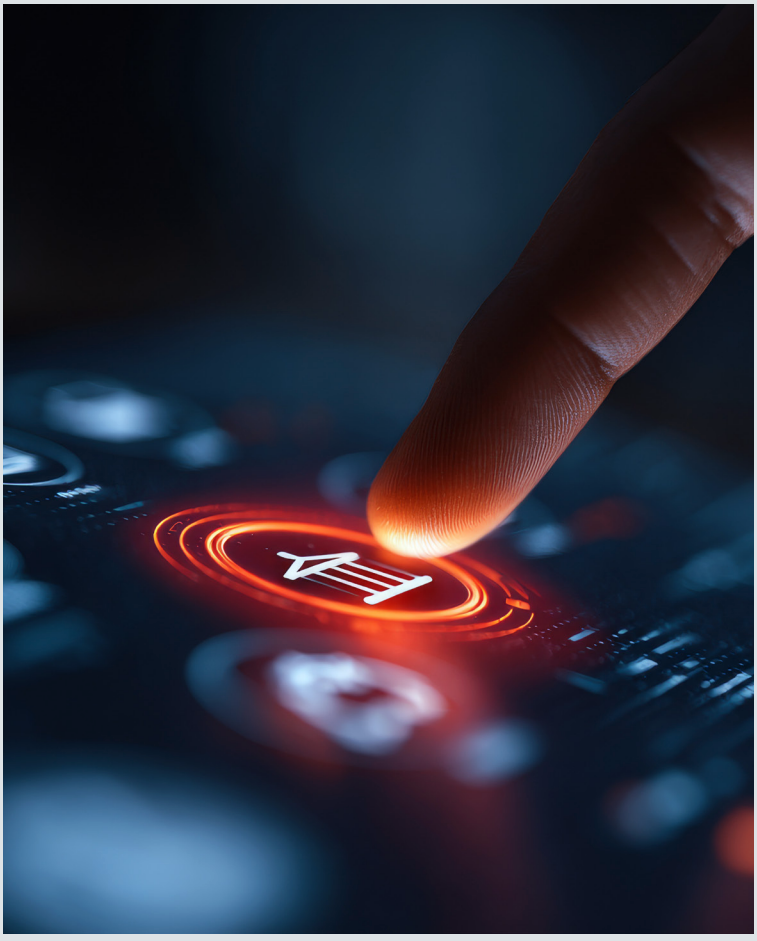
anunta

Whitepaper

RBI, DPDP, AND SEBI
THE NEW REALITY OF DIGITAL WORKSPACES FOR FINANCIAL INSTITUTIONS IN INDIA

Why Compliance Is Moving from Governance to Architecture



04th May, 2026

Executive Summary

Financial institutions in India are entering a new phase of regulatory enforcement.

Compliance is no longer defined solely by policies, audit frameworks, or governance processes. It is increasingly being defined by how digital environments behave in real time.

Regulatory expectations are becoming more precise, more operational, and more difficult to satisfy through traditional approaches.

Three forces are driving this shift:

- The Reserve Bank of India's (RBI) increasing focus on IT risk, cybersecurity, and data control
- The Digital Personal Data Protection (DPDP) Act, which introduces stricter accountability for data usage and handling
- The Securities and Exchange Board of India (SEBI) guidelines, reinforcing governance, auditability, and operational resilience

Individually, these frameworks introduce important requirements.

Together, they create a unified expectation:

Financial institutions must be able to demonstrate continuous, enforceable control over how data is accessed, processed, and governed.

This expectation exposes a structural gap in most enterprise environments.

The digital workspace, where users interact with systems and data, is not designed to consistently enforce compliance.

This is where **Sovereign Cloud models are gaining relevance**, enabling financial institutions to enforce data residency, access governance, and auditability within controlled, jurisdiction-aligned environments.

Table of Contents

What You Will Learn

Regulatory convergence across RBI, DPDP, and SEBI is shifting compliance from policy to architecture, requiring financial institutions to embed continuous control, data residency, and auditability within digital workspaces.

01 The Changing Nature of Regulatory Enforcement

Historically, compliance in financial institutions has been driven by:

- Defined governance frameworks
- Periodic audits and reporting cycles
- Layered controls across infrastructure and applications

This model assumes that:

- Environments are relatively stable
- User behavior can be managed through policies
- Compliance can be validated at defined intervals

These assumptions are no longer valid.

Modern environments are:

- Distributed across cloud, data centers, and hybrid infrastructure
- Accessed from multiple locations, devices, and networks
- Continuously evolving to support business requirements

Regulatory expectations have evolved accordingly.

They now require:

- Continuous visibility into user activity
- Enforced control over data access and movement
- Real-time auditability
- Accountability at the level of user interaction

These expectations are increasingly difficult to meet using fragmented infrastructure approaches, leading institutions to evaluate **Sovereign Cloud-aligned digital workspace models** that embed compliance directly into how environments operate.

This represents a shift from **audit-driven compliance** to **operational compliance**.

02 The Convergence of RBI, DPDP, and SEBI Requirements

Each regulatory framework focuses on different aspects of compliance.

However, when viewed together, they converge toward a single architectural requirement.

RBI: IT Risk and Cybersecurity Framework

The RBI framework places increasing emphasis on:

- Data localization and control
- Endpoint governance across branches and distributed environments
- Continuous monitoring and risk management

The key implication is clear:

Institutions must demonstrate control over how systems are accessed, not just how they are configured.

DPDP Act: Data Protection Becomes Enforceable

The DPDP Act introduces a new level of accountability.

Organizations must now ensure:

- Personal data is accessed and processed within defined boundaries
- User interactions with data are traceable
- Responsibility for data protection extends across the entire lifecycle

This moves compliance beyond policy into infrastructure.

SEBI: Strengthening Governance and Auditability

SEBI guidelines reinforce:

- Data governance and access control
- Disaster recovery and operational resilience
- Continuous audit readiness

For institutions operating across capital markets, this introduces additional complexity in managing user environments.

03 The Combined Impact

When these requirements are combined, they create a unified expectation:

- Data must always remain within controlled boundaries
- Access must be consistently governed across users and environments
- User activity must be traceable end-to-end
- Compliance must be continuously demonstrable

This is not a policy challenge.

It is an architectural one.

Addressing this unified requirement is driving a shift toward Sovereign Cloud architectures, where data, access, and user environments are governed within defined boundaries rather than across distributed systems.

04 Where Current Workspace Models Fall Short

Most financial institutions operate in environments that have evolved.

These environments typically include:

- Legacy virtual desktop infrastructures
- Distributed endpoint environments across branches and remote users
- Cloud-based systems integrated with existing infrastructure

While functional, these models introduce systemic issues.

Inconsistent User Environments

Different users operate in different environments based on their roles, locations, and access methods.

This leads to variability in control and enforcement.

Fragmented Access Governance

Access policies are defined centrally but enforced inconsistently across systems and environments

Limited Visibility into User Activity

User activity is captured across multiple tools and systems, making it difficult to build a unified view.

Data Residency Exposure

Data may be stored within compliant regions, but there is limited control over how it is accessed and moved during usage.

Dependence on Audit Reconstruction

Compliance is often demonstrated by aggregating logs and reconstructing events.

This approach is increasingly insufficient.

05 Why Incremental Improvements Are Not Enough

To address these challenges, institutions often:

- Expand cloud adoption
- Invest in additional security tools
- Enhance monitoring capabilities
- Strengthen governance processes

These steps are necessary.

However, they do not address the underlying issue.

They improve visibility and control at the individual layer level.

They do not unify control across the environment.

06 The Emerging Requirement: Workspace-Centric Compliance

ATo meet regulatory expectations, control must be enforced at the point where users interact with systems and data.

This places the digital workspace at the center of compliance. In practice, this is increasingly achieved through Sovereign Cloud-based workspace environments, where control is consistently enforced across users, locations, and systems.

A workspace-centric model enables:

Centralized Control
User environments are standardized and governed consistently across the organization.

Enforced Data Boundaries
Data residency is maintained during access and interaction, not just storage.

Consistent Access Governance
Access policies are applied uniformly across all users, devices, and locations.

Continuous Auditability
User activity is captured and correlated in real time.

This model shifts compliance from reactive validation to embedded control.

07 Implications for Financial Institutions

CIO
Workspace architecture becomes a strategic decision, directly linked to regulatory compliance and operational resilience.

CISO
Control moves closer to the user environment, improving visibility and reducing reliance on fragmented security layers.

Executive Leadership
Compliance risk becomes tied to infrastructure design, not just governance frameworks.

08 A Reality Check

Most institutions cannot answer key questions with certainty:

- Is data residency enforced during actual usage?
- Are access policies applied consistently across all environments?
- Can user activity be traced end-to-end in real time?
- Is compliance maintained continuously?

These gaps are often only identified during audits or incidents.

09 The Path Forward

Addressing these challenges requires a shift in approach.

Organizations must move from:

Policy-led compliance → Architecture-led compliance

This begins with understanding the current state.

Institutions must evaluate:

- Workspace architecture and control points
- Data flow and residency enforcement
- Access governance models
- Audit readiness at the user level

10 Closing Perspective

The regulatory environment for financial institutions in India is not becoming more complex. It is becoming more precise.

Compliance is no longer about demonstrating readiness periodically. It is about sustaining control continuously.

And that depends on how digital workspaces are designed and governed.

Organizations that recognize this shift will be better positioned to meet regulatory expectations without increasing operational complexity.

A Sovereign Cloud approach provides financial institutions with a structured way to align regulatory requirements with operational control, reducing fragmentation and improving audit readiness.

Those that do not will continue to rely on fragmented models that fail under scrutiny.

About Anunta

Anunta builds secure and compliant digital workspaces across private, public, and hybrid clouds for enterprises. Our comprehensive range of managed virtual desktop, managed endpoint & cloud services allow users to access applications and data securely. Our managed services are powered by our platforms, which leverage AI & Machine Learning to automate and optimize operations. We've been consistently featured in the Gartner Magic Quadrant for Desktop as a Service. With over a decade of experience, we've successfully migrated **1 Million+** remote desktop users, boosting security, enhancing workforce productivity, and delivering superior end-user experiences.

For more information about Anunta, visit www.anunta.com

Follow us on: