



EUROPEAN CENTRAL BANK

BANKING SUPERVISION

IT and cybersecurity risks – key observations in 2024



Background

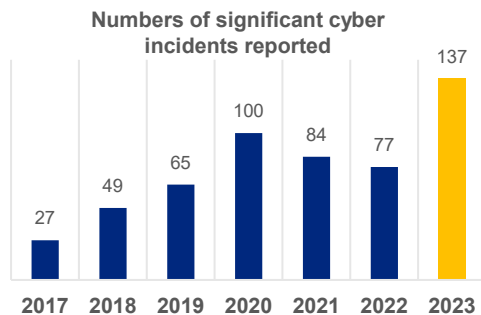
Deficiencies in **cyber resilience** and **IT outsourcing** continue to be a **key vulnerability** and will be addressed by ECB Banking Supervision as a priority in the period 2024-26. Continuous improvements to cybersecurity controls, effective management of IT outsourcing and change risks, robust incident management and business continuity plans, and strong IT governance are all essential in order to safeguard the integrity and stability of the banking sector in 2024 and beyond.

The following slides provide an overview of the key observations from the annual horizontal analysis of IT and cybersecurity risks, which is based on data from the IT Risk Questionnaire as well as findings from on-site inspections in 2023.

Key observations in 2024 – IT security



Need for supervisory attention



1

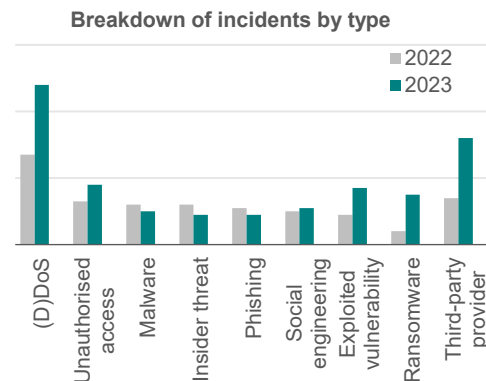
Numbers of **cyberattacks** and **significant cyber incidents** have increased considerably, with **ransomware attacks** on **service providers** soaring.¹ However, none of those incidents have yet resulted in a critical impact. This can be explained by observed cyber incidents representing the body of the distribution, with tail events probably not being observed owing to the small sample size.

On-site inspections and the **targeted review of cyber resilience** have consistently revealed **shortcomings** in the following risk control areas:

- **IT security risk assessment** policies and processes (e.g. second line of defence not challenging first line of defence);
- **security testing frameworks and vulnerability management** (e.g. incomplete vulnerability scanning);
- **security detection capabilities**, owing to limitations in configuration and management of SIEM² tools – including **audit logs** not being collected or fed to the SIEM tool;
- **network segmentation**, data leakage prevention (**DLP**), protection against **DDoS** attacks and **firewall implementation**;
- **identity and access management (IAM) tools and processes**.

IAM, **patch management**, **network segmentation** and **DLP** were also self-identified by banks as the least compliant areas in terms of IT security risk controls.

2



¹ Distributed denial-of-service (DDoS) attacks remain the most common type of incident, however.

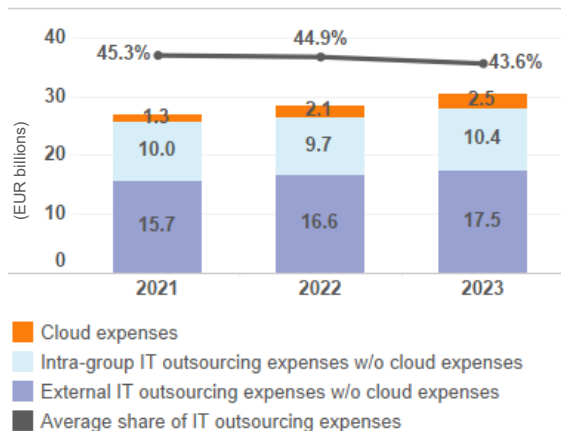
² Security information and event management

Key observations in 2024 – IT outsourcing



Need for supervisory attention

Overview of IT outsourcing expenses



3

IT outsourcing expenses increased by about 7% in 2023, exceeding the general level of inflation, which indicates that the banking industry's reliance on third-party service providers has increased further. **Cloud expenses rose by 21%** – a smaller increase than the year before – and accounted for 8.2% of total IT outsourcing expenses.

Despite that **growing dependence** on the conduct and resilience of service providers, some banks still reported weaknesses in relevant risk controls: 8% of institutions reported that they lacked a **comprehensive framework for outsourcing risk**; 21% showed weaknesses regarding the design and implementation of **contingency and exit plans**; and 12% reported shortcomings in the **monitoring processes** used to ensure compliance with service level agreements (SLAs) and **proper management of cybersecurity risk**.

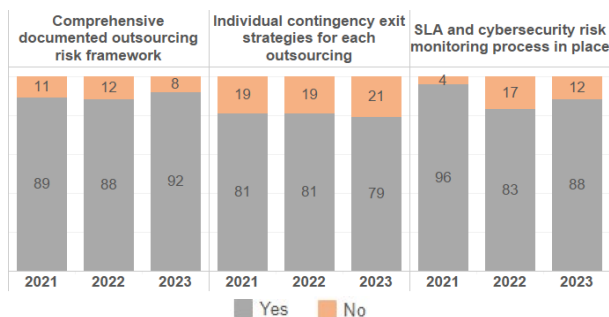
4

5

On-site inspections consistently identified weaknesses in banks' **oversight frameworks**, with deficiencies observed in areas such as **pre-outsourcing analysis, mitigation of identified risks**, the development and regular testing of **exit strategies**, and **data quality in outsourcing registers**.³

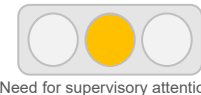
6

In some cases, the involvement of third-party service providers in the **response to cyber incidents** is not properly documented or challenged, while the **recovery capabilities** of outsourced services are not always aligned with banks' **recovery objectives**.

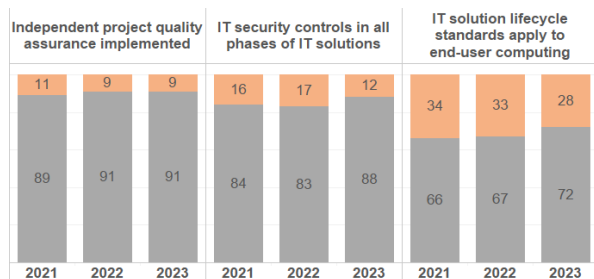
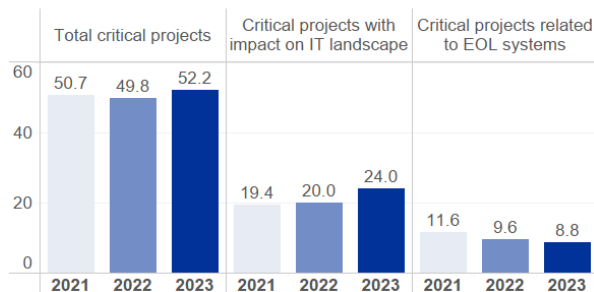


³ The forthcoming DORA regulation will introduce changes to the outsourcing templates under the EBA guidelines, requiring new practices and further emphasising the need for robust outsourcing registers.

Key observations in 2024 – IT changes



Average numbers of critical projects per bank*



■ Yes ■ No

* Excluding relevant outliers.

7

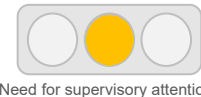
While the impact of IT change risks remained limited in 2023, the ever-increasing **number of critical projects** and the fact that IT changes are still **by far the most important reason for downtime** mean that **further supervisory attention** is warranted.

Although individual controls were reported as being lacking in some cases, almost all banks reported that **key risk controls** around change and release management were **generally implemented**.

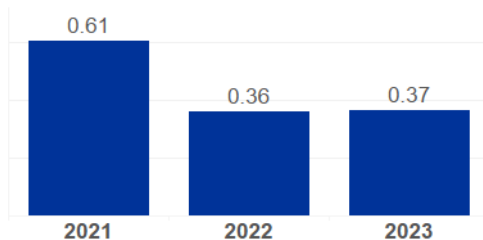
8

However, **on-site inspections** identified specific weaknesses in **change management processes**, including **inadequate documentation, testing and approval** of the relevant changes prior to deployment. The **comprehensiveness** and **effectiveness** of these controls should therefore be assessed in more depth.

Key observations in 2024 – IT availability and continuity



Median unplanned downtime per critical IT system (hours)



9

Banks report that the **unplanned downtime of critical IT systems** has **stabilised** since 2022. Losses due to disruption totalled €72 million in 2023, returning to their longer-term trend after a peak in 2022.

On-site inspections and the targeted review of cyber resilience identified numerous issues in the area of **business continuity management**, such as:

10

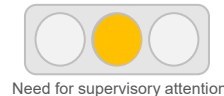
- outdated or **incomplete business continuity plans** that did not adequately consider extreme but plausible scenarios (e.g. severe cyber incidents);
- **insufficient recovery tests** (including, in some cases, a complete absence of such tests);
- weaknesses around the definition, consistency and testing of **recovery objectives**;
- a lack of **recovery priorities** based on proper risk assessment.

11

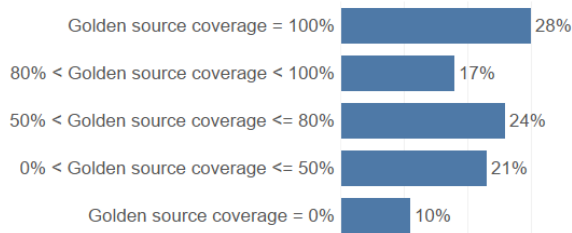
Deficiencies were also identified in the areas of **incident and problem management** and **crisis communication**, with weaknesses including the following:

- lack of **formal incident frameworks**, unclear procedures, absence of formalised resolution times and insufficient policies for data back-up and recovery;
- lack of documented **crisis communication strategies** and absence of **proactive communication**/predefined messages.

Key observations in 2024 – data quality management

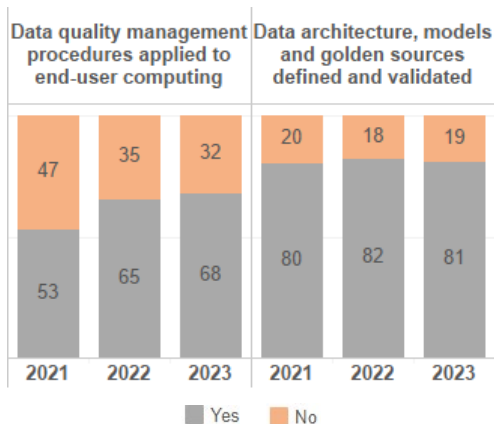


Percentage of critical functions for which golden sources of data are defined



12

Only 28% of banks report that **all data used by critical functions are derived from golden sources**, while 10% do not derive any of their critical data from golden sources. **Losses due to data-related incidents rose** to €38.6 million in 2023 (up from €16.4 million in 2022), driven by a few banks reporting increased losses.

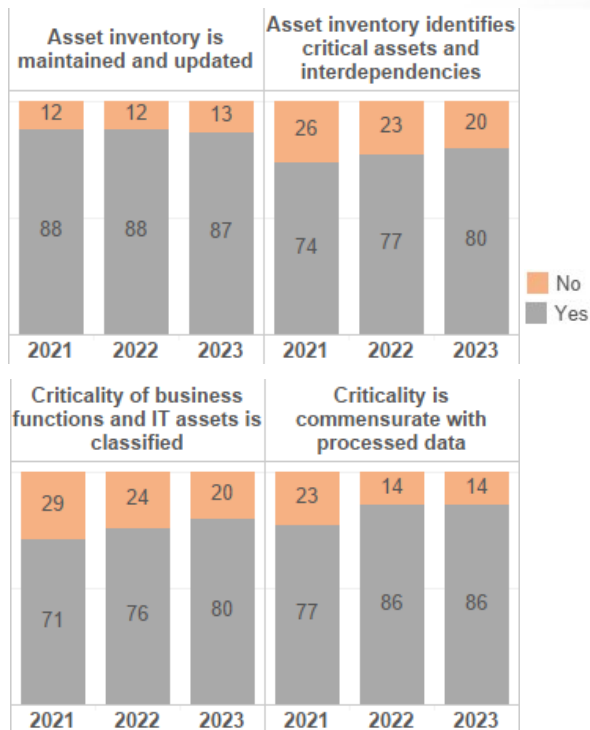


13

Data quality management remains the area with the **least mature risk controls** according to banks' self-assessments, with limited progress made in 2023 relative to the previous year. **Some key controls are still not fully implemented in many banks:**

- 19% of significant institutions have not implemented a data architecture model.
- 32% of significant institutions do not apply data quality management principles to end-user computing (EUC).

Key observations in 2024 – IT governance, risk management and audits



14

Some banks still report gaps in **IT asset management**, which is considered **fundamental for proper management of IT risk**. Several banks have not yet implemented basic **IT risk identification measures**. Few affected banks have resolved these weaknesses over the last three years, **indicating a lack of remedial action**. **On-site inspections** identified inconsistencies in the use of IT asset management tools, leading to the **fragmentation of IT asset management processes**.

15

In some cases, **on-site inspections** in 2023 indicated that **IT strategy**-related key performance indicators were **not sufficiently monitored or reviewed**. Additionally, **IT risk indicators** were **insufficiently reported** to management bodies (MBs) or **not reported regularly**, owing to a lack of criteria and escalation processes.

16

IT expertise⁴ at board level is still lacking in several cases, with 8% of institutions reporting that they have no **non-executive MB members** with IT expertise. Additionally, it is good practice to have an executive MB member with IT knowledge; alternatively, such knowledge can reside with a senior manager one level below.

⁴ IT expertise includes both education/certification and relevant professional experience (i.e. positions held).

Way forward

The results of the horizontal analysis **confirm that cyber resilience and IT outsourcing** should be considered **focus areas** for ECB Banking Supervision.

Joint Supervisory Teams will follow up with individual significant institutions on the key observations and weaknesses identified.