



EUROPEAN CENTRAL BANK  
BANKING SUPERVISION

# IT and cyber risk – key observations



# Background

Deficiencies in **IT outsourcing and cyber resilience** have been identified as a **key vulnerability** to be addressed by ECB Banking Supervision as a priority in the 2023-25 period. IT security is still a concern for supervisors and significant institutions alike. This concern is exacerbated by **findings from several on-site inspections** on cyber security over the last few years, which showed weaknesses in IT asset management, deficiencies in asset protection, limited incident detection capabilities, and limited cyber incident response and recovery preparedness.

Significant institutions are asked to submit an **IT risk questionnaire** to the ECB on an annual basis. This questionnaire covers five IT risk level domains and ten IT risk control domains in addition to general data on the supervised entity's IT environment. The following slides provide an overview of the **key observations from the annual horizontal analysis** of IT and cyber risk, which is mainly based on data from the questionnaire.

Note: the following information is mostly based on self-assessment data submitted by significant institutions.

# 2023 key observations – IT outsourcing risk

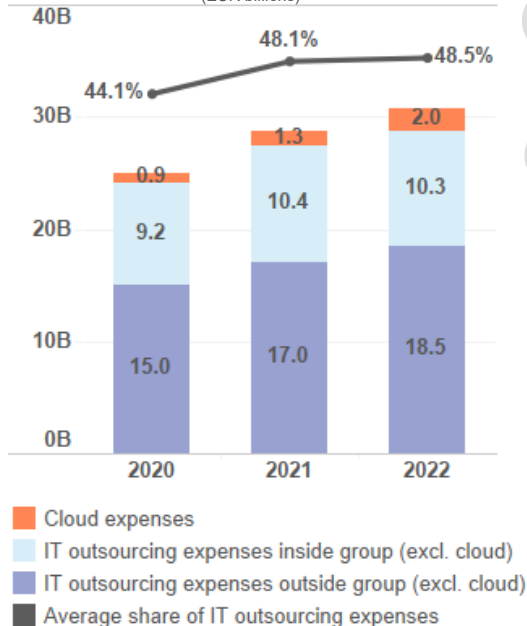
Main indicators suggest a high but stable **IT outsourcing risk level** in line with **institutions reporting stable risk level scores** on average.

Risk level trend

IT outsourcing

=

Overview of IT outsourcing expenses  
(EUR billions)



1

IT outsourcing expenses remained stable, suggesting a **stable risk level**.

2

**Cloud expenses increased by 56%**, albeit from a low basis compared with other IT outsourcing expenses (total cloud expenses account for 6.7% of total IT outsourcing expenses and 3.1% of total IT expenses).

3

**Losses caused by the unavailability or poor quality** of outsourced services increased by 360% to €148 million overall (highly concentrated within a few significant institutions and therefore not indicating a sectoral trend).

4

19% of institutions reported weaknesses in the drafting of **contingency and exit plans** for outsourced services.

# 2023 key observations – IT security risk (1/2)

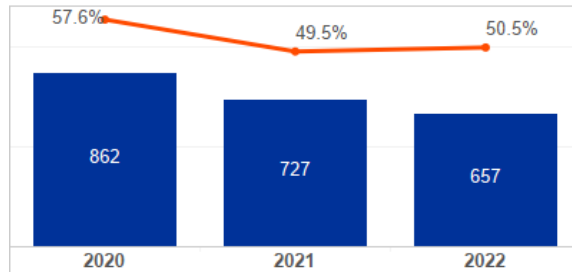
Based on the risk indicators, the **IT security risk profile is stable but elevated.**

Risk level trend

IT security

=

Successful cyberattacks



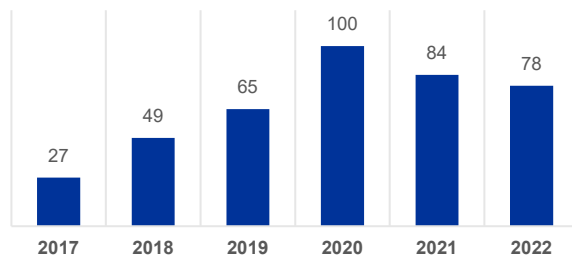
5

Although the cyber security authorities (e.g. ENISA<sup>1</sup>) report an **increasingly hostile environment**, the **number of reported cyber incidents decreased** (total successful cyberattacks by 10%, significant cyber incidents by 9%).

6

However, **reported gaps in risk control areas** and the results of on-site inspections still show **room for improvement** in banks' cyber security, e.g. basic measures such as proper identity and access management, timely vulnerability patching or network security.

Cyber incident reports



<sup>1</sup> European Union Agency for Cybersecurity

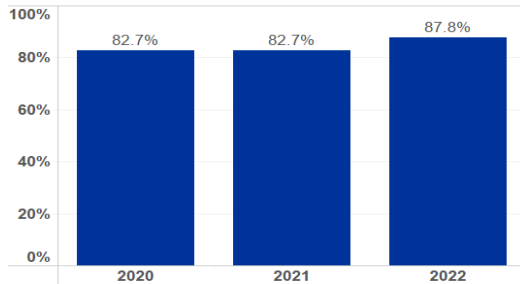
# 2023 key observations – IT security risk (2/2)

Based on the risk indicators, the **IT security risk profile is stable but elevated**. Cyber risk controls have proven effective, despite existing gaps.

Risk level trend

**IT security** =

% of SIs dependent on at least one EOL system supporting business critical activities



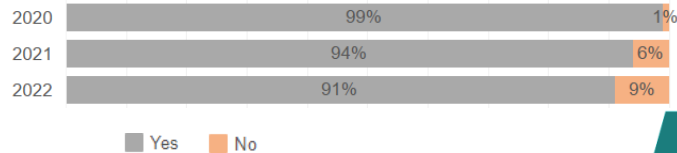
7

The average ratio of **end-of-life (EOL) systems supporting critical activities decreased** from 17% to 12% in 2022. However, **88%** of SIs **depend on at least one EOL system for** business critical activities (+5 percentage points compared with 2021).

8

9% of banks reported gaps in the implementation of their **regular security awareness programmes**, such as measuring success rates and proper follow-up, e.g. in case of failure.


Supervised entities run regular IT security awareness programmes to inform their employees and contractors. The programmes (i) explain the protection and safe use of supervised entities' IT systems, (ii) raise awareness of the main IT security and related risks, particularly cyber threats including computer viruses, possible internal or external abuses and cyberattacks, and (iii) explain the role of employees and contractors in mitigating security breaches. The programmes also measure understanding and identify gaps in knowledge to improve and coordinate future training. (% of SIs by reference year)

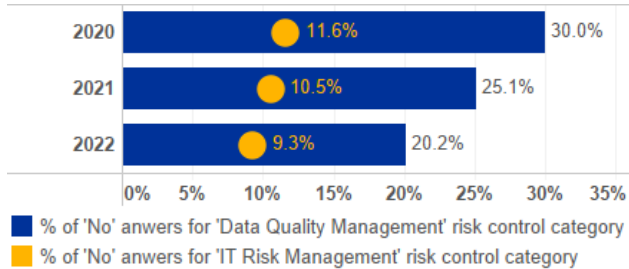


# 2023 key observations – data quality management

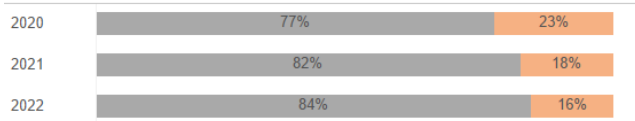
Despite some improvements in 2022, **data quality management** remains one of the **weak spots** of banks' risk control environments.

Risk control trend

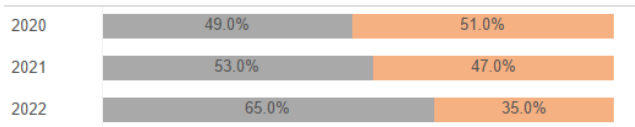
**Data quality mgmt.** 



The supervised entity has defined and documented its data architecture, data models and data flows, and validated them with relevant business and IT stakeholders (% of SIs, by reference year)



Data quality management procedures also apply to end user computing (% of SIs, by reference year)



■ Yes ■ No

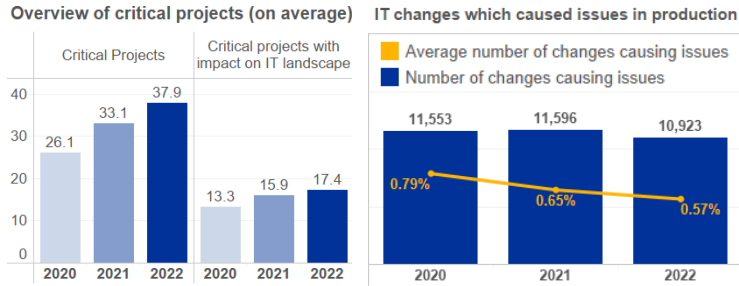
- 9 Data quality management remains the **least mature IT risk control domain** with the lowest self-assessment scores reported by institutions. **However, only about 40% of SIs reported losses caused by data-related IT incidents**, but these were immaterial and have decreased year-on-year.
- 10 Some **key controls are still not fully implemented in many banks**:
  - data architecture model not implemented by 16% of SIs;
  - data quality management principles not applied to end user computing applications by 35% of SIs;
  - information criticality and sensitivity not outlined by 15% of SIs.

# 2023 key observations – IT change risk

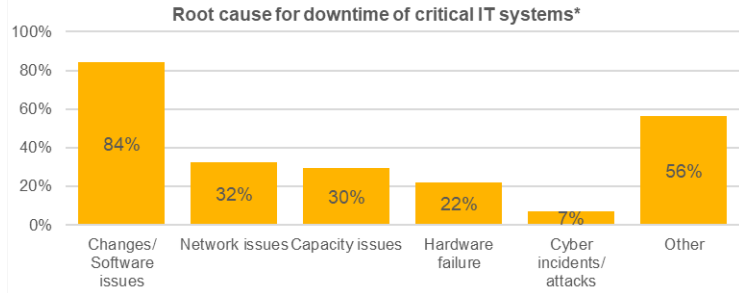
While the impact of IT change risk remained limited in 2022, the ever **increasing number of critical projects** and IT changes reported as the reason for **downtime** warrants **further supervisory attention**.

Risk level trend

**IT change** 



- 11 While the average number of **critical projects increased by a further 15%** in 2022, the number of **IT changes causing issues in production environments decreased** both absolutely and as a share of all IT changes reported.
- 12 **Changes and software issues** were again identified as the **root cause for critical services downtime**.

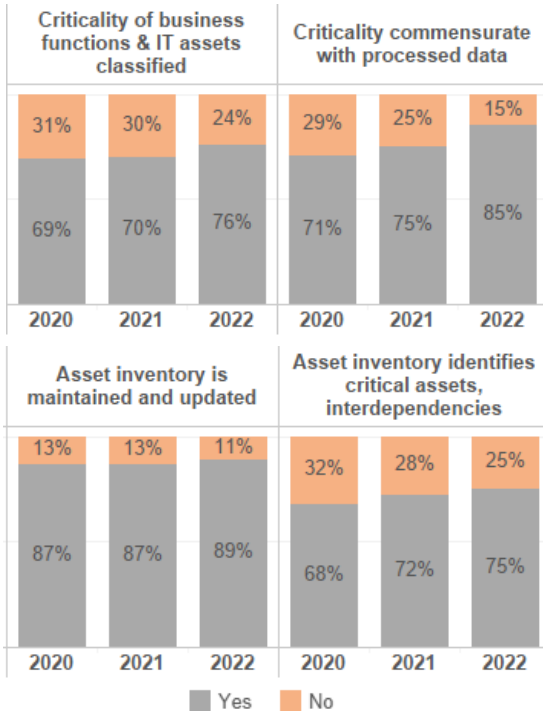


\* Share of institutions reporting the category among the three root causes for critical services downtime.

# 2023 key observations – IT governance and risk management

While banks report improvements in certain areas, **many banks** still report **gaps in IT asset management**.

Risk control trend  
**IT governance & risk management =**



13

The level of board members' IT expertise remains similar to the previous year. **13% of significant institutions still report that no board members have IT expertise.**

14

Many banks (45%) still report at least one gap in **IT asset management**, which is a prerequisite for **proper IT risk and IT change management**.



# The way forward

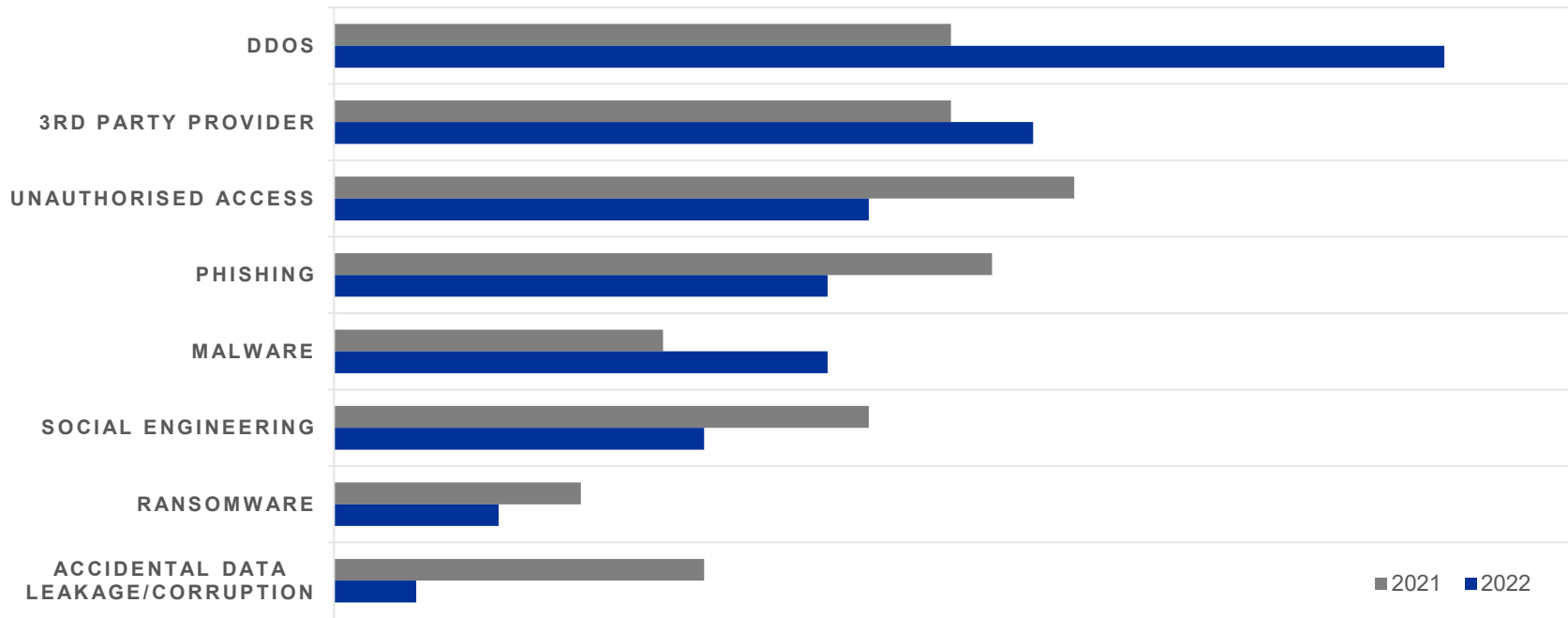
The results of the horizontal analysis **confirm that IT outsourcing and cyber resilience** should be considered **focus areas** for ECB Banking Supervision.

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

# Annex: Cyber Incidents

---

# Cyber incidents: most common types



Note: One incident can be classified as several incident types at the same time.