require rider agreements to satisfy the Direction; check with your legal team before signing.

Which NBFCs must comply with the 2023 Master Direction on IT Governance?

NBFCs classified in the Middle Layer, Upper Layer, or Top Layer under RBI's Scale Based Regulation framework. Base Layer NBFCs continue to operate under the 2017 IT Framework for the NBFC Sector, including its Information and Cyber Security chapter. NBFC scale classification is published by the RBI and updated periodically.

How do RBI incident-reporting timelines interact with CERT-In's six-hour requirement?

Both apply concurrently. CERT-In (Directions issued 28 April 2022) requires notification of cybersecurity incidents within six hours; RBI cyber-security frameworks require reporting to RBI within timelines specified for the entity type; DPDP Rule 7 requires notification to the Data Protection Board within seventy-two hours where personal data is involved. Any material cyber-security incident affecting a regulated BFSI entity typically triggers all three. Prepare templates and workflows for each in advance; do not attempt to draft them under incident conditions.

Which controls are most likely to be flagged in the first RBI IT inspection under the 2023 Master Direction?

Based on Proactive's engagements and industry observation, the most frequently flagged areas in first-cycle inspections are: separation of the ITSC (Board-level) from the IT Steering Committee (senior management level), currency of the Cyber Crisis Management Plan tabletop, treatment of hyperscaler cloud engagements as material outsourcing under the 2023 Outsourcing Direction, and closure evidence for prior BCP test findings. Preparing for these four areas covers a substantial share of typical first-cycle inspection observations.

Why This Guide, From Proactive

Every RBI-regulated Indian BFSI entity we work with faces the same problem: the Directions are precise, the inspectors are precise, and the gap between the two is where most implementation programmes struggle. Proactive Data Systems has spent the last decade closing that gap for scheduled commercial banks, small finance banks, payment banks, NBFCs across every Scale-Based Regulation tier, insurance companies, AMCs, brokerages, and non-bank payment system operators.

We are a Cisco Preferred Partner across five portfolios - Networking, Security, Collaboration, Data Center, and Services - with the Cisco Advanced Customer Experience Specialised designation. Founded in Delhi NCR in 1991. Over 1,500 enterprise customers across India. More than 100 certified engineers. A dedicated BFSI compliance practice with implementations across the frameworks discussed in this guide.

When Indian BFSI CIOs and CISOs ask us to compare our approach to the alternatives - internal build-out, big-four consulting-led programmes, or generalist SIs - three points typically decide the engagement. First, we deliver the compliance programme and the underlying infrastructure as one integrated engagement, not as separate workstreams that later have to be reconciled. Second, we hold specialisations across Cisco, plus current vendor partnerships across the security stack Indian BFSI actually uses (NGFW, EDR, SIEM, MDR, PAM). Third, our implementations produce evidence packs formatted for RBI inspectors, not just for the internal compliance team.

We are not the only Cisco partner with BFSI experience in India. Where a specific engagement demands a competitor's strength, a particular application specialisation, a specific vendor relationship, a distinct methodology, we say so. What we consistently do better than most is the join between infrastructure delivery and RBI evidence generation, on a timeline that respects the compliance clock.

If you are approaching an RBI IT or cyber inspection, entering a Master Direction on IT Governance implementation cycle, or reassessing your outsourcing arrangements against the 2023 Direction, book a 30-minute conversation with a Proactive BFSI infrastructure architect. Not a sales engineer. Not an SDR. Someone who has delivered against these Directions for institutions that look like yours.

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.

Headquartered in Delhi NCR, with offices in Mumbai, Bengaluru, Pune, Hyderabad, Indore, and Singapore.

To learn more about our solutions, write to us
at pro@proactive.co.in

www.proactive.co.in

PROACTIVE™
Enhancing Digital Experience