RBI's **Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (RBI/2023-24/107)** — the ITGRCA Directions — replaced three decades of fragmented IT guidance with one principles-based standard, in force since **1 April 2024**. It is built around named committees, named officers, and named cycles: you cannot satisfy it with documents alone. This roadmap gives a Middle-Layer NBFC or smaller bank the governance architecture, the obligations, and a 12-month build sequence. Full guide: vcisodesk.com/rbi-it-governance-framework-implementation-guide-india/.

Scope and the instruments around it

Applies to: all banking companies (excl. RRBs) · small finance banks · payments banks · NBFCs in the Top, Upper and Middle Layers · credit information companies · AIFIs (EXIM, NABARD, NaBFID, NHB, SIDBI).

Does NOT apply to: Local Area Banks, NBFC-Core Investment Companies, Base Layer NBFCs — Base Layer stays on the lighter 2017 NBFC IT Framework (8 Jun 2017). If you are Middle Layer or above and still reading the 2017 document as primary, you are reading the wrong document.

Adjacent instruments: IT Outsourcing MD (10 Apr 2023) · Operational Resilience Guidance Note (30 Apr 2024) · PSO Cyber Resilience MD (30 Jul 2024) for payment-touching entities · Digital Lending Directions (eff. 8 May 2025) · NBFC Outsourcing Directions 2025 (existing-contract transition by **10 Apr 2026** or renewal, whichever earlier).

Enforcement: the MD sets no monetary penalty schedule — enforcement runs through the BR Act 1949 / RBI Act 1934 and supervisory action. RBI's preferred lever is **business restriction**, not headline fines: weak IT governance shows up as constrained growth.

1. Governance architecture — three structures that cannot be collapsed

- [ ] **A1 IT Strategy Committee (ITSC)** — board committee, minimum three directors, chaired by an **independent director with substantial IT expertise**, meeting at least quarterly with documented minutes. The missing IT-qualified director is the most common early supervisory gap — and cannot be remediated retroactively.
- [ ] **A2 IT Steering Committee** — senior management; translates ITSC direction into delivery: project prioritisation, vendor selection, investment plan, IS-audit response. CISO is a permanent invitee.
- [ ] **A3 Information Security Committee (ISC)** — separate senior-management committee with cyber as its only mandate, **headed from the risk vertical, not IT**. Folding ISC into IT Steering is non-compliant and will be flagged.

2. The CISO appointment — the most scrutinised role

- [ ] **C1** Senior-level executive with relevant qualifications — not a designation handed to a mid-level IT manager.
- [ ] **C2** Reports to the **Executive Director (or equivalent) overseeing risk management** — never into the IT delivery line, never through a business head.
- [ ] **C3 No business targets** — hybrid CISO-plus-P&L; roles are ruled out.
- [ ] **C4** Permanent invitee to ITSC and IT Steering; core member of the ISC. Owns infosec policy, cyber policy, third-party risk, vulnerability management, incident response, and the board posture report.
- [ ] **C5** If your "IT head" informally carries the CISO title alongside infrastructure delivery: unwind it with a clean appointment.

3. Incident reporting — get the source of the clock right

The 2023 MD (¶27) requires **prompt notification to RBI** (Department of Supervision) of significant incidents — it does not itself fix an hour-count. The hard **6-hour initial-report clock is CERT-In's** (April 2022 Directions, binding on everyone in India; payment entities also carry the PSO MD's own 6-hour rule; the 2016 bank framework set 2–6h). Detailed follow-up reporting runs on the timeline the supervisor specifies — no fixed "21-day" rule exists, so do not represent one.

- [ ] **I1** Runbook-driven detection-to-report pathway: on-call rotation, classification trigger, templated initial report, named escalation to CISO/ISC, parallel CERT-In submission workflow.
- [ ] **I2** "Significant" is undefined — defensible interpretation: anything affecting customer data, customer-facing services, transactions, or critical systems beyond a transient period. Under-reporting carries supervisory consequences; over-reporting does not.

4. BCP/DR, IS audit, outsourcing — the evidence cycle

E1 BCP/DR: board-approved framework — business impact analysis, ITSC-approved RTOs/RPOs per critical system, geographically separate DR site, **DR drills at least half-yearly for critical systems**, annual board review. Your cloud provider's resilience SLA is evidence, not a substitute for your own tested BCP. ☐

E2 Operational resilience (30 Apr 2024 Guidance Note): identify Critical Operations, set impact tolerances, run severe-but-plausible scenario tests, and demonstrate continuity through component failure. ☐

E3 IS audit: at least annual for critical systems, independent of IT operations, by qualified personnel (CISA/DISA or equivalent), reporting to ITSC and the Audit Committee, with prior-year finding closure tracked. Outsourcing the audit is fine; outsourcing programme ownership is a finding. ☐

E4 Vulnerability management: VA at least half-yearly and PT at least annually for critical/internet-facing systems, with patch SLAs. ☐

E5 Outsourcing: board-approved policy + materiality framework; due diligence incl. cloud; contracts with audit rights, data ownership, breach notification, sub-contracting limits, exit terms; tested exit strategy per material arrangement; concentration-risk monitoring (10 Apr 2023 MD + NBFC Outsourcing Directions 2025 — transition deadline 10 Apr 2026 or renewal). ☐

E6 Cyber drills: tabletop at least annually, technical exercises aligned to the IR runbook; training programme for staff and Board. ☐

5. The 2025–26 wave — now largely in force

Date	Obligation (check what touches you)
8 May 2025	Digital Lending Directions 2025 in force (DLA reporting 15 Jun 2025; multi-lender LSP rules 1 Nov 2025). Governance must demonstrably cover the lending app, LSP integration, and data flows.
1 Jan 2026	Banks need authorisation under the Digital Banking Channels Authorisation Directions to offer internet/mobile/USSD/SMS banking (bank-specific; NBFCs feel it via partner banks).
31 Mar 2026	Board-approved group-governance ring-fencing plans were due to RBI (full alignment by 31 Mar 2028).
1 Apr 2026	Dynamic 2FA mandate in force — at least one dynamic factor (SMS-OTP not banned outright, but single-factor SMS-OTP no longer suffices); digital-deposit liquidity recalibration.
1 Jul 2026	Customer-liability framework for digital banking fraud — still in draft, pending notification. Watch this one.

6. Twelve-month build sequence (Middle-Layer NBFC waking up to the MD)

R1 Months 0–3: constitute ITSC, IT Steering, ISC. Appoint the CISO with the right reporting line. Board-approve IT, infosec, cyber, BCP and outsourcing policies. Build the risk register. ☐

R2 Months 3–6: incident-response runbook (6-hour-ready). BCP documented with RTOs/RPOs. First annual IS audit. Outsourcing register + contract review against the 2023 and 2025 MDs. ☐

R3 Months 6–12: first DR drill. First board cyber posture review. First independent VAPT cycle. Close IS-audit findings. First management-level cyber drill. ☐

R4 Months 12+: embed the annual cycle; move from documents to evidence; layer digital-lending, outsourcing-2025, and (if payment-touching) PSO overlays. ☐

The supervisory review looks for both halves: the policy AND the minutes showing it operating; the BCP AND the drill report; the runbook AND the actual 6-hour report from the last incident. Start with the committees. Then the CISO. Then the runbooks. Then the evidence. The order matters.

Content current as of 5 June 2026. Full pillar guide: vcisodesk.com/rbi-it-governance-framework-implementation-guide-india/ — free, like everything on GRC RADAR.