DSCI
PROMOTING DATA PROTECTION

Brief on

RBI CYBERSECURITY, TECHNOLOGY, RISK, RESILIENCE AND ASSURANCE FRAMEWORK DIRECTIONS, 2026 FOR COMMERCIAL BANKS

Brief on:

RBI Cybersecurity, Technology, Risk, Resilience and Assurance Framework Directions, 2026 for Commercial Banks

The Reserve Bank of India issued the RBI (Commercial Banks - Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026 on July 31, 2026, formally titling and bringing into effect a consolidated set of rules governing cyber security, technology risk and operational resilience for commercial banks. The Data Security Council of India (DSCI) welcomes the directions as a timely and necessary step, coming into force immediately upon issuance and applicable to all commercial banks, collectively and individually referred to as banks throughout the framework. The immediacy of the effective date, without the transition windows that accompanied earlier circulars, reflects the commitment to strengthening the sector's cyber resilience, and keeping pace with an evolving threat landscape. The directions apply immediately to commercial banks, including banking companies, corresponding new banks, and the State Bank of India, though small finance banks, payments banks and local area banks remain outside their scope for now.

At the heart of the framework is a much more prescriptive testing regime than before. Banks must now conduct vulnerability assessments every six months and annual penetration tests for systems that are critical or internet facing, with additional testing required whenever new systems or major upgrades go live. Disaster recovery drills must happen every six months, and crucially, banks are expected to operate their DR site as the primary site for a full business day rather than simply confirming it can technically take over. Recovery Point Objectives for critical systems are expected to approach zero, meaning banks will need infrastructure resilient enough to lose almost no data even during a major disruption.

Governance structures are also being tightened in ways that should improve accountability. Boards must approve and review IT, cyber security and business continuity policies annually, and are required to set up a dedicated Board level IT Strategy Committee that meets at least quarterly. Perhaps the most consequential organisational change is the requirement that the Chief Information Security Officer report to the executive overseeing risk management, not to the Head of IT. This separation addresses a longstanding structural weakness where security functions sat under the same reporting line as the teams they were meant to check, potentially diluting independent oversight. The CISO must also present cyber security preparedness to the Board every quarter, keeping senior leadership continuously engaged rather than only during annual reviews.

Category	Requirement(s)
Vulnerability Testing	Conduct vulnerability assessments and penetration testing for all critical and internet-facing systems
	Perform vulnerability assessments at least every six months and penetration testing at least every 12 months for critical customer-facing systems

	Conduct testing after implementation of new systems and major upgrades
	Fix identified vulnerabilities within defined timelines and monitor closure of findings
	Use independent and qualified auditors for testing
Business Continuity and Disaster Recovery	Conduct disaster recovery drills for critical systems at least every six months
	Test disaster recovery sites by operating them as the primary site for at least one full business day
	Regularly restore backups to verify their usability
	Aim for near-zero Recovery Point Objective (RPO) for critical information systems
	Ensure disaster recovery environments mirror production environments
	Test resilience across interconnected vendor systems
Incident Response	Put in place a cyber incident response and recovery policy
	Report cyber security incidents on the DAKSH platform within six hours
	Define incident classification, reporting mechanisms, communication plans, recovery measures and threat information sharing processes
	Allocate responsibilities for employees and outsourced personnel handling incidents
Board Responsibilities	Boards must approve IT, cyber security, information security and business continuity policies
	Review these policies at least annually
	Constitute a Board-level IT Strategy Committee
	The Audit Committee will oversee information systems audits
Management and Organisational Structure	Banks must establish an IT governance framework covering strategy, risk, performance and business continuity
	Maintain separate information security and cyber security policies

	The IT Strategy Committee must meet at least quarterly
	Senior management must oversee implementation of IT strategy and cyber security
	Banks must establish an IT Steering Committee and an Information Security Committee
	Appoint a senior Head of IT Function and an independent CISO, with the CISO reporting to the executive overseeing risk management rather than the Head of IT
	The CISO must present cyber security preparedness to the Board or relevant committee every quarter
Risk Management	Include IT and cyber security risks in enterprise risk management
	Review IT risk policies at least annually
	Establish a formal IT and information security risk management framework
	Assess information assets using recognized security standards
	Review security infrastructure and policies at least annually
	Categorize risks based on their severity and evaluate the effectiveness of existing controls

On the operational side, the framework goes well beyond generic advice. Banks must maintain detailed inventories of data, applications and infrastructure, classify information by sensitivity, and implement data loss prevention tools along with remote wipe capability for mobile devices. Access control requirements are stricter too, with mandatory multi factor authentication for privileged users, removal of dormant accounts, and centralized identity management. Email security gets specific attention through mandatory DMARC implementation, while network security requirements include IPv6 support and layered defenses such as firewalls and intrusion detection systems.

Vendor and third-party risk, often a weak link in bank security, is explicitly addressed. Contracts must now include RBI audit rights, and even ATM switch providers are required to meet prescribed baseline controls, closing a gap that has historically been exploited through outsourced infrastructure. Incident response timelines have also been sharpened considerably. Banks must report cyber security incidents through the RBI's DAKSH platform within six hours of detection, a window tight enough that manual reporting processes will likely need to be replaced with automated detection and escalation systems.

Taken together, these directions represent a meaningful step forward for the banking sector's cyber resilience. For banks with mature governance and technology functions, compliance offers a valuable opportunity to formalize and showcase practices that are already largely in place, reinforcing the

strong foundations they have built over the years. For banks still developing their structures, particularly around CISO independence, data classification and vendor oversight, the framework provides a clear and well-defined roadmap to close those gaps quickly and decisively. The immediate applicability can be seen as a catalyst, giving the industry a strong push to accelerate investments in cyber security and emerge more resilient, better governed and more trusted by the customers and stakeholders who depend on them.

*****