Deloitte.

2025

# The risk transformation challenge:
# Building strategic advantage and resilience

A look into risk management practices across Nordic organisations.

# Foreword

On behalf of Deloitte, we are pleased to present the findings of our survey on risk management and resilience practices across Nordic organisations (excluding the financial services and public sectors). This report offers valuable insights regarding how companies in the region are navigating an increasingly complex risk landscape marked by technological disruption, geopolitical uncertainty, and evolving stakeholder expectations. We extend our sincere gratitude to the 52 organisations that contributed their perspectives, providing the foundation for this comprehensive analysis. In this report, we share their aggregated perspectives.

Our survey highlights both progress and persistent challenges in elevating risk management from a control-focused discipline to a strategic enabler of business resilience and value creation. While many organisations demonstrate confidence in their current risk capabilities, gaps remain in areas such as integrating with core business processes, achieving strategic alignment, enhancing emerging risk identification, and the adoption of advanced technologies like generative AI.

At Deloitte, we believe that effective risk management is essential for organisations to thrive amid uncertainty. By embracing a holistic approach that combines strong governance and tone from the top, a proactive risk culture, and innovative tools, companies can transform risk into a source of competitive advantage. Through active use of scenario modelling and cutting-edge AI tools, underpinned by comprehensive and accurate risk data, organisations can build strategic foresight. This report aims to support Nordic organisations on that journey by sharing insights, identifying common challenges, and highlighting opportunities for strengthening risk practices.

We hope the findings and perspectives presented here provide useful guidance for risk practitioners, business leaders, and boards seeking to enhance their organisation's resilience and strategic agility in a rapidly changing environment.


**Lasse Ingström**
**Partner**
Enterprise Risk lead
Deloitte Global

**Tom Clifford**
**Partner**
Regulatory, Risk & Forensic lead
Deloitte North South Europe

**Elisabeth Egdetveit**
**Director**
Risk Management lead
Deloitte Nordics


November 2025

# Executive summary

# Executive summary

**Nordic organizations face an unprecedented convergence of challenges:** rapid technological disruption, geopolitical volatility, escalating operational costs, and increasingly intricate supply chains. This dynamic environment demands that leadership teams take a fundamental look at the risk management domain, which often needs to evolve from a defensive discipline focused on threat mitigation to a strategic enabler that transforms uncertainty into competitive advantage, empowering organisations to accelerate innovation and capitalise on emerging opportunities.

This shift rings true across all organisations. However, the existing degree of risk management maturity provides organisations with different starting points on the transformational journey. Within the Nordic region, we observe that the financial services sector generally tends to have in place more advanced risk management tools and processes, driven by a current and historically strong regulatory push. Given its unique external drivers, this sector is not part of the analysis discussed within this report. This survey has collected responses from organisations within the consumer, retail and manufacturing sector, the technology, media and telecom sector and the energy, resources and industrials sector.

Our survey finds that organisations have built positive core capabilities within risk management, implementing regular processes for risk identification and assessment, establishing key interaction points with executive leadership teams and boards (including for strategic planning, business continuity management and periodic business reviews), and displaying sound awareness of the skills required to continue to address the evolving risk landscape. However, we also observe integration gaps when it comes to the ability of firms to elevate risk management to the position of a strategic capability which can enable and drive agile decision-making and comprehensive organisational resilience.

# Executive summary

**Our report discusses these elements across six areas:**

**1. Risk governance and culture** – despite risk cultures improving over the last three years, risk practitioners are concerned that there exists inadequate ownership of risks within their organisations, often coupled with insufficient understanding and engagement from executive and board stakeholders.

**2. Strategic partnering** – risk functions across Nordic organisations have a clear vision of becoming a strategic partner to the business, a narrative often harder to build from an organisational position within a CFO domain often associated with a business controlling objective. Whilst recognising the need to align risk processes to strategic objectives, key enabling tools such as risk appetite frameworks and scenario planning capabilities remain underutilised by organisations and risk practitioners. This is compounded by a near-exclusive focus on threat mitigation, displaying significant potential for firms to focus and capitalise on active opportunity management.

**3. Strengthening skills and perceptions** – risk practitioners recognise the need to develop skills and capabilities to leverage artificial intelligence, enterprise level analytics and risk modelling to be prepared to tackle the evolving risk landscape, for example driven by geopolitical risks. Whilst a focus on strong technical skills is important to distil and understand key risks, practitioners appear to underplay the significance of softer skills like stakeholder management and business understanding. The survey highlights a clear need for risk practitioners to build increased organisational awareness of the value-add components of effective risk management (shifting from risk activities being perceived as a compliance exercise), in which developing strong internal networks and storytelling capabilities will be key enablers.

**4. Risk outlook** – strategic risk is consistently perceived to be at the forefront of boards minds, followed by a focus on financial risks to ensure sound and profitable operations in an uncertain environment. Our survey show that risk practitioners expect geopolitical risks to rise in prominence across all organisations in the next three years, a significant change from a more disparate view of priorities today. Cybersecurity and digital risks remain among organisations top concerns in the future, reflecting an expectation that digital threats will intensify rather than stabilise in the coming years.

**5. Building resilience** – Nordic organisations inhabit a cyber-centric view of resilience with a focus on traditional methods such as business impact analyses, diversifying supply chains, and risk assessment forming resilience strategies and practices. With few resilience programs focussing on the holistic threat landscape spanning beyond cyber-risks, organisations remain exposed to localised disruptions (e.g. from operational and fraud risks) and systemic disruptions beyond their preparedness scope.

**6. Technology** – the majority of Nordic organisations leverage GRC systems to enable oversight and risk management activities. System use remains focussed on the core capabilities of risk identification, measurement and monitoring. Our survey shows limited progress on building use cases for advanced analytics and GenAI deployment within the risk function and broader business processes, offering an opportunity for risk practitioners to explore the benefits of wider technology adoption.

Overall, our survey reinforces that whilst progress has been made, the majority of risk practitioners see significant opportunities to enhance businesses and create value by further maturing the risk management capabilities, to ensure strategic business resilience for Nordic organisation in an uncertain world.

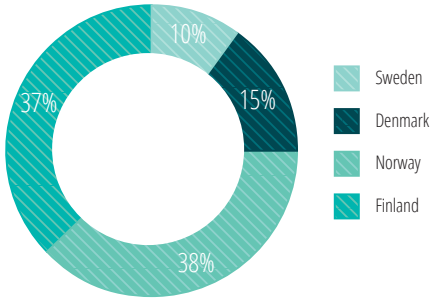
# About the survey

# About the survey

Our survey collected insights on risk management and resilience practices across 52 large organisations in the Nordic region. It was carried out between May to August 2025.

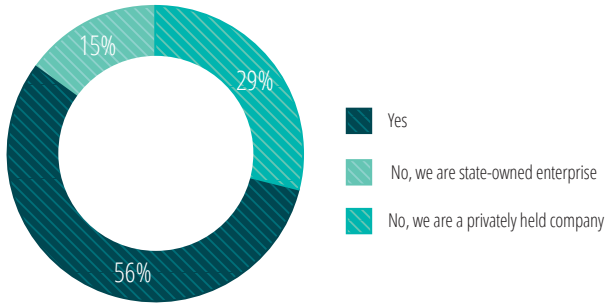
From the responding organisations, approximately equal numbers are headquartered in Norway and Finland, whilst Swedish and Danish organisations together make up 25% of the respondent population. The majority of organisations are publicly listed.

**Figure 1. Country of organisations headquarter**




Q: In which country is your organisation headquartered? N=52

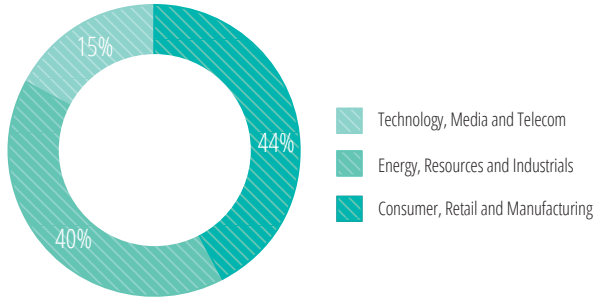
**Figure 2. Ownership structure**




Q: Is your organisation publicly listed? N=52

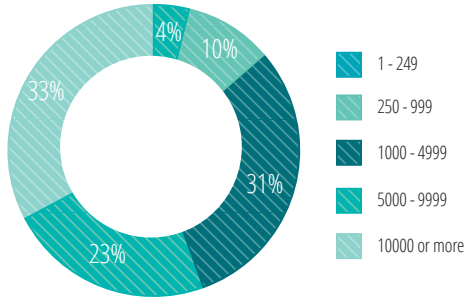
The surveyed organisations comprise firms which operate within the Consumer, Retail & Manufacturing (CRM), Technology, Media & Telecom (TMT), and Energy, Resources & Industrials (ER&I) sectors. The vast majority have a large workforce, with 56% of respondents having over 5,000 employees.

**Figure 3. Sector split for responding organisations**




Q: What is the primary industry of your organisation? N=52

**Figure 4. Number of employees within responding organisations**

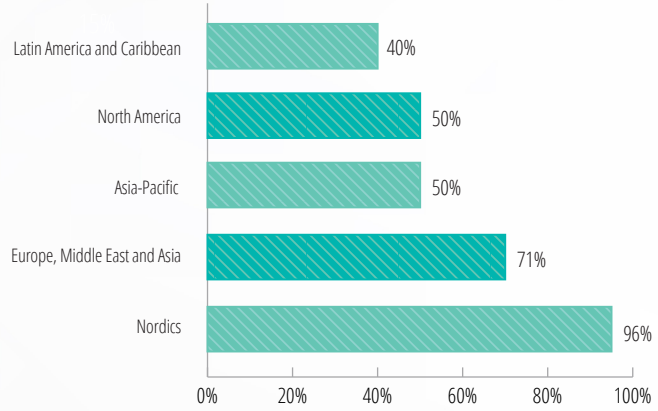



Q: How many employees are currently part of your organisation? N=52

# About the survey

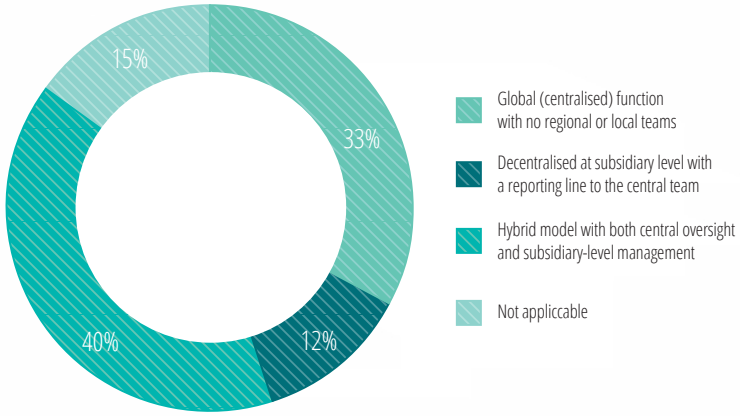
A significant number of the surveyed organisations operate cross-boarders, with as much as 71% having a presence in the EMEA region. Nearly half of organisations also have a presence in the remaining global regions; APAC, North America and Latin America. For risk practitioners managing multiple legal entities and countries of operation, both hybrid and centralised model of risk oversight are applied, with a slight lean towards the former.

**Figure 5. Regions with operations**




Q: In which region does your organisation operate? Select all that apply. N=52

**Figure 6. Structure of risk management oversight**




Q: If your organisation comprises multiple legal entities, how is the Risk function structures across the parent company and its subsidiaries? N=52

# Risk governance and culture

# Risk governance and culture

Effective governance and culture are fundamental to achieving and embedding risk management practices successfully. In an environment of rapid change, organisations need to empower individuals at all levels to understand, own, and proactively manage risk. Despite respondents reporting progress in this area, many organisations continue to face fundamental gaps in board engagement and risk ownership. Moreover, inadequate monitoring systems, insufficient training programmes and ineffective mechanisms to assess root causes hinder the development of genuinely proactive risk cultures.

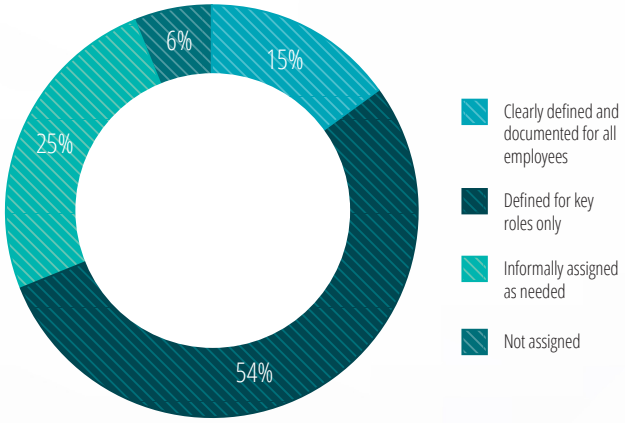
### Traditional organisation demands strong escalation mechanisms

Our survey shows that 62% of respondents position their risk function under the Chief Financial Officer (CFO), with only one respondent having established a dedicated Chief Risk Officer (CRO) role. While situating the risk function within the CFO's domain may enhance alignment between risk and financial processes, we observe that firms seeking to shift from risk control to strategic risk management increasingly locate the risk function under Heads of Strategy or the CEOs office. However, positioning risk functions under first-line leadership requires robust mechanisms that empower risk teams to escalate issues directly to the board, particularly when such issues may conflict with established financial objectives or business strategies.

### Limited formal ownership

For risk to be an integrated part of strategic and operational business decision making, it is imperative that all employees understand their role within the risk management lifecycle. Our survey shows that establishing risk ownership within the first line is a challenge for a significant portion of respondents, with 46% citing poor or limited levels of accountability within their organisation. This is compounded by a significant variation in the degree to which formalised responsibility for risk exists, with only 15% of respondents having implemented structured accountability across the employee population.

**Figure 7. Assignment of risk responsibilities in the organisation**




Q: How are risk management responsibilities assigned within your organisation?
Nordic Managing Risks Survey, N=52.

# Risk governance and culture

### Furthering a risk-conscious culture

The powerful benefits of establishing and embedding an effective risk culture[1] has gained increasing recognition, with risk management professionals needing to command a strong voice within organisations. According to our survey, 69% of respondents report improvements in risk culture over the past three years, with 63% rating the current risk culture at or above adequate. Some sector variances emerge, with ER&I demonstrating the highest confidence in current risk culture (with 76% describing it as adequate or strong), whilst 63% of respondents within TMT say their risk culture remains under development.

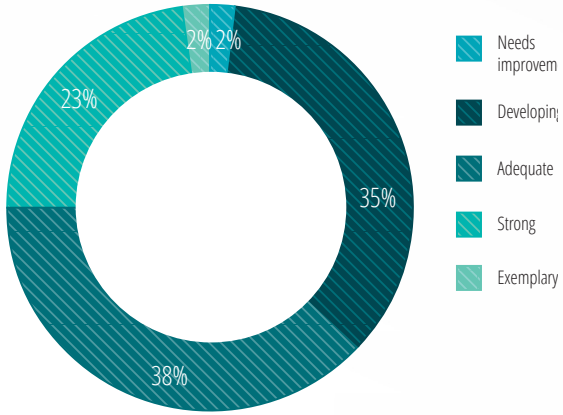
If successful in building a strong risk culture, organisations can capitalise on employees that shift from displaying reactive to proactive behaviours, for example, enabling early trend detection and timely mitigation of potential threats. In our experience, achieving a strong risk culture is dependent on commitment from senior leadership – particularly in the first line – with the tone from the top consistently showcasing role model behaviours and competences related to risk awareness and broader risk management.

"Risk culture isn't just important, it's the difference between organisations that excel amid relentless change and evolving risk profiles and those that collapse under the weight of poor decision-making."

However, maintaining and developing risk awareness and consistent behaviours require continuous attention. Our survey shows that less than 30% of respondents undertake regular risk awareness training for employees, which compromises the organisation's ability to sustain effective risk management as a shared value.

Our survey found that 65% of respondents do not formally measure risk culture. While traditional approaches, such as surveys or specific indicators, offer useful initial insights into cultural developments, they rarely capture the underlying behaviours or root causes when used in isolation. Fewer than 10% of respondents employ a multi-method approach, typically combining surveys with audits or white book exercises. We encourage Nordic firms to adopt these emerging best practices by exploring additional tools such as leader labs, focus groups, or behavioural analytics to gain a deeper understanding of the risk culture and where improvements might be needed.

**Figure 8. Contents in board risk reports**

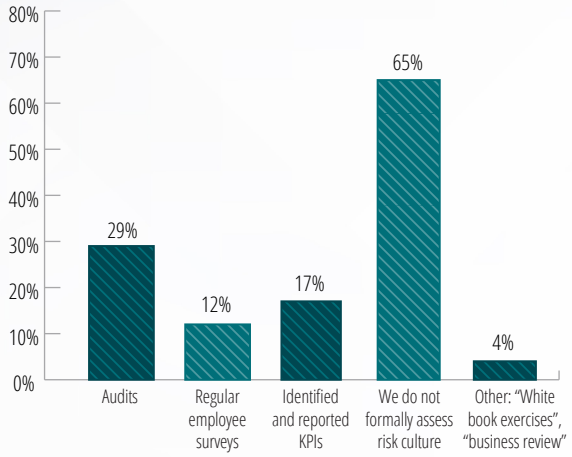



Q: How would you rate the overall risk culture in our organisation?
Nordic Managing Risks Survey, N=52.

[1] Risk culture refers to a culture where individuals understand the organisation's approach to risk management, take personal responsibility for managing risk, and encourage others to do the same. It's characterised by open communication, a shared understanding of risk, continuous improvement, and the integration of risk considerations into all activities.

# Risk governance and culture

**Figure 9. Assessing the strength of risk culture**




Q: How is risk culture measured and assessed? Select all that apply.
Nordic Managing Risks Survey, N=52.

### Board engagement through the eyes of the risk practitioners

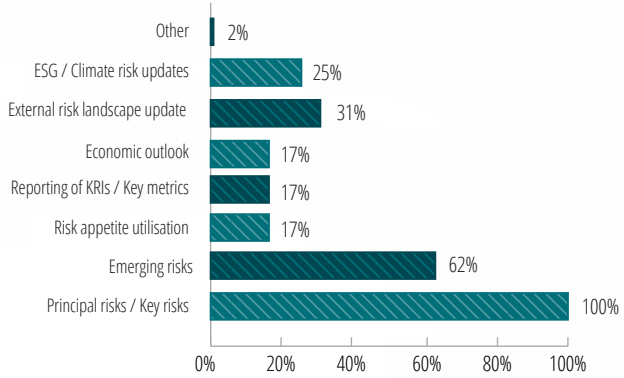
The board is a critical enabler for ensuring that strategic objectives are based on a clear understanding of underlying risk drivers and emerging trends. However, our survey reveals concerns among risk leaders, with only 17% perceiving their boards as being fully engaged (and 42% perceiving their boards as only partially or minimally engaged) in the oversight of risk management. To drive leadership engagement, Nordic risk functions primarily involve their boards through formal risk profile and strategy reviews, alongside ongoing reporting. The most common frequency of formal board engagement is semi-annually or quarterly. This corresponds to risk reporting practices, where 38% of firms produce quarterly risk reports and 35% produce semi-annual reports, while 21% do so only annually. To enable board members to effectively oversee risk, it is essential to provide tailored, familiar, and regular information that fosters contextual understanding and sustained engagement.

50% of respondents cite lack of engagement and understanding by stakeholders as a key obstacle to effective risk reporting.

Boards and senior management need to see relevant information to make decision making, understand the risk profile and assess the potential impacts of relevant scenarios for their firm.

When generating risk reports, respondents focus on the status of principal risks, with 62% including insights on emerging risks. Sectoral differences emerge, with respondents from ER&I tending to also incorporate risk appetite and climate risk, whereas risk reporting within the respondents

**Figure 10. Contents in board risk reports**




Q: Which topics are typically addressed in board-level risk management reporting?
Select all that apply. Nordic Managing Risks Survey, N=52.

from the TMT sector placing greater emphasis on the external risk landscape. One-sided risk reporting and perceived limited board engagement provides an opportunity for risk functions and professionals to reassess and enhance how risk information is communicated, utilised and used as a basis for decision-making by the board. In our experience, limited engagement often comes as a consequence of one or more of the following:

- Boards historically not understanding the value from risk reporting and discussions, with detailed reporting on operational-level risks and controls not serving the broader board agenda.

# Risk governance and culture

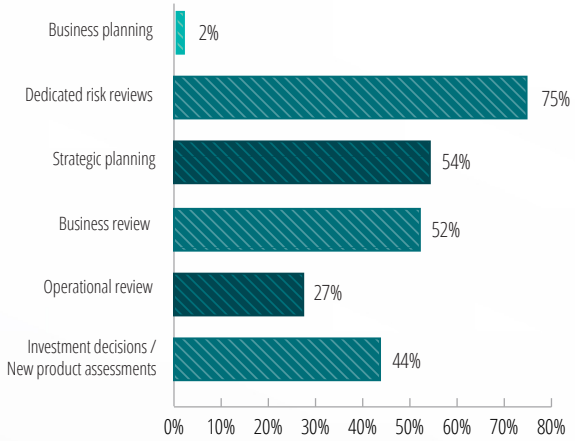
- Risk information often lacking sufficient degrees of external market data to provide context and perspectives to internally observed data points and developments.
- Increasingly complex risk environments and risk transmission mechanisms driving up the level and depth of risk knowledge required by board members, plus reporting from risk professionals to be more accessible, in order to move from passive oversight to informed strategic decision making.
- Data presented is often qualitative and subjective, making it a difficult basis for steering decision-making, with work needed to better quantify financial and non-financial risks in relevant scenarios, supported by the appropriate data quality to enable trusted, deeper insights.

We observe that risk practitioners who actively challenge board members to articulate their specific information needs, provide training and upskilling in technical risk areas, and who contextualise risk data within relevant business scenarios, are better positioned to foster meaningful dialogue and enhance the effectiveness of strategic risk oversight.

## Executive engagement

Within responding organisations, executive management engages with risk through multiple operational processes and activities, with risk reviews being the most utilised forum. Over half of respondents incorporate risk considerations into strategic planning discussions, investment decisions and product approvals, with the ER&I sector leading the way.

**Figure 11. Venues of risk involvement**




Q: In what context is risk management typically discussed on a C-suite or executive level? Select all that apply. Nordic Managing Risks Survey, N=52

Despite integrating risk management considerations into these processes, the ongoing assessment and awareness of risk developments mirror the challenges observed at board level. Although executive management are the primary recipients of risk reports, reporting frequency is limited and risk practitioners continue to face lack of engagement and understanding.

Enhancing risk culture and leadership engagement requires continuous effort, but in a rapidly changing environment, an organisation which displays a proactive approach and understanding of risk will have greater capacity to make informed decisions grounded in risk-reward analysis. Moving towards objective-centred risk management will enable risk practitioners to unite business functions behind risks. Ultimately, risk management is not the sole responsibility of a dedicated function - it is everyone's job, requiring engagement and accountability at all levels to be truly effective.

# Strategic partnering

# Strategic partnering

Nordic risk functions are increasingly aspiring to become strategic business partners, shifting their focus from traditional risk prevention to value creation. In this transition, risk practitioners are having to overcome challenges of resource constraints, limited integration with broader business processes, and limited adoption of stress-testing and risk appetite frameworks.

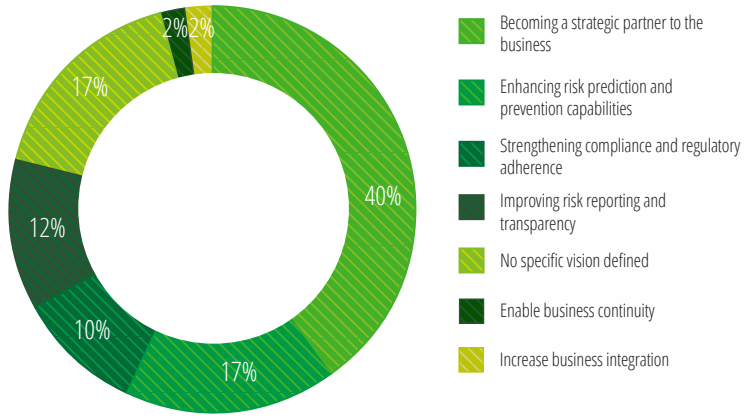
**A vision of partnership**

Risk management leaders in Nordic organisations increasingly envision their risk functions as strategic partners to the business, with 38% of respondents identifying this as the primary vision for the function over the next five years, surpassing more traditional objectives such as enhancing risk prediction and prevention (17%). This reflects a growing recognition of the potential of effective risk management to drive value creation and support business success, moving beyond the conventional focus on risk mitigation alone.

"Risk should be fully integrated into all aspects of the business" - Survey respondent

However, 17% of respondents do not have an articulated vision, which may undermine their future ability to advocate for investments or funding needs. Developing and clearly communicating a functional strategy to key stakeholders offers risk functions the opportunity to position themselves as strategic partners who provide critical decision-support.

**Figure 12. Vision for risk functions in the next 5 years**




Q: What is the primary vision for the Risk function in your organisation over the next 5 years?
Nordic Managing Risks Survey, N=52

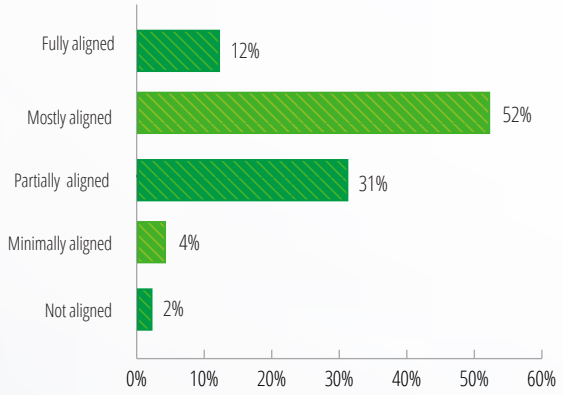
# Strategic partnering

## Establishing required links to business strategy

The shift towards strategic partnership requires direct links between risk and strategy processes, both in annual planning and ongoing assessments. Objective-based views of risk developments within current priorities needs to be coupled with analysis of trends and emerging risks which could threaten the validity of strategic choices in its entirety. Encouragingly, our survey finds that more than half of respondents consider their risk management objectives as being mostly or fully aligned to strategic objectives. This is primarily achieved through integrating risk review exercises with strategic planning processes – an approach adopted by 79% of respondents.

However, significant gaps remain in advancing from alignment to embeddedness. Nordic organisations show a low degree of maturity in leveraging key tools which could drive further integration, such as stress testing and risk appetite frameworks, and modelling upside as well as downside risks.

**Figure 13. Alignment to strategic objectives**

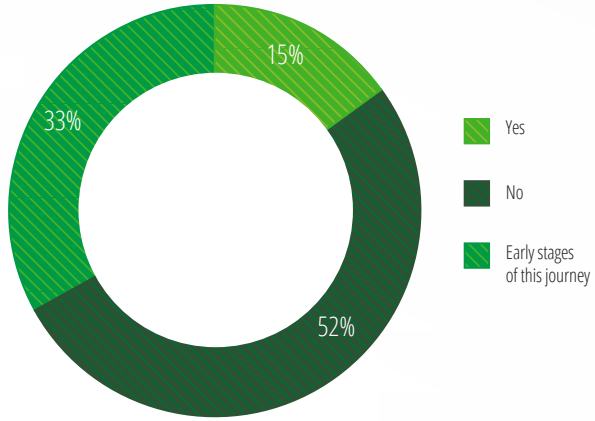



Q: How would you rate the alignment of risk management objectives with the organisation's strategic objectives? Nordic Managing Risks Survey, N=52

## Stress testing

Half of surveyed risk practitioners do not undertake stress-testing of their organisations' strategic assumptions, with 33% stating they are in the early stages of developing such capability.
This deficiency persists across industries, company sizes and countries. Using stress testing- and scenario analysis to understand strategic and operational resiliency is instrumental in today's business environment where past assumptions frequently no longer hold true. With the identification of risk drivers that could emerge in the future and the possible associated outcomes on business operations, boards and executive management can confidently validate all major strategic decisions.

**Figure 14. Use of stress-testing on strategic assumptions**




Q: Have you stress-tested the underlying assumptions of your organisation's strategy to help you identify risks or threats to achieving your strategy? Nordic Managing Risks Survey, N=52

# Strategic partnering

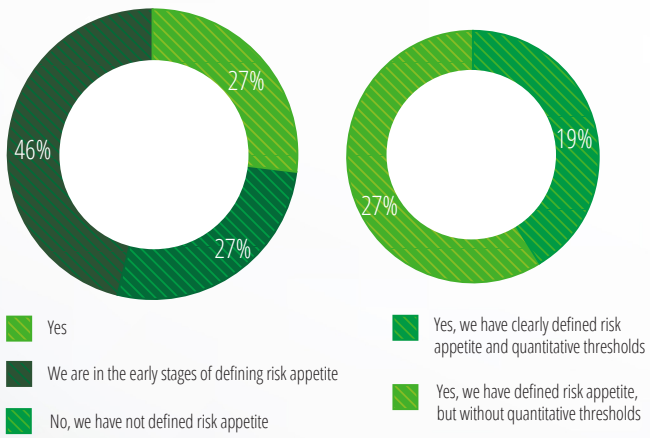
## Risk appetite

Our survey shows that over half of respondents make little or no use of risk appetite frameworks to align risk-taking with business priorities, with only 19% applying risk appetite statements with quantitative limits. For those that operate with defined risk appetite statements, only 45% leverage it in business planning.

Getting these practices right is no doubt a challenge. Firms and risk functions that succeed enable their organisation to prioritise resources towards key objectives while providing transparency and clarity to stakeholders regarding how acceptable current and future risk levels are. Our survey indicated that Nordic risk practitioners have a particularly large barrier to cross, with 68% emphasising the ability to establish a clear understanding within the business as their key obstacle in operationalising risk appetite.

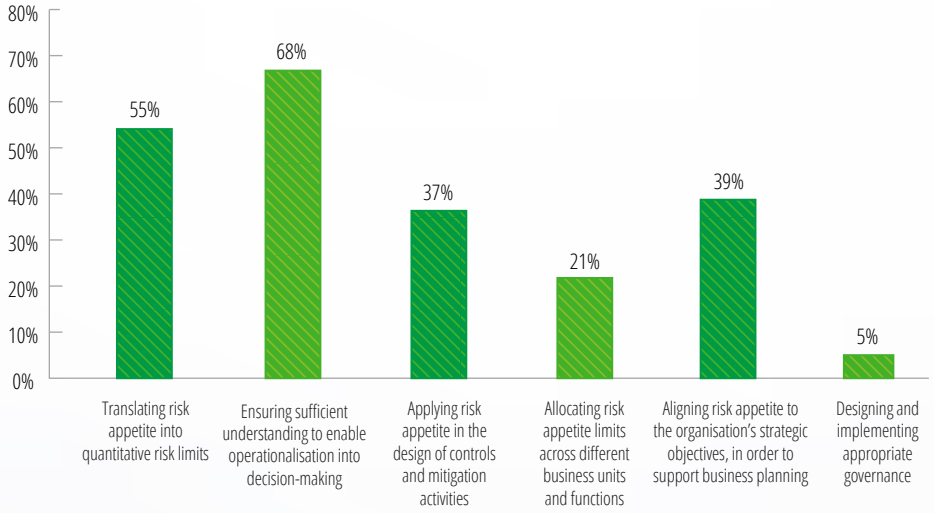
"Defining risk appetite is the hardest piece of the puzzle when implementing risk management. But without those clear boundaries you can actually measure, your entire risk framework grinds to a halt."

**Figure 15. Maturity of risk appetite statements**




Q: Has your organisation defined its risk appetite along with associated quantitative thresholds? Nordic Managing Risks Survey, N=52

**Figure 16. Firms with defined risk appetite and their challenges to operationalising it**



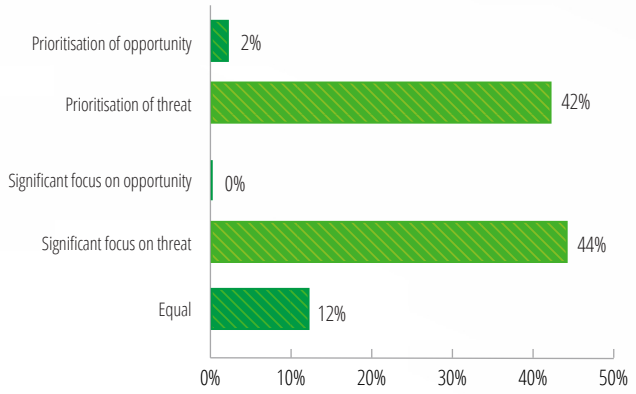

Q: What are some of the specific challenges faced by your organisation when operationalising risk appetite? Select all that apply. Nordic Managing Risks Survey, N=38

# Strategic partnering

## Opportunity management

Risk management practices in Nordic organisations remain predominantly focused on downside protection, with the identification and capture of upside opportunities being notably uncommon. Only a small minority of respondents indicate that their risk management processes actively address both risk and opportunity management. The narrow focus on threat mitigation limits the potential for risk management to contribute to competitive advantage – highlighting a significant opportunity for Nordic organisations to enhance their capabilities. Cultivating horizon scanning and scenario analysis capabilities enables organisations to gain earlier visibility into emerging opportunities and generates the critical lead time necessary to evaluate and exploit them strategically.

**Figure 17. Focus on opportunity versus threat management**




Q: What is the current split of activity performed by your function between opportunity management and threat management? Nordic Managing Risks Survey, N=52

# Strengthening skills and perceptions

# Strengthening skills and perceptions

For risk practitioners to effectively assess and manage the risk landscape, close cooperation with stakeholders across the organisation is vital. Our survey shows there are strong incentives for Nordic organisations to further the integration of risk with other business functions and transformation programmes, in order to build more sophisticated and integrated processes which capture and analyse novel and emerging risks, plus integrate traditional risk management more effectively.

**Building bridges to the organisation**

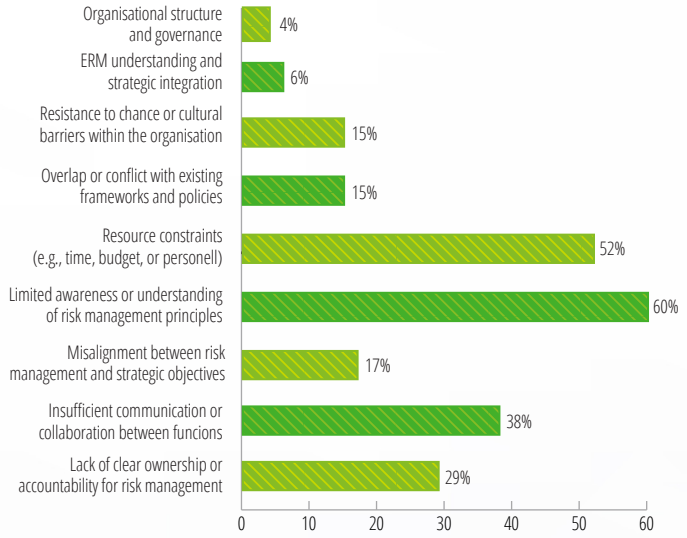
Nordic risk practitioners indicate a limited degree of integration between risk management and broader management capabilities , including compliance frameworks and quality programs. Whilst risk practitioners acknowledge the importance of linking risk management to wider business processes, further work is needed to articulate the practical benefits of integration: more effective oversight, improved data quality and the ability to leverage synergies across functions for greater efficiency and insight.

The key barrier identified is the existence of limited awareness or understanding of risk management principles within the broader organisation. This is closely followed by resource constraints related to time, budget, personnel, and insufficient communication. These challenges are consistently reported across industries, company sizes, and countries, ranking among the top three barriers in all respondent groups.

"ERM is seen as a box-ticking exercise instead of a tool to drive and manage strategic objectives." – Survey respondent

The identified barriers to integration are compounded by an underlying perception of risk management as a driver of compliance exercises. Consequently, the risk functions potential as a strategic partner remains insufficiently recognised beyond the risk management teams themselves.

**Figure 18. Challenges to integration**




Q: What are the main challenges, if any, to integrating risk management with other management functions in our organisation? Select all that apply. Nordic Managing Risks Survey, N=52

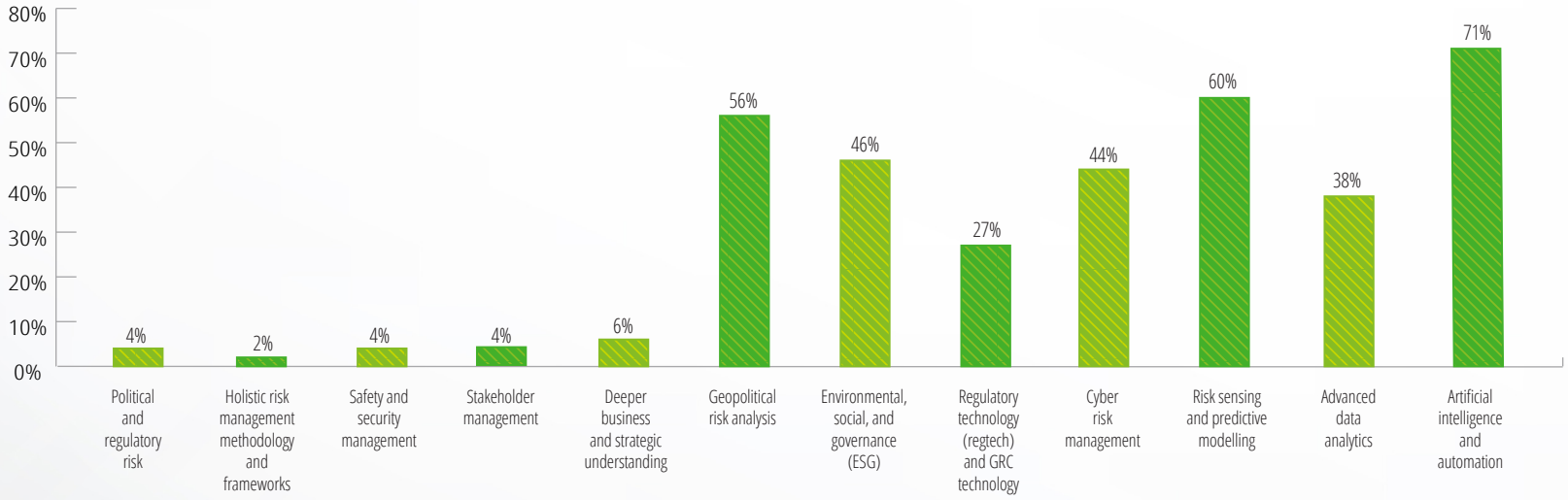
# Strengthening skills and perceptions

## Capabilities for the future

Although the need to build internal awareness and communication is recognised among risk practitioners, core technical skills are prioritised when assessing future capability needs. Survey respondents highlight a broad set of skills will be required to succeed in the future, with artificial intelligence, risk sensing and geopolitical risk analysis as the top priorities. Collectively, these skill areas signal a shift towards a more forward-looking, data-driven, and contextually aware approach to risk management – capabilities that are vital for supporting informed decision-making and strengthening organisational resilience. Leveraging analytics and AI-driven risk identification tools serves a dual purpose in also enabling empowerment of the first line in risk management through facilitating easier, self-driven access to risk insights.

Whilst priorities are largely consistent across sectors, continuing to build capability in cyber risk management remains a prominent focus for the TMT sector (ranking 2nd), whilst the ER&I sector highlights risk sensing and geopolitical analysis as priorities ahead of AI risk management. For the Consumer sector, priorities are to ensure the skills are in place to form an aggregated view.

**Figure 19. Skill requirements for the next 5 years**




Q: Which emerging skills do you believe will be essential for risk management professionals in the next 5 years? Select all that apply. Nordic Managing Risks Survey, N=52

# Strengthening skills and perceptions

### Risk identification at a crossroads

Underpinning the development of risk practitioners' technical skills lies the ability to effectively detect and identify risks on an ongoing basis. Symptomatic of increasing external changes, 54% of organisations are actively developing processes to identify and monitor emerging and novel risks, yet fewer than 16% extensively utilise horizon scanning techniques. The ER&I sector stands out as more mature, with 67% of respondents actively monitoring emerging risks.

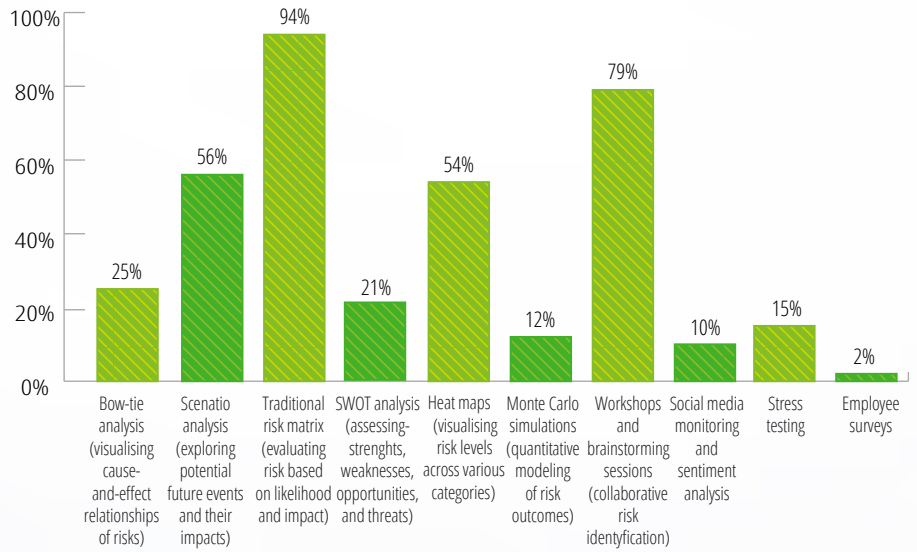
Nearly half of the organisations surveyed have implemented defined trigger points that prompt out-of-cycle risk identification activities. These triggers cover a broad range of internal and external factors, including regulatory changes, significant market fluctuations, geopolitical events such as conflicts and tariffs, executive leadership inquiries, internal incidents, revised business strategies and plans, or large new investments and projects. The variety of trigger mechanisms employed shows that organisations increasingly recognise the importance of systematic prompts that enhance their risk identification capabilities.

"The trigger system is essential because it stops us from overlooking risks. We track external events and collaborate with teams like Public Affairs and Group Communications. And where we've done scenario planning, we'll often set up dedicated triggers for those specific areas." – Survey respondent

Nordic organisations heavily rely on traditional methodologies for risk identification and assessment, with risk matrices and workshop sessions forming the foundation of their approach across the region. These conventional tools provide a structured framework that supports systematic risk evaluation and management. Scenario explorations and heat maps complement these primary tools, though their adoption remains more selective.

Although traditional approaches remain useful, an increasingly complex and interdependent operating environment encourages

**Figure 20. Risk identification tools**




Q: Among the following, which methods does your organisation primarily use for risk identification and assessment? Select all that apply. Nordic Managing Risks Survey, N=52

# Strengthening skills and perceptions

the use of additional risk identification mechanisms designed to identify a broader-set of conditional risk-drivers. More mature organisations increasingly leverage modelling and quantification tools to form a more empirical view of risk exposures grounded in broader, data driven insights.

### The resource challenge

Current resourcing of risk functions presents a potential challenge in meeting practitioners' future ability to strengthen practices. More than half (58%) of organisations have only 0-2 full-time dedicated risk employees, with limited plans to expand these teams in the near term. This constrained internal capacity is further compounded by low utilisation of external expertise, with only 12% of respondents regularly engage third-party providers or adopt co-sourcing arrangements to augment internal capabilities. Given the increasing complexity and dynamism of today's risk landscape, external partnerships could offer critical benefits – providing access to the breadth and depth of specialised knowledge required – combined with the fresh perspectives and additional capacity that are essential for risk functions to fulfil their strategic roles effectively.

### The future needs of the risk function

As it stands today, the aspiration within Nordic organisations to elevate risk functions to strategic business partners appear paradoxical. Budget constraints and limited talent pools create barriers to hiring, resulting in constrained capacity for existing resources to focus on building the organisational understanding, integration and engagement required to support this transformation.

However, effective use of the advancements within technology offers potential solutions to this predicament. Conscious use of generative AI and GRC technologies, for example for horizon scanning and web scarping, enables data collection and analysis at-speed – keeping the need for additional human resources down. Risk practitioners should further aim to upskill the business in risk management activities and provide the first line with the tools to undertake effective own analysis, enabling risk teams to remain small and agile. To take the next step, many risk practitioners find themselves in a Catch 22. Without a strong regulatory pull for risk capability enhancements, they need to demonstrate value-driven insights to obtain the necessary pull from the business to back additional resource or technology investments. Conversely, without making these investments, organisations lack the bandwidth to develop strategic risk intelligence while fulfilling their embedded compliance and control mandates.

If successful in shifting their focus towards strategic support, the strong-performing risk practitioner of the future will be reliant on supplementing technical ability with the following skills:

- **Curiosity and questioning** – risk practitioners need to continuously be in dialogue with the business and develop a strong understanding of their processes, priorities and challenges.
- **Collaboration and relationship building** – an increased degree of integration with other management frameworks and processes, as well as driving a unified approach towards developing organisational robustness, requires strong collaboration within the organisation.
- **Adaptability** – in a constantly changing landscape, being flexible to in adapting methodologies, analysis and outlooks to address new risk landscapes, evolving interconnectedness and novel risk drivers is crucial.
- **Storytelling** – cutting through complexity and crafting a story where risk exposures become comprehendible across all stakeholder groups is critical in creating necessary understanding of the value of sound risk management.

# Risk outlook

# Risk outlook

Nordic organisations generally share a common view of the priority risk areas, with strategic risks at the forefront of practitioners' minds. As organisations look to anticipate the full second order effects of today's political environment, together with expectations of continued global disruption and the re-emergence of nation-state led threats, the prominence of geopolitical risk emerges as the highest priority risk area for the future.

**Current outlook: strategic risks dominate boardrooms**

Risk practitioners in Nordic organisations identify strategic risk as the most prominent concern at board level. This focus reflects the complexities of today's business environment, where companies must navigate market disruptions, competitive pressures and evolving stakeholder expectations. Ranking second, financial risks retain their traditional prominence, highlighting the importance of financial resilience amid the first and second order impacts of economic uncertainty.

Operational risks are a focus for attention across sectors, given the criticality of operational incidents to the ability of an organisation to operate and deliver products or services.

This includes the growing importance of supply chain risks. Nordic organisations increasingly rely on complex third-party networks, which introduce a broad spectrum of risks, including operational disruptions, fraud risks, regulatory breaches, reputational damage and strategic misalignment. The absence of comprehensive and effective third-party governance frameworks creates dangerous blind spots, allowing vulnerabilities to emerge across multiple risk dimensions simultaneously. Consequently, a thorough understanding of the extended enterprise and the organisation's value chain needs to be a key priority for risk practitioners.

Positioned fourth in ranked priorities, cybersecurity continues to receive significant attention.

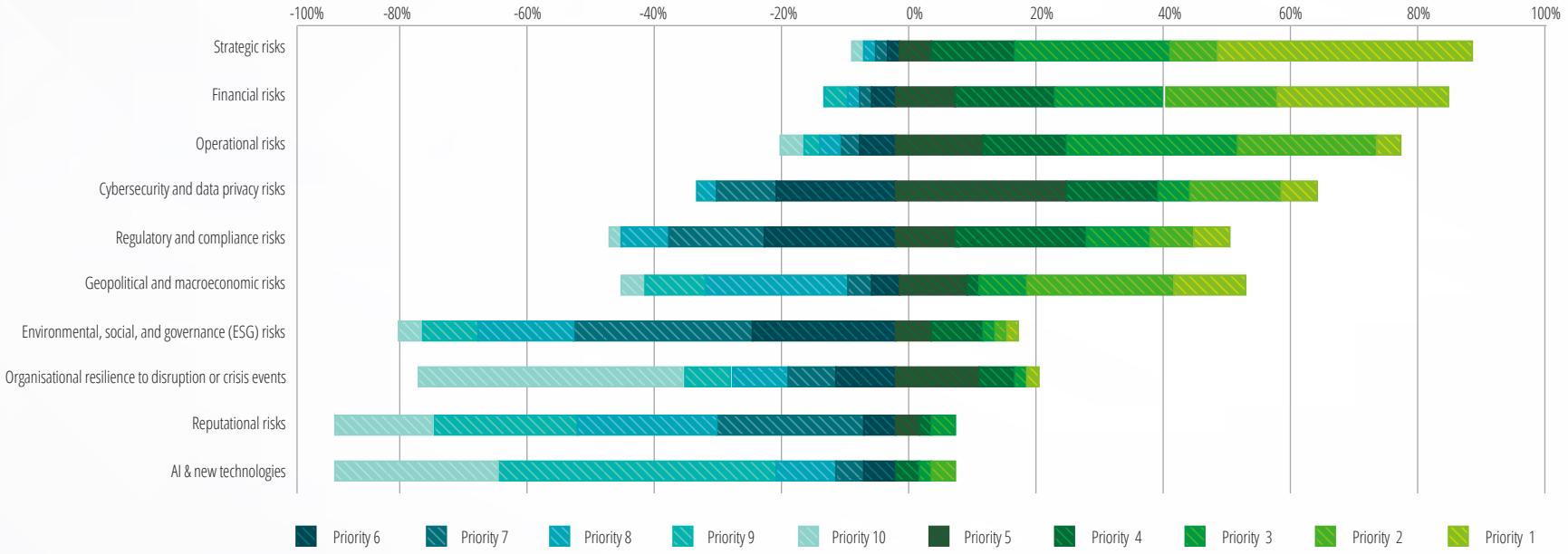
This sustained focus reflects the persistent and evolving threat landscape, as well as the critical role digital infrastructure plays in business operations. In contrast, operational resilience and AI-related risks are ranked considerably lower on organisations agenda. This aligns with broader trends of a decline in top management interest in generative AI technologies[2] , possibly due to uncertainties surrounding regulatory frameworks and the ethical considerations, for example related to data privacy and protections. However, with AI's rapid evolution and its growing integration across organisations and ecosystems, firms cannot afford complacency regarding emerging technological risks.

[2] Our recent "The State of Generative AI in the Nordics – Q4" report find that interest from Nordic C-suite leaders and boards in Gen AI are on a downward trend. To read more: state-of-gen-ai-nordic-cut-q4.pdf

# Risk outlook

**Figure 21. Perceived board risk priorities**

The graph below details the ranked distribution of prioritised risks, with green bars showing the percentage of respondents ranking each risk as a top 5 priority. The blue bars show the percentage of firms ranking each particular risk as 6th or lower (to 10th) priority.




## Cross-industry consistency with divergent views on geopolitical risk

The survey findings reveal a notable consistency in the prioritisation of the top three risks areas across different industry sectors, suggesting that the current risk landscape largely transcends sector-specific differences. However, some distinctions appear: cybersecurity risks receive greater emphasis within the TMT-sector, reflecting the nature of their products and customer interactions, while regulatory risks hold a more prominent position on board agendas within the ER&I sector.

In contrast, perceptions of geopolitical risk presents a more complex picture, with considerable individual variation in ranking. This suggests a divided view, where organisations tend to regard geopolitical risk as either highly significant or of limited concern, with few adopting a moderate stance in their assessments.

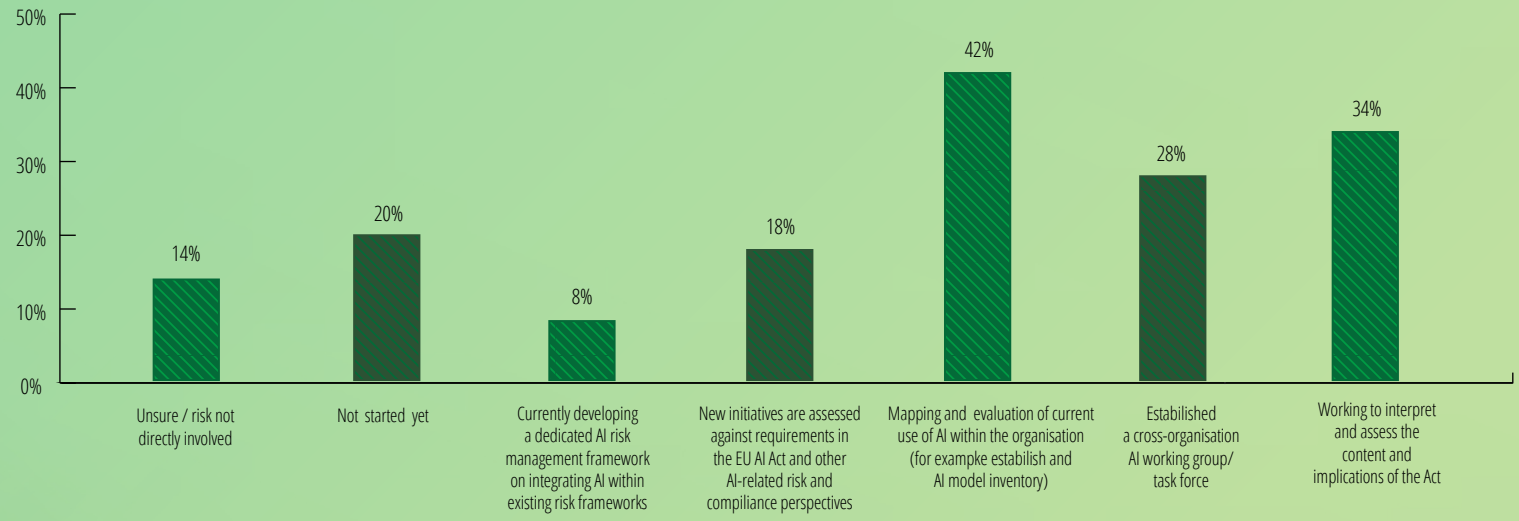
# Risk outlook

## Managing AI risks

The integration of artificial intelligence into risk management frameworks appears to be at an early stage among Nordic organisations. Currently, 76% of respondents are focused on foundational activities, such as interpreting the implications of emerging AI regulations and developing a comprehensive understanding of existing AI applications within their organisations.

As AI technologies rapidly advance, their influence is beginning to permeate the entirety of the organisation, from enhancing basic employee productivity to enabling more complex business process integrations. Encouragingly, 28% of survey respondents have established cross-functional working groups that bring together expertise from business, technology, data, legal, risk, and compliance to address the compounding risks of agentic AI. The TMT sector is perhaps unsurprisingly, the most advanced in this area, being the only sector where respondents report actively developing dedicated AI risk management frameworks.

**Figure 22. Approach to implementing the EU AI act**




Q: What is your organisation's approach to implementing the EU AI act? Nordic Managing Risks Survey, N=50

# Risk outlook

AI presents distinctive challenges that transcend traditional risk category boundaries, amplifying existing threats while creating entirely new ones. The technology has already reshaped the operational risk landscape across information security and cyber, technology and data management, model risk, conduct, compliance, and third-party relationships. Beyond intensifying these familiar operational risks, AI introduces novel 'AI-native' risks that are inherent to the technology itself.

To begin the journey towards effectively managing the risks emerging from AI adoption, risk professionals should consider the following activities:

- **Build organisation-wide AI competency and understanding** through comprehensive training programs across all levels. Fostering AI literacy equips employees in pursuing AI-driven opportunities whilst recognising potential risks.
- **Create a shared organisational definition of AI** to ensure consistent application and clear boundaries. Adopting standardised definitions, such as those provided by the EU AI Act, offers organisations a common foundation for discussions.
- **Embed AI into existing risk taxonomies** and assigning explicit responsibility for oversight and management. This integration enables effective governance and provides the Board with appropriate visibility to determine acceptable risk thresholds.
- **Incorporate AI risks and AI-risk drivers into existing risk detection and evaluation mechanisms,** such as Risk and Control Self-Assessments, product approval workflows, and developing AI-focused scenario testing to identify both internal and external AI vulnerabilities.

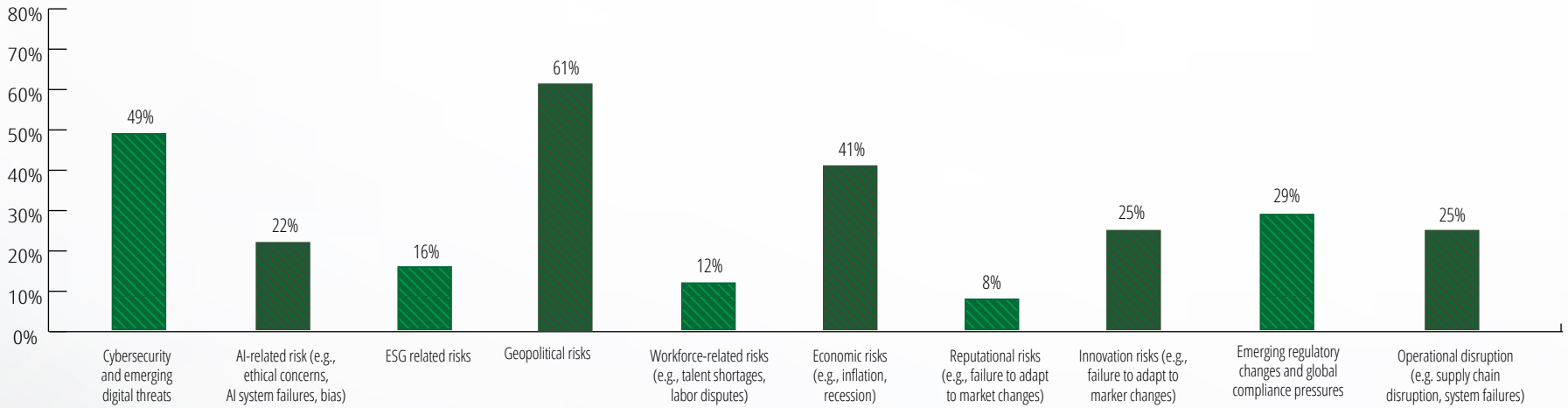
# Risk outlook

## Future risk outlook: Geopolitical risk emerges

Nordic organisations foresee a notable shift in their risk landscape over the next three years, with geopolitical risks expected to become increasingly prominent. The majority of survey respondents operate cross-border, with 71% having a presence in the EMEA region and half of organisations operating in the remaining global regions; APAC, North America and Latin America. Therefore, geopolitical risk considerations are unsurprisingly, on the rise as organisations recognise the potential impact that international tensions, trade disputes, and political instability have on business operations, supply chains, financial markets, economic growth and inflation.

Cybersecurity and digital risks are expected to remain top concerns for organisations in the future, reflecting an expectation that digital threats will intensify rather than stabilise in the coming years. Several factors drive this expectation: organisations continue to digitalise their operations and increase system dependencies, while sophisticated AI-powered attacks are spreading throughout business ecosystems. The threat landscape is evolving rapidly, as new technologies also lead to new sources of vulnerability. Attackers now leverage AI to automate targeted phishing campaigns, create realistic deepfakes, and identify software weaknesses at remarkable speed and scale. Meanwhile, emerging quantum computing capabilities present a fast-evolving source of risk to current encryption methods that currently safeguard sensitive data.

**Figure 23. Risks expected to increase in prominence over the next years**




Q: Over the next three years, which risk types do you think will increase the most in their importance for your business? Please select at most 3 options. Nordic Managing Risks Survey, N=51

# Risk outlook

Economic risks, ranking third in the three-year lookout, underscores the persistent concern among Nordic organisations regarding the impact of market volatility, inflationary pressures and the possibility of economic downturns to business performance. These factors pose significant challenges to organisational stability and strategic planning. Market volatility could disrupt supply chain, effect investment decisions and create uncertainty in budgeting and forecasting. Inflationary pressures could increase operational cost and squeeze profit margins further and may necessitate price adjustments that could impact firms' competitiveness. In addition, the risk of economic slowdown or recession raises concern about reduced consumer spending, tightening credit conditions, and potential liquidity constraints. Together, these economic risks require organisations to adopt robust financial management practices, scenario planning and agile strategies to navigate an uncertain economic environment.

While Nordic organisations are clear on their top three future risks, they also recognise a wide range of risks that are gaining significance. This indicates a future risk landscape defined by complexity and diversity, rather than dominated by singular or few dominant threats.

### Sector-specific priorities reflect industry characteristics

Some sector-specific nuances transpire in the future risk prioritisation, reflecting the unique characteristics of each industry:

- **Energy, Resources and Industrials** prioritise geopolitical risk closely followed by operational disruption, economic risk and emerging regulatory challenges. This is reflective of the sector being highly regulated, active in international trading and operating critical infrastructure which inherently demands heightened safety and security considerations.
- **Technology, Media and Telecom** organisations hold cybersecurity and digital risks as the clear top future priority. Evolving customer demands, expanding digital ecosystems, 5G implementation, and blurring industry lines are accelerating the need for technological innovation. As companies compete to deliver new solutions and preserve their competitive edge, innovation-related risks have risen to become one of their four highest priorities.
- **Consumer, Retail and Manufacturing** organisations largely mirror the aggregated priorities, with geopolitical risk ranking first, closely followed by cyber and digital risks, economic risks and innovation risk. This reflects a sector characterised by extensive supply chains and sensitivity to market fluctuations and inflationary pressures, which directly influence consumer spending behaviours.

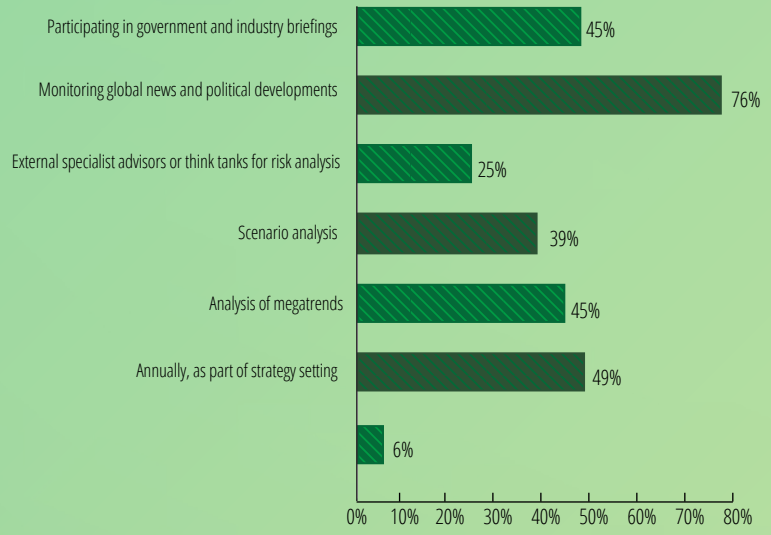
Across all respondent groups assessing both current conditions and future risk outlooks, there is universal acknowledgment of navigating an unstable external environment defined by accelerating change. In this context, it becomes critical for organisations to apply their risk knowledge toward building resilience capabilities that enhance their capacity to predict, absorb, and adapt to disruptions irrespective of their origin.

# Risk outlook

## Managing geopolitical risk

In managing geopolitical risks, organisations place strong reliance on traditional monitoring methods, with 80% of respondents primarily tracking media and news sources and political developments to identify changes in risk levels. More advanced analytical tools, including scenario analysis, megatrends assessment, and participation in industry forums, remain underutilised.

**Figure 24. Identification methods for geopolitical risk-drivers**




Q: How does your organisation identify and assess geopolitical risk? Select all that apply? Nordic Managing Risks Survey, N=49

In response to geopolitical uncertainties, supply chain strategies have become the primary mechanism for risk mitigation. 70% of organisations employ diversification strategies to reduce risks from trade policies, sanctions and resource controls, while 28% have adopted nearshoring approaches. Traditional contingency planning also stands strong as a mitigating activity, with 70% of respondents relying on these plans to prepare for an uncertain operating environment.

**Figure 25 Mitigating strategies for geopolitical risks**


Q: What strategies, if any, does your organisation employ to mitigate the impact of geopolitical risks? Nordic Managing Risks Survey, N= 47

Globalisation is being fundamentally reshaped by geopolitical tensions. To navigate complex geoeconomic dynamics, build resilience, and maintain competitiveness, businesses must adopt a long-term, geopolitically informed strategy in which risk management tools and mindset play a key role.

# Building resilience

# Building resilience

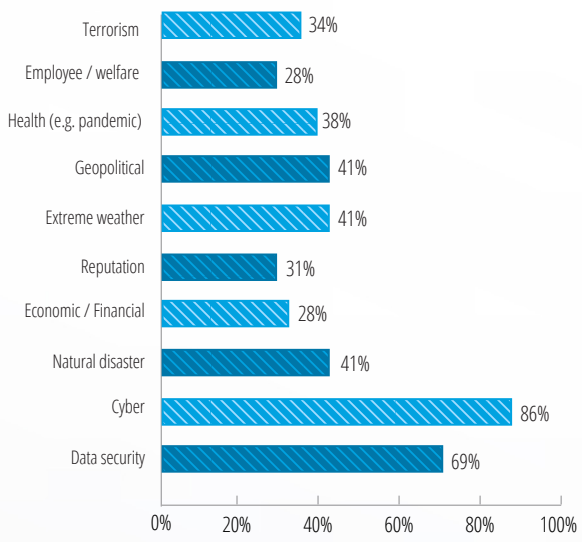
Nordic organisations show strong confidence in their cyber-focused resilience but face critical gaps in addressing broader, interconnected risks. Emerging regulatory requirements, as well as novel risk drivers, demand a shift toward holistic, all-hazards resilience. Against this backdrop, strategic leadership and programme expansion is required to develop the true resilience needed to thrive in an uncertain environment.

### Resilience through the cybersecurity lens

Nordic organisations present a paradox in their approach to resilience. While an overwhelming 94% of respondents rate their resilience maturity as moderate to very high, a deeper examination reveals a strong imbalance in the extent to which their resilience programmes address different risk categories.

The scope of most resilience and business continuity programmes is heavily skewed towards cyber threats and data protection scenarios: 86% of programmes cover preparedness for cyber disruptions, and 69% include data security. In stark contrast, other critical risk categories receive significantly less attention—natural disasters and geopolitical scenarios feature in just 41% of programs, while health-related disruptions like pandemics attract only 38% focus, and terrorism preparedness a mere 34%.

**Figure 26. Scenarios considered by resilience programmes**




Q: Which scenarios did you mobilise for? Select all that apply.
Nordic Managing Risks Survey, N=29

This cyber-centric programme design understandably reflects the reality of our digital age, as well as the regulatory emphasis on preparing for cyber-related disruptions. As a result, many resilience and business continuity programmes are led by technology and information security functions, whose technical expertise is foundational to IT-driven organisational resilience. However, the focus should not be solely on the specific nature of threats, but rather on the organisation's capability to anticipate, absorb, adapt to, and ultimately thrive amid any disruptive scenario. While current programmes strengthen defences against digital disruptions, true organisational resilience requires expanding the scope beyond individual threat types to develop transversal capabilities that enable effective response and recovery across all forms of disruption. This requires developing an understanding of the interconnectedness of threats and actively using crisis exercises and war gaming covering a variety of scenarios to enforce processes and muscle memory.

# Building resilience

"A critical success factor for expanded resilience capabilities, functions or programmes is their integration with Enterprise Risk Management, which when done effectively, ensures resilience efforts align with comprehensive risk assessments and the organisation's risk appetite, enabling coordinated risk prioritisation, efficient resource use, and proactive responses across all threat types."

### Sector variations in risk perceptions

Our survey highlights how resilience priorities differ across industries, shaped by sector-specific risk exposures:

- **Energy, Resources and Industrials** firms adopt a broader view, recognising natural disasters, extreme weather and terrorism alongside cyber risks, reflecting their exposure to physical infrastructure threats and broader operational risks.
- **Technology, Media and Telecom** organisations, while strongly cyber-focused, also emphasise economic and geopolitical risks, acknowledging the complexity of global markets and regulatory environments.
- **Consumer, Retail and Manufacturing** firms show the most concentrated focus on cyber threats, potentially overlooking supply chain vulnerabilities and operational disruptions that could be equally damaging.

These sectoral variations underscore the need for tailored resilience frameworks and strategies that address the full spectrum of relevant risks for each individual business, while delivering and maintaining a comprehensive level of coverage.

### The strategy gap: high confidence, low commitment

One noteworthy observation from our survey is the gap between perceived resilience maturity and the level of strategic commitment. While respondents express confidence in their resilience capabilities, only 30% treat resilience as a strategic priority with executive-level sponsorship and comprehensive oversight. Applying a sectoral lens, TMT leads the way with 43% viewing resilience strategically, CRM demonstrate moderate engagement at 32%, while ER&I trail with the lowest strategic commitment at just 24%.

This disconnect suggests that resilience often remains relegated to operational teams and technical specialists, failing to receive the C-suite attention necessary for a comprehensive organisational perspective and potentially explaining the need for periodic transformation and enhancement to address gaps observed post events.

### Communication challenges undermine strategic clarity

One of the key barriers to strategic commitment is a lack of a shared understanding of the sources of risk and how the transmission channels drive resilience topics, with. 36% of respondents reporting no common understanding or shared definition of what resilience means. This fragmentation can create confusion, as teams interpret resilience differently: IT may focus on cybersecurity, operations on supply chain continuity, and leadership on broader strategic risks. Such misalignment hampers clear communication, budgeting, and strategic planning, keeping resilience discussions at a technical rather than integrated to the strategic agenda.

### Gaps in organisational structures reflect and reinforce priorities

Organisational structures to support resilience vary widely with just over half of respondents (52%) having dedicated business continuity and resilience functions. Again, sectoral differences emerge; whilst 71% of TMT respondents report dedicated functions, the figures for ER&I and CRM stand at 62% and 36% respectively. The absence of dedicated teams or

# Building resilience

formalised functions to champion resilience in many organisations hinders systematic planning and rapid response, increasing, vulnerability during crises plus the resulting scale of impact

### Limited use of advanced technology

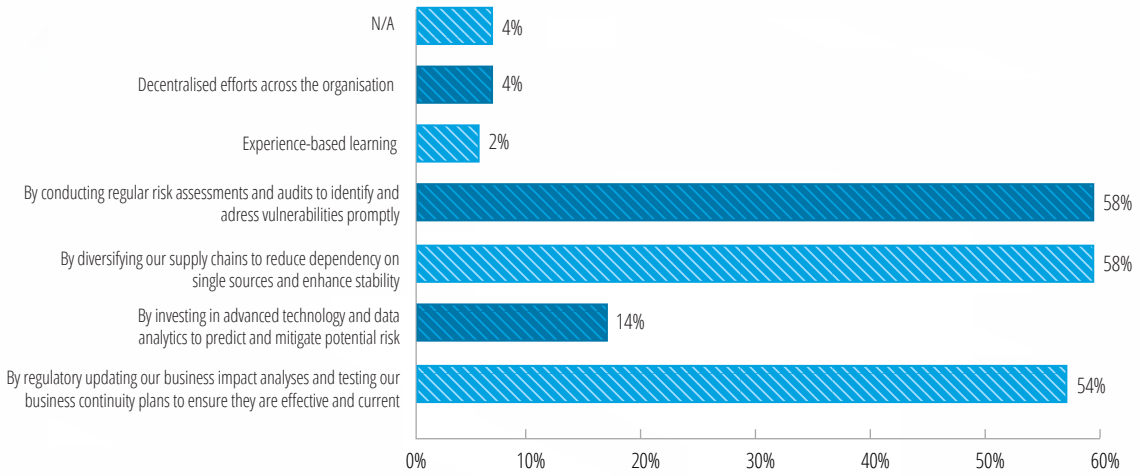
While Nordic countries often pride themselves on technological advancement, resilience practices remain surprisingly traditional. Most respondents (57%) focus on established approaches: updating business impact analyses, diversifying supply chains, and conducting regular risk assessments and audits.

In contrast, only 14% of respondents invest in the modern technology and data analytics which is available to enhance resilience capabilities and deliver management relevant insights. This innovation deficit represents a significant missed opportunity. In an era of rapid change and complex interdependencies, predictive analytics, artificial intelligence, and real-time monitoring could transform resilience from reactive damage control to proactive risk management.

### The need to move towards holistic resilience

To build resilience in an increasingly complex and turbulent world, both individual organisations and entire sectors must adopt more comprehensive, integrated resilience and continuity strategies. For Nordic organisations, this imperative is reinforced by rapidly evolving regulations that create strong drivers for such transformation. Emerging EU legislation, such as the Critical Entities Resilience (CER) Directive[3], will require critical infrastructure operators and essential service providers across TMT, ER&I and CRM sectors to adopt comprehensive resilience measures that extend far beyond cybersecurity. Organisations subject to CER requirements will need to demonstrate resilience capabilities across physical security, supply chain continuity, personnel security, and operational continuity, areas that the survey findings indicate are currently inadequate. This regulatory framework represents a paradigm shift from narrow, technical approaches to holistic, all-hazards preparedness.

**Figure 27. Initiatives to strengthen resilience**




Q: How does your organisation work to become more resilient? Select all that apply. Nordic Managing Risks Survey, N=50

[3] Navigating the EU Critical Entities Resilience Directive

# Building resilience

"In today's complex geopolitical and security landscape, resilience is no longer just an organisational concern, it is a societal imperative. Defence of critical infrastructure and services across Europe is a key driver, alongside the need to manage cascading effects that ripple across sectors and borders. Cross-sector collaboration and shared responsibility are essential to safeguarding public welfare and maintaining societal stability. Upcoming European regulations are a timely call to action, urging organisations to align their resilience efforts not only internally but also as part of a broader European ecosystem."

The survey findings suggest that the shift towards truly holistic resilience will require significant programme expansion and strategic reorientation. Moving beyond the current state and meeting emerging regulatory requirements demands fundamental shifts at the organisational level:

**Expanding programme scope** beyond cybersecurity to encompass the full spectrum of potential disruptions, from climate change and supply chain failures to social unrest and regulatory shifts.

**Elevating strategic integration** by securing genuine C-suite sponsorship and treating resilience programmes as core business imperatives rather than technical functions.

**Investing in programme innovation** by embracing advanced technologies and data-driven approaches that enable predictive risk management and dynamic response capabilities across broader threat landscapes.

**Integrate Resilience programmes with Enterprise Risk Management** will help ensure a comprehensive, organisation-wide view of risks, enabling better prioritisation, resource allocation, and more effective, coordinated risk mitigation efforts[4].

The regulatory drivers now emerging across Europe provide both the imperative and the framework for this transformation, pushing organisations beyond narrow technical solutions toward the comprehensive, integrated approaches necessary to leverage true resilience to thrive in an uncertain environment.

[4] For a deeper exploration of how to achieve this integration and maximise organisational resilience, see our blog series on the topic.

# Technology

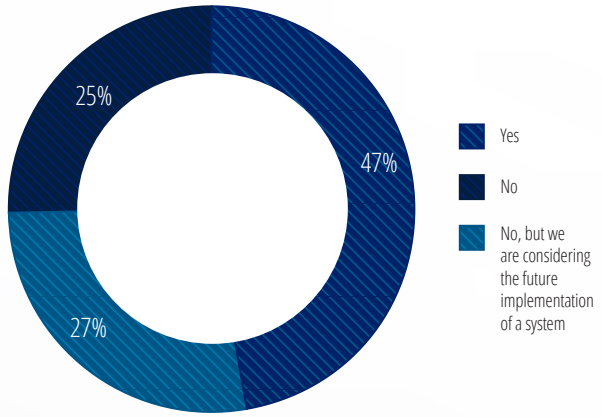
# Technology

Nordic organisations face a pivotal moment in risk management technology adoption. While almost half of respondents have adopted Governance, Risk, and Compliance (GRC) systems, most are only beginning to tap into their full potential. The benefits of adopting Generative AI (GenAI) remains largely unexplored although there is a recognition that there is a need to invest in data analytics and GenAI, with the drive to revolutionise risk management underway.

### Adoption of GRC systems

Effective GRC systems strengthen risk management by offering organisations a clear, current view of risks and controls. Risk practitioners gain tangible benefits such as quicker access to quality data, streamlined operations through automated processes, and enhanced credibility with stakeholders through more robust risk controls. Among respondent organisations, nearly half have implemented GRC systems, while 27% are considering adoption. Systems usage and investment plans span industries and company sizes, reflecting broad recognition of the value derived from integrated risk platforms. However, the technological landscape is fragmented, with a diversity of systems in use: from ServiceNow and OneTrust to SAP GRC, Workiva and Archer.

**Figure 28. Organisational adoption of GRC systems**

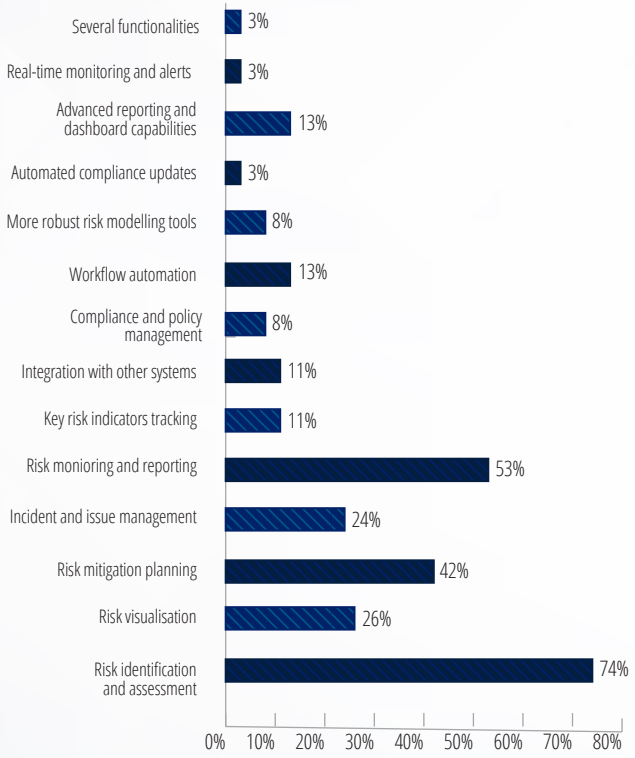



Q: Does your organisation have Enterprise Risk Management software / Governance, Risk and Compliance system in place? Nordic Managing Risks Survey, N=51

When selecting GRC systems, key functionalities prioritised by respondents include traditional risk identification and assessment (74%), alongside risk monitoring and reporting (53 %). Other features like incident management, compliance automation, and workflow integration receive less focus. System capabilities such as advanced risk reporting and visualisation tools have a lower priority, although 40% of respondents use dashboards or visual aids for senior leadership (most relying on general office software like PowerPoint, Excel, Power BI). This could suggest many organisations are not maximising their systems' potential to enhance risk communication and enhance management understanding of the risk and resilience universe.

# Technology

**Figure 29. Prioritised functionalities within GRC systems**



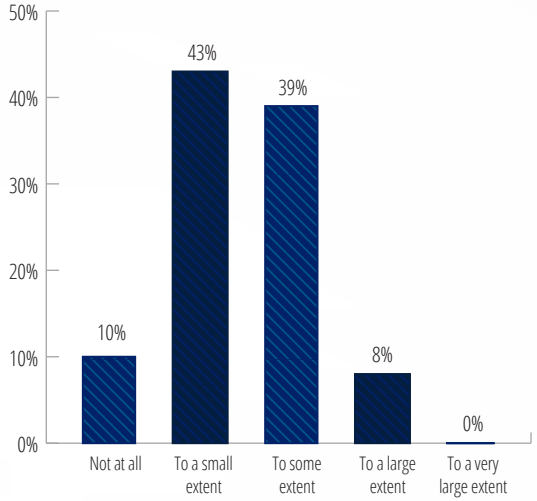

Q: Which functionalities are most important for your organisation in Enterprise Risk Management software/Governance, Risk and Compliance system? Please select at most 3 options.
Nordic Managing Risks Survey, N=38

## Generative artificial intelligence: emerging but underutilised

Artificial Intelligence is recognised as a critical emerging competency, with approximately 71% of respondents identifying knowledge of AI as essential for future risk practitioners. Despite this, practical AI adoption remains limited, with over half of the surveyed risk practitioners reporting minimal or no current use of AI in risk management activities, while just under 40% indicate some degree of utilisation.

Risk functions face a pivotal choice in whether and how to best harness artificial intelligence. GenAI offers the opportunity to dramatically streamline and accelerate traditional manual processes such as documenting, monitoring and analysing risk data. In addition, it holds transformative power with its ability to uncover and address risk dimensions and risk drivers that conventional tools are unable to. Together, this creates a strong use case for risk practitioners to focus their limited available time towards more proactive risk management activities and, crucially, enable more sophisticated monitoring of dynamic changes in the operating environment that influence risk profiles and strategic choices.

**Figure 30. AI adoption within risk management**




Q: Are you exploring how to use AI to support your activities within risk management?
Nordic Managing Risks Survey, N=51

# Technology

### Investment priorities in risk management technology

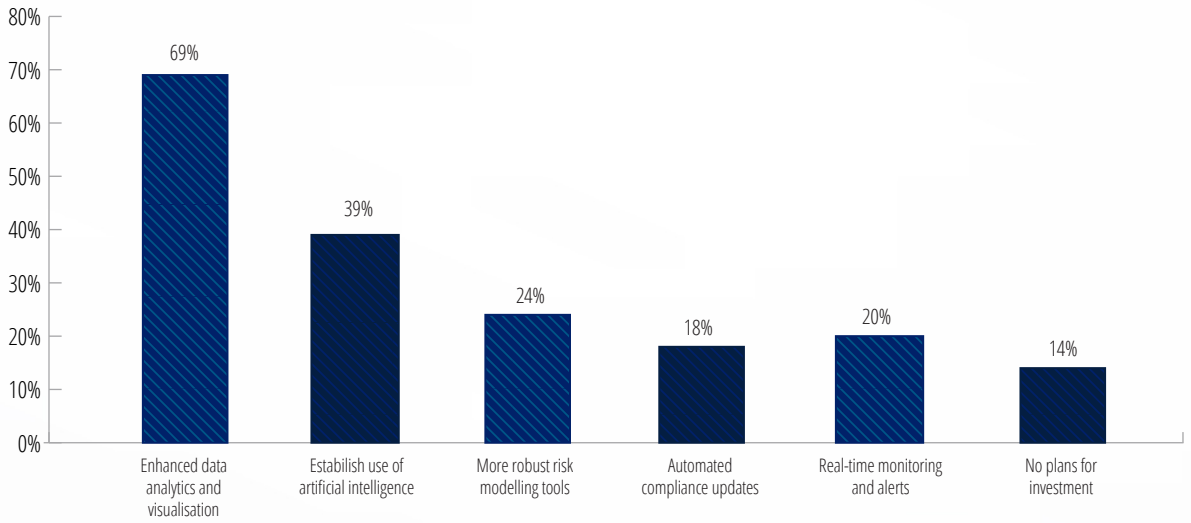
Looking ahead, technological investment priorities by Nordic practitioners align closely with the identified challenges. 69% of respondents plan to increase capabilities in enhanced data analytics and visualisation, aiming to improve the quality, timeliness, accuracy and the illustration of risk information for decision-makers. Establishing GenAI capabilities is a priority for 39% of respondents, often as part of broader digital transformation rather than risk-specific initiatives.

Other areas receiving moderate attention include more robust risk modelling tools, automated compliance monitoring, and real-time risk reporting. This balanced approach reflects a growing awareness that transforming risk data into actionable insights, and harnessing the potential of GenAI, is critical to advancing risk management maturity and resilience in Nordic organisations.

Our survey shows that Nordic organisations demonstrate deliberate approaches to technology deployment and future investment planning. Significant value is potentially available to risk practitioners who fully explore and unlock the sophisticated visualisation, reporting, and analytical capabilities embedded in current GRC systems.

With GenAI widely acknowledged as essential for the future of risk management, risk functions and teams must urgently shift focus - moving beyond supporting first-line applications to identifying and implementing GenAI within their own operations and workflows. Risk leaders must reframe the role of technology, transforming it from a productivity enhancer into a strategic asset that can unlock new risk insights beyond the reach of conventional approaches. Organisations taking decisive action today, will establish the strategic positioning required to address complexity with enhanced responsiveness and resilience.

**Figure 31. Technological investment priorities**




Q: Which technological capabilities will your organisation prioritise for investment in the future? Select all that apply. Nordic Managing Risks Survey, N=51

# Acknowledgements

Building resilience

# Acknowledgements


### Lead authors

**Elisabeth Egdetveit**
Enterprise Risk Management specialist

**Hanne Eikrem Heggstad**
Risk & Resilience specialist



### Contributors

This report is the result of a team effort that includes contributions by experts of the member firms of Deloitte Touch Tohmatsu Limited listed in this report. Special thanks is extended to the following people from Deloitte who have made this survey a success by administering the survey, assessing the results and creating this document:

**Tomi Seppa,** Director
**Antti Nylund,** Manager
**Martin Tripax,** Director
**Sheetal Menon,** Manager
**Ylva Gjelten,** Senior Consultant
**Kristian Snilsberg Andersen,** Consultant



### Subject matter advisors

**Emma Price**
emprice@deloitte.co.uk

# Contacts

Our Enterprise Risk services enable clients to see and manage risk from an ecosystem and enterprise level, helping them maximize their potential, uncover strategic opportunities, and be faster, more innovative, and more resilient in the face of adversity. For local discussions, please contact our experts below.


**Norway**

**Elisabeth Egdetveit**
Director
eegdetveit@deloitte.no

**Hanna Eikrem Heggstad**
Senior Manager
hheggstad@deloitte.no

**Denmark**

**Brian Skopek Hansen**
Partner
brianshansen@deloitte.dk

**Anne Brændstrup**
**Partner**
abraendstrup@deloitte.dk

**Haris Khan**
**Director**
harikhan@deloitte.dk

**Martin Tripax**
Director
mtripax@deloitte.dk

**Sweden**

**Sophie Holgersson**
Partner
sholgersson@deloitte.se

**Finland**

**Tomi Seppa**
Director
Tomi.Seppa@deloitte.fi

**Antti Nylund**
Manager
Antti.Nylund@deloitte.fi

Deloitte.



Designed by CoRe Creative Services. RITM1450428