Operational risks and resilience

General trends

The relevance of operational risk and operational resilience for the banking sector has grown further. Operational risk capital requirements have been rising and account for over 10% of total capital requirements for the first time since December 2020, when operational risks were high amid the pandemic. The scope and relevance of operational risk expanded in recent years, and this is not least driven by technological advances and digitalisation.[1] Financial institutions and supervisors also continue to monitor closely reputational challenges and the risk of financial crime, including anti-money laundering (AML) risk and further conduct-related and legal risk that banks have been exposed to. More recently, fraud risk is increasingly coming to the fore.

Potentially very severe implications of this broadened scope of operational risk underline the importance of ensuring operational resilience. This is not least reflected in RAQ responses, according to which cyber risks and data security rank the highest of the operational risks (78%). Risk of ICT failures as a related risk remains high as well. Conduct and legal risks are the second most relevant drivers of operational risk, at 48% agreement. They have become key operational risk drivers for banks in the past years, albeit slightly decreasing since September 2022. Risks related to financial crime, but also further digitalisation and technical innovation, including growing usage of artificial intelligence (AI) in financial crime, may have contributed to a continuously growing risk of fraud. At 42% agreement (10% agreement in autumn 2022), risk of fraud has become the third most relevant driver of operational risk, according to the RAQ. On fraud, already last year the Basel Committee on Banking Supervision (BCBS) pointed to rising fraud risks following the pandemic and amid rising digitalisation.[2]The EBA has also identified new types and patterns of payment fraud, and proposes measures to mitigate underlying risks and protect customers from resulting losses.[3] Outsourcing risks also continue to increase in banks' perceptions, according to the RAQ, as reliance on outsourcing business activities and data

has grown (Figure 49). Beyond existing risks in this area, CBDC-related operational risks linked to e.g. ICT failures as well as fraud or cyber risks might arise with the introduction of CBDCs (see the textbox on CBDCs in Chapter 3.4).

Figure 49: Main drivers of operational risk as seen by banks *
Source: EBA Risk Assessment Questionnaire

* Agreement to up to three options was possible for respondents.

Digitalisation and ICT-related risks

Cyber risk and data security continue to be by far the most prominent driver of operational risk for banks as the digital transformation continues. Technological advances with increased sophistication of ICT, growing reliance on digital and ICT solutions, but also growing capabilities of cyber offenders, which might not least increasingly find support through AI, have all resulted in enhanced risk exposure for banks, including vulnerability to sophisticated cyber-attacks. As a related risk, 38% of respondents in the RAQ also point to ICT failures as a main driver of operational risk. ICT failures and cyber incidents can affect financial entities' operational capabilities to provide critical and important functions and services, which ultimately might affect financial stability. The European Union Agency for Cybersecurity (ENISA) observes a dynamic cyber threat landscape and points out that threats rapidly evolve. They identify dynamic threats marked by evolving attack vectors, including advanced persistent threats, nation-state actors and complex cybercriminal organisations. They also caution against increasingly technology-driven challenges whereby the adoption of emerging technologies introduces both opportunities and vulnerabilities. ENISA calls for proactive cybersecurity measures to address risks.[4] Regulators and banks are accordingly prioritising ICT and cyber risks in operational risk management. For the Financial Stability Board (FSB), to enhance cyber and operational resilience is one of the priority areas for its work in its 2024 work programme.[5]

Vulnerability to cyber-attacks has grown further

Indicating a materialisation of high risks, more than half of banks noted that they had been victim of at least one cyber-attack in the second half of 2023 in their RAQ responses. The share of banks having been victim to up to ten cyber-attacks steadily increased since 2022, to 48% now, while the share of banks falling victim to more than 10 cyber-attacks remained

stable. RAQ responses also suggest that, while the volume and frequency of cyber-attacks as such are unabatedly high, a strongly growing share of responding banks (27% compared to 11% one year ago) report that they faced at least one successful attack which resulted in an actual major ICT-related incident (Figure 50). These figures indicate that the scope, sophistication and impact of successful cyber-attacks across the banking system have increased further in spite of further investments in ICT security infrastructures.

Figure 50: Number of successful cyber-attacks resulting in 'major ICT-related incidents' in the last semi-annual assessment period *

Source: EBA Risk Assessment Questionnaire

* This question covers ICT-related incidents with a potentially high adverse impact on the network and information systems that support critical functions of the firm as reported under Article 17 of DORA.

Publicly available data also indicates a continued high frequency of cyber incidents impacting the financial sector. For example, the ECB observes a significant increase of cyber incidents reported in 2023 on a year-on-year basis.[6] The International Monetary Fund (IMF) cautions that financial institutions are uniquely exposed to cyber risk, and highlights that the risk of extreme losses from cyber incidents is increasing, with an estimated quadrupling of the size of extreme losses since 2017 to ca. USD 2.5bn in 2023.[7] High vulnerability to cyber-attacks highlights the relevance of further investments in ICT and in related security, not least as digitalisation and ICT usage will further expand.

Enhancing operational resilience with DORA implementation

Further effort is therefore required at banks to manage and address ICT security risk. Not least in response to the growing risk of cyber-attacks and threats, Digital Operational Resilience Act (DORA) will apply from 2025, with the purpose of establishing a comprehensive framework on digital operational resilience for EU financial entities. The EBA in January published a first set of rules under DORA aimed at enhancing digital operational resilience by strengthening financial institutions' ICT and third-party risk management and incident reporting frameworks. In May, the ESAs launched a voluntary 'dry run' exercise for the collection of the registers of information on contractual arrangements for the use of ICT third-party service providers by the financial entities.

Financial crime risks

The high number of cases of ML/TF involving European banks in recent years has caused substantial reputational damage to the banking system and undermines the integrity of the EU/EEA banking sector. A comprehensive legislative package to address these risks and strengthen the EU's legal and institutional framework on AML/CFT was adopted in April with the approval of the European Parliament. It includes a single rulebook on AML/CFT systems and controls, a revised directive that sets out requirements for supervisors and Financial Intelligence Units and a regulation establishing an EU Anti-Money Laundering Authority, which will be established this year. At the same time, the EBA has continued to address ML/TF-related risks through regulation, including two sets of guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures, and guidelines on the 'travel rule', i.e. information accompanying transfers of crypto assets and funds. It has also extended its Guidelines on ML/TF risk factors to crypto-asset service providers.

Based on the RAQ results, banks appear to attribute decreasing significance to ML/TF risk, with 13% agreement that it is a main driver of operational risk (18% agreement in autumn 2023). Risks related to the implementation of restrictive measures in connection with the Russian war of aggression against Ukraine continue to be a priority for banks. According to the RAQ, risks related to customers' transactions received from, or sent to, jurisdictions that are subject to international sanctions remain the most relevant financial crime risks for banks, although with a decreasing trend.

Reporting of AML/CFT weaknesses through EuReCA

The EBA has further developed its AML/CFT database, EuReCA, and in May 2024 started to collect information on natural persons directly associated with AML/CFT material weaknesses. In 2023, 37 national competent authorities reported to EuReCA 601 serious deficiencies, or 'material weaknesses', that they had detected in 216 credit and financial institutions' systems and controls. These material weaknesses expose those institutions to ML/TF risks. Most reports concerned credit institutions, but there is an increasing trend in the submissions related to payment and e-money institutions. This reflects the high ML/TF risk EU competent authorities identified within these sectors, which in turn informed their supervisory priorities.[8] Most deficiencies reported in 2023 related to institutions'

approaches to CDD. The large majority of measures reported in 2023 were designed to correct the deficiencies themselves through orders to comply, orders to implement measures and orders to put in place a remediation plan. Also, a large number of measures were punitive and included fines or administrative pecuniary sanctions (Figure 51).

Figure 51a: Financial crime risks in 2023 (cumulative numbers per month)
Source: EuReCA (EBA's AML/CFT database)

Figure 51b: Financial crime risks in 2023 (Where do material weaknesses occur?)
Source: EuReCA (EBA's AML/CFT database)

Figure 51c: Financial crime risks in 2023 (What are the top 5 types of measures?)
Source: EuReCA (EBA's AML/CFT database)

Figure 51d: Financial crime risks in 2023 (What are the top 5 sectors where material weaknesses are identified?)
Source: EuReCA (EBA's AML/CFT database)

Further legal and reputational risks

Conduct and legal risk continues to be the second most relevant operational risk to RAQ respondents, and its relevance remains high with 46% of RAQ respondents considering it as the main operational risk. New cases of past misconduct causing considerable redress costs and reputational damage continued to emerge in the first half of 2024. Legal and reputational risks go beyond those related to digitalisation and ICT-related risks as well as ML/TF risks, and include reputational damage for the banks concerned. Misconduct costs stemming from legal or reputational damage, including from exposures to Russia and other 'rogue states', have been substantive for banks concerned. They also indirectly affect banks' ability to extend lending to the real economy. Misconduct can, moreover, undermine trust in the banking system and the proper functioning of the financial system.

[1] See BIS definition of operational risk in BIS Principles for the Sound Management of Operational Risk.

[2] See the BCBS's discussion paper on digital fraud and banking from November 2023. They also point to analysis from LexisNexis, whose latest report points to rising human-initiated attacks in financial services, whereas automated bot attacks declined in 2023.

[3] See the EBA Opinion on new types of payment fraud and possible mitigations.

[4] See ENISA report Foresight Cybersecurity Threats for 2030 – Update 2024 from April 2024.

[5] See the FSB Work Programme for 2024 from January 2024.

[6] See the ECB SSM annual report on supervisory activities in 2023.

[7] See the IMF blog 'Rising cyber threats pose serious concerns for financial stability' from April 2024.

[8] See, for instance, also the EBA's report on ML/TF risk associated with payment institutions from 2023, which, for instance covers that supervisors should do more in light of the high risks.