

New Singahi Guide: RBI's 2026 Rules Bring Bank Suppliers Into Continuity Testing

The guide lists the business continuity questions banks ask software, cloud and IT suppliers, the rule behind each one, and the evidence that answers it.

LUCKNOW, INDIA, October 30, 2026 /EINPresswire.com/ -- Software, cloud and IT companies that sell to Indian banks should expect closer questions about how their service recovers from an outage. Directions issued by the Reserve Bank of India on 31 July 2026 ask banks to extend business continuity and disaster recovery to critical systems run by their vendors and partners, and to show readiness through coordinated resilience testing that meets the bank's recovery time objective.



The same Directions tell banks to base their continuity and recovery policy on best practices such as ISO 22301, the international standard for business continuity. RBI's version for NBFCs carries both provisions. Separate RBI Directions on outsourcing, issued in November 2025, already required banks to make sure their service providers document, maintain and test their business continuity and recovery procedures. Existing IT outsourcing agreements had to comply at renewal or by 10 April 2026, whichever came first.

“

Banks want specifics. What is your recovery time for the service they are buying? When did you last test it? Which of your own vendors could take you down?”

Rahul Verma, Cybersecurity Sales Specialist, Singahi

Indian banks have already felt a supplier failure. On 19 July 2024, RBI said a faulty CrowdStrike update had caused

minor disruptions at 10 banks and NBFCs. Twelve days later, NPCI cut C-Edge Technologies off from retail payment systems after a suspected ransomware attack. C-Edge provides technology to co-operative and regional rural banks, and until it was reconnected, customers of those banks could not use the payment systems.

The new rules bind the bank, not the supplier. They reach suppliers through due-diligence questionnaires, contract clauses and audit rights, often late in a deal.

The tightest deadline in those questionnaires is for incident reporting. RBI's outsourcing Directions require a bank to ensure its provider reports cyber incidents without undue delay, so the bank can report to RBI within six hours of the provider detecting the incident. A supplier whose own procedure promises notice "within 24 hours" cannot support that.

"By the time the continuity questions arrive, the deal is usually close, and nobody wants to slow it down," said Rahul Verma, Cybersecurity Sales Specialist at Singahi. "Banks want specifics. What is your recovery time for the service they are buying? When did you last test it? Which of your own vendors could take you down? A supplier can answer most of that before the questionnaire shows up. The guide takes each question in turn and shows the evidence that answers it."

The guide, "[Selling to banks: the business continuity questions you will be asked](#)", covers 13 questions on the supplier's plan, recovery targets, testing, incident handling, audit and exit. Each question is mapped to the clause of ISO 22301 that addresses it. Banks in other markets work under similar rules, so the guide sets the Indian requirements alongside the EU's Digital Operational Resilience Act (DORA), the UK PRA's supervisory statement SS2/21, Australia's CPS 230 and the US interagency guidance on third-party relationships. Under DORA, for example, a technology provider supporting a critical or important function must take part in the bank's threat-led penetration testing.

None of these rules requires a supplier to be certified to ISO 22301. RBI does, however, let a bank rely on globally recognised third-party certifications held by a provider in place of its own independent audits, depending on the bank's risk assessment.

The guide closes with the six pieces of evidence that most of the questions come back to: a continuity policy approved by management, the business impact analysis behind the recovery targets, the plan itself, the latest exercise report, a list of critical suppliers and their own arrangements, and the reports from the last internal audit and management review.

It links to Singahi's [ISO 22301 toolkit](#), which explains each of the standard's 26 clauses in plain language and includes a free Control Pack of templates for each one, such as a business impact analysis procedure and an exercise programme.

[Read the guide.](#)

Watch the video: <https://youtu.be/YtMTOmMsUJ4>

About Singahi

Singahi helps growing companies prove security to customers, investors and regulators. One

team for compliance, testing, and managed security. Singahi is headquartered in Lucknow, India, with representatives in Bengaluru, Noida and Chandigarh.

Rahul Verma

Singahi Technologies Private Limited

+91 95802 30300

media@singahi.com

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/953128434>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.