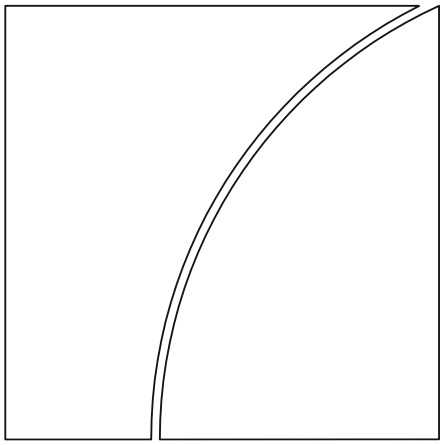
Basel Committee
on Banking Supervision



Information and communication technology (ICT) risk management: range of practices

June 2026

BIS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-956-0 (online)

Contents

Executive summary

Information and communication technology (ICT) risk management is a key component of operational risk management, playing a vital role in supporting the broader goal of achieving operational resilience. Banks' operational resilience to ICT incidents has become increasingly important in an evolving and digitalised technology landscape, particularly to mitigate the prevalence and impact of ICT incidents. In line with this, the Basel Committee undertook an analysis of global practices and developments in ICT risk management as part of its 2025–26 work programme.

This report describes a range of observed ICT risk management practices across jurisdictions worldwide relevant to addressing non-malicious ICT incidents in global systemically important banks (G-SIBs), domestic systemically important banks (D-SIBs) and other banks of interest (eg digital-only banks) that affect the delivery of critical operations. In preparing this range of practices report, the BCBS relied on input from its member jurisdictions, including selected case studies, and industry engagement. In addition, relevant regulatory and supervisory approaches from banking authorities were reviewed. Overall, 16 jurisdictions participated in the survey.[1]

Below is a summary of the key results of the survey:

1. Some jurisdictions experienced an increase in non-malicious ICT incidents between 2022 and 2024. Others saw a decline, particularly between 2023 and 2024. Importantly, the regulatory requirements for incident reporting vary across jurisdictions in terms of definitions, criteria and thresholds, which are reflected in both the type and the number of incidents reported in this survey.

2. The most frequently reported root causes of ICT incidents across surveyed jurisdictions include:

- change control gaps
- gaps in systems design, development and testing
- system capacity and performance issues
- external dependency operational failure.

3. The five most frequently reported ICT risk management practices across surveyed jurisdictions include:

- **ICT change management**: to manage the risks arising from changes to ICT systems and infrastructure
- **Third-party risk management**: to manage the ICT risks arising from using and reliance on third-party services
- **ICT continuity testing**: to maintain the banks' ICT business continuity and test the effectiveness and robustness of their business continuity and disaster recovery measures
- **ICT incident and problem management**: to ensure effective incident response, containment, root cause identification and remediation
- **ICT project management and system development**: to implement ICT systems to meet business requirements and to achieve the necessary quality, reliability and security assurance.

[1] The 16 jurisdictions that participated in the survey are Argentina, Australia, Brazil, Canada, Germany, Hong Kong SAR, India, Japan, Korea, Mexico, Saudi Arabia, Singapore, South Africa, the European Union Single Supervisory Mechanism (SSM), the United Kingdom and the United States. Not all jurisdictions responded to every question.

4. In all surveyed jurisdictions, the banking authorities have indicated that they have ICT risk management regulations and/or guidance in place. In many surveyed jurisdictions, banks are also subject to additional ICT risk management regulations and/or guidance at the national level from other government agencies. However, banking authorities retain the primary authority to develop and issue ICT risk management regulations and/or guidance, and exercise supervisory oversight on banks. In most surveyed jurisdictions, the banking authorities adopted a risk-based and tailored approach to supervising banks' ICT risk management through a combination of on-site examinations, thematic reviews and/or off-site assessments. The banking authorities also engage in a wide variety of other activities to support their primary regulation and supervision efforts.

5. Surveyed jurisdictions report several challenges faced by banks in their implementation of ICT risk management practices. For example, challenges were observed in maintaining traceability from business services to ICT assets and ensuring the completeness of system dependency mapping and ICT asset inventory, also for third-party services. Talent shortages at banks, particularly in cyber security, cloud, artificial intelligence / machine learning (AI/ML), and legacy systems, are exacerbated by competition with the technology industry. Banks in the surveyed jurisdictions face challenges from the lack of visibility into risk management controls at their technology service providers, as well as their own third-party concentration risks and supply chain interdependencies.

6. At the industry outreach event, some panellists highlighted significant progress in reducing failure rates through the banks' technical and/or process controls. To support effective ICT risk management, the panellists highlighted the importance of:

- **adopting a modular and layered approach** in the implementation of new system components to replace legacy systems and reduce complexity
- **implementing automation**, including through new technologies and AI/ML, while maintaining an appropriate level of human oversight and control
- **managing nth-party dependencies** and maintaining visibility across the ICT supply chain
- **addressing talent shortages** by partnering with universities and creating technical career tracks internally.

Information and communication technology (ICT) risk management: range of practices

1. Introduction

To strengthen banks' operational resilience to ICT incidents in an increasingly digitalised world, and considering the prevalence, impact and spread of ICT incidents, the Basel Committee conducted an analysis of global practices and recent advancements in ICT risk management as part of its 2025–26 work programme.[2] Fundamentally, ICT risk management is a subset of operational risk management, contributing to the broader goal and ultimate outcome of achieving operational resilience.

The Basel Committee's previous range of practices report on cyber resilience focused on the management of vulnerabilities and threats related to malicious cyber incidents and remains highly relevant.[3] In contrast, the current range of practices report on ICT risk management complements the earlier work by concentrating on non-malicious ICT incidents in banks that affect the delivery of critical operations and services. This focus is framed within the context of operational resilience and takes into account the growing ICT dependency in the banking sector. By addressing non-malicious ICT incidents, this report distinguishes itself from the Committee's previous studies, offering a unique perspective on this important aspect of ICT risk management.[4]

The evolving technology landscape and the rapid adoption of innovative approaches have also significantly increased banks' reliance on third-party service providers for services they had previously not undertaken. In the light of these developments, the Basel Committee published a new set of Principles for the sound management of third-party risk in December 2025.[5] These principles aim to address the expanding and increasingly diverse third-party service provider landscape within the banking sector.

In advancing the work on ICT risk management, the Basel Committee, in collaboration with its members, conducted a survey to identify and document the range of ICT risk management practices across banks, with a particular focus on global systemically important banks (G-SIBs) and domestic systemically important banks (D-SIBs). The survey also sought to identify ICT practices that may be relevant for digital-only banks. Additionally, the survey gathered insights from 16 participating banking authorities on supervisory and regulatory practices relevant to the oversight of banks' ICT risk management practices. Selected case studies complemented the analysis and helped to provide practical insights and real-world examples to enrich the survey findings.

In addition, an industry outreach was conducted to gather insights on banks' practices and experiences, which helped to further enrich the report. The event invited representatives from various internationally active banks across Asia, Europe and North America, to explore challenges, share practices and discuss emerging trends in ICT risk management.

[2] See European Union Agency for Cybersecurity, *ENISA Threat landscape: Finance sector*, February 2025, UK's Financial Conduct Authority, *FCA's observations and lessons learnt from the July 2024 global IT incident*, November 2024, Speech by Anneli Tuominen, Member of Supervisory Board of the ECB, *Improving banks' resilience to hybrid threats*, November 2025, International Monetary Fund, Global Financial Stability Report, *Chapter 3: Cyber risk: a growing concern for macrofinancial stability*, April 2024.

[3] See BCBS, *Cyber resilience: range of practices*, December 2018.

[4] According to POR Principle 6, "Incidents are current or past disruptive events the occurrence of which would have an adverse effect on critical operations of the bank".

[5] See BCBS, *Principles for the sound management of third-party risk*, December 2025.

This range of practices report aims to identify, describe and compare observed bank ICT risk management practices and regulatory and supervisory approaches across jurisdictions that may contribute to enhancing banks' operational resilience to ICT incidents. The report encompasses both effective practices in managing non-malicious ICT risks and examples of inadequate practices that have resulted in non-malicious ICT incidents. It is intended to facilitate banks' review and evaluation of their ICT risk management practices based on their size, complexity and risk profile. Similarly, supervisory authorities can use these insights to inform their oversight approaches and regulatory frameworks. The practices documented may serve as reference points for banks and supervisory authorities to adapt and develop practices that are most appropriate for their specific circumstances.

The remainder of this report is divided into the following sections: Section 2 outlines the survey observations regarding causes of non-malicious ICT incidents, Section 3 discusses the survey observations regarding banks' ICT risk management practices and Section 4 provides an overview of regulatory and supervisory approaches to the oversight of banks' ICT risk management practices. Each section is complemented by insights gathered from an industry outreach event and information obtained through selected case studies. Section 5 concludes.

2. Causes of non-malicious ICT incidents

This section summarises the survey observations about non-malicious ICT incidents across 12 jurisdictions for the period 2022–24. The taxonomy under the FSB Format for Incident Reporting Exchange (FIRE) has provided a common framework for incident categorisation and reporting where applicable.[6] Such cross-sector collaboration and coordination efforts aim to reduce variation and enhance the comparability and utility of the aggregated data for identifying patterns and enabling meaningful comparison.

2.1 Observations on incidents in banks and their root causes

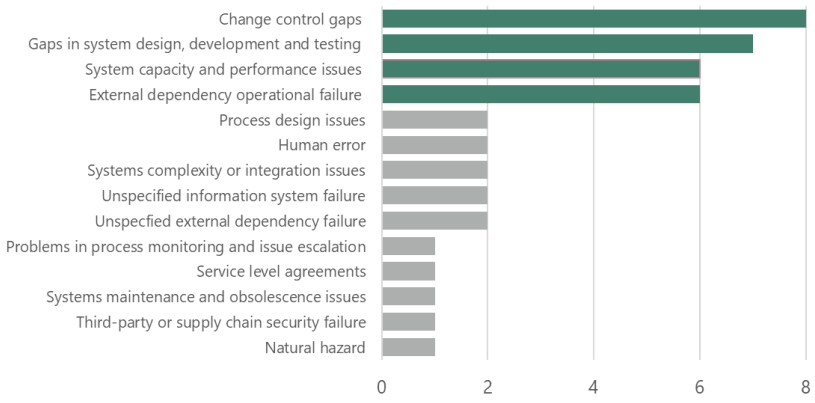
The analysis of ICT incident observations found that the number of non-malicious incidents at the jurisdictional level varied significantly. While some jurisdictions experienced an increase in incidents, others saw a decline, particularly between 2023 and 2024. While analysing the results, it was important to recognise that regulatory requirements for incident reporting varied across jurisdictions in terms of definitions, criteria and thresholds, with FIRE anticipated to enhance incident reporting practices in the future. These variations could affect both the type and number of incidents reported in this survey.

Non-malicious ICT incidents in banks have led to various impacts on their critical operations and customer services, with some cases proving to be particularly significant. For example, failure in system migration in one case caused a multi-channel service disruption affecting about 10% of population in one jurisdiction. In another jurisdiction, a similar incident rendered critical banking operations unavailable for several days.

The survey asked members to identify the most frequently observed root causes of non-malicious ICT incidents in their supervised banks, based on the taxonomy from the FSB FIRE. The results reflected four primary root causes: (i) change control gaps; (ii) gaps in system design, development and testing; (iii) system capacity and performance issues; and (iv) external dependency operational failure, where (iii) and (iv) are jointly ranked in third place (Graph 1).

[6] See Format for Incident Reporting Exchange (FIRE): Final report - Financial Stability Board.

Graph 1: Most frequently reported root causes associated with reported non-malicious ICT incidents



Source: Information and communication technology risk management survey.

Change control gaps refer to modifications to banks' ICT environment or its configurations without proper authorisation, review and rigor.[7] While survey data indicate that banks in most jurisdictions generally demonstrate a mature approach to ICT change management, ICT change control gaps still remain the most frequent root cause of ICT incidents, cited by eight jurisdictions. This finding is further corroborated by insights gathered through the industry outreach (Box 1). A possible explanation for this observation is that the increasing complexity of system architectures and interconnections have made change management more challenging. At the same time, inadequate change control systems can lead to issues that severely disrupt the continuity of banking services, particularly in customer-facing channels, with widespread impacts on them.

[7] Change control gap is defined as "changes made to information systems or their configuration by a process lacking appropriate authorization, review, and rigor" (FSB, Format for Incident Reporting Exchange (FIRE): Final report, 2025, p 64).

Box 1: Insight gained from industry outreach – challenges in ICT change management

The dynamic interplay between legacy systems, adoption of new and emerging technologies, and the rapid digitalisation of banking operations and services, compound the complexity of ICT change management in banks as they strive to keep their infrastructure up-to-date and fit for purpose. Panellists underscored that due to these intricacies, even minor missteps in the process of making changes can lead to significant ICT issues and outages, highlighting the critical need for rigorous processes.

Panellists commented that the increasing volume and complexity of changes reflect broader industry trends, with continuous improvement of ICT systems and infrastructure expected to remain a priority in banks. Panellists stated that many banks are managing an unprecedented volume of changes and this volume is poised to increase. One bank claimed to have implemented over 5 million changes in 2025, while significantly reducing its failure rate. The focus remains on minimising failures and building resilience supported by robust change management, incident management and problem management processes.

To manage the increasing volume of ICT changes, panellists emphasised the importance of prioritising changes based on criticality and risk. Automated processes for standard changes (eg pre-approved, low-risk changes) have proven effective, particularly for large, internationally active banks, with some institutions automating up to 85% of such changes. Critical changes require more stringent control gates, including multi-layered, risk-based governance, segregation of duties, mapping of end-to-end system dependencies, extensive pre-implementation testing, comprehensive system testing in a production-like environment, post-change validation and contingency plans. Lessons learned from past incidents are continuously integrated into processes to improve resilience. Finally, several panellists highlighted the importance of automation in managing the complex ICT environments within banks. However, they emphasised the need for appropriate safeguards to ensure its safe and efficient use.

Gaps in system design, development and testing processes are the second-most cited root cause, reported by seven jurisdictions. Issues such as poorly defined or inadequate ICT requirements, deviation from established ICT requirements during system development and implementation, and ineffective or irregular testing practices due to lack of an established testing process, can affect the quality, reliability and/or security of the software and give rise to ICT failures and service disruptions.

For example, as demonstrated in one of the case studies, a combination of factors (such as the lack of an appropriate testing environment for thorough validation, poor system design that introduced data mismatches, and development errors that went undetected during testing) led to failures in banks' critical systems. Remediation of such issues could be prolonged and complex, may sometimes require extensive manual intervention or third-party support and may result in extended service outages, delayed recovery and widespread disruption to banking services.

System capacity and performance issues, cited by six jurisdictions, highlight challenges in managing peak loads or operational demands, as well as the inability to complete tasks and processes within acceptable parameters (that are jurisdiction-specific).

Similarly, external dependency operational failure was also cited by six jurisdictions.[8] As illustrated in one of the case studies, the failure of a data centre provider's cooling system was triggered by unsupervised modifications to the cooling infrastructure where operators failed to follow proper change management procedures, resulting in critical temperature elevations that necessitated emergency system shutdown that affected a number of major banks whose systems were hosted in the data centre. This shows how an operational failure at a common third-party provider can cascade across multiple banks, and lead to service disruptions that extend beyond a single bank.

[8] External dependency operational failure is defined as "failure to meet expectations or contractual obligations for provision of services or goods, due to ineffective or failed internal processes, people, controls or systems", see Format for Incident Reporting Exchange (FIRE): Final report, page 65.

3. Banks' ICT risk management practices

This section highlights the ICT risk management practices observed across the surveyed jurisdictions.

3.1 Governance

Jurisdictions reported that most banks under their supervision have established a documented risk management framework that is reviewed at least annually. Updates are made as required, including when triggered by material events or regulatory changes. ICT oversight is typically integrated into the broader risk management structure, with periodic reporting to the board or a designated board-level committee. While some banks assign ICT oversight to a general risk committee, others establish dedicated technology risk committees. Board responsibilities often include approving policies and strategies and allocation of resources.

From the industry outreach, it was noted that some banks are leveraging automation and AI to enhance ICT risk management, although human oversight is involved where critical decisions need to be taken to ensure that they are made with the right context and judgment. The panellists expressed that a balanced approach that combines the strengths of automation and human expertise is considered key to manage the risks effectively.

Member jurisdictions reported that the integration of ICT risk management into bank-wide risk management frameworks is well established across supervised institutions. Across all surveyed jurisdictions, ICT risk is commonly categorised under operational risk, with regular reporting to senior management and the board/management body. In 14 of the 16 jurisdictions, banks had established an ICT risk appetite or tolerances based on their bank-wide frameworks and standards. In several of the surveyed jurisdictions, the banks commonly rely on the three lines of defence, as described in the BCBS Principles for the Sound Management of Operational Risk (PSMOR).[9]

According to the survey, most banks maintain a formal ICT strategy or multi-year plan, which is designed to anticipate both internal and external changes. Such plans usually include architecture review and/or change management roadmaps and milestones, and incorporate operational resilience requirements, such as availability targets and recovery objectives. These plans also embed the use of key performance indicators (KPIs) and key risk indicators (KRIs) to guide execution and monitoring of risks. The analysis of strengths, weaknesses, opportunities and threats (ie "SWOT" analysis) are commonly employed. Long-term strategies often account for the need to manage technological disruption, albeit with varying levels of detail.

The survey reflected that banks are using the following KPIs and/or KRIs to support ICT risk management:

- **System outages**: number of outages and average time to resolve incidents
- **System patching**: percentage of systems with up-to-date patches
- **System availability**: percentage of time a system is functional and accessible
- **Disaster recovery preparedness**: percentage of critical systems with disaster recovery planning
- **Change-related stability**: percentage of changes causing incidents
- **Obsolescence**: percentage of end-of-life or end-of-support assets
- **Third-party performance**: monitored through provider scorecards and SLA adherence.

[9] BCBS, Revisions to the Principles for the Sound Management of Operational Risk, 2021, paragraph 6.

As evidenced by the survey, banks frequently reference internationally recognised frameworks and industry standards, often in conjunction with regulatory requirements and supervisory guidance. The most cited frameworks include Control Objectives for Information & Related Technology (COBIT), National Institute of Standards and Technology (NIST) standards, International Organization for Standardization (ISO) standards such as the 2700x/22301 series on information security and business continuity management, and the Information Technology Infrastructure Library (ITIL) for IT service management. Additionally, banks increasingly refer to architectural guidance from cloud service providers and data centre certifications to enhance their ICT risk management practices.

3.2 Asset and inventory management

Based on the surveyed jurisdictions, asset and inventory management practices are widely implemented across banks but vary in depth and maturity. Most banks maintain registers of hardware and software assets, including criticality levels, and use configuration management tools to update their registers periodically.[10] Many institutions operate centralised platforms that integrate configuration management databases (CMDBs) with asset, change, incident and problem records.[11]

As evidenced by the survey, automated discovery tools are widely used across banks, though practices for reconciliation and ensuring completeness vary. Many banks maintain multiple inventories segmented by asset type or domain, which are often managed separately. Banks' management of shadow IT remains an area of focus for several jurisdictions, with banks employing ICT practices such as scanning, network discovery and centralised procurement controls to address this challenge.[12]

Survey findings indicate that hardware assets, software assets and their criticality levels are consistently tracked, while software versions and virtualised assets also are widely monitored. A challenge for banks reported by surveyed jurisdictions is the difficulty of achieving comprehensive dependency mapping from critical business services to the underlying ICT assets, particularly when third-party services are involved. Another observed challenge is banks' lack of visibility into supply chains which support critical services, such as nth-party suppliers, who often fall outside banks' direct oversight and monitoring.

The survey also highlighted the importance of obsolescence management within ICT asset management. Tracking third-party service provider support timelines is a standard practice for banks across most jurisdictions, where proactively replacing assets before the end of vendor support remains a key objective. When immediate replacement is not feasible, banks typically implement mitigation measures such as network isolation with strict access controls or transition plans approved by ICT risk committees to ensure risks are effectively managed during the transition.

3.3 Incident and problem management

Surveyed jurisdictions reported that banks under their supervision generally maintain documented incident and problem management frameworks that clearly define roles and responsibilities. These frameworks provide a structured approach to help banks manage incidents more effectively and prevent

[10] Configuration management tools are software applications that automate the provisioning, configuration and management of IT infrastructure to ensure consistency, reliability and security. They enable administrators to manage code versions, track changes and apply standardised settings across the networks, servers and applications.

[11] A CMDB is a centralised repository that stores information about IT infrastructure components (referred to as "configuration items") and their relationships. It acts as a "single source of truth" for hardware, software, documentation and personnel, enabling effective IT service management.

[12] Shadow IT refers to the IT assets (eg ICT systems, devices, software, applications and services used) maintained by business units which directly operate without management and oversight by the organisation's corporate IT/security function. These increase operational risk exposure to the bank as they are not subject to the official policies, standards, processes and controls.

recurring incidents. The incident management frameworks also integrate with business continuity plans (BCPs) and outline the incident classification and escalation protocols. These frameworks provide a structured approach to help banks manage incidents more effectively and lessen the re-occurrence of incidents.

To ensure prompt and effective incident response capabilities, the survey results reflect that banks typically invest in preparatory measures including comprehensive logging and audit trails. Early warning indicators are also generally present at banks in most surveyed jurisdictions. Surveyed jurisdictions also reported that banks increasingly are transitioning towards real-time and AI-enabled monitoring to facilitate proactive detection of anomalies before they lead to service degradation. Additionally, early warning and automated detection systems are increasingly being utilised to enhance monitoring and risk management.

As demonstrated in one case study, a bank encountered an incident where failure of heating, ventilation and air-conditioning (HVAC) components in the data center led to the disruption of banking services. Following the post-incident review, the bank implemented real-time monitoring by integrating with the data center's HVAC management system to enable prompt detection and timely response to HVAC issues, before they ultimately affect the bank's systems and services.

These advancements are being integrated into existing incident management processes, such as crisis "war rooms", incident monitoring dashboards and incident communication protocols. Member jurisdictions reported that containment and recovery practices are well supported by playbooks and structured communication plans designed for both customers and the media.

Based on the survey, post-incident reviews with tracked remediation actions are standard practices. In general, it was reported that banks maintain documentation and record-keeping across the entire incident management life cycle to ensure accountability and transparency. The survey also observed increasing integration of incident management, problem management and change management processes, which helps to improve the effectiveness of problem remediation and reduce the likelihood of incident recurrence.

Banks also scope the services provided by TPSPs in their ICT incident management frameworks and processes, though the level of integration of TPSPs into banks' incident management frameworks varied across banks. According to the survey, this is sometimes hindered by control and visibility limitations that banks have over the TPSPs.

3.4 Business continuity management and disaster recovery

ICT business continuity management programmes are widely implemented across banks in surveyed jurisdictions and typically involve multiple layers of testing. Routine activities include BCP tests, tabletop exercises and ICT disaster recovery testing at the system or component level. Additionally, banks in some of the surveyed jurisdictions participate in financial sector-wide exercises conducted through the banking authorities and/or industry associations.

In several of the surveyed jurisdictions, business continuity and disaster recovery testing is often risk-based and focused on critical ICT systems. Examples of scenarios covered in the testing include network and telecommunications failures, power outages, data recovery issues and personnel unavailability. Some banks were observed to carry out more extensive disaster recovery testing, where an alternative site is activated to process the full production workload over a period of one week or longer.

Several case studies demonstrated how banks had experienced delayed or extended recovery beyond their recovery time objectives when they were unable to effectively activate their business continuity or disaster recovery procedures during incidents. Examples of such cases included: (i) failure of planned rollback procedures following unsuccessful system migration, leading to prolonged system

outage; and (ii) when DNS fallback mechanisms designed to reroute traffic did not function as intended. Additionally, delays in service recovery could also be caused by configuration gaps that affect the backup connections to the secondary data centres, and procedural deficiencies due to failure scenarios that are not covered in the documented recovery procedures.

To enhance disaster recovery capabilities and minimise service recovery delays, the affected banks implemented several measures based on lessons learned from these incidents. Based on the facts presented in the case studies, these include:

- Enhancing IT disaster recovery plans across a range of plausible disruption scenarios, such as power outages, equipment failures and network disruptions that can leave systems in corrupted states requiring special recovery steps, given that system disruptions tend to occur abruptly.
- Setting up critical systems in high-availability configuration with redundant servers in an "active-active" or "active-passive" architecture.[13]
- Establishing backup connections between secondary data centres and critical TPSPs with extended testing of failover capabilities.
- Automating recovery procedures to accelerate system restoration during IT disruptions. Such automated recovery procedures also help to reduce human errors and improve execution consistency.

Beyond routine exercises that usually take place over a weekend, some banks conduct extended operations from disaster recovery sites and use unscripted scenarios (eg unexpected network or power failures at the disaster recovery site, data recovery issues and personnel unavailability) to test operational continuity under varied conditions.

3.5 Change management

Change management processes are formalised across most surveyed jurisdictions. These processes typically include key components, such as predefined approvals, risk assessments, documented rollback plans, post-implementation reviews, structured change windows and deployment schedules. Automated workflow tools are commonly employed to enhance traceability and streamline the process. Rollback testing is widely implemented, with 13 out of 15 jurisdictions reporting that banks require documented rollback plans and testing for all changes, or at least for higher-risk changes.

The survey highlighted that banks are increasingly adopting progressive delivery techniques to minimise customer impact during change deployment (see Box 2). In addition, surveyed jurisdictions report that some banks leverage strategic change scheduling and planning to minimise disruptions. This includes allowing sufficient preparation time, reducing the risk of conflicting schedules and ensuring coordinated execution. According to the survey, the automation of standard, low-risk changes to improve consistency and reduce human error is expanding significantly. Some banks in surveyed jurisdictions report high levels of automation for pre-approved, low-risk changes, combined with multi-layer control gates, segregation of duties, dependency mapping and production-like testing.

The industry outreach highlighted different approaches to address flawed change implementations. One approach is rolling forward to maintain operations with subsequent fixes for cases where rollback to the previous state is not technically feasible after a flawed change implementation.

[13] In an active-active setup, all servers operate simultaneously, sharing the workload and providing immediate failover in case of a server failure. In contrast, an active-passive configuration designates one server as active while the other remains on standby, ready to take over if the active server encounters an issue.

Another approach is to proceed without rollback and continue to operate with the flaw with management-approved risk acceptance and enhanced monitoring while proper remediation is being developed.

All surveyed jurisdictions report that banks maintain defined processes for emergency changes or releases affecting ICT systems that support critical operations. These processes are documented within broader ICT risk management policies and include approval protocols. Banks in surveyed jurisdictions track the frequency and rationale for emergency changes, maintaining oversight of this high-risk, expedited process. Post-implementation reviews are conducted to confirm that changes, both planned and emergency, achieve their objectives. These reviews address any deviations or issues promptly and help to enhance the processes governing the change implementation life cycle.

While many banks across surveyed jurisdictions test both functional (eg business logic) and non-functional (eg performance and load) requirements eg, availability, response time, maintaining testing environments that mirror production environments remains a challenge. Testing in environments that closely mirror production is often constrained by differences between the test and production environments, which may be due to: (i) test data sets; handling (eg, anonymisation or masking), (ii) integration with external systems; (iii) configurations; and (iv) security controls. These residual differences between test and production environments may sometimes reduce the effectiveness of testing and could contribute to non-malicious incidents in the production environment.

Box 2: Insight gained from industry outreach – change management and governance

Progressive delivery releases, such as phased rollouts through 'canary releases', 'shadow traffic testing', and actively managing the 'blast radius' are also helping to control and minimise customer impact. Other examples of change deployment strategies include 'blue-green deployments' and implementation of 'feature flags' to roll out changes to a subset of users and observe the results before transitioning to full deployment of the change, as well as adopting the approach of micro- changes, i.e., more smaller changes than instead of a single big bang. Beyond deployment techniques, panellists emphasised the importance of strategic change scheduling and planning to minimise potential impact, allow sufficient preparation time and lower the chance of conflicting schedules.

The represented institutions mandate rollback and contingency plans for all significant changes. When rollbacks are not feasible, panellists at the outreach event reported that a 'roll-forward' approach is adopted. Comprehensive contingency plans, which include clearly defined roles and responsibilities, clear trigger conditions for rollback decisions, communication protocols with stakeholders, and fallback mechanisms, are critical to managing complex changes.

Notes on definition of terms:

- Canary releases: a software deployment strategy that rolls out a new feature or version to a small, controlled group of users first, acting like a "canary in a coal mine," to test it in a live environment before a full release, minimizing risk and catching bugs early.
- Shadow traffic testing: risk-reduction technique where a new software version runs in parallel with the live version, receiving a copy of real production traffic (like a "shadow") to test its performance and behaviour without impacting actual users.
- Blast radius management: if a faulty software update is deployed, these risk-management techniques, including as canary deployments, segmentation, and automated rollback, can limit the impact to a small subset of users or systems, preventing widespread disruption.
- Blue-green deployments: software release strategy used in change management that aims to minimise downtime and risk by running two identical production environments in parallel. Feature flags: a software development technique where developers use conditional statements in their code to selectively enable or disable functionality at runtime, without deploying new code.

3.6 Capacity management

In most surveyed jurisdictions, banks align their capacity planning with their operational resilience objectives. According to the survey, ICT capacity management practices at banks focus on monitoring and ensuring readiness for demand spikes. Automated monitoring with real-time alerts is commonly adopted, particularly at the infrastructure layer (eg CPU, memory and storage), and increasingly at the service level (eg number of concurrent users). Insights from the survey suggest that banks often conduct manual reviews before major releases and have in place playbooks to handle peak loads during known critical periods with high demand, such as during end-of-year processing or major market events. Panellists at the industry outreach event recognised the value of measures (such as capacity monitoring, workload management and rate limiting) that can be implemented to track and manage capacity and resource utilisation.

The survey indicates that some banks implement more advanced capabilities that are not commonly observed across surveyed jurisdictions, such as predictive analytics or AI/ML-based forecasting, dynamic scaling across hybrid cloud architectures (ie those combining multiple cloud environments), scenario-based reviews and business-aligned service level objectives (SLOs) with adaptive thresholds. Furthermore, while some banks are exploring the use of AI/ML for predictive detection of failure patterns, panellists at the industry outreach stated human oversight remains critical to interpret these signals and prioritise mitigation actions effectively.

3.7 Software development and project management

Project management and software development life cycle (SDLC) controls are well established across banks in the surveyed jurisdictions. Key practices include: (i) requirement analysis; (ii) dependency mapping; (iii) system testing and quality assurance; (iv) change integration; and (v) post-implementation reviews.

Findings from the survey show that risk controls are applied consistently, regardless of the development methodology. Common measures include checkpoints (ie control gates) to ensure quality and compliance, incorporating security and resilience into requirements and design artefacts and enforcing secure coding standards, supported by periodic source code reviews and automated scanning tools.

The use of open source software is common, with banks adopting specific risk management practices to mitigate associated risks. Common measures to address such risks include:

- **Maintaining inventories** of open source components
- **Using software composition analysis** and other tools to assess software defects, among others
- **Conducting periodic configuration reviews and thorough testing**, including system and integration testing, and user verification testing
- **Managing license risks** through policies and repository whitelisting.

The insights from the survey indicate that some banks may prefer the use of open source software applications due to their transparency and explainability by comparison with proprietary vendor software. Where permitted by regulation or banks' internal policies, the use of open source components in supporting critical systems services/operations might require controls, such as source code review and validation (ie perform a detailed review of the open source code to identify software defects, or checks of vendor or community trustworthiness (ie assess the reputation and activity level of the open source project's maintainers or community). Panellists at the outreach event emphasised the need for banks to maintain strong governance to manage risks associated with the use of open source software code, especially if they are used in critical services/operations.

Box 3: Insight gained from industry outreach – novel approaches and use of AI and open source technologies

At the industry outreach, participating institutions noted that existing open source technologies are gaining traction as a means to reduce dependency on proprietary third-party solutions, but also come with potential risks. In general, open source software can provide greater transparency than proprietary software, provided banks have processes for code review and remediation of software defects, among others. Newer technologies such as automated rollback mechanisms and active recovery strategies are also being explored to minimise system disruptions. Panellists stressed the importance of balancing innovation with risk management to ensure resilience. Business process workarounds complementing technical measures and contingencies should also be considered as a means to build resilience and minimise customer impact in the event that ICT systems are disrupted.

Based on the industry outreach, AI/ML solutions are playing an increasingly important role in ICT risk management. These tools are being embedded by the represented institutions into risk management practices to proactively identify issues, predict potential failures and improve response times. For example, AI tools are used to scan for changes likely to cause disruptions, enabling proactive mitigation. Specific applications noted by the represented institutions include: (i) enhancing software development productivity through tools such as AI-powered coding assistants; (ii) detecting software defects with increased coverage; (iii) improving test coverage by identifying blind spots in testing; (iv) enhancing observability across production environments; and (v) seeking to develop predictive capabilities for potential change failures. AI-driven tools can provide real-time insights to support better decision-making. While AI has promising results in automation, panellists emphasised the need for human oversight to ensure accountability.

3.8 ICT risk awareness, skills & training

Training and awareness programmes are widely implemented across banks in the surveyed jurisdictions, reflecting a shift in perspective, where resilience is seen as an outcome of integrated practices and organisational culture rather than a compliance requirement. Clear accountability across technology, business and control functions is regarded as essential for reducing non-malicious ICT incidents.

Across surveyed jurisdictions, banks typically provide annual risk awareness training for all employees in areas such as information security, business continuity and disaster recovery, with completion rates monitored at the organisational level. More advanced programmes include:

- **Role-specific training**: tailored for roles (eg software developers, system administrators, ICT risk managers) to equip staff with the necessary technical skills that are specific to their roles and responsibilities.
- **Targeted content**: focusing on employees' roles in ICT continuity and disaster recovery plans and addressing risks from non-malicious incidents (eg accidental data loss or physical infrastructure failures) and focusing on broader governance topics (eg data protection, data privacy and ICT risk awareness).
- **Senior management briefings**: focused on emerging risks and technology trends (eg, artificial intelligence quantum computing and), catering to topical requests from senior management.

Talent shortages are a recurring challenge for banks across many surveyed jurisdictions. Commonly reported skills gaps include expertise in cyber security, cloud engineering, data management and generative AI, as well as legacy skillsets (eg COBOL programming and mainframe administration). These shortages are exacerbated by competition with big tech and fintech firms, long recruitment cycles and region-specific challenges. To address these challenges, banks are adopting strategies, such as external hiring (eg targeting specialised talent) or selective outsourcing (eg engaging managed services for hard-to-fill roles).

Box 4: Insight gained from industry outreach – technology talent

The industry outreach revealed that the global shortage of technology talent presents a significant challenge for banks. Institutions are competing with "BigTech" firms for skilled professionals in ICT risk management. To attract and retain talent, participating banks are implementing initiatives such as partnerships with universities, reskilling programs, and internal technical career tracks that offer clear development opportunities. Leadership plays a critical role in fostering a positive culture and managing generational expectations. Managing generational expectations promotes a unified, engaged, and adaptable workforce, while investing in technology talent ensures the organisation has the expertise needed to navigate digital transformation and technological challenges.

3.9 ICT risk management tools and technology solutions

In the surveyed jurisdictions, banks are gradually moving from isolated point solutions to more integrated platforms for managing operations. While many institutions still rely on separate tools for inventory, change and incident management (and require manual reconciliations), more advanced practices include service management suites built upon a centralised configuration management database (CMDB) or AI-assisted tools (e.g. those that support root cause analysis and predictive incident detection). From the industry outreach, it was noted that some banks are integrating data analytics and AI/ML solutions that provide predictive insights to help them to identify potential issues related to changes and detect blind spots in testing.

Technologies enhancing operational resilience are also evolving, with banks adopting solutions, such as:

- **High-availability architectures**: active-active and active-passive configurations.
- **Clustering and virtualisation**: these technologies enable the implementation of system redundancy to achieve high availability and operational resilience in the event of components failures or disruptions. For instance, clustering combines multiple physical servers to act as a single, highly available and high-performance system. Virtualisation is the technology of creating virtual representations of physical resources (servers, storage, networks) to run multiple systems on one physical machine.
- **Data availability measures**: including scheduled backups, periodic restore tests and, increasingly, immutable backups or secure vaults to protect against data corruption.
- **Cloud-native architectures**: digital-only institutions often cite scalable designs and alternative backup channels as key enablers of faster recovery and continuity of critical services.

Box 5: Insight gained from industry outreach – managing technological complexity

Bank panellists reported that banks face the dual challenge of maintaining legacy systems while adopting modern technologies. Legacy systems often lack flexibility, making changes more complex and time-consuming. To address this, the represented institutions at the outreach event are breaking down monolithic systems into more modular components implemented based on layered approaches to decouple and reduce those complexities, so that the individual components can be more easily replaced and upgraded without affecting the rest of the system. Panellists noted it is also important to simplify and streamline business processes where possible and align them with ICT strategies.

3.10 Third-party risk management

Banks in the surveyed jurisdictions manage risks associated with third-party dependencies through a combination of:

- existing governance structure to support effective oversight on the risk management of third-party risks over the course of the third-party arrangement. This includes risk-based due diligence programmes, regular audits such as pooled audits for shared service providers, and ongoing monitoring frameworks with defined metrics for continuous assessment of third-party performance and compliance;
- contractual provisions, such as right to audit clauses to enable regulators and banks' audit of the service providers, notification clauses to ensure prompt reporting of ICT incidents and service disruptions by service providers to banks, terms to support banks' third-party risk management data portability and step-in rights;[14]
- tailored exit strategies and contingency planning, such as identification of alternative service providers, and preparation for scenarios such as termination or failure of service providers;
- visibility into nth party relationships, where possible, to identify and monitor dependencies beyond direct third-party service providers to understand potential concentration risks and cascading failure points in the supply chain;
- on-premises retention of critical applications by some banks to reduce reliance on external providers to ensure continuity of critical operations during third-party disruptions; and
- compliance with data localisation requirements, where applicable. This ensures critical financial records remain within local borders, preventing foreign legal or geopolitical issues from impeding a bank's access to its data.

In some jurisdictions, regulatory requirements play a significant role in supporting banks in their contract discussions with TPSPs, particularly in securing key contractual clauses.

Some banks are carefully weighing the benefits and trade-offs of TPSP diversification against the operational simplicity of managing fewer TPSP relationships. Exit strategies and ongoing evaluation of TPSP resilience are widely regarded as essential components of third-party risk management for critical TPSPs.

The approach to third-party TPSP due diligence and monitoring varies across jurisdictions and institutions, ranging from: (i) regulatory-driven frameworks (eg prescribing risk assessments and audit rights); (ii) risk-based approaches (eg combining qualitative and quantitative assessment); and (iii) on-site

[14] It is generally understood that step-in rights are contractual rights that allow a client to temporarily take control of, or appoint another party to take over, a supplier's services when the supplier fails to meet its obligations, in order to ensure continuity of the service.

reviews. Some jurisdictions also highlight the use of pooled audits to enhance the effectiveness and efficiency of assessing the adequacy of controls in common service providers, which are explicitly provided for in certain regulatory frameworks or through industry-driven initiatives.[15]

4. Regulatory and supervisory practices

This section summarises the observed range of practices of the surveyed jurisdictions regarding regulations and guidance related to ICT risk management, as well as the approaches used to supervise banks' ICT risk management.

4.1 Regulations and guidance

All surveyed jurisdictions reported they have ICT risk management regulations and/or guidance in place. Regulation and guidance in the areas related to operational risk management-, operational resilience-and ICT risk management are often considered together when assessing banks.

In most surveyed jurisdictions, regulatory requirements are applied in a risk-based and proportionate manner based on the size and complexity of the supervised institutions. Internationally recognised standards and frameworks (eg COBIT, NIST standards, ISO 2700 series and BCBS PSMOR and Principles for operational resilience) often inform a jurisdiction's ICT risk management regulation and guidance, while not being mandatory.

In many surveyed jurisdictions, other government agencies (eg Ministry of Finance, Information and Communications Ministry) may publish national-level ICT risk management guidance for critical infrastructure that could also be applicable to G-SIBs or D-SIBs. For the financial sector, the primary authority for issuing sector-specific ICT risk management regulations and guidance, as well as conducting supervisory oversight, lies with financial regulators and central banks.

All surveyed jurisdictions have regulations or guidance that address ICT system development, testing, training, communication and maintenance of business continuity and disaster recovery plans (BCP/DRP), including BCP/DRP tests (eg full-scale tabletop exercises and simulations with scenarios considering ICT systems availability during network and utilities outages, and scenarios considering TPSP unavailability).

There is comprehensive guidance or regulation across all respondents related to the availability and continuity of ICT systems, data and related processes. Surveyed jurisdictions typically set expectations regarding business impact analysis, BCP/DRP, recovery time objectives, recovery point objectives, maximum allowable downtimes and data backups.

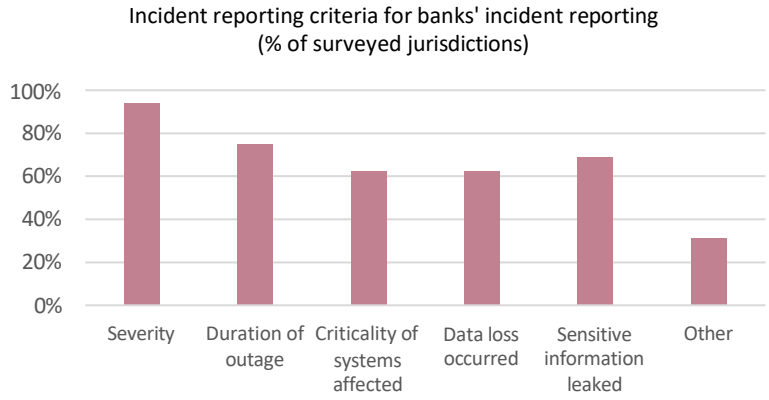
Some surveyed jurisdictions have expectations with respect to availability of data through on-/off-site backups, including regulatory-mandated backups and leveraging hybrid cloud models for storage and backup of critical data. Generally, the frequency of backups is expected to be risk-based, although specific frequencies are required in some jurisdictions. Notably, a majority of the surveyed jurisdictions have guidance or regulation regarding immutable data backups. Many of the surveyed jurisdictions do not have explicit expectations for banks to maintain: (i) on-premise backup of critical data that are primarily stored in the cloud; or (ii) secure off-site storage of backup media.

All surveyed jurisdictions have requirements for reporting of ICT incidents by supervised banks. Surveyed jurisdictions apply varied criteria and thresholds to focus banks' reporting on the incidents'

[15] See BCBS, *Principles for the sound management of third-party risk*, December 2025.

impact, from either a bank or sector perspective. The most common criteria are duration of outage, criticality of systems affected, data loss occurred and sensitivity of information leaked, as shown in Graph 2. Additional criteria, such as geographical spread and reputational impact, are also considered in some surveyed jurisdictions.

Graph 2: Incident reporting criteria for banks (% of surveyed jurisdictions)



Source: Information and communication technology risk management survey.

Most surveyed jurisdictions require initial, interim and final reports for incidents. However, reporting criteria and timelines vary significantly. In one surveyed jurisdiction, immediate notification is required, while in another, supervised entities are required to submit a comprehensive report within five days from the initial incident notification. In most surveyed jurisdictions, no distinction is made in the requirements for initial reports based on whether the incident is malicious or non-malicious, as the nature of the incident may not always be clear during its early stages.

Box 6: Insight gained from industry outreach – regulatory frameworks

Participants noted challenges in some jurisdictions between the growing use of automation (including AI) and supervisory expectations for human oversight. Managing TPSPs is further complicated when providers fall outside financial sector regulation or operate under disparate frameworks. Participants welcomed initiatives such as the EU DORA regime, which strengthens direct oversight of critical TPSPs, and suggested requirements for TPSPs to disclose software bills of materials (SBOMs) to improve vulnerability management. Panellists expressed that while regulation cannot eliminate all challenges, it plays a central role in setting minimum expectations for critical TPSPs.

4.2 Supervisory practices

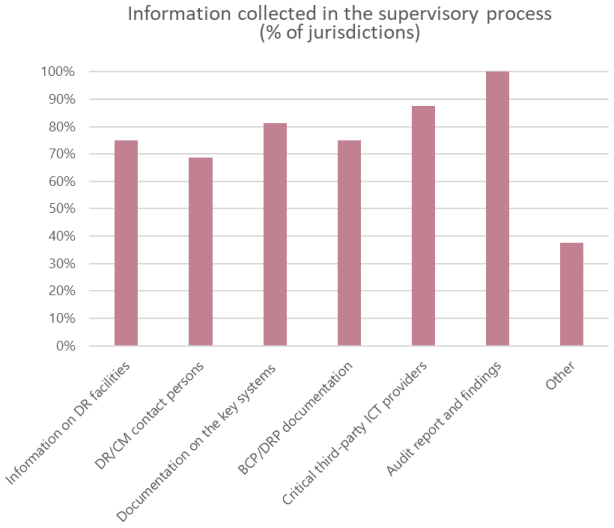
Most surveyed jurisdictions have adopted a risk-based, tailored approach to ICT risk management supervision, employing a variety of procedures and activities. This aligns with their broader regulatory approaches. On-site inspections or examinations are frequently cited as an effective supervisory activity, which involve the supervisors going into banks to review bank policies and procedures, verify supporting documentation and perform control testing over sampled evidence. Other methods include ongoing monitoring, horizontal reviews and the use of questionnaires.

Several surveyed jurisdictions regularly collect information related to ICT risk management from the supervised banks irrespective of the supervisory cycle. The most frequently collected documents include audit reports, information on critical TPSPs and documentation of key systems (Graph 3). Some surveyed jurisdictions collect further data, for example entity-specific documentation in line with

supervisory priorities, risk assessment forms, scheduled outages to retail services and board and risk committee documents.

To support the supervision of banks' ICT risk management posture practices, most of the surveyed jurisdictions rely on custom tools and information sources. The deployment of supervisory platforms that cover supervisory processes end to end, integrating all available information and providing support for the different ICT risk management supervision activities, is relatively rare.

Graph 3: Information collected by banking authorities in the supervisory process



Source: Information and communication technology risk management survey.

4.3 Additional activities

The surveyed jurisdictions engage in a wide range of activities beyond the regulation and supervision of ICT risk management. These activities include media monitoring, promoting information-sharing and collaboration with other supervisory authorities, including exercises and crisis simulations. Half of respondents use incident reporting data to publish aggregated reports for the benefit of the industry. Other reported activities include issuing letters, speeches, ad hoc bulletins, advisories, collaborating with bankers' associations and engaging with public-private action groups.

5. Conclusion

This report provides an overview of the diverse range of practices in banks' ICT risk management. Drawing on a survey of a subset of Basel Committee member jurisdictions, it includes an analysis of the root causes of non-malicious ICT incidents, offering insights into common weaknesses and patterns across surveyed jurisdictions. It also examines the risk management practices adopted by banks to mitigate these risks, including governance frameworks, continuity planning, incident management and third-party risk management. The report also explores supervisory and regulatory approaches implemented by participating authorities, highlighting a broad range of approaches. Based on the sample size, this report encompasses a variety of practices observed across the surveyed jurisdictions and should not be interpreted as fully representative of all banks or supervisory authorities within Basel Committee member jurisdictions.

Based on the survey, the most frequently reported causes of non-malicious ICT incidents include: (i) change control gaps; (ii) gaps in system design, development and testing; (iii) system capacity and performance issues; and (iv) external dependency operational failure. Banks employ various ICT risk management practices to mitigate these risks, with third-party risk management being a key focus through enhanced governance, monitoring tools and exit strategies.

At the industry outreach, panellists highlighted the adoption of novel ICT change management processes, including automation, progressive software deployment and contingency planning to minimise risks during system updates or modifications. Banks are also expanding continuity testing to cover broader scenarios, such as power outages, network failures and natural disasters. Efforts to manage third-party concentration risks and improve incident management practices, supported by advanced tools and post-incident reviews, were also noted.

The report highlights primary sources of reported risks and root causes associated with banks' non-malicious ICT incidents. These incidents can be severely disruptive, affecting the continuity of critical operations, negatively affecting customers and disrupting banking sector stability. The interconnected nature of financial services can amplify the impact of such incidents, if disruptions in one institution or system swiftly cascade across the broader financial ecosystem.[16] Limited visibility into the resilience of TPSPs and their supply chains remains a challenge that banks are grappling with. The complexity of ICT environments, driven by legacy systems, digitalisation and emerging technologies like AI and ML, adds further challenges. Banks use testing environments to test and verify updates before deploying to the production systems, but it is noted that these testing environments are often not identical to production environments, which could affect the effectiveness of the testing. A shortage of skilled ICT professionals, especially in areas like cyber security and cloud engineering, is exacerbated by competition from technology firms. Additionally, over-reliance on automation without human oversight, while improving efficiency, can introduce additional risk in complex scenarios.

The survey highlighted that regulatory and supervisory approaches with respect to banks' information and communication technology risk management vary across the surveyed jurisdictions. However, such approaches are generally mature, with risk-based principles addressing areas such as incident reporting, business continuity planning and third-party risk oversight.

By shedding light on ICT incident root causes and related risk management practices, this report aims to support banks' development of robust ICT risk management frameworks and promote greater operational resilience in the financial sector.

[16] See BCBS, *Cyber resilience: range of practices*, December 2018.