SPEECH

The art of bending without breaking – banking on operational resilience

Speech by Frank Elderson, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB, at the joint European Banking Authority and European Central Bank international conference on "Addressing supervisory challenges through enhanced collaboration"

Frankfurt, 4 September 2024

I'm delighted to see supervisors from all around the globe here with us in Frankfurt to exchange views on some of the most pressing issues we face. The banks we supervise operate in an ever more complex risk environment, marked by heightened climate and nature-related risks, increasingly sophisticated cyberattacks and risks stemming from non-bank financial institutions – to name just a few for discussion today. The common denominator of all these risks is that they affect all of us: from Asia to the Americas, from Africa to Europe. To get a better grip on these risks enhanced international cooperation is essential – and this conference is a testament to that.

In my remarks today, I will focus on a cornerstone of prudential supervisors' mission to keep banks sound: ensuring that banks build up and maintain adequate operational resilience.

Let me start with a small detour into the world of botany. In an environment subject to more extreme weather conditions, certain tree species have proven particularly resilient to strong winds due to their distinct characteristics. The silver birch, for instance, is known for its flexible branches and widespread root system. These characteristics help it master the art of bending with the wind without breaking, even under hurricane-like conditions.

The same resilience is needed in today's risk landscape, swept by heightened operational headwinds such as cyber incidents, technology disruptions and natural disasters: to master the art of bending without breaking under such headwinds, banks must develop distinct characteristics.

Now, you might primarily associate a bank's resilience with its financial strength – particularly given the significant increases in capital and liquidity buffers following the post-crisis reforms. But I'll highlight why financial resilience alone is far from sufficient to weather the storms brewing over today's risk landscape.

Consider the example of Amsterdam Trade Bank (ATB), which filed for bankruptcy although it had ample capital and liquidity. What went wrong? Imagine the bank's credit officers turning up at the office one Friday morning in April 2022, trying to access their documents – and all they see on the screen is that access is denied. Why?

Owing to sanctions ATB had lost access to its IT systems, which were run by third-party providers. As a result, the bank couldn't provide banking services anymore. There weren't adequate contingency

arrangements in place – because a scenario in which IT systems weren't operable had seemed too unrealistic – and so the bank had to close shop.

In 2023 when the New York arm of an investment bank was hit by a ransomware attack, it literally sent a runner with a USB stick across downtown Manhattan to help settle trades in the $25 trillion US treasury market.[1]

And most recently, the CrowdStrike incident caused the operating system of a major provider to crash, displaying the so-called blue screen of death, leading to significant disruptions across sectors – including at a few banks.[2]

All these examples underscore a fundamental point: financial resilience alone is a necessary but not sufficient condition to weather operational headwinds. You can have ample capital and liquidity but still face major operational issues or even fail if you lack robust contingency planning for operational shocks that are impossible to avoid. In other words, some banks were missing an essential safeguard – operational resilience.

Operational resilience goes beyond capital and liquidity

While operational risk management aims to minimise the likelihood and impact of operational risks, operational resilience assumes that disruptions will inevitably occur. Hence banks must protect themselves from threats, and be able to respond to disruptive events, recover and learn from them in order to be able to "deliver critical operations through disruption".[3]

First the good news: regulators and supervisors have understood that merely scrutinising banks' balance sheets with an eagle eye is not sufficient to probe banks' resilience. As a result, operational resilience has made it to the top of the supervisory agenda around the globe.[4]

For instance, operational resilience has now been engraved in the marble of supervision: the Basel Core Principles. They now explicitly cover operational *resilience*, including enhanced requirements for aspects ranging from governance and business continuity planning to third-party dependency management.[5] The revised Core Principles will help supervisors around the world to encourage banks to increase their resilience to operational threats. Such threats are unlikely to decline given heightened geopolitical, cyber, and climate and nature-related risks.

Moreover, the Digital Operational Resilience Act (DORA), which will apply as of 17 January 2025 in the EU, will help to further boost operational resilience. Among other things, DORA provides a robust framework requiring banks to foster a culture of continuous IT and cyber risk management.

In the banking union, we flagged addressing deficiencies in banks' operational resilience frameworks as one of the SSM supervisory priorities for 2024-2026. This means, for instance, conducting on-site inspections of banks' cybersecurity management or targeted analysis of banks' outsourcing arrangements with third-party providers, including potential concentrations of risk in certain providers.

IT and cyber risks challenging banks' operational resilience

One important factor challenging banks' operational resilience is IT and cyber risk. This can have a material financial, reputational and legal impact on banks. Cyberattacks can significantly disrupt banks'

critical functions and services, such as providing credit or processing payments, and hence damage the trust in the banking system.

According to the International Monetary Fund, cyberattacks have almost doubled since before the COVID-19 pandemic.[6] This is reflected in the number of significant cyber incidents reported to the ECB too, which almost doubled from 2022 to 2023.[7] Worryingly, the attacks have not only increased in number but also in sophistication.

In order to help banks pinpoint their vulnerabilities to cyber risks, earlier this year we conducted a cyber resilience stress test.[8] It wasn't a stress test in the traditional sense, with capital impact. Instead, it was a qualitative exercise aimed at encouraging banks to better understand how well they would be able to respond to and recover from a successful cyberattack while maintaining their critical functions and services.

The cyber resilience stress test showed that, although banks do have high-level response and recovery frameworks in place, there is room for improvement.

Banks need to ensure that their recovery capabilities are sufficient to handle even worst-case scenarios, and that they can protect customers' assets and data, and in doing so maintain confidence in the banking system.

We are therefore calling on banks to prioritise operational and cyber resilience and ensure that this resilience is integrated into their core business strategies. This will enable them to adapt and respond proactively to the fast-paced changes in the cyber threat landscape.

Cloud outsourcing risk

Let me now turn to another key challenge for banks' operational resilience that warrants closer attention – their use of cloud services.

While there are undoubtedly benefits associated with banks steadily increasing their use of cloud services in recent years, there are also risks. This is why the Basel Committee stresses that "regulatory interventions are needed to address the risks arising from cloud adoption."[9] But what exactly are these risks?

We only have to look back to May this year to find a good example. A misconfiguration at a major cloud service provider erased the equivalent of €82 billion of clients' money from a pension fund, making the accounts of more than half a million customers inaccessible for a week.[10] This incident shows that if an organisation can't easily replace outsourced services during a failure, its functioning may be severely affected. Hence if you outsource functions to a service provider you also need to ask whether the service provider has the same risk controls in place as if that service were provided in-house. To get a better insight into risk controls at cloud service providers, European banking supervision has started conducting on-site inspections of some of these providers.

Another issue is concentration risk. The Bank of England has estimated that more than 70% of banks and 80% of insurers rely on just two cloud service providers.[11] Ultimately, the failure of either of these providers could have a significant negative impact on markets and consumers, and on financial

stability. This level of concentration implies that operational incidents may become more correlated among financial institutions that outsource critical functions to a common critical service provider.

An emerging challenge in the digital financial landscape is the blurring of lines between policy areas. Prudential supervisors would be well advised to coordinate with other supervisory authorities, such as competition authorities, to understand the dynamic market forces at play. Coordination is crucial for ensuring that the drive towards digitalisation, which may result in an increase in market concentration, does not undermine financial stability.

Concerning banks under ECB supervision, we found room for improvement in their cloud outsourcing strategies. We acted on this by publishing for public consultation a guide that sets out our supervisory expectations and provides recommendations on the outsourcing of cloud services. Importantly, the guide also outlines specific good practices that banks can use as a basis for tackling cloud outsourcing risk.[12]

Clearly, cloud outsourcing risk doesn't stop at national borders; it affects multiple jurisdictions. We've therefore teamed up with other prudential authorities to conduct a joint review into cloud outsourcing practices. This will enable us to better understand how banks are adopting cloud technology and the risks it may pose. For instance, we're collectively exploring banks' third-party risk management practices and their business continuity plans, as well as their exit strategies – including stressed exits.

Bolstering operational resilience requires investment

So how can banks strengthen their operational resilience? In contrast to financial resilience, operational resilience cannot be bolstered by accumulating additional basis points of Common Equity Tier 1. Rather, mastering the art of bending without breaking under operational headwinds requires multi-year investment in capability-building. We know that you should put your house in order in good times so that you are well prepared for bad times. Given the current uptick in banks' profitability, the time is right for banks to continue investing in building their operational resilience.

This means, for instance, replacing legacy systems with state-of-the-art IT infrastructure, including in the areas of IT risk management and cyber hygiene, as well as ensuring that business continuity plans and third-party dependency management are implemented consistently.

Importantly, operational resilience-building is not only a matter of systems and processes – it is also about people. Investment in human capital is therefore essential. Banks must ensure that employees at all levels of the organisation have the appropriate skillset, whether they are experts or managers. Soberingly, from our analysis of the effectiveness of banks' management bodies we can see that there are still boards that lack in-depth IT expertise, which may ultimately put into question the collective suitability of the board.[13] We expect all boards to have a sound understanding of IT and cyber risks so that they can assess the impact of these risks on banks' various business areas.

Conclusion

Let me conclude.

The novelist Max Frisch once said: "Crisis is a productive state. You just have to take away the aftertaste of disaster". Shocks stemming from cyber incidents or cloud outsourcing and IT risks are an

opportunity for banks to further bolster their resilience – to nurture their capacity to bend without breaking.

Financial resilience alone is far from sufficient to weather operational headwinds – you need operational resilience. And in order to bolster and maintain operational resilience banks must continue investing in future-proof systems, processes and people. This is not a steady state exercise. Operational resilience demands continuous attention and must keep pace with the changing risk environment.

As I have highlighted, no jurisdiction is immune to operational shocks. All of us will be affected by them at some point.

Let's therefore share good practices and use cases from our supervisory work.

Let's reinforce policy and supervisory coordination across both jurisdictions and sectors.

And let's strengthen communication channels to enable us to coordinate closely when shocks hit.

Thank you for your attention.

1.

Financial Times (2024), "Cyber attacks reveal fragility of financial markets", 16 January.

2.

Financial Times (2024), "Global IT outage could take weeks to resolve, experts warn", 20 July; "Companies around the world hit by Microsoft outage", 19 July

3.

The Basel Committee on Banking Supervision (BCBS) defines operational resilience as follows: "the ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption. In considering its operational resilience, a bank should assume that disruptions will occur, and take into account its overall risk appetite and tolerance for disruption." See paragraph 11 of the BCBS principles for operational resilience.

4.

See the BCBS principles for operational resilience, the Bank of England web page on operational resilience, the Federal Reserve System web page on operational resilience, and Tuominen, A. (2024), "The Digital Operational Resilience Act: the next step in a connected digital world", contribution for Eurofi Magazine, 20 February.

5.

In 2024 supervisors from around the world revised the Core Principles for Effective Banking Supervision, which were first published in 1997 and last updated in 2012. The Core Principles are one of the most important sets of global supervisory standards, establishing comprehensive requirements

for both supervisors and banks. See also Elderson, F. (2024), "Updating the Magna Carta of supervision: review of the Core Principles for Effective Banking Supervision", *The Supervision Blog*, ECB, 25 April.

6.

International Monetary Fund (2024), "The Last Mile: Financial Vulnerabilities and Risks", *Global Financial Stability Report*, April.

7.

Tuominen, A. (2024), *Interview with Il Sole 24 Ore*, 28 March.

8.

See also Tuominen, A. (2024), "Enhancing banks' resilience against cyber threats – a key priority for the ECB", *The Supervision Blog*, ECB, 26 July.

9.

Koh, T.Y. and Prenio, J. (2023), "Managing cloud risk – some considerations for the oversight of critical cloud service providers in the financial sector", *FSI Insights on policy implementation*, No 53, Bank for International Settlements.

10.

The Guardian (2024), "Google Cloud accidentally deletes UniSuper's online account due to 'unprecedented misconfiguration'", 9 May.

11.

Bank of England (2020), "How reliant are banks and insurers on cloud outsourcing?", *Bank Overground*, 17 January.

12.

For instance, it is good practice to have multiple data centres in different geographical locations. Banks should also have exit strategies in place – with clearly defined roles, responsibilities and cost estimates – for all outsourced cloud services linked to critical functions. And banks should also assess concentration risks to a specific provider, geographical location and functionality.

13.

For instance, 17% of banks do not have a management body member with more than five years of ICT experience. See Elderson, F. (2024), "Banks' governance and risk culture a decade on: progress and shortcomings", The Supervision Blog, 24 July. To ensure diversity of skills and collective suitability, for instance, we expect at least one non-executive member of the management body to have a minimum of five years of recent and specific knowledge and experience in the field of ICT and security risk management. See ECB Banking Supervision (2024), "New policy for more bank board expertise on ICT and security risks", Supervision Newsletter, ECB, 21 February.