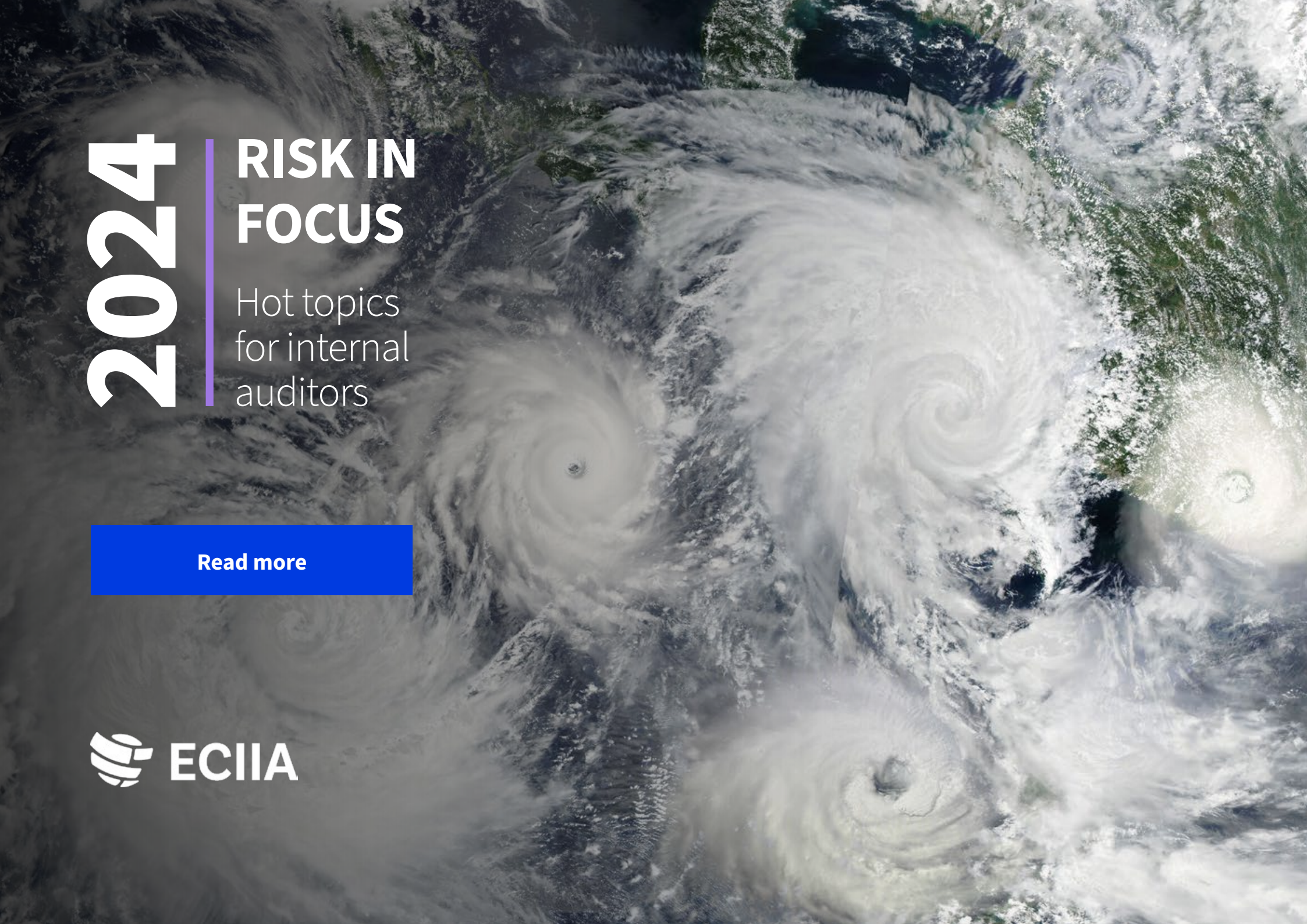
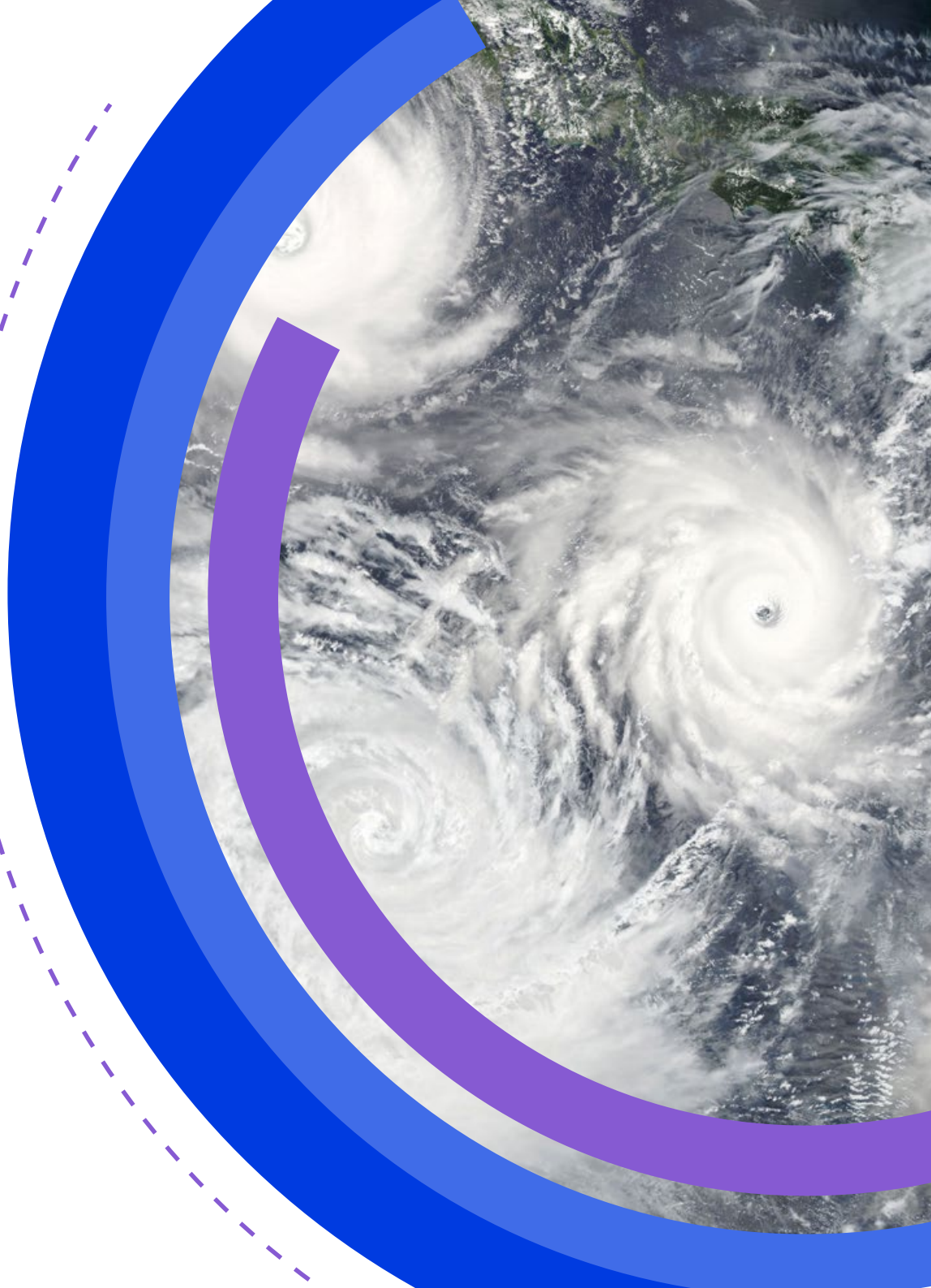

2024
RISK IN FOCUS
Hot topics for internal auditors
Read more
ECIIA

CONTENTS



Contents

EXECUTIVE SUMMARY:

Organisations squeezed by tight economic conditions need an unwavering focus on resilience and a growth mindset to navigate the poly-crisis and spring back when conditions are right

Economic uncertainty has driven the perfect storm of interlocking risks described in last year's Risk in Focus in new directions in 2023. Organisations are now grappling with an ensuing poly-crisis – with multiple catastrophic events occurring simultaneously. With Europe's biggest economy Germany slipping into recession following last year's energy price shock,[1] some organisations are facing declining cash balances and higher net debt.[2] Organisations are preparing for possible trouble ahead – and to leap forward when conditions improve.

But post-pandemic, the ground rules have changed. Growing geopolitical turmoil has weakened the bonds of globalisation that made the flow of goods, services, and customer behaviour predictable. Disruptive technologies such as artificial intelligence, ChatGPT and blockchain that are evolving at lightning speed promise to impact business strategies and improve operating systems – and potentially overturn them. And staff and customers have decoupled from traditional corporate values – creating both a human resources crisis and a scramble to understand changing market forces.

Organisations must successfully steer through the ongoing poly-crisis if they are to thrive when conditions improve.

Risk in Focus 2024 draws on a survey of almost 800 CAEs, 5 roundtable events and 11 one-to-one interviews to chart the key challenges these circumstances create, organisational responses and internal audit's role in five hot topics:

- CAEs ranked **macroeconomic and geopolitical uncertainty** as their organisations' 3rd biggest risk – jointly with changes in laws and regulations. But this year, weathering the economic effects of higher inflation and interest rates and the market changes they engender (a new risk category this year) cut across all areas, from financial liquidity and insolvency risk to business continuity and supply chain resiliency.

[1] Germany falls into recession as consumers in Europe's biggest economy spend less, CNN Business, May 2023.
[2] BCG Transform Index: The European Economy and the Resilience Imperative, Boston Consulting Group, May 2023.

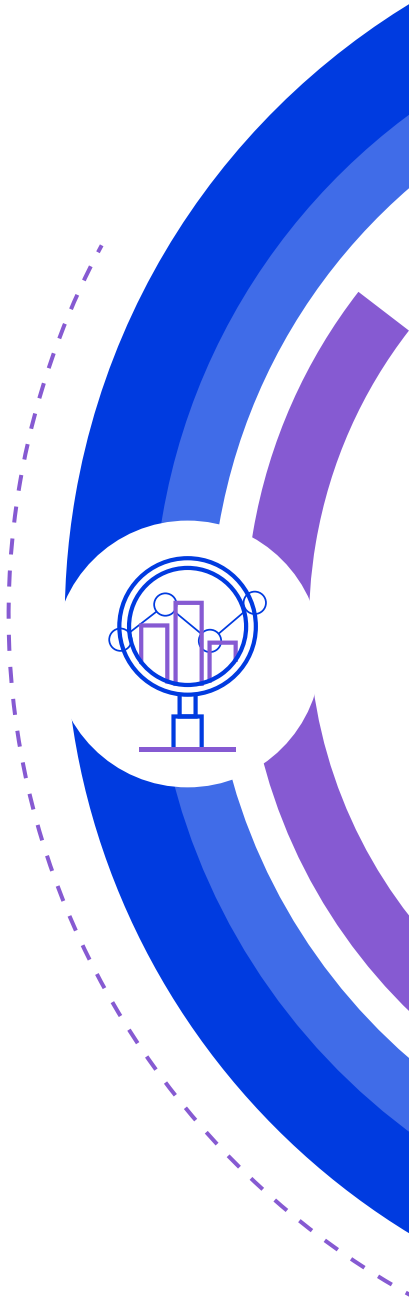
Contents

- **Cybersecurity and data security** retained its long-standing pole position as the region's top threat with risk and internal audit effort well-balanced (84% and 79% respectively). These levels appeared to have settled at the heights fuelled by the pandemic – but disruptive technologies such as AI could propel them higher by 2027.
- **Human capital, diversity, talent management and retention** also retained its 2nd place ranking in the report as many businesses find themselves out of sync with post-pandemic culture. This is a vital area to tackle as both strategic goals and risk management require a broad and deep base of talent and skills for success.
- **Climate change, biodiversity and environmental sustainability** may have slipped down the rankings to 7th place, but a raft of new regulations – including Europe's Corporate Sustainability Reporting Directive - means that CAEs expect it to be their organisations' 3rd biggest risk by 2027. Keeping a strategic, entrepreneurial attitude will be key if they are to avoid being mired in compliance.
- **Supply chain, outsourcing and nth party risk** ranked 8th place in the survey, a key area where dynamic, fast-moving interconnected risks – economic headwinds, deglobalisation, climate-related weather events and new regulations, make strategic and operational innovation a must.

CAEs and boards have focused on helping organisations build general resilience while getting into more granular detail on risk and mitigation strategies – and testing those in scenario run-throughs to capture inter-related risks that could otherwise remain hidden. More than that, leading CAEs are adopting two related strategies. First, as business cultures abandon the old, siloed view of risks and organisations, CAEs are increasingly co-ordinating efforts across the three lines to strengthen risk identification and mitigation, and to ensure scarce expertise and skills are properly deployed. Second, they are recalibrating their audit methodologies towards agility to better match the increased velocity of risks. That entails being awake to opportunities for supporting the business in rapid-fire consultancy exercises, advice and brainstorming, at the same time as shortening audit times through automation and more precise planning and timing. Boards and business leaders appreciate early, targeted and quick assignments that support strategic efforts.

Logically, that makes sense. Where risks are not easily predictable, interrelated and swift, the response has to focus on general resilience, cross-functional teamwork and agility.

Practically, it is hugely challenging. Not only are experienced, qualified people hard to attract and retain during a cost-of-living crisis – especially in lower-waged countries and public sector organisations – but the growing compliance effort is soaking up internal audit time just when it needs



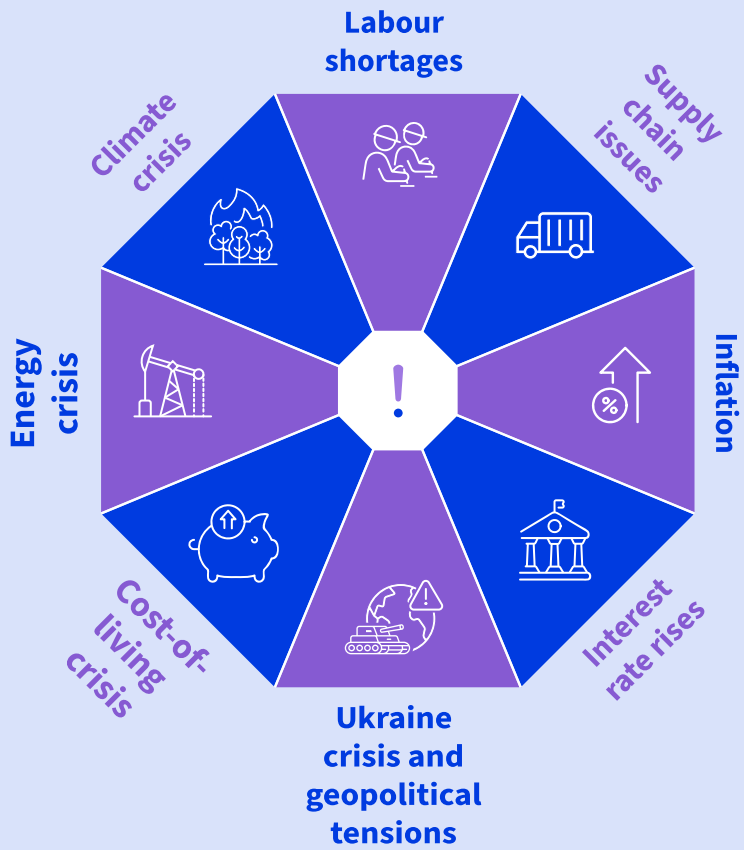
Contents

to focus more on building processes that can help engender success. An emerging strategy is to keep talent within organisations by recalibrating culture, communicating purpose, deprioritising department silos and ensuring clear, longer-term career progression and development.

In these unique and challenging times, CAEs must continue to work with boards to ensure the long-term sustainability of their organisations at the same time as responding rapidly to immediate, fast-moving threats. Organisations must not sacrifice opportunities to innovate and advance – as well as cutting where necessary with a growth mindset. For CAEs, being courageous and having the confidence of their convictions to get their messages across, being brave and initiating conversations in areas where no answers exist, and collaborating across the business are critical strategies for success.

The poly-crisis that we now face creates huge challenges for internal audit, but it also creates huge opportunities for the profession to exceed expectations and play a leadership role in building resilience for organisational success. We hope that this year's Risk in Focus provides you with the ideas, insights and inspiration to navigate these difficult times.

The poly-crisis of risk



Contents

METHODOLOGY

In the first half of 2023, a quantitative survey was distributed among chief audit executives (CAEs) by 16 European Institutes of Internal Auditors, spanning 17 countries including Austria, Belgium, Bulgaria, France, Germany, Greece, Hungary, Italy, Luxembourg, the Netherlands, Norway, Poland, Spain, Sweden, Switzerland, and the UK & Ireland. The survey was also conducted in partnership with the European Confederation of Institutes of Internal Auditing (ECIIA). The survey elicited 799 completed responses.

Simultaneously, five roundtable events were hosted with 46 participants and 11 in-depth interviews were conducted with a range of CAEs, Audit Committee Chairs and industry experts from a range of countries to specify the most pressing topics organisations face and provide relevant suggestions as to how these might be addressed in the risk-based plan of the internal audit function.

The topics in this report were determined by the quantitative survey results and the qualitative feedback from the roundtable events and one-to-one interviews. The comments made during one-to-one interviews include the names of the participants but because the roundtable sessions were conducted under anonymity, those names have been withheld. The format of this report builds on the success of a change in approach to last year's report and takes a deeper look into areas of pressing importance to internal audit and their stakeholders.

This report should not be considered prescriptive, but as a tool to inform internal audit's thinking in making their annual plans and provide a benchmark against which CAEs can contrast and compare their own independent risk assessments.

We hope that CAEs will use this report as an agenda item for audit committee discussions and as a sense-checking tool to support their internal audit planning and strategy.

The report is also of relevance to a broader range of governance stakeholders including audit committee chairs, board members, risk management, along with other assurance and governance professionals.

Key survey findings

What are the top five risks your organisation currently faces?

Business continuity and operational resilience moved up two places this year in response to continuing global turmoil with market changes coming in as a new category.

Looking ahead

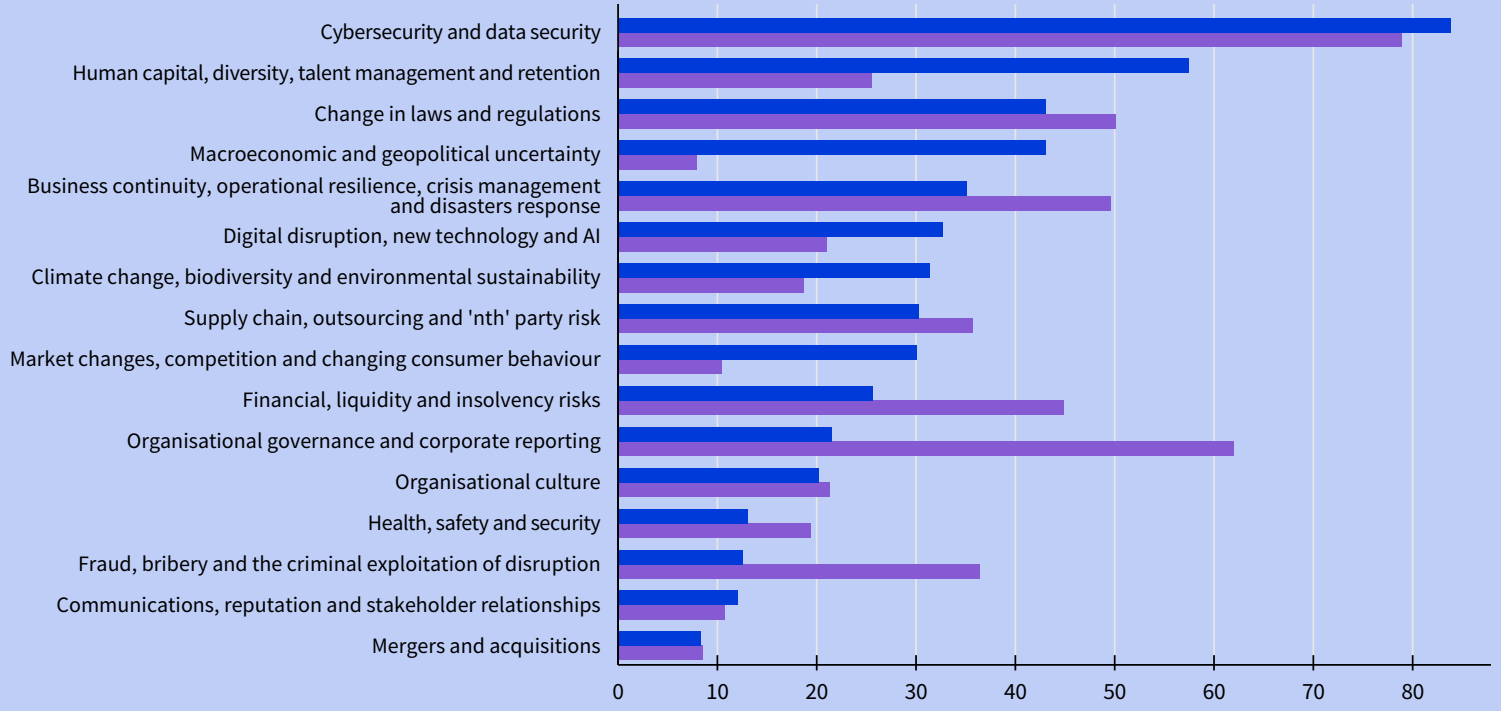
What do you think the top five risks to your organisation will be in three years' time?

Human capital, diversity, talent management and retention together with climate change, biodiversity and environmental sustainability cemented themselves in the top three risks for 2027 behind cybersecurity and data security.

Risk priorities vs. audit's focus

Top 5 risks compared with where internal audit spends the most time and effort

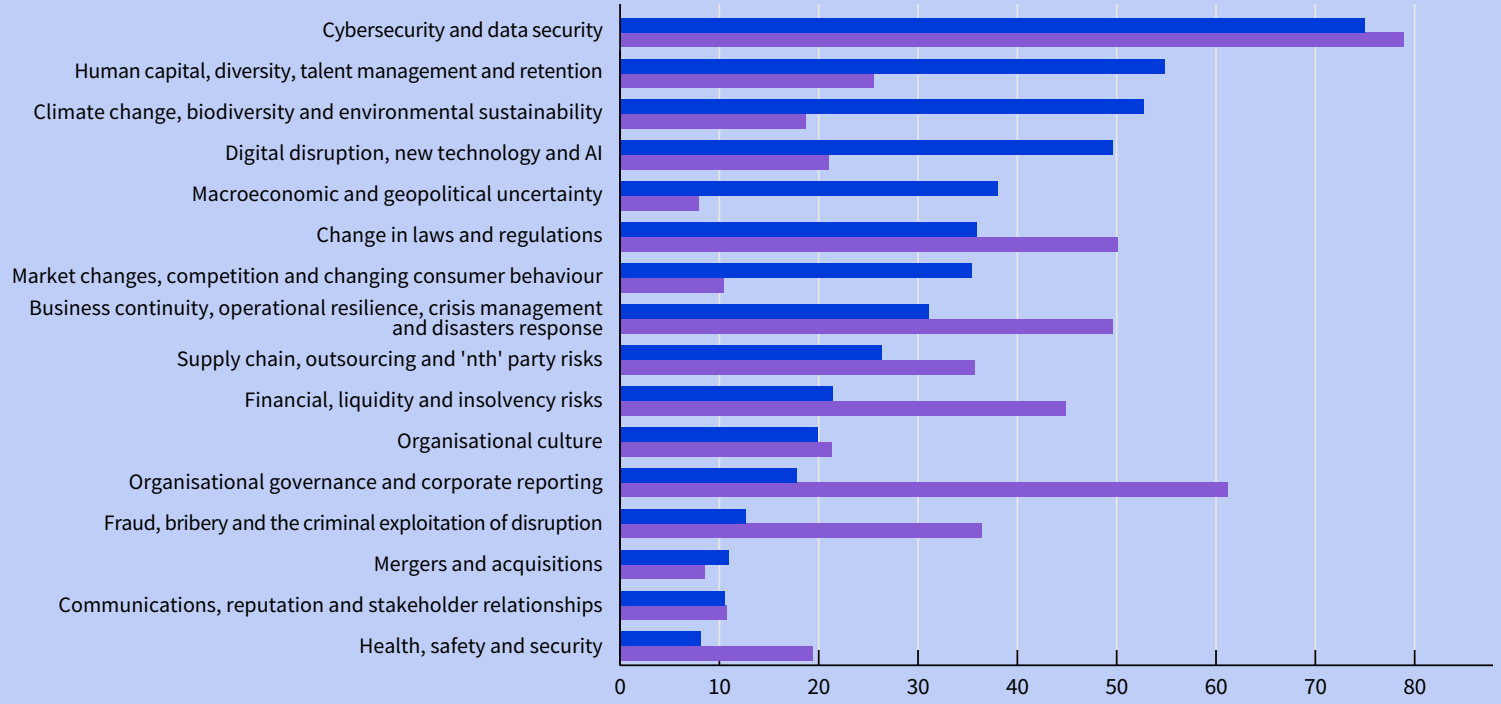
Internal auditors focus heavily on cybersecurity and organisational governance and corporate reporting but spend much less time on macroeconomic and geopolitical uncertainty. While responses to those threats may fall into categories such as business continuity and insolvency risks, it is a challenge for internal auditors to get out of their comfort zones and increase focus on such areas.



Looking ahead

What are the top 5 risks you expect internal audit to spend the most time and effort addressing three years from now?

Internal auditors expect to spend significantly more time on human capital, climate change and digital disruption, while organisational governance and business continuity are among the areas that will ease.



MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY

Preparing to prosper

While organisations are focused on weathering the economic storm, they must build growth strategies into their resilience initiatives if they are to prosper in future.

Macroeconomic shockwaves hit most organisations during 2023 – raising the risk of insolvency as customers tightened their belts or struggled to stay in business in the wake of a cost-of-living and cost-of-doing-business crisis. As governments reversed twenty years of loose monetary policy to deal with higher inflation – accelerated by gas shortages from Russia after it started a war in Ukraine in 2022 – financial stability in Europe remained fragile.[3]

Respondents ranked macroeconomic and geopolitical uncertainty joint 3rd in the Risk in Focus 2024 research – its highest position since the survey began in 2018 – with 33% of those ranking it first. Sitting joint third with changes in laws and regulations, macroeconomic and geopolitical risk is a true umbrella category.[4] Businesses are grappling to identify, assess and mitigate a wide range of interconnected risks that are transforming at speed: from supply chains and changes in customer behaviour, to financial liquidity, insolvency and fraud risk: all while organisations are failing to attract and retain the skills needed to cope. From an economic perspective, most pressingly, a new category in the survey – market changes, competition and changing customer behaviour – ranked 9th, but would jump to 2nd place if there were to be an economic downturn in Europe.

Resilience efforts must focus on weathering this broad range of pressures to ensure businesses are in a position to prosper when conditions improve.

Struggling to compete

For many, economics trumped politics this year. “We have found our balance on geopolitical risk, even though the course of the war in Ukraine and tensions over China remain big open questions,” a CAE speaking at the Risk in Focus 2024 roundtable said, “but the macroeconomic impact is happening right now as we speak.”

Tighter monetary policy, higher interest rates, a cost-of-living crisis and a cost-of-doing-business crisis threatens to increase those pressures. “You are beginning to see an environment where it is not that easy for companies to strategically invest in R&D and innovation for the future,” a professor of Internal Auditing and Corporate Governance and head of a Center for Internal Auditing Excellence in Germany. “This will be a major risk for European businesses because competitors in the US and China do not face the same complexity of macroeconomic and political risk.”

[3] Financial stability outlook remains fragile, ECB review finds, European Central Bank, May 2023.
[4] See CIIA’s 2023 report “Navigating geopolitical risk”.

MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY

He said both businesses and politicians tend to be too short-sighted in their responses to rapid technological innovation that is happening outside the region "When organisations face these dramatic economic and competitive risks, CAEs are in danger of over-rating the local threats their own companies face and hugely under-rating the risks arising from outside of Europe that will hit them".

Investment mindset

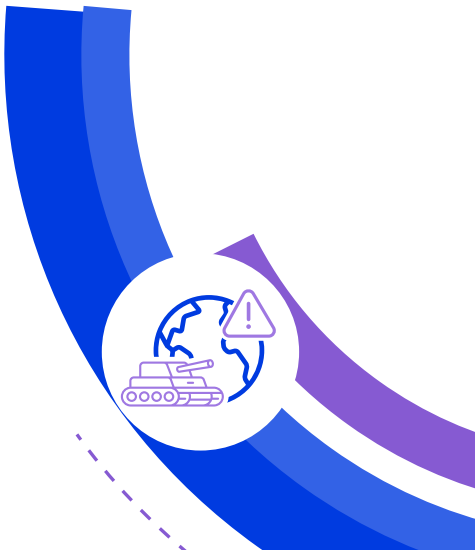
Driving costs down is crucial, but organisations cannot afford to become too reactive. They must invest smarter now that the cost of money has increased, a CAE at a Swiss-based pharmaceutical manufacturer said in an interview for this project: "If a company sees employees and manufacturing as simply big cost buckets in their profit and loss accounts, and if that is the only driver of the decision to make savings, I believe that is wrong," he said: "You need to make those changes part of the overall growth plan you have in mind so that you are working to create an operating model that is state of the art."

A key part of most business models up until 2020 had been open supply chains. Now, businesses are diversifying and supporting suppliers in vital areas, as well as investing in alternative technologies. Partnering arrangements are on the rise. But shortages have made prices higher and a lack of goods in some sectors has narrowed supply chain options leaving some organisations potentially dependent on a sole supplier for core resources. At the same time, European legislation aimed at promoting sustainable development goals is likely to complicate that process by increasing due diligence on third-party risk.[5] Not only will a lack of proper reporting processes be a bigger compliance risk, but greater transparency also feeds into the demand from customers for greener, more ethical products.

Making connections

Macroeconomic and geopolitical uncertainty ranked last place – 16th – in terms of internal audit effort in this year's survey. But that could be partly an artifact of the nature of the risk because huge amounts of effort are expended on the consequences of those threats. In fact, to capture the broad range of threats sitting beneath those umbrella categories, CAEs must ensure they focus on both specific threats and the inter-relations between disparate risks.

"It is extremely important for the business not to become too siloed in a world of interconnected risks," a CAE at an Italian financial services group said at the roundtable: "Internal audit must participate in discussions about the governance structure of the organisation so that silos are opened up and management and risk management has the right focus, including on the connection between threats."



[5] Corporate sustainability reporting, European Commission.

MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY

CAEs must help build processes that capture emerging risks more rapidly and ensure appropriate committees and business groups review them. At a strategic level, internal audit functions must identify region-specific risks where organisations need to reduce their dependencies – and ensure that the business maintains a global strategic perspective on risk.[6] That will not only help identify and monitor important emerging risks that could impact Europe but also those factors that will aid the business to prosper when conditions improve.

Given the velocity of risks associated with macroeconomic uncertainty, organisations are implementing control systems that are more agile, adaptive, and incorporate more real-time monitoring of key risks.[7]

Internal audit's role

CAEs must play a leading role in coordinating such efforts and assuring that they are in place and effective. Providing lighter-touch advisory services and engaging in pre-audit sessions with the first and second lines that are more predictive, proactive, and supportive is key. "We are doing a lot more brainstorming and sharing best practices before we do an audit," a CAE working in a London-based financial services organisation said at this year's roundtable. "Where we see organisations struggling outside the business, we share that with our first line, ask them to fix their controls, so that when we come to do the audit, things are in better shape." That may partly explain why internal audit time is relatively low, despite the high impact these rapid assignments can have. Survey respondents said that by 2027 they expected to spend only marginally more specific time on macroeconomic and geopolitical risk than they do today. But CAEs must be prepared to get out of their comfort zones and tackle the threat head-on if they do not do so already.

Most internal audit functions are backing up this lighter approach to providing assurance in areas such as macroeconomic and geopolitical risk with data analytics, data-driven internal auditing - and moving up the value chain.

> "We are doing a lot more brainstorming and sharing best practices before we do an audit"

[6] See for example, EU ministers calling for less dependency on China.
[7] See "A reference model for auditing organisational resilience".

MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY

CAEs must also follow up on how decisions have been implemented where they are of critical strategic importance. Including such risks in other audit areas – such as financial and liquidity risk – is essential to ensure that yesterday's assumptions do not catch the business unprepared for the changing risk landscape, as happened with Silicon Valley Bank. In addition, where localisation has made on-the-ground audit coverage difficult, joint audit approaches with other assurance providers are key.[8]

CAEs must ensure that they are recruiting people today with the business knowledge, skills, and talent to understand tomorrow's emerging risks and their potential interactions. Leading internal audit functions are investing heavily in additional training and education to plug knowledge gaps – essential given that in three years' time, CAEs ranked macroeconomic and geopolitical uncertainty as the 5th largest risk their organisations will face.

How can internal audit help the business?

1. Evaluate the effectiveness of the organisation's mechanisms to identify, assess and monitor changes in the macroeconomic and geopolitical environment
2. Assess whether the process for planned strategic investment in R&D is adequate to help the organisation achieve its long-term strategic goals and to remain competitive globally
3. Assess whether the assumptions made on financial stress testing align with reality and that economic scenario planning and simulation exercises are awake to emerging risks
4. Assess whether the organisation has adopted agile strategies and is adaptive and resilient where risks continue to be fast-moving and unpredictable
5. Advise the company on the processes of adapting and mitigating risks associated with macroeconomic and geopolitical uncertainty
6. Evaluate internal controls to ensure compliance with regulations and legal requirements related to macroeconomic and geopolitical trends, such as international sanctions and anti-money laundering rules

[8] See, "Breaking the barrier: on the use of joint audits in the internal audit profession".

CYBERSECURITY AND DATA SECURITY

Strengthening the digital nervous system

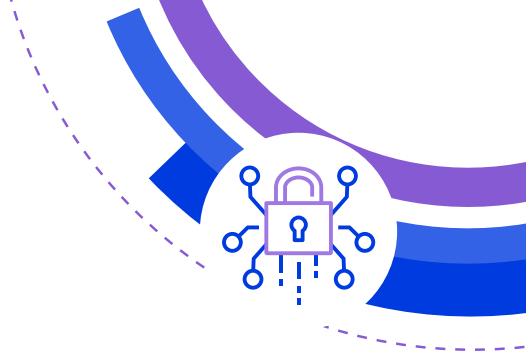
Cyber-risk maturity is improving and as the threat landscape continues to evolve internal auditors are increasingly co-ordinating efforts across the three lines.

Cybersecurity and data security strengthened its hold in the Risk in Focus 2024 rankings with 84% of respondents saying it was a top five risk - up from 82% in 2023 and 2022. Of those, 60% rated it as their 1st or 2nd priority this year, which has edged down from 67% in 2023 suggesting a growing risk management maturity in some businesses. In addition, these risks are among internal audit's key priorities with 79% rating it in their top five areas measured in time spent.

Cybersecurity and data security will remain the number one threat in 2027 but there is a sense that the threat is plateauing at a high level of intensity – especially since it is fired by recent developments in AI. CAEs taking part in the Risk in Focus 2024 roundtable on the issue tentatively agreed that the gross risk exposure was flat or slightly up, and net risk exposure down. Awareness is now good among management and boards and defences are more mature. CAEs are building their own cybersecurity and data security tools, or working with IT functions so that network activity is continuously monitored.[9]

84% of respondents cited **Cybersecurity and data security** as a top five risk compared to 82% last year.

[9] Embracing Data Analytics, Chartered IIA.



CYBERSECURITY AND DATA SECURITY

More dangerous

But the unfortunate truth is that the online world is now more dangerous. First, hacking has professionalised and commercialised and many attacks are more sophisticated - a trend discussed in Risk in Focus 2023. In the UK, for example, British Airways, Boots, and the BBC were among businesses infiltrated by a ransomware outfit through their payroll provider's software.[10] Second, state-sponsored actors are using so-called wiper attacks to breach cyber defences and destroy the affected organisations – these are rare but have increased in frequency since the war in Ukraine.

Third, as wars are increasingly waged both online and on battlefields, organisations must assess how geopolitical events could not only damage businesses, but also critical infrastructures. One Swedish CAE at the report's roundtable said cyberattacks spiked immediately after the government announced its intention to join NATO: another saw increased activity after a major product launch. In addition, threats to the global underwater network of cables that carry much of the internet could also increase, highlighting how cyberattacks have been weaponised.

Fourth, many organisations have moved to the cloud, digitalised their operational technologies, and integrated with suppliers. The so-called "attack surface" of businesses is broader as a result – there are more ways in. Finally, emerging technologies, such as the generative AI program ChatGPT and blockchain offer both important new business opportunities at the same time as adding speed, complexity and additional risk exposures. For example, malware can test an organisation's security patching status and then request AI to generate an attack that targets specific vulnerabilities. Because such hacks can exploit legitimate software, they can be difficult to defend against. By 2027, CAEs said that digital disruption, new technology and AI would be their organisations' 4th biggest risk, potentially increasing cyber threats further.

Fundamentals

"We invest a lot in making sure we keep the known risks under a tight grip with new controls and security measures," a CAE from a Swiss-based financial services firm said at the roundtable, "but the biggest challenge now is what we should invest in to identify and tackle the unknown cyber and data risk exposures." Given that cybersecurity and data security sit at the centre of the turbulent meeting place of many interconnecting risks – from geopolitical uncertainty to digital disruption – constant vigilance and control innovation is a must.

> "The biggest challenge now is what we should invest in to identify and tackle the unknown cyber and data risk exposures."

[10] BA, Boots and BBC staff details targeted in Russia-linked cyber-attack, The Guardian, June 2023.

CYBERSECURITY AND DATA SECURITY

Since COVID-19, organisations have got better at cyber risk fundamentals: strengthening perimeter defences, monitoring network activity, patching updates, penetration testing, and even employing ethical hacking on both internal systems and online services. Security automation means that AI programs can monitor threats by scanning patterns of activity rapidly and accurately across entire networks. To combat people risk - a huge challenge in a world of ubiquitous digital communication and social media - businesses regularly conduct awareness training and assess the maturity of their cybercultures by measuring response rates to spoof phishing campaigns.[11] Most organisations are also assuming that a major hack will occur. Advanced recovery solutions include ensuring that the systems that underpin critical activities can be rebuilt from scratch in case hackers have corrupted the organisation's backups.

More regulation

The risk associated with changes in laws and regulations rises one place to joint 3rd in the Risk in Focus 2024 survey (together with macroeconomic and geopolitical risk). While this has been a cause for concern in most areas, CAEs at the roundtable on the topic said they embraced recent EU regulations on cyber and data security.

The requirements mandated by legislation such as General Data Protection Regulation are being extended by rules such as the EU's Data Act, EU Cyber Resilience Act, NIS2, and Digital Operational Resilience Act (DORA)[12] – to name a few. These initiatives provide CAEs with a platform to reinforce the importance of good cyber security and data practices, and they are helping to create a common language of risk around the topic.

"Firms must address any 'reasonably identifiable' IT risk that could compromise enterprise networks"

DORA, for example, which affects financial entities in the European Union, explicitly states that firms must address any "reasonably identifiable" IT risk that could compromise enterprise networks. That could include anything from updates from intelligence agencies to known shortcomings of ChatGPT-style apps – potential data leaks and inbuilt biases. CAEs at the roundtable were both experimenting with such apps and admitted not knowing whether staff in other parts of the enterprise used them. In addition, since DORA applies to suppliers too, financial organisations will have to reassess their due diligence processes around nth party cyber risk.

[11] IIA's Global technology audit guides (GTAGs) provide extensive guidance on many related topics.
[12] Cyber Resilience Act, European Commission, September 2022

CYBERSECURITY AND DATA SECURITY

More broadly, NIS2 Directive sets a new mandatory level of measures (effective October 2024) aimed at preventing cyber incidents. Those include policies on risk analysis, information security, cyber security training, multi-factor and continuous authentication solutions. The idea is to standardise measures across Europe at the same time as imposing fines for non-compliance.

The role of internal audit

Boards and CAEs must both ensure they are ready for compliance across a wide spectrum of requirements and use those rules to further improve resilience. The Risk in Focus 2024 survey suggests some of that effort is going into business continuity, operational resilience, crisis management, and disaster response - which ranked in 4th place in terms of where internal audit spends its time this year - up from 5th place in 2023.

One CAE at the roundtable used the certification process for ISO 27001[13] to develop a very detailed business continuity plan for the specific cyber risks the organisation faced. “Behind the certification there is a strong focus on risk monitoring, risk management activities, and, in particular, identifying exactly which equipment, factory, operation, and application is vulnerable and how to fix it,” he said. “From there, you can plan your BCP in detail and construct scenarios that you can test.” The lessons learned from those scenarios can then be used to improve responses further.

In each of these areas, CAEs are seeking as much detail and specificity as possible to identify gaps and strengthen controls. The board’s strategy at one German media business, for example, has been to drive the three lines[15] to co-ordinate efforts on cyber and data security, said its CAE in an interview for this year’s report. Given the switch to digital operating models, he said that in three years’ time, most internal auditors should be trained IT security specialists at the business.

> “Attracting and retaining people with the right technical and security expertise is a big, expensive problem to solve”

Securing operational technology from threats is key. Because of higher levels of digitalisation and automation, internal auditors must view their organisation’s cyber and data risks through an IT lens. One CAE based at a German multinational healthcare company at the roundtable said that she had worked with the first and second lines to redefine in detail the company’s risk domains by paying close attention to its digital infrastructure.[14]

“But attracting and retaining people with the right technical and security expertise is a big, expensive problem to solve,” he said.

[13] ISO/IEC 27001.
[14] For more detail on the effectiveness of this approach see IIA’s executive knowledge brief, “Understand the elements of combined assurance”.
[15] See The IIA’s three lines model.

CYBERSECURITY AND DATA SECURITY

To do so, he has focused on building a team that concentrates more on hardcore technical issues and less on compliance – something smaller audit functions must co-source to achieve. But that has helped attract talent, such as new chief information security officer (CISO) (himself a former IT auditor), to the business – and to go more granular on recommendations. "The key is to go beyond your average compliance audit and provide actual risk-based technical assessments of the environment and engage in frank, technical discussions with the auditees in a language they understand," the CAE said.

Raising the profile of the CISO and working closely across all lines of assurance is crucial. But CAEs must ensure that risks identified by CISOs are clearly quantified in terms of business risk and communicated clearly to the board or its equivalent.

How can internal audit help the business?

1. Assess how well the organisation complies with relevant cybersecurity laws, regulations and industry standards and is prepared for the impact of upcoming rules
2. Assess how far risk taxonomies and controls on cybersecurity and data security for digital operating systems are aligned across the three lines
3. Assess how effectively the three lines (including the CISO) are working together and with the board
4. Evaluate the effectiveness of cybersecurity controls in the first and second lines and for the organisation's key assets
5. Assess whether the organisation is conducting adequate vulnerability assessments to identify potential entry points for cyberattacks and weaknesses
6. Assess the effectiveness of the business' ongoing monitoring processes to track and assess its cybersecurity posture
7. Assess the effectiveness of the organisation's incident response and recovery plans and its capabilities to execute it
8. Evaluate the organisation's cybersecurity awareness and training programmes and assess whether those produce the desired outcomes
9. Assess how vulnerable backup data is to corruption and whether the organisation has the capability to rebuild its systems at speed from scratch
10. Assess whether senior management and the board are sufficiently informed and show serious commitment to cybersecurity

HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

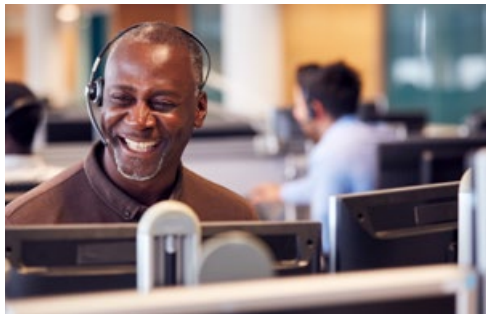
Cultivating a better culture

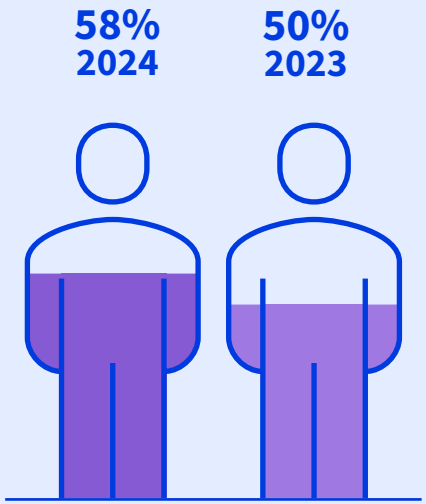
Corporate culture is lagging social change and failing to attract and retain sufficient talent. It is time to re-energise human capital strategies.

Human capital, diversity, talent management and retention is the second biggest risk organisations in Europe continue to face, according to the Risk in Focus 2024 survey. This year, 58% of respondents cited it as a top five risk - up from 50% last year and 40% in 2022. In fact, until the pandemic, human capital was never a top five risk in the survey rankings. Frustrated, one CAE at the project's focus group on the issue said attracting and retaining the right people was his organisation's "biggest nightmare".

In three years' time, it is expected to remain organisations' second most challenging issue. A special question in this year's survey suggests the trend is a structural change accelerated by the pandemic because even in a downturn with higher unemployment a scarcity of talent and skills would remain.

Businesses are faced with rises in labour costs triggered by inflation just when changes in customer behaviour have reduced demand for consumer products and triggered switches in loyalties to cheaper brands.[16] In addition, while many older staff retired in the wake of the pandemic, one in three younger workers in one survey[17] said they were actively looking to move on. Without the right staff, achieving strategic goals and effectively managing risk is less likely.





58% citing **human capital, diversity and talent management and retention** as a top five risk this year compared to 50% last year and 40% in 2022.

[16] 'We're witnessing the biggest movement in consumer behaviour in over five decades', Food Navigator Europe, Oct 2022.
[17] Why a recession won't ease the talent gap, New Street Consulting Group, Feb 2023.

HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

Cultural shift

Many corporations are out of sync with the post-pandemic culture. Demands for flexible working and a desire among staff to work in organisations with a strong social purpose have grown post-pandemic. Organisations have seen attrition rates spike when they insist workers return to the office. Communicating the business' wider purpose and building a more diverse culture can make organisations more attractive.[18]

"One of our biggest risks is trying to keep up with the pace of expectations coming from stakeholders in general and staff in particular in areas such as diversity and work-life balance," a CAE from a Spanish financial services group said at the roundtable - echoing a trend identified in Risk in Focus 2023.

Most CAEs attending the event agreed that there was greater diversity in terms of gender, race, and age in their organisations, including within internal audit functions. But other diversity problems remain harder to crack. There are fewer well-qualified females in some science, technology, engineering, and mathematics fields,[19] for example, and often fewer females in top management roles. European businesses will need to do better in boardrooms – by 2026, 40% of those roles must be filled by women.[20]

Psychological well-being

Since the pandemic, psychological well-being has also become a bigger issue. Many people feel isolated using remote and hybrid working practices, and the risk of economic downturn has created more stress and anxiety.

[18] Chartered IIA warns boards to "get a grip" on unhealthy corporate cultures in the wake of a string of culture-related scandals.
[19] See Women in STEM in EU, Know How, Mar 2023.
[20] Gender Equality: The EU is breaking the glass ceiling thanks to new gender balance targets on company boards, European Commission, Nov 2022.

HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

CAEs at the roundtable agreed that organisations must go beyond narrowly focusing on conventional human resources KPIs and job specifications. Implementing a cultural transformation that is visible, real, and properly aligned with what both staff expect and with the business' own values is a critical first step.[21] It must also be sympathetic to the psychological well-being of staff – an emerging issue.[22]

Timeliness is key: "The board often does not get told soon enough when there is a problem and whether the organisation is able to identify and solve it in an agile way," a former CAE and member of an audit, risk and finance committee at a global sporting body in an interview for the report said.

Internal audit must look at those processes and assess whether they are fit for purpose, she added. CAEs must fully embrace hybrid internal audit methodologies with a good balance between well-targeted, focused audits and rapid and less formal assessments to identify emerging problems. Once remediation plans have been made, internal audit can support and monitor progress with light-touch checks and agile assessments.

"We have had a revolution in attitudes during the pandemic and we mustn't lose the opportunity this represents for CAEs to really support their organisations and win the trust of the board and management in this area," a CAE at the roundtable said. "CAEs are sometimes too dependent on expressing themselves through numbers and risk registers, where today people want a more empathic approach - they want a CAE they can trust on a more personal level."

That approach may not only be more effective but also more realistic. Some CAEs at the roundtable said they had difficulty auditing the business in this area because of their own lack of adequately experienced staff: "For the past two years, we put human capital on the audit plan and then had to take it off again because we don't have the right staff to perform such an internal audit," said one CAE at the event. Integrating human capital issues in other audits is important, but sometimes doing something as simple as sitting down with management to discuss the problem and brainstorming potential solutions can add value. In fact, CAEs must show leadership and empathy in helping the organisation work through new solutions.

"CAEs are sometimes too dependent on expressing themselves through numbers and risk registers, where today people want a more empathic approach - they want a CAE they can trust on a more personal level"

[21] See CIIA's 2022 paper Cultivating a healthy culture for best practice in this area.
[22] What Is Psychological Safety at Work? How Leaders Can Build Psychologically Safe Workplaces, Center for Creative Leadership, Jan 2023.

HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

Internal audit staffing

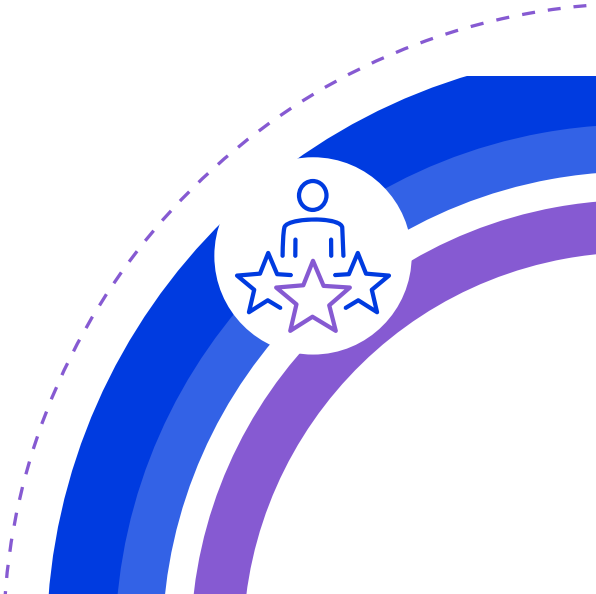
The battle for human resources is one that CAEs cannot afford to lose in their own functions. That is because without the right breadth and depth of skills and talent in the internal audit function the organisation will ultimately be less able to weather the risks it faces or be permanently dependent on third-party help. The varied skillsets internal audit functions need to operate effectively make them particularly vulnerable to human resources pressures.

"Internal auditors must have a combination of very strong analytical skills and IT competencies," a professor of Internal Auditing and Corporate Governance in Germany said in an interview for Risk in Focus 2024, "as well as good personal experience of the business and a heart, brain, and gut feeling for the results they see from their work. This is a much greater risk than just saying we don't have enough human capital."

CAEs must think creatively, he said, to attract new talent from beyond those coming from financial and accountancy backgrounds.

Anecdotally at least, that approach is successfully attracting a broader range of new people into internal audit functions. A CAE at a Belgium financial services firm told the roundtable that he had noticed a "striking evolution" in the increased number of candidates applying for roles in his function since he developed clear diversity policies, flexible working opportunities, and work-life balance arrangements. Another said he had attracted more business-savvy candidates from Big Four accountancy firms looking for better work-life balance. And several agreed that they have restructured their talent pipelines to promote diversity among candidates who are making their way up the promotion ladder.

But staff retention is a problem: "Out of a team of 20, in the last 18 months I've lost 10," said another. "As we attract a more diverse range of people from the business, we find they have more choice about where to go as a next step."



HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION

Instead of fighting the trend, CAEs must create talent management programmes for their functions that link closely to their human resources departments. Developing and communicating staff growth plans that keep talent within the business requires honesty, transparency, and tact. Coupled with a deliberate system of smart rotations in and out of internal audit, CAEs can help strengthen the risk culture within the business over time. That can include using the internal audit function as a management training ground.[23] To do so, CAEs must make their functions visible within their organisations through internal message boards, talent exchange programmes and by promoting the ethos and value of internal audit in conversations with management.

How can internal audit help the business?

1. Assess how competitive the organisation's policies on diversity, equality and inclusion, and work-life balance are and whether they fit the needs of staff in key business areas
2. Assess whether the organisation's values and objectives align and are clearly communicated within and outside the business to engage with potential and existing talent
3. Evaluate how well the organisation's policies and procedures on career progression, training and promotion are designed to attract and retain staff, and whether they are clearly communicated
4. Assess whether the policies on diversity, equity and inclusion are compliant with applicable regulations and whether controls are there to assure they are effective
5. Assess whether employees feel able to speak up and feel psychologically safe
6. Evaluate whether the organisation's employee engagement surveys, exit interviews, and other feedback mechanisms effectively assess employee satisfaction levels and issues affecting morale

[23] The Effects of Using the Internal Audit Function as a Management Training Ground or as a Consulting Services Provider in Enhancing the Recruitment of Internal Auditors, American Acoounting Association, Mar 2015.

CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

Focusing on purpose

Organisations must incorporate sustainability goals into their strategies as increased stakeholder interest and reinforced legislation propel ESG up the risk rankings by 2027.

Respondents to the Risk in Focus 2024 survey ranked climate change, biodiversity and environmental sustainability down from 6th place in 2023 to 7th place this year. With 31% of respondents ranking it as a top 5 risk in 2024 compared with 38% in 2023. However, this fall in the rankings is likely to be short-lived with extensive new rules and reporting requirements[24] forecast to propel climate-related risk up to 3rd place in the risk rankings by 2027.

Urgent organisational action is gathering pace as extreme weather batters Europe and puts severe stress on infrastructures. The return of the El Niño phenomena could make 2023 one of the hottest summers[25] at the time of writing wild fires across Greece were destroying livelihoods and holidays, and putting lives at risk. A CAE at a Swiss food manufacturer told the Risk in Focus 2024 roundtable, for example, that suppliers in badly hit countries were struggling: "Climate change could ultimately impact our ability to obtain essential natural products in the long run," he said, "so investing in alternative solutions is imperative."

Unpredictable drivers

The business response is taking place in a very fluid landscape. In July 2022, for example, the European Parliament voted to alter their taxonomy of sustainable energy sources when they relabelled gas and nuclear energy as sustainable. Intended to reduce Europe's dependence on Russian gas supplies, this angered some investor groups[26] and climate-change campaigners.[27] In addition, raw materials to be labelled as strategically important for Europe's green transition strategy are undecided.

[24] Europe's Corporate Sustainability Reporting Directive came into force in 2023, European Sustainability Reporting Standards is expected to be finalised and come into effect in 2025 as described later in this chapter.
[25] Twelve European countries broke temperature records in 2022, The Guardian, Jan 2023.
[26] IIGCC publishes open letter calling for gas to be excluded from the EU Taxonomy, IIGCC, Jan 2023.
[27] EU taxonomy labelling gas and nuclear as 'Green" faces legal challenges, Earth.org, Oct 2022.

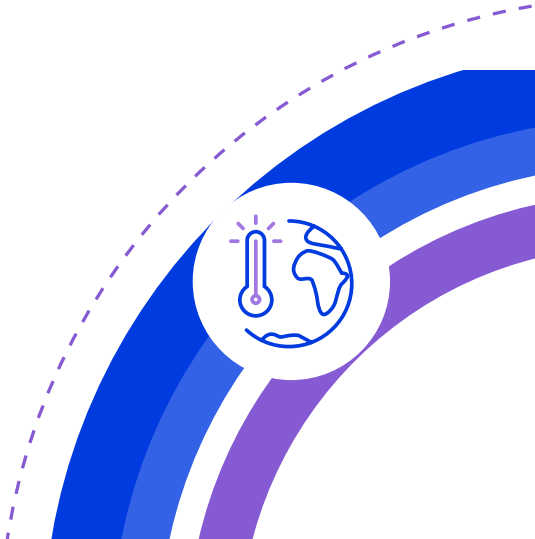
CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

Market changes, competition and changing customer behaviour (which, as a new category, ranked 9th in this year's survey) are also driving climate-related initiatives.[28] Organisations are rushing to enhance their environmentally-friendly credentials to tap into this growing market. But over-stated marketing claims make charges of greenwashing a key threat. Reputational risk and financial risks are rising as legal action steps up. In 2022, for instance, the climate charity Client Earth won a case against the UK government by arguing it had failed to demonstrate that its policies would reduce emissions. With growing legal challenges, the threat of a high-profile greenwashing scandal will escalate.

New compliance requirements

This year, CAEs at the project's climate roundtable said burgeoning regulation was the biggest risk for organisations operating in Europe. In 2023, Europe's Corporate Sustainability Reporting Directive (CSRD)[29] came into force, which strengthens the mandatory reporting requirements on social and environmental information. In addition, the exposure draft of the European Sustainability Reporting Standards (ESRS) is expected to be finalised and come into effect in the 2024 financial year – to standardise reporting requirements across the region.[30] The International Sustainability Standards Board's climate-related standards will also start in January 2024. And more focus is now turning to the natural world with the Task Force on Nature-related Financial Disclosures issuing its final draft framework due for publication in September 2023. Those rules are in addition to the UK's adoption of mandatory climate-related reporting requirements for accounting years after 5 April 2022, which are in line with Taskforce on Climate-related Financial Disclosures (TCFD) recommendations. The UK Corporate Governance Code is to be amended to specifically include a greater focus on the responsibilities of the board regarding ESG reporting, climate transition and climate metrics.

"I predict as the laws become clearer in this area next year, specifically in Europe, that people start to become reactive and it will end up higher in the Risk in Focus rankings for 2025," a CAE at a Swiss-based pharmaceutical manufacturer said in an interview for this project: "There is a risk that people will turn from doing the right thing and will revert to focusing on reporting requirements."



[28] See European consumers drive the sustainability demand, Forrester 2022.
[29] Corporate sustainability reporting, European Commission.
[30] See exact details of the transition arrangements.

CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

The data challenge

A persistent weakness is poor quality climate change, biodiversity and environmental sustainability data. Getting a firm grip on accurate information will be a key for complying with CSRD. It pays more attention to employee health, human rights and other forms of social reporting – with mandatory external assurance needed. In addition, data must be submitted in a standardised digital format – which is likely to involve realigning organisations' reporting programs to fit the new requirements. ESRS data disclosure is more intensive around greenhouse gas emissions, energy, waste and other metrics. Not all organisations' data processes are mature enough to deal with this burden and governance processes and structures must be aligned to the new regime quickly.

Where no data exists, CAEs must start from scratch. In lower-maturity organisations, it is a common error to align an organisation's purpose to sustainable development goals when no data is available, a leading sustainability and ESG advisor and audit committee member said in an interview for the report: "CAEs must first help organisations identify the data that they do have and build a strategy from what exists - then strengthen reporting in areas where there are gaps," he said in an interview for this report. For many internal audit functions, it will be a balancing act whether to simply help identify data and whether also to verify the quality of the data, which may depend on whether there is an ESG team within the organisation. They will need to find their role by communicating with the board.

In addition, partnering with a specialist NGO is critical, he said, because they are highly motivated to help organisations embed the right values in their infrastructures and their deep knowledge of the impact of environmental challenges (such as deforestation or drought management) can help strengthen reporting data.

"CAEs must first help organisations identify the data that they do have and build a strategy from what exists - then strengthen reporting in areas where there are gaps"

CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

Double materiality

In 2023, the IPCC's sixth assessment report[31] urged organisations not only to take measures to keep carbon emissions low to stay below 1.5 degrees Celsius of warming, but to also ensure that those measures had a social impact or improved biodiversity in regions where businesses operated. That will be tough. While climate-related disclosures are maturing, those relating to social and biodiversity impacts are less advanced - but both are requirements of CSRD and ESRS.

Double materiality risk assessments can improve resilience. A CAE at this year's roundtable said that he had included double materiality measures in a recent project, including examining the effectiveness of governance processes around risk reporting: "It pushed us to dive into more detail, compare operations in different parts of the business and created some genuinely new perspectives for our clients," he said. "By doing these assessments you can get ahead and use the information to your competitive advantage because you achieve deeper insights into both risks and opportunities."

"By doing these assessments you can get ahead and use the information to your competitive advantage"

Purpose and strategy

Boards and CAEs must not be driven by compliance alone. "Businesses working in a heightened regulatory environment need to make sure they do not switch from pursuing entrepreneurial strategies to strategies that seek only to be compliant," a non-executive director at a Scottish finance firm said in an interview for this report. CAEs must focus on the organisation's key risks. If a high proportion of their audit plan becomes dominated by regulatory risk, that is a sign that the goal may be in danger.

More broadly, CAEs have a key role to play in educating their organisations about the organisation's strategy and objectives, and in interpreting rules and regulations in ways that are accessible and manageable. Conducting enterprise-wide climate change readiness audits and sharing the data among the first and second lines helps spread best practice.[32]

[31]Sixth Assessment Report, ippc, Mar 2023.
[32]See CIIA's 2021 paper, Harnessing internal audit against climate change.

CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY

The key is to stay focused. “Choosing which sustainability goals fit with the business strategy and prioritising and setting realistic, measurable targets for those is critical,” a CAE at a Swedish financial services group said in another interview. “It is vital to ensure that the sustainability metrics organisations choose to measure are important, clear and can be integrated into the organisation’s business plan.” They must also align with CSRD, ESRD and TCFD regulations.[33]

In three years’ time, survey respondents expected a huge leap in internal audit effort in this area – by 2027 it will jump from 12th place today to rank joint 3rd with changes in laws and regulations. Meeting that demand looks challenging. Strong action to attract, retain and develop the right people is needed to make this a reality. Given that many young people want to work for organisations with strong social purpose, making a decisive move to address the sustainability agenda could play an important part in that process.

How can internal audit help the business?

1. Assess whether environmental sustainability goals are aligned with business strategy and have clear metrics
2. Evaluate whether the organisation’s internally- and publicly-stated climate and environmental sustainability objectives are built from data and thorough analysis and are aligned to relevant regulations
3. Assess whether the implementation of these objectives will be adequate to reach its objectives
4. Assess the effectiveness of (risk) management and controls related to sustainability objectives
5. Evaluate whether the organisation adheres to current business environmental regulations and reporting requirements, and is prepared for forthcoming regulations and requirements
6. Assess the organisation’s monitoring mechanisms to track its environmental performance and achieving its goals, and realising continuous improvement
7. Evaluate how well the organisation is engaging with stakeholders (including NGOs with specialist knowledge) on environmental sustainability issues to ensure it can draw upon the right level of expertise and knowledge
8. Assess whether the organisation’s own goals, values and standards are adequately reflected in suppliers’ contracts

[33]COSO Publishes Guidance for Internal Control Over Sustainability Reporting, Thomson Reuter, Apr 2023.

SUPPLY CHAIN, OUTSOURCING AND 'NTH' PARTY RISK

Securing the extended enterprise

Geopolitical uncertainty, a growing risk of insolvencies and new regulations are helping reshape supply chain strategies and forcing businesses to focus on better resilience.

Supply chain, outsourcing and "nth" party risk is an area of critical stress for many organisations across Europe with 30% of respondents to the Risk in Focus 2024 survey saying it was one of their top five risks – retaining its 8th place in this year's rankings. CAEs placed it 7th in terms of where they spend their time.

While it is easy to think of suppliers as being external risks, they often provide mission-critical products, services and digital infrastructures into businesses and effectively inject higher levels of fast-moving, complex, interconnected global risks into the organisations they serve. Yet because they often do not sit at physical arm's length, the origin, scale and velocity of those risks is difficult to assess and mitigate. CAEs at the Risk in Focus 2024 roundtable agreed that the pandemic, the war in Ukraine and heightened geopolitical tensions between the US and China had complicated international trade and weakened supply chain resilience.[34]

Back in Risk in Focus 2020,[35] organisations were juggling between outsourcing and insourcing – not because they posed an existential threat to their operations, but to protect profit margins. Today, as globalisation continues to loosen, supplier relationships have become mired in the headwinds of last year's perfect storm of interconnected risks. If organisations are to weather adverse economic headwinds and bounce back stronger, achieving supply chain resilience is crucial.

Deglobalisation trends

Deglobalisation is already impacting supply chain strategies via legislation. The US has introduced generous subsidies for companies relocating to the US, for example, in legislation such as the Inflation Reduction Act, the US Infrastructure Bill, and the Chips Act. The moves are designed to address weaknesses in the North American supply chain (identified by the pandemic) and lessen its dependence on China. At the time of writing, the European Union was expected to develop similar measures to prevent migration of businesses from Europe.

[34]Internal Audit Foundation's 2022 paper Are we speaking the same language?
[35]Risk in focus 2020.

SUPPLY CHAIN, OUTSOURCING AND 'NTH' PARTY RISK

In addition, sustainable development goals are appearing in specific supply chain regulation, such as the EU's Critical Raw Materials Act.[36] In June 2023, the European Parliament backed mandatory due diligence legislation – the EU Corporate Sustainability Due Diligence Directive – to make companies liable for human rights and environmental issues in their global supply chains.

Together with Europe's Corporate Sustainability Reporting Directive (CSRD), such rule changes have pushed supply chain due diligence and potential compliance hot spots into the limelight. "Not all supplier contracts have ESG KPIs and it is not always possible to impose your own standards on your suppliers during negotiations," a CAE at a global infrastructure business in Spain said in an interview for the report. Following compliance standards from a larger business partner can add costs to an organisation's products or services, which in an inflationary environment can be hard to pass on, he said.

Finally, the physical environment remains a growing problem. The memory of the Ever Given container ship's grounding in the Suez Canal is a reminder of the fragility of physical supply chains. But recent climate-related extreme weather events, such as the flooding in Germany in 2021, and hotter weather created further stress. A recent study found that few CAEs include topics such as climate impact in their supply chain assignments, which represents both a risk and a missed opportunity.[37] As the new laws begin to be enforced, not doing so will also become a compliance risk.

Organisations are focusing on their business continuity initiatives to cope with the growing scarcity and expense of key products: respondents ranked business continuity, operational resilience, crisis management and disasters response as the 5th biggest threat in this year's survey. Fifty percent of CAEs said it was a top five area of focus – moving internal audit effort up from 5th to 4th place compared with 2023 and up from 8th place when the category was first introduced to the survey in 2021.[38]

[36]Critical Raw Materials: ensuring secure and sustainable supply chains for EU's green and digital future[38]Risk in focus 2020, European Commission, Mar 2023.
[37]See IIA Netherlands' 2023 paper Internal audit and supply chain risks.
[38]Risk in Focus 2021.

SUPPLY CHAIN, OUTSOURCING AND 'NTH' PARTY RISK

Previously, most organisations ranked their suppliers based on cost, quality, and speed of delivery. In today's unpredictable macroeconomic climate attention has switched to securing basic materials and products. "I need to know if my supplier is 100% committed to providing me with what I need, otherwise I could be out of business," said a CAE of a global auto parts company at the Risk in Focus 2024 roundtable.

Internal audit's role

Given the existential nature of this threat, CAEs should look to see if the organisation's key suppliers' potential problems are considered as part of the organisation's own risk universe. Helping them diversify or survive by creating closer partnerships with them is becoming more common. This has become critical where organisations are depending on a single region (or even source) for a key supply.

Diversification of supply has also become important. With an increased risk of supplier insolvency, climate-related catastrophe, or geopolitical disruption in the medium- to long-term, businesses are exploring whether they can find more readily available, cheaper alternatives. That includes investing more in research and development to invent replacement goods and materials - an often-difficult initiative to secure money for when financial liquidity and insolvency threat may loom if there is a serious economic downturn.

CAEs must convince executive management to look at high-impact, less likely risks, "it costs money to create and go through a scenario that has only, say, a 10% likelihood of happening, and before the pandemic, we were not in the mindset where we would do those kinds of exercises," a CAE at a German healthcare business said at the project's roundtable on supply chains, "today, we see it as critical."

In line with a major trend emerging in this report, CAEs are supporting the first and second lines with their supply chain business continuity plans. Post-pandemic, most front-line operations do have more realistic, up-to-date plans drawn up, but CAEs now insist that the scenarios they cover have been tested in simulations before they consider them to be adequate.

Internal audit is more focused on how well risk management processes are effective in practice (rather than, say, simply checking the effectiveness of reporting processes) and that the key risk indicators point to the actual challenges the business faces. Without testing, it is unlikely that plans will capture the way different risks may influence each other, or how risks associated with mitigating controls can be identified and dealt with.

SUPPLY CHAIN, OUTSOURCING AND 'NTH' PARTY RISK

"Internal audit is there to help management be successful in the longer term by protecting and enhancing value, which requires a commercial mindset," the founder of a UK-based global assurance, governance and risk consultancy said in an interview for this report. That entails getting involved in strategy discussions and thoroughly understanding the commercial goals of the business. To combat recommendation fatigue from audit findings, he said CAEs must highlight fewer, more critical risks and actions in a way that makes sense to management. "CAEs are not there to be brilliant internal auditors in an academic sense," he said, "they are there to provide the type of internal auditing services the organisation needs to meet its strategy and objectives."

Supply chain expertise is itself in short supply in both the business and internal audit functions. While the amount of time internal auditors spend on supply chain-related issues is expected to drop to 9th place by 2027 – business continuity efforts will move up to 2nd place. Given the deeply interconnected relationship between the two activities, solving the human capital risk has become imperative.

How can internal audit help the business?

1. Assess how well the organisation ensures supply chains are resilient to the effects of macroeconomic and geopolitical developments and risks
2. Assess how well the business understands the supplier's challenges and whether adequate monitoring are in place to detect potential problems early
3. Assist in conducting due diligence on potential suppliers to ensure they align with the organisation's strategy
4. Review contracts and agreements related to outsourcing arrangements to ensure compliance with all regulations
5. Assess and help in updating effective vendor management frameworks for vendor selection
6. Assess whether the organisation is evaluating third-party and outsourced vendor performance and compliance to quickly detect problems
7. Assess whether management has effective business continuity and crisis management plans in place to cope with supply chain disruption and whether those scenarios are actively rehearsed and refreshed
8. Assess how well the governance structures for the three lines are defined and implemented to improve the effectiveness of supply chain risk management

ABOUT RISK IN FOCUS

For the past eight years, Risk in Focus has sought to highlight key risk areas to help internal auditors prepare their independent risk assessment work, annual planning and audit scoping. It helps Chief Audit Executives (CAEs) to understand how their peers view today's risk landscape as they prepare their forthcoming audit plans for the year ahead.

This year, Risk in Focus 2024 involved a collaboration between 16 European Institutes of Internal Auditors, spanning 17 countries which included Austria, Belgium, Bulgaria, France, Germany, Greece, Hungary, Italy, Luxembourg, The Netherlands, Norway, Poland, Spain, Sweden, Switzerland, and the UK & Ireland. The highest number of European countries involved so far.

The survey elicited 799 responses from CAEs across Europe. Simultaneously, five roundtable discussions were organised with 46 CAEs on each of the risk areas covered in the report. In addition, we also conducted 11 one-to-one interviews with subject matter experts that included CAEs, Audit Committee Chairs and industry experts to provide deeper insights into how these risks are manifesting and developing.

ECIIA

IIA Austria

Institute of Internal Auditors Belgium

The Institute of Internal Auditors Bulgaria

ifaci institut français de l'audit et du contrôle internes

DIIR Deutsches Institut für Interne Revision e.V.

Institute of Internal Auditors Greece

The Institute of Internal Auditors Hungary

Associazione Italiana Internal Auditors

IIA Luxembourg

The Institute of Internal Auditors Netherlands

IAW Instytut Audytorów Wewnętrznych IIA Polska

The Institute of Internal Auditors Norway

40 años Instituto de Auditores Internos de España

IIA Sweden

The Institute of Internal Auditors Switzerland

Chartered Institute of Internal Auditors