



Ashok Sathyanathan
Founder
Mobile: +91-9619787832
Email: ashok@lexaashraya.in

PROCESS OUTSOURCED, LIABILITY NOT: RBI'S RENEWED WARNING ON FINANCIAL SERVICES

1. Introduction

India's financial services ecosystem increasingly relies on fintechs, Lending Service Providers (LSPs), Direct Selling Agents (DSAs), cloud providers and technology platforms for lending, credit analytics, collections and customer servicing.

At the FE Modern BFSI Summit, Mumbai, on 15 October 2026, RBI Deputy Governor Swaminathan J cautioned against sacrificing essential controls for speed, scale and convenience. His address was published on 21 October 2026.

Core principle: Processes may be outsourced, but regulatory accountability remains with the regulated entity to the extent imposed by law. Technology, automation and AI cannot replace required controls.

2. Regulatory Framework: Distinct Directions, One Principle

Applicability depends on the regulated entity, outsourced activity and relevant directions.

- **Financial services outsourcing:** RBI's 2006 bank guidelines address outsourcing, risk management, customer protection and Board oversight.
- **IT outsourcing:** RBI's 2023 Directions, effective 1 October 2023, address governance, third-party risks, data confidentiality, supervision and exit planning.
- **Digital lending:** Applicable RBI directions govern LSP arrangements, customer protection, data handling and grievance redressal.
- **Default Loss Guarantee (DLG):** RBI caps qualifying DLG cover at 5% under its digital-lending framework. This is not a universal credit-risk transfer cap.
- **Cybersecurity:** Applicable RBI directions and CERT-In requirements govern security, incident reporting and operational resilience.
- **Data protection:** The DPDP Act, 2023, and Rules, 2025 establish the data-protection framework, subject to phased commencement.

These frameworks are distinct but complementary. **Outsourcing must not compromise customer protection, regulatory compliance or effective RBI supervision.**

3. Key Regulatory Takeaways

A. Efficiency Cannot Override Control

- Outsourcing can improve scale, speed and cost efficiency.
- The regulated entity must retain effective oversight, risk management and control.
- Vendor dependence does not remove regulatory obligations.

B. Credit Decisions and AI Require Oversight

- Outsourced credit analytics and automated decision-making require appropriate validation and monitoring.
- Accountability for lending decisions must remain aligned with applicable regulatory requirements.
- Models, data quality, bias, explainability and human intervention should be addressed where relevant.

C. Customer Protection and Systemic Trust

- Customers should not be left navigating gaps between a regulated entity and its service provider.
- Grievance redressal, service continuity and accountability must remain clear.
- Weak controls across multiple institutions can create broader operational and reputational risks.

4. Third-Party and Fourth-Party Risk

Risk extends beyond the immediate service provider to subcontractors, cloud infrastructure and other downstream dependencies.

Regulated entities should:

- Identify critical vendors and material dependencies.
- Assess financial, operational, cybersecurity and concentration risks.
- Obtain appropriate visibility into subcontracting and fourth-party arrangements.
- Ensure audit, access, reporting and regulatory-cooperation rights.
- Test business continuity, disaster recovery and exit arrangements.
- Maintain alternatives for critical services where proportionate and feasible.

A vendor assessment is not a one-time exercise. Risk must be monitored throughout the outsourcing lifecycle.

5. Cyber Incidents, Data Protection and Disclosure

A. Cybersecurity and Incident Reporting

- CERT-In's Directions dated 28 April 2022 require covered entities to report specified cyber incidents within six hours of noticing them or being informed of them.
- Applicable RBI directions may impose additional incident-reporting and security obligations.

- Contracts should require prompt vendor notification, evidence preservation, cooperation and support for regulatory reporting.
- Internal escalation timelines should leave sufficient time for the regulated entity to meet applicable reporting deadlines.

B. Data Protection

- The DPDP Act, 2023, and Rules, 2025 provide the framework for personal-data processing and protection, subject to their phased commencement.
- Responsibilities should be mapped between the regulated entity and its processors.
- Contracts should address permitted use, access controls, security, retention, deletion, breach notification and assistance with data-principal requests.
- Data minimisation and restrictions on unauthorised reuse should be built into operating processes.

C. Listed-Entity Disclosure

- Listed entities must assess material events under applicable SEBI LODR requirements, including Regulation 30.
- A vendor incident may trigger disclosure obligations depending on its nature, materiality and impact.
- Materiality should be assessed promptly and documented. Outsourcing does not, by itself, determine whether disclosure is required.

6. Contractual Accountability

Contracts must convert regulatory expectations into enforceable operational obligations.

Regulated Entities Should Consider

- Defined service levels, control standards and escalation protocols.
- Audit and inspection rights, including access required by regulators.
- Incident notification, investigation support and evidence preservation.
- Data security, confidentiality, retention and deletion obligations.
- Business continuity, disaster recovery and tested exit plans.
- Indemnities, liability allocation, insurance and appropriate remedies.
- Controls over subcontracting and changes to critical services.

Fintechs and Service Providers Should Consider

- Clear allocation of responsibilities and reporting obligations.
- Documented compliance and security controls.
- Timely incident escalation and cooperation with investigations.
- Appropriate restrictions on data use and onward outsourcing.
- Practical transition support and return or deletion of data at exit.

Operational timelines, such as a two-hour incident alert, periodic vendor-register reviews, source-code escrow or a 30-day deletion period, may be adopted where appropriate. They should be treated as

contractual or governance choices, not universal legal mandates unless specifically required by an applicable rule or direction.

Regulatory accountability and contractual liability are distinct. A regulated entity may remain answerable to its regulator even where the service provider is contractually liable for a failure. Contractual recourse does not automatically transfer regulatory responsibility.

7. Board-Level Governance

The Board and senior management should ensure that outsourcing risks are visible, owned and monitored.

Key priorities include:

- Approving appropriate outsourcing and third-party risk frameworks.
- Identifying critical services, dependencies and concentration risks.
- Reviewing material incidents, recurring control failures and remediation.
- Ensuring adequate audit coverage and independent assurance.
- Monitoring compliance with applicable reporting and customer-protection obligations.
- Testing continuity, recovery and exit arrangements.

Vendor performance metrics alone are insufficient. Oversight should also measure control effectiveness, resilience and customer impact.

8. The Road Ahead

Financial institutions should treat outsourcing as a governed risk relationship, not merely a procurement decision.

The priority is to align vendor selection, due diligence, contracting, monitoring, incident response and exit planning with the institution's regulatory obligations and risk profile.

The process may be outsourced. The licence, customer obligations and regulatory responsibilities remain with the regulated entity to the extent imposed by law.

Disclaimer: *This article is for general legal information and does not constitute legal advice. The applicable facts, documents and law should be independently examined in each case*