Data Resilience in BFSI: The Trust Test After Recovery

Why restoring systems is only the first step towards safely resuming financial services

Executive Summary: The Data Trust Paradox

In modern banking, financial services and insurance (BFSI) systems, recovering and restoring every server does not necessarily constitute successful business recovery.

Traditional BFSI programmes focus on availability. Their primary concerns include how quickly systems can be restored and how much data can be lost. Consequently, Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are essential measures. However, a pertinent question is unanswered

"Can institutions establish sufficient confidence in the integrity of the data they have recovered to resume business?"

In the BFSI sector, data directly impacts monetary positions, customer rights, regulatory reporting, and market confidence. Financial institutions may restore their infrastructure while addressing incomplete transactions, altered records, inconsistent balances, or uncertainty about whether compromised information has propagated to downstream systems. Hence, ensuring data integrity is not a secondary concern, but a prerequisite for a safe resumption.

This creates the **Data Trust Paradox**. Data becomes technically available before it becomes operationally trustworthy. Therefore, resilience maturity must extend beyond system restoration to include data validation, reconciliation, remediation, and accountable authorisation for **business resumption**.

1. Structural Vulnerabilities: When Bad Data Travels

The resilience challenge in BFSI is fundamentally shaped by the **interconnectedness and velocity of financial data**. A transaction, customer record or financial position rarely remains confined to the system in which it originates. In milliseconds, information may traverse applications, APIs, data platforms, analytics engines and customer-facing channels, becoming an input to multiple downstream processes and decisions.

Illustrative propagation path

Source → System	**Interface → API**	**Downstream → Application**	**Data / → Analytics**	**Automated → Decision**	**Customer / Regulatory Outcome**

If corrupted, incomplete or manipulated information propagates through downstream systems before the original compromise is detected, restoring the source system alone may not reverse its consequences. Institutions must instead determine **where the affected data travelled, which systems consumed it, and what business or regulatory decisions were made using it**.

Therefore, distinguishing between **system recovery and data recovery** becomes unavoidable. A system can be restored to an operational state while the information it contains remains unreliable. **The recovery process must therefore account not only for the state of individual systems, but also for the provenance, propagation and downstream impact of critical data**.

Artificial intelligence introduces a new dimension to this challenge. AI does not need to be compromised for its outputs to become unreliable. If information is corrupted, manipulated, or incomplete, it can distort the data or knowledge context on which an AI-enabled process depends, making the resulting output appear reasonable yet be operationally or financially unsound. Two risks are particularly important:

- **Contextual poisoning:** corrupted or manipulated information enters the data or knowledge context used by an AI-enabled process.
- **Output validity:** the model produces a plausible recommendation, classification or decision based on information that should not have been trusted.

The resulting risk is therefore not limited to the question of the model being compromised. The question is whether the information that influences outputs is reliable.

2. The Six-Stage Recovery-to-Resumption Blueprint

A resilient recovery process must treat **system restoration as the initial step, not the endpoint**. Safe resumption of critical financial services requires a structured pipeline that maps technical recovery to validated business continuity. Below is a 6-stage recovery pipeline:

STAGE	ACTION
1. Recovery	Restoration of systems and critical data in a controlled environment
2. Validation	Checking completeness, integrity and evidence of compromise in recovered data
3. Reconciliation	Comparing critical transactions, balances and records across dependent systems
4. Resolution	Investigation and correction of missing, duplicate, altered or inconsistent records
5. Authorisation	Obtaining accountable approval that critical data is fit for business use
6. Resumption	Reconnection of services and resumption of operations in a controlled manner

A resilient recovery process must be supported by an architecture that prevents **contamination by accelerating validation to establish data integrity**.

ARCHITECTURAL CAPABILITY	HOW DOES IT STRENGTHEN DATA RESILIENCE?
Immutable or WORM recovery copies	Protect recovery points from alterations or deletion.
Append-only transaction records	Supports reconstruction of events and provides a tamper-evident history where appropriate.
Continuous integrity monitoring	Detects unexpected changes and integrity anomalies earlier.
Automated reconciliation	Rapidly identify discrepancies across transactions, balances and systems.
Isolated recovery or clean-room environments	Enables validation and investigation before reconnecting recovered data to production.
Data lineage for critical datasets	Trace where affected data originated, travelled and influenced downstream processes.

The underlying principle should be to ensure that **critical recovered data is independently verifiable, protected from further compromise, and reconciled before it supports business decisions**. The objective is not to prescribe a universal technology architecture.

3. Governance & Accountability: Who Decides It Is Safe?

Technology recovery and business resumption are related but are **not the same decision**.

- Technology can establish if the systems have been restored.
- Cybersecurity can determine whether the compromise has been contained.
- Data and operations teams can validate and reconcile critical records.
- Business teams conduct assessments to understand the urgency and consequences of continued disruption.
- Senior Management provides authorisation for service resumption based on defined evidence and risk acceptance.

These are **functional assurances, not decisions to resume**. None of these individually answers the following enterprise question

Who has the authority to declare that the recovered data is adequately trustworthy for the institution to resume operations?

Without explicit ownership, recovery creates **accountability gaps.** Teams own individual recovery activities, but no one owns the final decision to resume.

To ensure that resumption is an accountable, evidence-based decision rather than an implicit consequence of technical recovery, decision **authority, evidence thresholds and escalation criteria must be defined before.**

The operating model may differ across institutions, but the governance principles should not.

4. Board & Leadership Imperatives

Data resilience is no longer a mere technological concern. It is a critical **business continuity, risk and governance issue**. Boards and senior management should therefore move beyond asking whether backups exist and test whether the institution can **establish trust in its data before resuming critical services**.

1. **Which datasets are critical enough to be proven accurate and complete before the institution can safely resume operations?**
2. **Can we independently establish the last known trustworthy state of critical data, even if the primary environment has been compromised?**
3. **How rapidly can we validate and reconcile critical transactions, balances and customer records following a disruption?**
4. **Can we trace, contain and remediate compromised data before it propagates into downstream systems, automated processes or AI-driven decisions?**
5. **Who is accountable for accepting residual data-integrity risk and authorising the resumption of critical services?**

These questions are increasingly relevant in a regulatory environment that expects financial institutions to demonstrate not only technology recovery capability but also operational resilience, effective controls, testing and the ability to recover critical services safely. RBI's IT governance and assurance expectations provide an important India-specific context, while global frameworks such as the EU Digital Operational Resilience Act (DORA) and NIST guidance on data integrity reinforce the importance of recovery, validation and resilience against destructive cyber events.

Conclusion: From System Recovery to Trusted Resumption

The next stage of resilience maturity in BFSI will not be defined solely by who can restore systems fastest. It will increasingly depend on who can establish with evidence and governance that critical data can be trusted again. RTO, RPO, and backups remain important. Disaster recovery is still a critical capability. For financial institutions, the objective after a disruption should therefore be clear.

- **Restore systems**
- **Validate data,**
- **Reconcile the business**
- **Make an accountable decision to resume.**

The distinction is fundamental: "**Proof of recovery ≠ Proof of integrity".**

The question for BFSI leaders is no longer simply, *"Can we recover our data?"* It is **"Can we trust it enough to resume business?"**

Reference Context for Editorial Review

- Reserve Bank of India — Information Technology Governance, Risk, Controls and Assurance Practices Directions.
- NIST SP 1800-11 — Data Integrity: Recovering from Ransomware and Other Destructive Events.
- NIST SP 1800-26 — Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events.
- Basel Committee on Banking Supervision — Principles for Operational Resilience.
- EU Digital Operational Resilience Act (DORA) — ICT risk management, testing, backup, restoration and recovery expectations.

ABOUT THE AUTHOR

Sumedha Adavade

Sumedha Adavade is a senior Technology Risk, Cybersecurity Governance and Operational Resilience leader with over 18 years of experience across the banking and financial services sector.

In her current regional leadership role, she works across multiple Asia-Pacific jurisdictions, driving technology risk oversight and strengthening governance and assurance across complex technology environments.

Her work involves partnering with senior business and technology stakeholders on regulatory expectations, control effectiveness, risk visibility and enterprise resilience. Her areas of expertise include technology and cyber risk management, information security governance, regulatory compliance, AI governance, operational resilience, business continuity, data governance and technology control frameworks. She has extensive experience working at the intersection of technology, risk and business decision-making, including engagement with regulators, senior management and cross-functional technology teams.

Sumedha is also an industry speaker and panelist, contributing to conversations on cybersecurity, technology risk, operational resilience, AI governance and the evolving challenges of the digital ecosystem. Through these engagements and her writing, she brings a practitioner-led perspective to emerging technology risk governance and compliance challenges.

Sumedha is the founder of CyberConnectLead, an initiative focused on connecting cybersecurity and technology governance conversations, ideas and capabilities across the evolving digital ecosystem.

She holds professional certifications including CISA, ISO 27001 Lead Auditor, Certified in Risk in Financial Services and CCNA.