The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy

SERVICE OUTAGES IN INDIA

CERT-In Rules, Data Protection and Cloud Regulation

1. Latest News and Background

The global Microsoft 365 outage on November 12–13, which disrupted access to Outlook and other productivity services worldwide, has raised questions about the accountability of cloud service providers and the adequacy of India's regulatory framework for reporting major digital service outages.

An infrastructure-related problem at Microsoft affected customers' ability to access Microsoft 365 services, including Outlook email, across the world. Microsoft attributed the disruption to a fault during an upgrade of its network capacity and issued an apology.

The outage also affected services in India. IndiGo and Akasa Air alerted passengers about disruptions to their email support, while Air India rerouted its email services.

The incident highlighted India's dependence on cloud-based digital infrastructure and raised an important regulatory question: Are service providers legally required to report technical failures that temporarily disrupt access to essential digital services?

2. India's Regulatory Framework for Service Outages

Three major regulatory frameworks are relevant to the reporting and management of digital service disruptions in India. However, each has certain limitations.

A. CERT-In Directions under the Information Technology Act, 2000

The Indian Computer Emergency Response Team (CERT-In) issued directions on April 28, 2022, under the Information Technology Act, 2000, requiring organisations to report specified cyber incidents within six hours of noticing them.

These directions primarily cover cybersecurity incidents such as attacks and intrusions. They do not explicitly include service outages caused by technical faults or infrastructure failures.

However, under Section 70B(6) of the IT Act, CERT-In has the authority to call for information and seek explanations from service providers, including Microsoft.

B. Reserve Bank of India (RBI) Directions on IT Outsourcing

The RBI's directions on managing risks in outsourcing, issued on November 28, 2025, carry forward the regulatory framework for outsourced IT services that initially took effect on October 1, 2023.

Under these directions, banks procuring cloud services must assess their dependence on service providers and maintain an appropriate exit strategy.

The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy

If an outsourced arrangement fails, the RBI can hold the bank accountable for ensuring continuity and managing associated risks. The bank may also seek an explanation from the cloud service provider under its contractual agreement.

C. Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection (DPDP) Act, 2023, introduces another dimension to the regulation of service outages.

The Act defines a personal data breach to include the accidental loss of access to personal data. Under the Rules scheduled to come into effect in May 2027, personal data breaches must be reported to the Data Protection Board and the affected individuals.

Failure to report a breach could attract a penalty of up to Rs. 200 crore.

However, the framework creates an important ambiguity: it is unclear whether a temporary service outage constitutes a legally reportable loss of access to personal data.

3. International Frameworks for Cloud Service Accountability

A. European Union

The European Union has introduced regulatory oversight of critical technology providers through two important frameworks.

- Digital Operational Resilience Act (DORA): The EU's financial supervisors identified 19 critical technology service providers under DORA on November 18, 2025. The framework places major technology vendors providing services to financial institutions under the supervision of European financial regulators.
- Network and Information Security Directive 2 (NIS2): Unlike DORA, NIS2 covers cloud service providers across sectors. Cloud service providers must notify the national authority within 24 hours and submit a detailed notification within 72 hours.

B. United Kingdom

As of July 13, 2026, the United Kingdom had placed Microsoft and three other technology companies under the oversight of the Bank of England. This framework, like DORA, focuses on technology services supplied to financial institutions.

C. Singapore

On October 7, Singapore passed a digital infrastructure law requiring large data centres and cloud service providers to obtain licences and report service interruptions to the regulator.

D. South Korea

Following a data centre fire in October 2022 that disrupted the messaging platform KakaoTalk, South Korea introduced stronger disaster-management requirements. Since July 2023, large digital platforms and data centres have been required to submit disaster management plans to the government.

The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy The Tutors Academy

4. Options Available to Indian Customers and Policy Measures

At present, a customer's primary recourse against a cloud service provider is generally governed by the contractual agreement. If the provider fails to meet the agreed service-level requirements, the customer may be entitled to service credits, which provide a discount on a future bill.

The regulatory framework could be strengthened through four possible measures:

- Expand CERT-In reporting requirements: Major service disruptions should be reportable irrespective of whether they result from cyberattacks, technical faults or infrastructure failures.
- Direct regulatory oversight: The government could bring the largest digital service providers under the supervision of a designated regulator.
- Clarify data breach obligations: The Data Protection Board could clarify whether temporary outages constitute personal data breaches under the DPDP framework and identify the entities responsible for reporting them before the Rules take effect in May 2027.
- Diversify service providers: Government organisations could reduce dependence on foreign cloud service providers by using domestic alternatives. In December 2025, the Union Government informed the Lok Sabha that 12.68 lakh official email accounts had shifted to a platform operated by Chennai-based Zoho. However, domestic providers would also need clear outage-reporting obligations.

Source: The Hindu (TH)

