SPEECH

Strengthening operational resilience for the age of AI

Keynote speech by Frank Elderson, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB, at the Goldman Sachs European Financials Conference 2026

Zurich, 3 June 2026

Thank you for inviting me to speak today.

Europe is facing a set of unprecedented challenges.

The geopolitical environment is becoming increasingly fragmented. Europe remains overly dependent on external providers for energy, technology, security and key financial infrastructures such as payment systems and capital markets. Reducing these dependencies is no longer a choice, but a necessity to safeguard the European way of life.

Ensuring that our future is not determined elsewhere demands investment on an unprecedented scale. Consider that the green, digital and defence transitions will require an additional €1.2 trillion of spending per year between now and 2031.[1]

No single actor, no single sector and no single country can meet these challenges alone.

As fiscal space tightens, much of Europe's investment needs will have to come from private investment, with capital markets playing a pivotal role.

In a bank-based financial system like Europe's, strong, competitive and resilient banks are even more indispensable than they are elsewhere. They sustain the flow of finance to businesses, households and the broader real economy. It is therefore no surprise that the competitiveness of European banks has moved to the heart of the policy debate.[2]

Yet the competitiveness of the banking sector is not solely determined by capital, market integration, scale or regulation. It also hinges on whether banks can continue to serve their clients and provide critical services when disruption strikes. That is why today I will focus on operational resilience.

Resilience goes far beyond capital

When some people hear supervisors speak about resilience, they immediately think of financial resilience.

However, in a world of more frequent, sophisticated and disruptive cyber incidents, technology failures and growing dependencies on third parties, a bank can be well capitalised and highly liquid and yet still unable to operate.

A striking example of the importance of non-financial resilience is the ransomware attack that hit the New York branch of the Industrial and Commercial Bank of China in 2023 – the largest bank in the

world by assets. Despite the bank's financial strength, the incident disrupted the settlement of trades in the US Treasury market, one of the most systemically important markets globally. The bank had to rely on manual workarounds – including reportedly dispatching a courier with a USB stick across downtown Manhattan – to meet its obligations.

Another example is the CrowdStrike incident in 2024, when systems using a major operating platform crashed and displayed the "blue screen of death". The disruption affected firms across sectors, including financial services.

At the same time, the threat environment is evolving rapidly with the rise of AI. One telling example involved criminals using AI-generated identities to create thousands of fake customers in order to obtain loans, causing millions in losses for the bank concerned.

We have also seen an increase in the number of cyberattacks reported by banks under our supervision in recent years.[3]

All these examples illustrate a fundamental point: a bank can have ample capital and liquidity but still face severe operational issues, or even fail, if it lacks preparedness and robust contingency planning for operational shocks. Today, resilience is not only about absorbing losses, but also about maintaining critical services – even under severe operational stress.[4]

This imperative to maintain operational resilience is all the more critical in banking – a sector built on trust in which cybersecurity failures can have profoundly damaging consequences.

Operational resilience firmly on the agenda of banks and supervisors

The good news is that banks and supervisors are not starting from scratch.

Over the past decade, cyberattacks on critical infrastructure – including energy and telecommunications providers, as well as banks – have become more frequent, more targeted and more sophisticated.[5]

Although cyberattacks are occurring everywhere, every day and at any time, and while notable incidents have affected financial services, we have not yet seen such events escalate into widespread disruption or threaten the viability of a major bank.[6]

This is not a coincidence.

The fact that financial services are among the sectors best prepared to deal with cyberattacks reflects years of capacity building in banks: in defence, detection and incident response and reporting. Moreover, governance arrangements have improved and there is a greater awareness of cyber risks, particularly among banks' management bodies.[7]

Importantly, banks' efforts have evolved in tandem with a stronger and sustained supervisory focus. Operational resilience and cyber risk have been a priority for European banking supervision for several years[8], during which we have worked closely with banks in both ongoing and on-site supervision.

For example, in 2024 we conducted a cyber resilience stress test on 109 banks, 28 of which underwent a more thorough assessment of their ability to respond to, and recover from, a severe but

plausible cybersecurity incident. While the exercise confirmed that banks have frameworks in place to respond to and recover from severe cyber incidents, it also highlighted areas for improvement for certain banks. Since then, almost three-quarters of our findings identified by the stress test have been addressed, with banks notably strengthening their cyber resilience.

The Digital Operational Resilience Act (DORA), which entered into force last year, provides a regulatory framework that requires banks to foster a culture of continuous improvement in IT and cyber risk management. It has also enhanced the oversight of critical third-party providers, such as cloud service providers.[9]

In addition, DORA gave supervisors the task of testing whether a financial institution can detect, respond to and recover from sophisticated attacks that mirror real-world threats, thereby providing a more systemic and enforceable framework for resilience.[10]

Taken together, these efforts have raised the cost and complexity of successful attacks, effectively pushing up the “price of admission” and prompting many threat actors to target less well-prepared sectors instead.

There is, however, no room for complacency.

Advancements in AI are reshaping the threat landscape, fundamentally altering the balance and asymmetry between defenders and adversaries.

Put bluntly, if ensuring operational resilience was already critical a few years ago, it certainly is today – amid a rapidly evolving threat landscape shaped by frontier AI models.

Artificial intelligence: a structural shift in the cyber threat landscape

AI adoption is already widespread among Europe’s significant banks. Our annual data collection on banks’ use of innovative technologies shows that more than 85% of banks under European banking supervision use artificial intelligence.

Used responsibly, AI can help banks strengthen their operations, improve risk management and enhance IT security. But AI also vastly improves the capabilities available to malicious actors.

Until very recently, launching a sophisticated cyberattack required deep technical expertise, extensive reconnaissance and coding, and often weeks – or even months – of trial and error.

Not anymore.

A new generation of large-scale AI models is emerging, with increasingly advanced cybersecurity capabilities. If these tools become more widely accessible, they could enable a much broader range of malicious actors to carry out complex attacks with greater speed and precision.

Our current understanding is that tools of this kind are not simply another incremental improvement; they are a structural shift in the economics of cyber risk. Tools like Mythos appear to be significantly more advanced than existing tools in three important ways. First, they can discover and exploit vulnerabilities at a speed and scale far beyond what we have seen before. Second, they can combine seemingly minor vulnerabilities into serious attacks. And third, they can help reverse-engineer patches into exploitable vulnerabilities and, again, do so at unprecedented speed.

Together, these characteristics suggest that the “price of admission” will fall. The marginal cost of identifying and exploiting vulnerabilities in IT systems will decline, possibly by orders of magnitude. Cyberattacks that previously required significant expertise, time and resources may in future be achieved more quickly, at scale, and by a much broader set of potentially malicious actors. Current evidence suggests that these models may be effective not only against environments with weak levels of defense but also against standards that were once previously considered state of the art.

The direction of travel is unmistakable: the speed, scale and accessibility of advanced cyber capabilities are increasing, and the time available to defenders is shrinking.

Banks therefore need to prepare more quickly, more effectively and more consistently across the sector. In musical terms, *andante* may have previously been good enough, but now we need to move to *presto.*

The pivotal role of management bodies in addressing this strategic challenge

Most importantly, the challenges posed by new generations of AI models should not be viewed solely as a cybersecurity issue – they are a firm-wide strategic challenge with potential implications for banks’ safety and soundness. It is therefore essential that banks’ management bodies take clear ownership of the issue, ensuring that resources and tools are commensurate with its scale. This approach is vital to close cyber resilience gaps, enable timely patching and maintain strong cyber hygiene.

Moreover, the critical infrastructure on which banks depend – including cloud providers, telecommunications networks, payment systems and electricity and water supplies – could also become targets. As a result, scenarios that were once considered tail risks may become more likely, such as vulnerabilities in a single, widely used infrastructure quickly escalating into disruption across an entire sector, with knock-on effects on banks’ ability to operate. This makes it all the more important to both strengthen the oversight and monitoring of third-party dependencies and enhance information sharing across the financial system. Given that many of these threats are similar in nature, the timely exchange of information on vulnerabilities, incidents and mitigation measures is a cornerstone of collective resilience.

Considering that some banks’ preparedness is still weak this is also where we, as supervisors, have a role to play. The SSM will use its system-wide perspective to support institutions by pointing out areas of attention and good practices, which could prove particularly beneficial for smaller banks with less sophisticated IT environments[11].

In this spirit, last week we brought together supervised banks to discuss the implications of frontier AI models for banks’ resilience and the practical actions needed in response. As a next step we will send a so-called ‘’dear CEO letter’’ to all banks in which we aim to ask banks to take proactive measures to ensure the continued robustness and security of their systems in the face of these transformative challenges and will follow up with individual banks in a targeted manner.

Our aim is straightforward: to ensure that banks take the necessary steps now, before these technologies are more widely used by threat actors.

Strengthening operational resilience requires investment

Operational resilience is not a stand-alone issue that is separate from the current debate on banking sector competitiveness. It is part of the foundational elements that shape banks' competitiveness.

If banks are unable to maintain their customers' trust by providing a reliable service, their ability to compete in an increasingly digitalised financial system will be undermined. Ensuring operational resilience is therefore not only a safeguard – it is also key to remaining competitive, both today and in the years ahead.

Strengthening operational resilience requires multi-year investment in people, systems and governance. In short, it is not a quick fix, it is a moving target which calls for continuous effort and ongoing improvement.

Banks should therefore give careful consideration to bolstering operational resilience in their investment strategies. The currently strong bank profitability provides an opportunity to continue investing.

At the same time, the banking sector's defensive capabilities are not evenly distributed, leaving parts of the system more exposed than others. While some larger banks have a size advantage when it comes to having the IT budgets that match the scale of the task, this may admittedly be more difficult for small and medium-sized banks.

This is, however, no reason for inaction. In a diverse banking system, where banks of different sizes and business models thrive and support the real economy, all banks must be able to ensure a sufficient level of operational resilience. This point is particularly important at a time in which further embracing proportionality in supervision and regulation has become a topical issue in the debate.

There are undoubtedly areas where a more proportionate approach is worth pursuing.[12] Such enhanced proportionality, however, cannot come at a cost of prudent risk management.

Conclusion

Let me conclude.

Europe is facing enormous financing needs to boost its autonomy. We must finance the transition to a cleaner economy, strengthen our collective defence, build the industries of the digital age and support societies that are growing older.

To do so, we need strong and competitive banks. But banks can only play their role if they are resilient, including to operational threats.

Frontier AI models are changing the cyber threat landscape. They are lowering barriers for attackers, increasing the speed of exploitation and exposing weaknesses that were too often tolerated for too long.

This is not about creating a sense of alarm, but rather a sense of urgency

Because we cannot afford to be complacent. Our message as supervisors is simple: act early, invest decisively now, and do not wait for the next incident to reveal where your vulnerabilities lie.

Such a proactive approach will contribute to a thriving, diverse banking system that is capable of supporting the real economy through the digital, green and defence transitions.

A resilient and thriving banking system is not simply a nice to have. It will be imperative to tackle the challenges we are facing both today and in the years ahead.

1.

Bouabdallah, O. et al. (2025), "Time to be strategic: how public money could power Europe's green, digital and defence transitions", *The ECB Blog*, ECB, 25 July.

2.

The ECB has actively contributed to this debate, including through its recent response to the European Commission's consultation on banking sector competitiveness; see ECB (2026), *Eurosystem response to the EU Commission's targeted consultation on the competitiveness of the EU banking sector*, April. For more details on the importance of overcoming fragmentation to boost competitiveness, see Elderson, F. (2026), "Boosting prosperity through deeper integration", keynote speech at the conference "Financing Europe: a new era of strategic investment", Brussels, 12 May.

3.

The number of cyber incidents reported by banks to the ECB rose sharply up to the end of 2024. The data for 2025 is not directly comparable because the incident reporting thresholds were changed following the entry into force of the EU's Digital Operational Resilience Act (DORA). As a result of DORA, the ECB now receives ICT (non-cyber but operational) incident reports as well as ICT cyber incident reports. However, the latter are smaller in number than before because the reporting thresholds differ from those under the ECB's former cyber incident reporting framework.

4.

In practice, this means being able to prevent, withstand, respond to, recover and learn from operational shocks The Basel Committee on Banking Supervision 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 Basel Committee's principles for operational resilience.

5.

See Tuominen, A. (2025), "Improving banks' resilience to hybrid threats", speech at the conference "The Current Hybrid Threat Environment and Financial Stability", jointly organised by Commerzbank and the European Centre of Excellence for Countering Hybrid Threats, Frankfurt, 18 November; Klaus, B. and Wendelborn, J. (2025), "Cyber threats to financial stability in a complex geopolitical landscape", *Financial Stability Review*, ECB, May. At a global level, finance and insurance companies

rank approximately fourth among the top ten industries affected by cyberattacks in volume terms, jointly with the educational services industry, and below the public administration, healthcare and technology industries; see the University of Maryland's CISSM Cyber Events Database. In the European financial sector as a whole, banks are by far the entities experiencing the greatest number of cyberattacks. See European Union Agency for Cybersecurity (2025), *ENISA threat landscape: finance sector*, February.

6.

Some incidents have disrupted payment channels, delayed customer services and, in a few cases, caused notable financial losses. But none has threatened the viability of a major bank or produced a systemic shock.

7.

Some 86% of CROs cite cybersecurity and technology risk as a top priority for the next 12 months, whereas only 62% cite credit risk. Institute of International Finance (2026), *Annual EY/IIF Global Bank Risk Management Survey – Shifting priorities: CRO agendas in a time of uncertainty and innovation*, IIF, 24 February.

8.

In addition to working with banks on their own preparedness. starting in 2023 the SSM organized cyber dry-runs to test our own preparedness to respond to large-scale cyber incidents. The simulations focused on detection, escalation, information sharing, and coordination capabilities during a systemic crisis, possibly when the ECB's and the NCAs own ICT systems are also affected. This kind of activity is key for improving our own operational resilience, strengthening contingency plans and identifying areas where cooperation should be improved.

9.

This is essential because banks increasingly rely on external providers for some critical functions that are difficult or impossible to replace, thereby exposing them to cascading effects from cyber incidents in the supply chain, even if they themselves have not been directly targeted.

10.

Threat-led penetration testing (TLPT) under the EU's Digital Operational Resilience Act (DORA).

11.

Good practices do not describe or establish new regulatory requirements and have no legally binding effect. This means that a bank may be fully compliant with the applicable legal framework without implementing any of the good practices pointed by the ECB, provided that it follows other practices that are more appropriate to its particular risk profile, business model and circumstances.

12.

Even if proportionality is already embedded in the European regulatory and supervisory approach, we see room to embrace it further. The small and non-complex institutions (SNCIs)regime, is the natural starting point, while maintaining the Single Rulebook, which ensures the risk-based nature of the prudential framework is retained for all banks. One could consider, for example, increasing the scope of eligible small banks through an increase of the €5 billion threshold of the SNCI regime as well as extending the scope of the simplified rules. Any simpler regime for smaller banks also needs to be accompanied by a credible, flexible and efficient crisis management framework for these institutions: See Elderson, F. (2026), "Boosting prosperity through deeper integration", keynote speech at the conference "Financing Europe: a new era of strategic investment", Brussels, 12 May; and ECB (2026), *Eurosystem response to the EU Commission's targeted consultation on the competitiveness of the EU banking sector*, April.

CONTACT

European Central Bank

Directorate General Communications

- Sonnemannstrasse 20
- 60314 Frankfurt am Main, Germany
- +49 69 1344 7455
- media@ecb.europa.eu

Media contacts