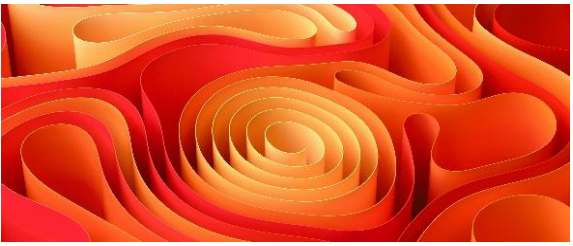
Pills

Regulatory/Supervisory Pills | N.91 June 2026

Author: Dario Esposito



TOPICS:

ICT Risk

SOURCE:

Bank for International Settlements

BIS: Information and Communication Technology (ICT) Risk Management - Range of Practices

- The Basel Committee has reviewed **ICT risk management practices** across 16 jurisdictions, focusing on non-malicious ICT incidents that can disrupt critical banking services and operational resilience.
- The report identifies **four primary causes of ICT incidents**: change-control failures, weaknesses in system design and testing, capacity and performance issues and failures involving external service providers. Change-management deficiencies were the most frequently reported root cause, reflecting the increasing complexity of banks' technology environments.
- **To address these risks**, banks commonly employ practices such as structured change management, incident and problem management, business continuity and disaster recovery testing, project and software development controls, asset management and third-party risk management. Many institutions are also adopting automation, artificial intelligence (AI), and machine learning (ML) to improve monitoring, testing, and incident detection, while maintaining human oversight for critical decisions.
- The report highlights **ongoing challenges**, including limited visibility into third-party and supply-chain risks, difficulties mapping system dependencies and shortages of skilled technology professionals. Banks are also balancing the need to modernise legacy systems while maintaining operational stability.
- All **surveyed jurisdictions** have ICT risk management regulations or supervisory guidance in place, generally applying risk-based approaches to oversight. The report concludes that strengthening governance, resilience testing, change management and third-party oversight is essential to reducing operational disruptions and supporting financial stability in an increasingly digital banking environment.