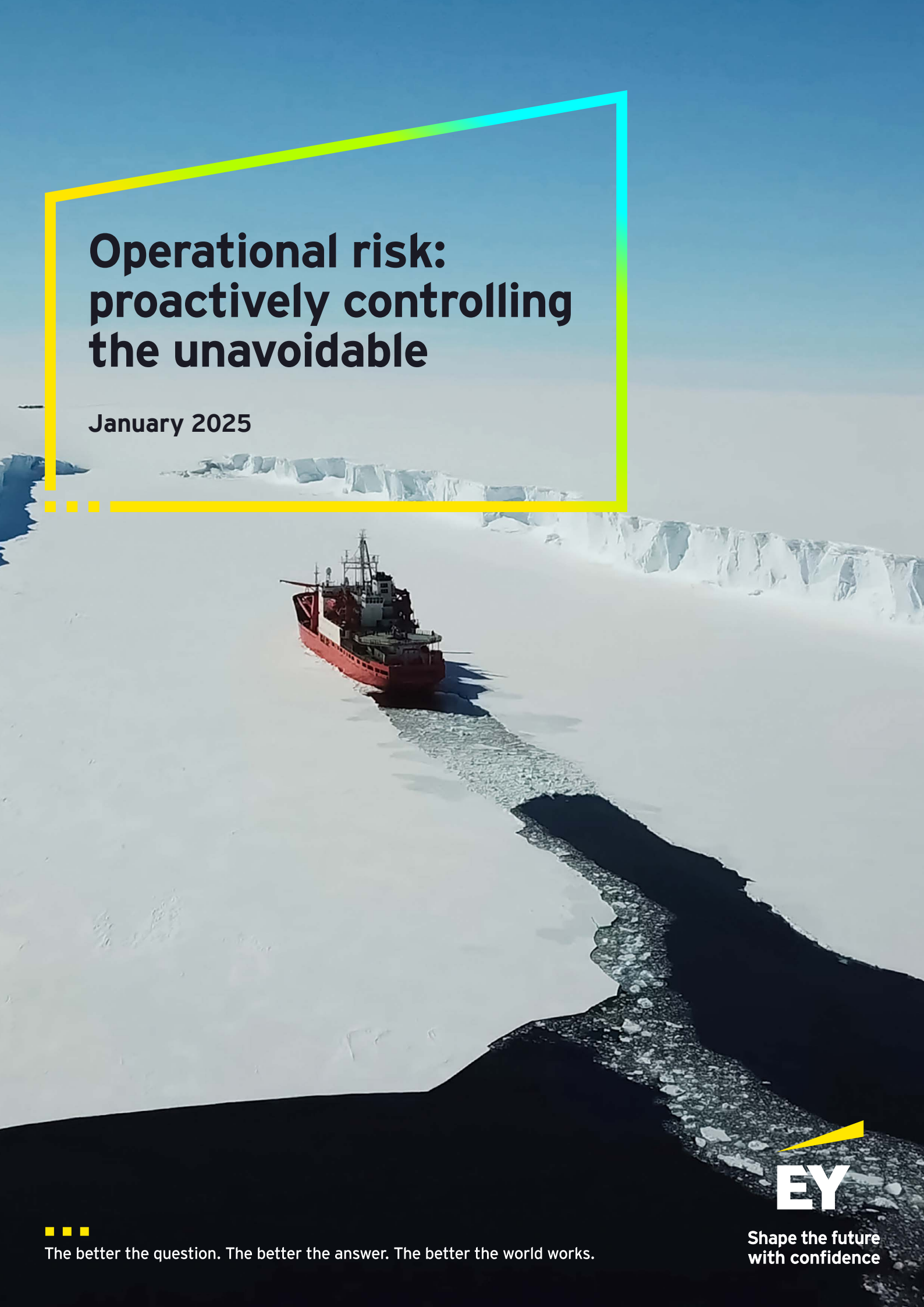
Operational risk: proactively controlling the unavoidable

January 2025



The better the question. The better the answer. The better the world works.

Shape the future with confidence

In brief

- **Operational risk is at the heart of significant losses and business failures.**
- **Being proactive rather than reactive delivers the opportunity to exceed regulatory expectations.**
- **Balancing risk management and value creation can be achieved with a clear vision.**

Failure can be an opportunity

- In recent years, there has been an increased focus on operational risk driven by global regulators' desire to make financial markets more resilient and minimise operational disruptions. Financial institutions are having to raise their level of awareness of the potential risks on the horizon and enhance the effectiveness of mitigating controls put in place to strengthen their frameworks and bolster their ability to respond to disruptions.
- Due to the increasing interconnectedness of risks that can create single or multiple points of failure, financial institutions need to embrace change and approach risk management as an iterative process as regulatory expectations evolve and new technologies and threats increase firms' exposure to new and emerging risks.[1] If this change is not appropriately managed, firms will struggle to manage their risks, which can result in costly failures.
- The Basel Committee on Banking Supervision (BCBS), the standard-setting body for prudential regulation, defines operational risk as the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events — including legal risk but excluding strategic and reputational risk.[2] More recently, the definition has evolved to include topics such as financial crime, conduct risk, third-party risk and cyber risk. The BCBS has issued several policies on best practices and regulatory expectations on operational risk. First published in 2003, several revisions were issued as risks evolved and ultimately brought forth the principles of operational resilience in 2021 with the rise in significant disruptions to banks' operations. Recent third-party outages are a reminder of how vulnerable many firms are to significant outage events that can disrupt global markets.[3]
- In this article from Ernst & Young LLP (EY UK), we explore how operational risk practitioners can focus on key areas that can help them go beyond meeting regulatory expectations and rebuild confidence in the three lines of defence's (3LOD) ability to effectively monitor, manage and mitigate risks.

1 *EY and IIF. (2022).* 12th Annual EY/IIF Global Bank Risk Management Survey: Seeking stability within volatility: How interdependent risks put CROs at the heart of the banking business. **Available here**

2 *Basel Committee on Banking Supervision. (2021).* Revisions to the Principles for the Sound Management of Operational Risk. Bank for International Settlements. **Available here**

3 *Lerman, R. (2024).* Global IT collapse puts cyber firm CrowdStrike in spotlight. **Available here**

Persistence of the problem

Banks continue to face varying challenges with respect to operational risk. At present, we observe various levels of maturity for several reasons. First, assessing potential losses from operational risk is challenging due to difficulties in modelling operational risk-related losses, whereby capturing definitional components (e.g., human error, system failures) in a formula and quantifying is more difficult than financial modelling. Second, the scarcity of tail risk event data points makes it challenging to develop statistical models. Third, operational risk is a relatively new risk taxonomy compared with financial risks. Lastly, poor data quality and inconsistent taxonomies used across the sector continue to create challenges. In the face of these persisting challenges, mismanagement of operational risk can cause significant harm and financial loss. The increased digitisation of financial services through AI, automation, and the proliferation of third-party FinTech also gives rise to the potential of both cyber and tech outages. Regulatory scrutiny is also increasing on operational risks that are more distant from firms' core businesses (e.g., cloud services).[4]

Recent research by Uddin et al.,(2023) argues that technology innovations in banking, while increasing business volumes, will also expose banks to more operational risks.[5] This is corroborated by the top operational risk categories cited by financial firms across several different survey sources. According to separate surveys conducted by both Risk.net and ORX, cyber-related risk remains a top concern among risk professionals (***Table 1***).[6,7]

Table 1: Top 10 operational risks according to Risk.net surveying 81 financial services firms

Risk	2023	2024
Cyber risk: information security	1	1
Cyber risk: IT disruption	3	2
Third-party risk	4	3
Regulatory compliance	2	4
Change management	7	5
Resilience risk	5	6
Geopolitical risk	8	7
Execution and process errors	6	8
External fraud	11	9
Conduct risk	10	10

4 *Financial Conduct Authority (FCA). (2023).* Our emerging regulatory approach to Big Tech and artificial intelligence. **Find it here**

5 *Uddin, M., Chowdhury, M., Zafar, S. and Ahmed, A. – ScienceDirect (2023).* Does digital transformation matter for operational risk exposure? **Find it here**

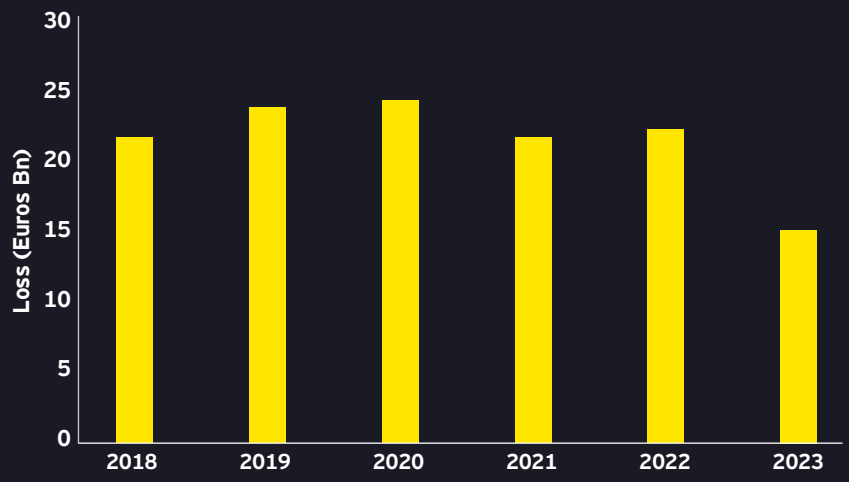
6 *ORX. (2020, 2023).* Analysis of Operational Risk Losses 2010-2019; Global banks report lowest financial losses in a decade. **Find it here**

7 *Risk.net. (2023).* Top 10 operational risks for 2024. **Find it here**

ORX's 2023 and 2024 surveys and the EY/IIF CRO 13th annual survey of banking CROs showed similar findings, with 89% of respondents citing cybercrime as one of the top five risks and 73% of surveyed CROs listing cybersecurity as their top risk concern, respectively.[8,9]

Although conduct risk is ranked further down the list, significant penalties are still being levied for conduct risk-related breaches to the tune of £175 million as of December 2024 (of which over 76% of this amount was paid by banking and capital market firms).[10] ORX data from recent years provides some important insights to note in ***Figure 1***:

Figure 1: Total gross loss of events reported per year



- A total of EUR129 billion in operational risk-related losses were reported between 2018 and 2023 among ORX's 82 member banks, with losses in 2023 alone amounting to EUR 15.2 billion.
- While the total value of losses from operational risk events has declined slightly, the losses are still material and can impact firms' profitability.[11]

Additionally, the FCA imposed over £49 million for failings in operational risk management to banking and capital markets firms in 2023.[12] These findings suggest that achieving effective operational risk management remains a persistent challenge despite improvements to date.

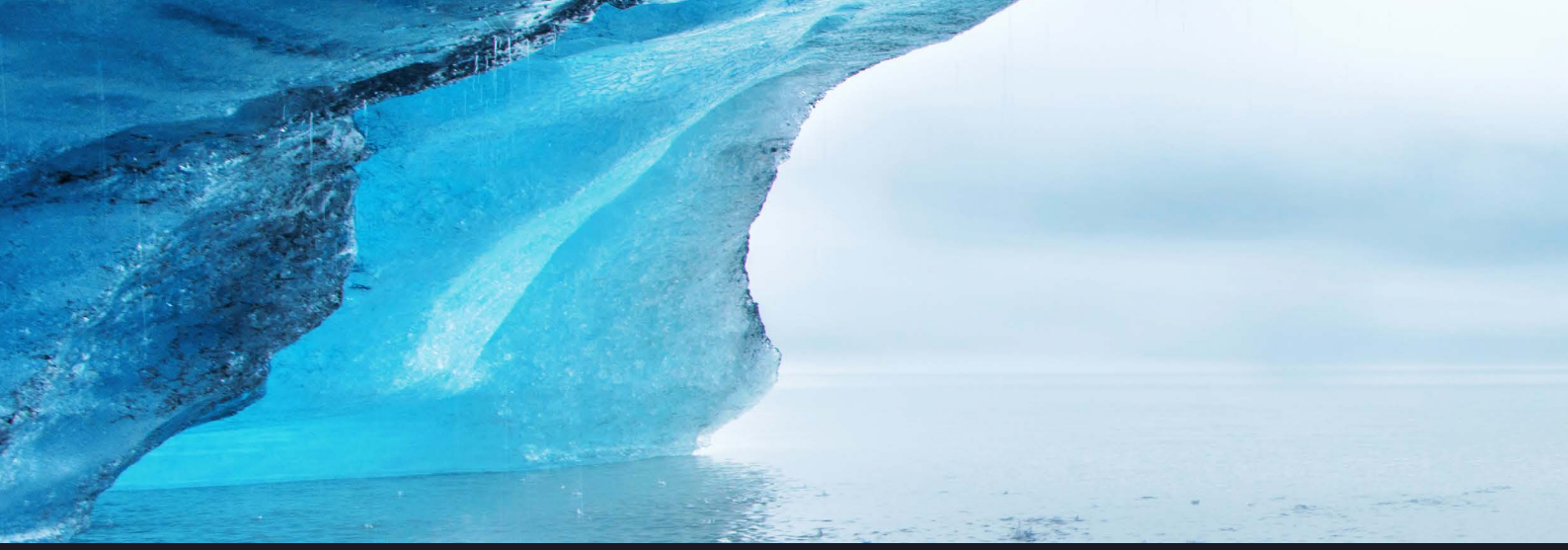
8 *EY and IIF. (2024). 13th Annual EY/IIF Global Bank Risk Management Survey:* Managing through persistent volatility: the evolving role of the CRO and the need for organisational agility. **Find it here**

9 *ORX. (2024). Emerging risks in 2024: A comparative analysis for insurers and banks.* **Find it here**

10 *Financial Conduct Authority (FCA). (2024).* **2024 fines**

11 *ORX. (2020).* Analysis of Operational Risk Losses 2010-2019. **Find it here**

12 Financial Conduct Authority (FCA). (2023). **2023 fines**. By contrast, the US regulators fined $193 million in Q4 alone in 2023. *ORX. (2023).* **Top 5 ORX News Losses: Q4 2023**



How to maintain a competitive edge

As firms increasingly adopt more robust and agile risk management frameworks and promote a healthy risk culture, this will enable better detection and prevention of risks. From our experience in the market, EY UK observes three key themes on which operational risk teams have heightened their focus, aligned with regulatory expectations.

1. **Embedding operational resilience in firms' broader risk frameworks**

   Operational resilience extends beyond business continuity and disaster recovery. Regulators expect financial institutions to have robust plans in place to deliver essential services in the event of any disruption.

   Regulators define operational resilience as the ability of firms to deliver critical operations through disruptions. On the other hand, operational risk focuses on managing risks resulting from inadequate and failed internal business processes of external events. While operational risk and operational resilience are closely interconnected – both aim to reduce the frequency and manage the impact of operational risk events – operational resilience is an outcome that arises from effective management of operational risk.

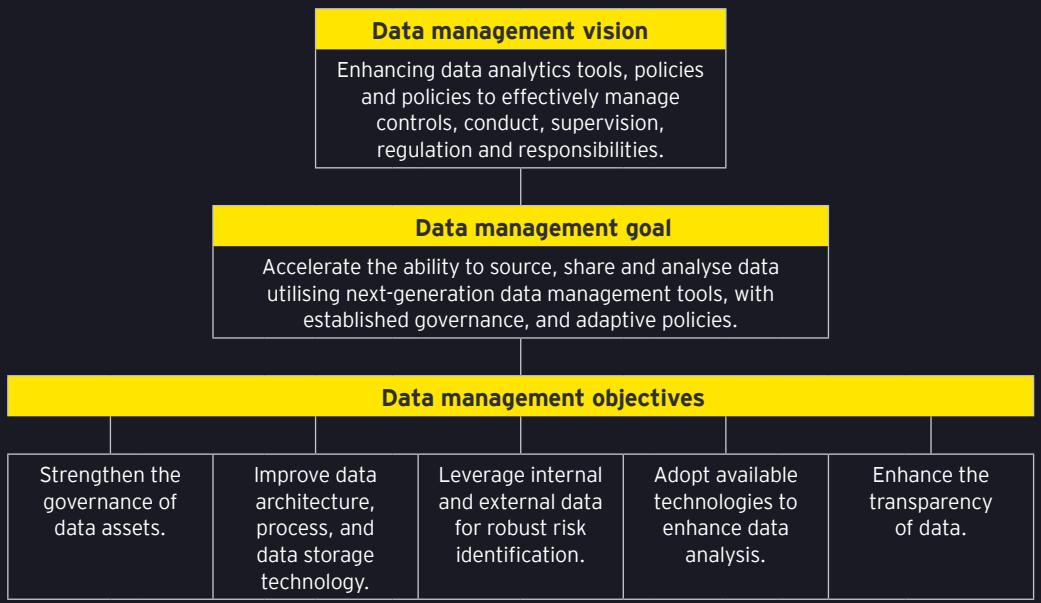
   This overlap between the two concepts produces distinct challenges to many firms' internal frameworks. We have often observed that financial institutions have developed their operational resilience frameworks around the core regulatory requirements, designed and managed in isolation from their wider operational risk management frameworks.

As firms prepare for the next wave of resilience deadlines in 2025, the goal should be to move away from the notion of operational resilience as a standalone project and embed it into the firm's DNA and culture.[13] Proactive integration of operational resilience requirements into firms' operational risk management frameworks will help banks go beyond meeting regulatory expectations to embed resilience into their day-to-day activities and strategy.

2. Utilising data and technology effectively

Modern businesses are inundated with data, yet harnessing this information to manage operational risk remains a significant challenge. Data collection itself presents numerous hurdles because identifying appropriate data sources and verifying the accuracy throughout the data chain are equally persistent challenges. Furthermore, the integration of external loss data to supplement internal loss data requires meticulous attention to detail and a robust data strategy. Penalties associated with poor data quality resulting in inaccurate reporting continue to persist across the banking sector. For example, more than US$100 million in fines as recently as July 2024 constitute a stark reminder of the impact of poor data management.[14]

To overcome these obstacles, we recommend that firms focus on their risk data vision and objectives in relation to the changing risk environment:



13 *UK Finance. (2024).* Operational resilience: compliance dates and new challenges. **Find it here**

14 *Financial Conduct Authority (FCA). (2024).* **2024 fines**.

To effectively manage both known and unknown risks, firms must prioritise their data vision, ensuring that clearly defined goals underpin the business objectives that encompass technology, governance, analytics and reporting ambitions:

- Aligning top-down with business priorities – i.e., business and data strategies
- Managing the data governance and collaboration surrounding people, processes, policies and culture
- Leveraging data for strategic advantages – e.g., business intelligence, analytics, modelling
- Integrating disparate data sources for better planning, security and management of assets, golden sources and metadata
- Replacing siloed applications and point-to-point data access with an integrated platform across the 3LOD
- Bottom-up management of data sources to support better document management, including semi-structured or unstructured data

In addition, we are seeing a heightened regulatory focus on risk data from the Basel committee through the BCBS 239 framework, which was deployed to address many of the challenges firms face in managing operational risk data.[15] The European Central Bank's (ECB) recent guide on Effective Risk Data Aggregation and Reporting states that managing and aggregating risk-related data is an 'essential pre-condition for sound decision-making and strong risk governance'.[16] Furthermore, the guide points out the significant economic benefits of more accurate data, including progress made around digitisation, automation and efficiency, improved risk management and increased revenues from enhanced decision-making.

BCBS 239 compliance continues to be a supervisory priority for the ECB, and it is enhancing its supervisory approach with an increased focus on seven key areas:

i. Responsibilities of the management body
ii. Sufficient scope of application
iii. Effective data governance framework
iv. Integrated data architecture
v. Group-wide data quality and management and standards
vi. Timeliness of internal risk reporting
vii. Effective implementation programs

15 *Bank for International Settlements (2013).* Principles for effective risk data aggregation and risk reporting. **Find it here**

16 *European Central Bank. (2023).* Risk reporting by financial institutions: supervisory expectations. **Find it here**

We note that the ECB refers to an integrated data architecture underpinned by sound IT infrastructure that ensures consistency of data for risk, financial and supervisory reporting, with effective implementation of data quality controls for key risk indicators (KRIs). All of this is expected to be managed by defining and measuring quality indicators covering the entire data lifecycle and reporting risk measurement effectiveness to the management body. Furthermore, this focus on data quality links to resilience, as this factor underpins the ability of firms to manage risk in both business-as-usual (BAU) and through periods of stress based on the quality of their data.

The ECB is committed to improving data quality by driving banks to invest in technology advancements that improve data accuracy, integrity, completeness, timeliness and adaptability for better risk aggregation and supervisory reporting capabilities. Ultimately, good data management and the right technology architecture should facilitate 2LOD's role of providing robust challenge and control mechanisms to ensure that all new systems and tools undergo rigorous scrutiny.

3. **Rethinking risk culture: connecting culture, governance and behaviours**

   Risk culture plays a pivotal role in a firm's ability to manage operational risk and should be coupled with a robust governance approach. Firms must proactively define their risk culture and framework from the outset as part of setting their risk appetite. The ECB considers a well-developed risk appetite framework to be the foundation of a sound governance framework and a strong risk culture.[17] Firms are expected to use their risk appetite framework to guide their risk awareness, drive their risk strategy and reinforce their risk culture.

   We have observed a clear link between risk culture and governance, which is not only in the composition and structure of firms' management bodies but also in the culture that drives the behaviour of their people. Firms striving to improve their risk culture focus on the following:

- **Accountability** — Owning and evaluating risks at the right level and consistently across the 3LOD.
- **Tone from the top** — Improving the capacity to challenge board members on the decisions they make in areas related to risk culture.
- **Capability across the 3LOD** — As the risk environment continues to become more complex, all lines of risk defence need to be upskilled so that responsibility is shared.
- **Regulatory change** — The speed of regulatory change and growing regulatory expectations on culture (e.g., Consumer Duty).

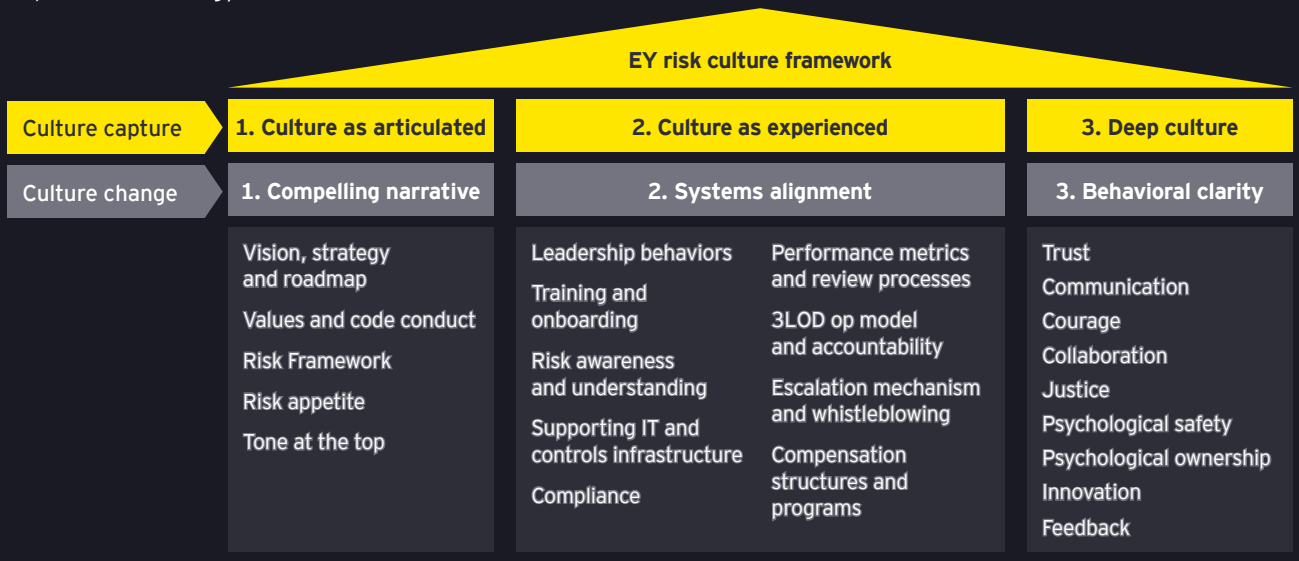
17 *ECB. (2024).* Draft guidance on governance and risk culture. pp. 8-9. **Find it here**

Moreover, instilling risk awareness through targeted training programs that help staff provide a credible, independent view of risk identification can also help cultivate a proactive risk mindset. Banks should consider a constructive challenge culture where employees feel safe to raise their concerns, debate or challenge proposals, and facilitate an enhanced decision-making process that captures diversity of opinion.[18] Training can support individuals in understanding the key behaviours required for an effective risk culture and provide opportunities for them to practice and apply these behaviours in a safe space.

Various cultural drivers, including collective mindset, behaviours and dynamics within teams, can be root causes for specific deficiencies. We have observed the following themes:

Leadership	Organisational structure	Risk management framework (RMF)	Organisational capability	Talent management
▪ Organisations that display a clear tone from the top towards risk management support alignment across departments and model desired behaviours.	▪ Carefully considered risk governance and operating models support delivery of effective governance and risk culture.	▪ RMF embedded in the way the business manages risk to deliver an appropriate gap analysis between current behaviours, regulations, and recommendations.	▪ Leadership builds trust with staff, addresses culture issues quickly and effectively, by learning from past behaviours and addressing root causes of deficiencies.	▪ Employee lifecycle and incentives are aligned with risk appetite and reinforce the delivery of desired behaviours.

For firms seeking to explore these themes, we recommend a wider diagnosis to help create value and propose changes that are aligned with the risk strategy of each firm, using our EY Culture Capture methodology:



18 ECB. (2024). Draft guidance on governance and risk culture. pp. 8-9. **Find it here**

By following this framework, we have helped firms evolve their culture by focusing on aligning leadership around a compelling vision for risk culture change and shifting capability and core behaviours across the 3LOD and identifying gaps in operating environments that prevent positive risk management behaviors.

Being proactive for better outcomes

The evolving nature of operational risk management means that there is a continuous need to maintain a robust set of risk policies, processes and systems that follow the Japanese concept of 'kaizen', translated to 'continuous improvement'. This requires senior management to be willing to be proactive in the face of emerging risks. We observe some examples of proactive risk management steps that will yield better outcomes for firms striving to improve their operational risk management approach:

#	Focus	Proactive risk management	
1	**Strategy and process**	▪ Support business strategy by understanding the bank's operational strengths and weaknesses. ▪ Ensure operational processes not only meet regulatory expectations but achieve competitive advantage. ▪ Design a common risk language and a central risk depository across all business lines. ▪ Establish a consistent process to identify and classify inherent and residual risks that threaten business objectives.	▪ Define, implement, document and monitor controls (preventative, detective, automated) to mitigate risks. ▪ Develop risk mitigation plans that are aligned with business objectives. ▪ Create a forward-looking process to proactively respond to emerging risks. ▪ Embed a cost-benefit approach to risk mitigation and controls to gain management buy-in.
2	**Organisation and governance**	▪ Establish effective risk governance with clear accountabilities, roles and ownership of operational risk. ▪ Develop a transparent risk culture that embeds risk management at every level of the organisation through risk reporting, with active debate and challenge around risk. ▪ Define the nature and level of risk that is acceptable to set boundaries and expectations for business activities. ▪ Document and communicate clear policies regarding risk, especially risk appetite, for each business line.	▪ Utilise both internal and external auditors to provide independent assurance on risk governance and risk management. ▪ Incentivise behaviors, rewarding good risk management and discouraging risky behaviours that exceed risk appetite. ▪ Establish a decision-making framework that ensures an appropriate balance between risk and reward.

#	Focus	Proactive risk management	
3	**Artificial Intelligence (AI)**	▪ Transform the operating model through the use of AI, balancing the risks and rewards of AI adoption while considering the lawful, ethical and robustness of the governing AI principles. ▪ Consider the necessary processes, procedures and enablement of operational risk management to deploy GenAI models.	▪ Re-engineer existing functions around people, roles and skills required to successfully adopt GenAI capabilities. ▪ Prototype, build and scale use cases into production environments. ▪ Collaborate, with the support of FinTech, to experiment and co-innovate.
4	**Data management**	▪ Report required data at an effective frequency. ▪ Ensure the integrity of data and validate against KRIs and business loss events. ▪ Unravel the complex data lineage between legacy internal systems and create the 'lineage by design' governance structures to retain control over the data.	▪ Add context to monitoring data to gain a better understanding of the state of the business. ▪ Create data quality processes that not only monitor and validate quality but enhance it on an ongoing basis using automation tools.
5	**Risk analytics and reporting**	▪ Define and clearly communicate the operational risk appetite to each business line. ▪ Compare the firm's risk appetite with residual risk levels by utilising business metrics and MI solutions. ▪ Compare the frequency of actual risk loss events with the residual risk profile developed by the Risk Control Self-Assessment (RCSA).	▪ Conduct root cause analysis to provide valuable information on observed risks and drivers. ▪ Create a multi-tiered risk reporting structure that aggregates risks upwards to provide an accurate sense of proportion in the context in which it is viewed. ▪ Define tolerances for KRIs and Key Control Indicators to encourage timely management intervention and action to avert emerging issues.
6	**Training**	▪ Continuously evaluate competence through capability assessments to identify 'people hot spots' and provide targeted training interventions. ▪ Create blended pathways of training content to enhance current and future risk management skills.	▪ Define and address organisational barriers and blockers to change. ▪ Create a compelling risk culture narrative that is consistently and programmatically embedded through the organisation.

Preparing for the unavoidable

The only real mistake is the one from which we learn nothing. Thus, when controlling risks brought about by technological advancements, the ever-evolving geopolitical climate and regulatory expectations, financial institutions should learn from the past and construct their roadmap to navigate the path from compliance to value creation. We recommend that banks start with a clear vision of five steps:

1. **Ensure operational risk management is an integral part of the risk oversight structure and risk processes.** This promotes a healthy linkage between good risk management and successful value creation. Senior executives must be clear on what they want to achieve by expanding their operational risk management capabilities, as this greatly increases the chances of long-term success. After solidifying this position, it is important for the company to choose the operational risks to be assessed.
2. **Utilise technological advancements to support change.** Operational risk management solutions are advancing at an accelerated pace, with many vendors competing to provide tailored solutions for banks and financial institutions. Such technology can provide significant competitive advantages to companies that implement it effectively. At the centre of this, and imperative to its success, lies the need to capture and aggregate high-quality operational risk data.
3. **Implement a consistent data strategy to monitor and report risks.** Internal functions need to align on the necessary data sources, methodology and metrics to monitor operational risks and drive effective reporting. Firms must move beyond the siloed approach to managing operational risk by promoting strategic objectives aligned across their different functions. This enables firms to assess their firm-wide exposures to risk and incorporate KRIs effectively.
4. **Leverage quantitative and qualitative methodologies to strengthen risk frameworks and governance.** Even with the challenges associated with quantifying operational risks, companies should strive to sharpen their view on their risk measurement, risk modelling, risk maturity assessment, risk mapping, risk prioritisation, scenario modelling and stress testing capabilities to truly extract the value of a robust risk framework. Furthermore, with the rising risk from large-scale transformation programs, companies should implement scalable frameworks that ensure integrated collaboration between control functions to promote successful, sustainable and timely change delivery.
5. **Establish a strong risk culture.** Successful management of operational risk is contingent on a strong risk culture. The motivation to achieve strong returns should be carefully balanced with good behaviors and conduct to protect clients' interests. Companies should promote restraint from rule violations and instead focus on reducing material risk exposures. Risk-taking should be centralised, top-down and diligently managed to ensure investment rewards outweigh the risks.

Closing remarks

Understanding the focus areas discussed in this article can help banks identify risks, spot trends and act accordingly. Senior risk leaders must be able to gain insights into why operational risk events occur and how to determine the necessary call to action. To do this successfully, we have shown how important resilience is, and its frameworks should be given a focus as regulatory expectations persist and more disruptive events unfold in the markets.

Moreover, the value derived from proficient use of data and technology will offer many firms the clarity and precision required for better data-driven decision-making. Banks can supercharge their risk teams to become more effective when coupled with the right culture and behaviours. Ultimately, we recommend that firms use the above insights to build a solid foundation that enables better operational risk management in these uncertain times to ensure compliance with new regulations, emerging risks and strategic objectives that heighten operational risk.

Author
Dr Alfie Lindsey

Contributors
Veneta Tuleva-Karasavova
Soofia Noor
Kieran Gehlan
Cansu Yurdakul
Kyoko Oishi

Acknowledgements
Special thanks to Savvas Koufou and Edward Morgan for their key industry insights, as well as Kyle Osborne, Soumaya Bidah and Guy Fleming for supporting the editorial process.

Contact us

Dr Alfie Lindsey
Director, UK Operational Risk Leader, Banking & Capital Markets
Ernst & Young LLP
alfie.lindsey@uk.ey.com
+ **44 207 785 8881**

Tim Hill
Partner, UK Operational Risk Leader, Banking & Capital Markets
Ernst & Young LLP
thill3@uk.ey.com
+ **44 207 785 8881**

Amy Hallett
Partner, EY UK Risk Consulting, Banking & Capital Markets
Ernst & Young LLP
ahallett1@uk.ey.com
+ **44 207 951 1374**

David Storey
Partner, UK People Consulting
Ernst & Young LLP
dstorey@uk.ey.com
+ **44 20 7806 9375**

Chris Richardson
Partner, EY UK Head of UKFS Risk Consulting
Ernst & Young LLP
crichardson4@uk.ey.com
+ **44 207 951 1012**

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

Ernst & Young LLP
The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.

EYG no. 011100-24Gbl
UKC-037139.indd 01/25. Artwork by Creative UK.
ED None

ey.com