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 supervisory priority in the period 2022-24. IT security remains 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.

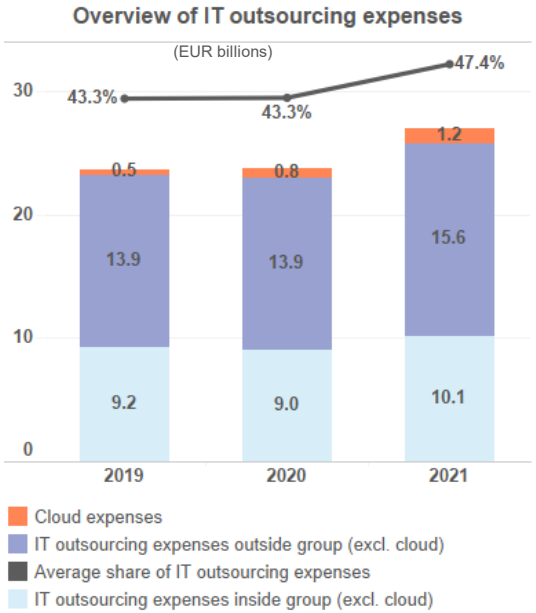
Significant institutions are asked to submit an **IT risk questionnaire** to the ECB on an annual basis. This questionnaire covers five IT risk level domains and ten IT risk control domains, in addition to general data on the supervised entity's IT environment. The following slides provide an overview 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.

2022 key observations – IT outsourcing risk

Main indicators suggest an **increasing IT outsourcing risk level**, in line with **institutions reporting higher risk level scores** on average.

Risk level development
IT outsourcing



1. **IT outsourcing expenses continue to grow: 14% increase compared with 2020**. Average share of IT outsourcing expenses among all IT expenses increased to 47% from 43% in 2020.

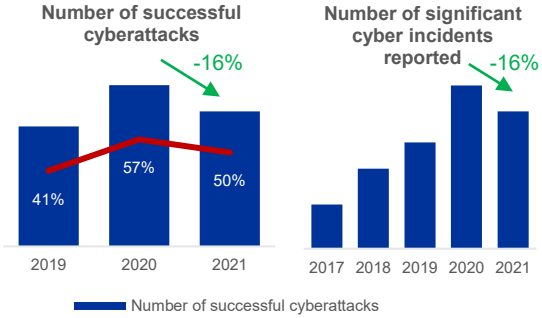
2. **Cloud expenses increased by 45%**, albeit from a low basis compared with other IT outsourcing expenses (total cloud expenses account for 4.2% of total IT outsourcing expenses).

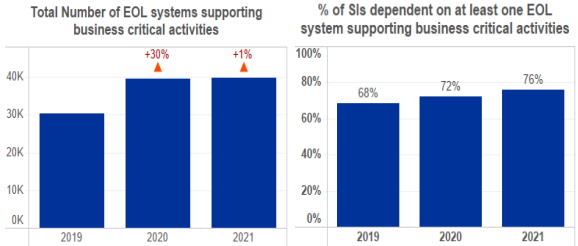
2022 key observations – IT security risk

Banks' self-assessment of the **IT security risk level slightly increased** while the **main indicators showed a slight improvement in comparison with 2020.**

Risk level development

IT security =





3 50% of institutions declared that they were the target of **at least one successful cyberattack in 2021** (57% in 2020).

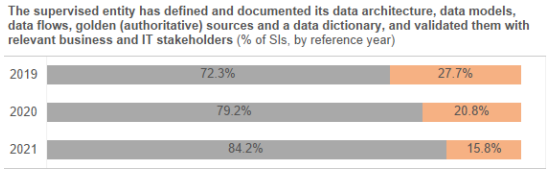
4 Number of successful cyberattacks decreased by 16%. About 12% were **significant cyber incidents, which also decreased** by 16%, with **DDoS (distributed denial-of-service) attacks** being most prevalent and **third-party provider** attacks increasing.

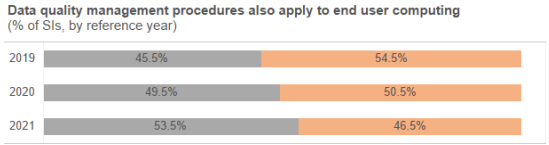
5 Total number of **EOL (end of life) systems supporting critical activities stabilised** in 2021. However, **76% of SIs are dependent on at least one EOL system** supporting business critical activities (+4 percentage points compared with 2020).

2022 key observations – data quality mgmt.

Despite some improvements in 2021, **data quality management** remains one of the **weak spots** of banks' risk control environments.

Risk control development
Data quality mgmt. =





6 **Data quality management** remains the **least mature IT risk control domain** with the worst self-assessment scores reported by the institutions, although the year-on-year rate of improvement increased in 2021 compared with 2020.

7 Some **key controls are still not fully implemented in many banks**:

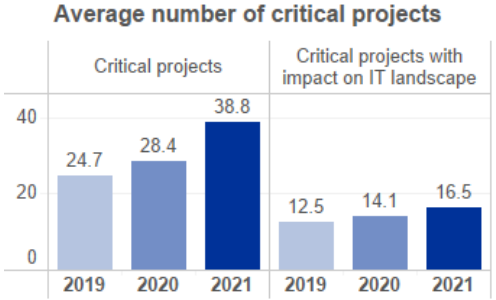
- data architecture model not implemented by 16% of SIs;
- data quality management principles not applied to end-user computing applications in 47% of SIs.

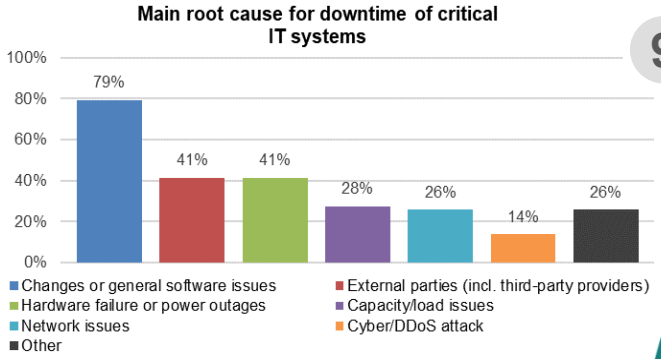
2022 key observations – IT change risk

Given the **general digitalisation trend**, the increasing number of critical projects means IT change is an emerging risk that **deserves further attention.**

Risk level development

IT change





8 The average number of **critical projects increased by 37%** in 2021, while critical projects **with an impact on the IT landscape/architecture** also increased substantially (by 17%).

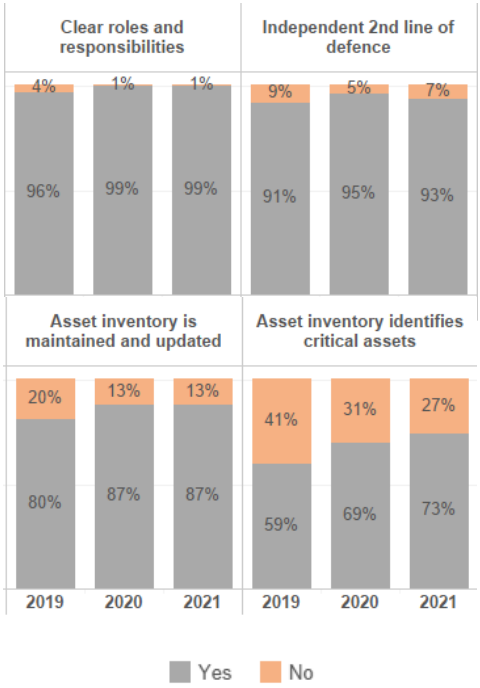
9 **Software changes** were again identified as the **main cause of critical services downtime**, and were mentioned by 79% of responding banks.

2022 key observations – IT governance and risk mgmt.

While banks report improvements in certain areas, **weaknesses in basic areas of IT governance and risk management** are still observed.

Risk control development

IT governance & risk mgmt. =



10 Level of IT expertise of board members similar to previous year. **14% of banks still report that no board members have IT expertise**.

11 Some banks still report a **lack of key risk control measures**, for instance:

- 7% report not having a **functional independence between 1st and 2nd line of defence**;
- 32% report not having an **up-to-date, reliable and complete IT asset inventory** identifying critical IT assets (2020: 36%).

Way forward

The results of the horizontal analysis **support IT outsourcing and cyber resilience** being considered **focus areas** for ECB Banking Supervision.

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