

2023

RISK IN FOCUS

Hot topics
for internal
auditors

[Read more](#)



CONTENTS

| | |
|-----------|---|
| 3 | Executive summary: Navigating the perfect storm of high-impact interlocking risks |
| 5 | Methodology |
| 6 | Key survey findings |
| 12 | Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis |
| 20 | Climate change and environmental sustainability: Transition to climate change auditing |
| 27 | Human capital, diversity and talent management: The human factor |
| 35 | Cybersecurity and data security: Auditing at the speed of crime |
| 42 | Digital disruption and new technology: Switching to automatic |



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

EXECUTIVE SUMMARY:

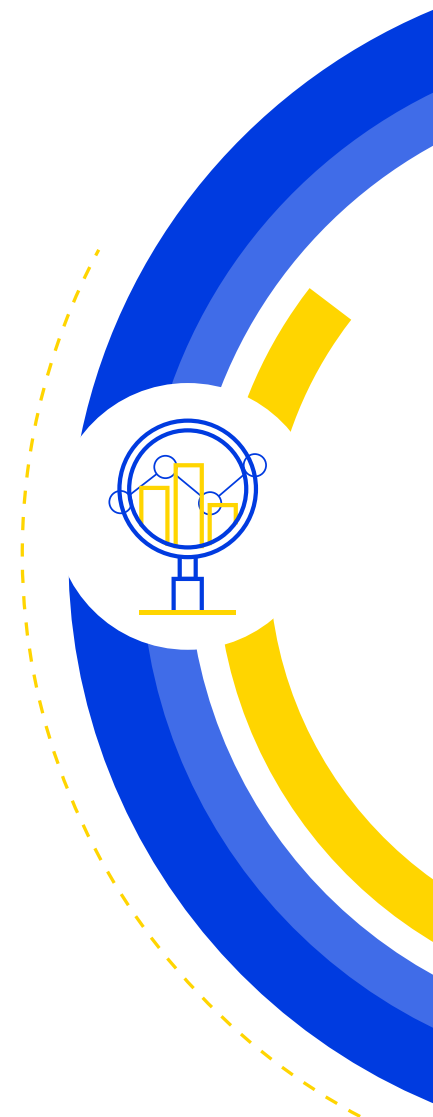
Navigating and auditing in the perfect storm of high-impact interlocking risks

In 2022, organisations were hit by a perfect storm of high-impact, interlocking risks that have thrown businesses into a permanent state of crisis. Following hard on the heels of the pandemic, the war in Ukraine has intensified supply chain failures, caused a spike in energy prices and fuelled inflation.

Now a state of crisis is the new normality. Climate-related natural disasters, looming recession, an accelerating cost of living catastrophe in Europe, food shortages, employee welfare and skills deficits, and a rapidly industrialising cyberattack landscape are overlaid by intensifying geopolitical tensions and the very real threat of financial liquidity and solvency risks for businesses.

This has forced many organisations not just to rewrite their risk registers, but to tear up outdated risk taxonomies that favour old-style siloed thinking. Sudden, systemic organisation-wide risks with contagious, unpredictable ramifications throughout the enterprise are no longer seen as Black Swan events - but as interlocking elements of a continuous storm.

Internal auditors need to get a rapid grip on this situation and support their organisations to navigate more risky, uncertain and volatile times ahead. Instead of thinking about what individual risks might arise over the next year or two, chief audit executives need to be thinking over the coming decade. And be thinking big. How would we survive an overnight, permanent supply chain break with China? How would we cope if inflation hit 25% and stayed there, as it did in the 1970s? Are we prepared for the sudden, permanent increase in temperatures in every area in which we operate? Are we in a position to understand and help our clients and staff with the stresses and strains they face over the coming months and years?



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

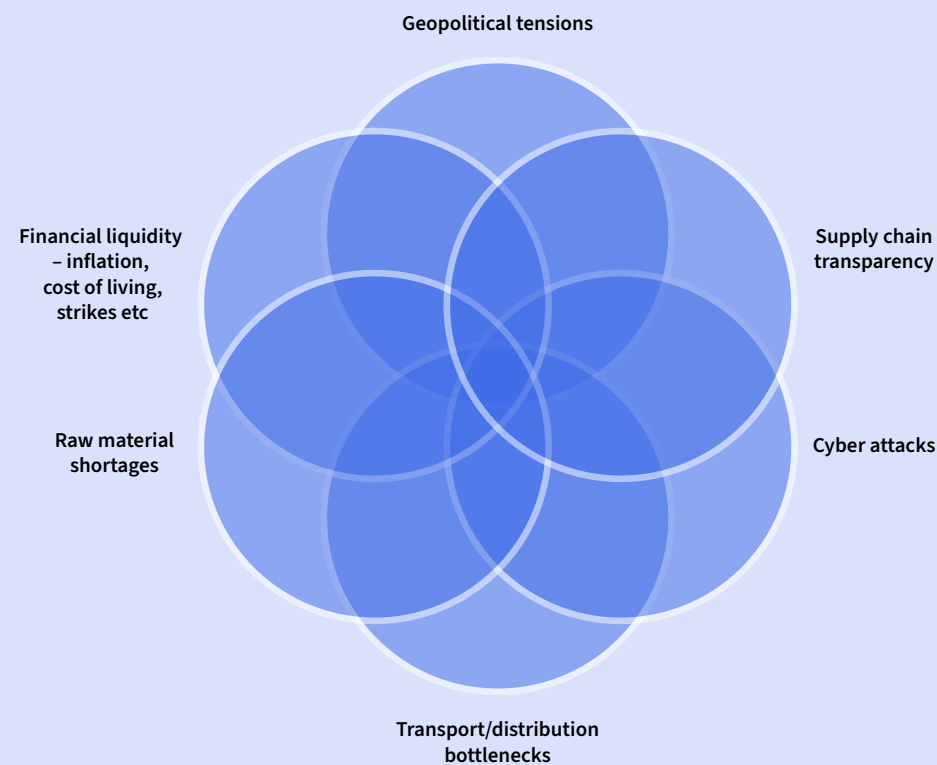
Digital disruption and new technology: Switching to automatic

The chief audit executives that participated in Risk in Focus 2023 are grappling with this reality. This year, the report explores five thematic risks – geopolitical uncertainty, climate change, organisational culture, cyber and data risk, and digitalisation and artificial intelligence. It outlines those challenges in detail and offers practical advice and know how about how to help organisations adjust to this new reality.

There are few obvious, easy answers to these problems. But internal auditors are uniquely placed to play their part in developing long-term solutions that have a real impact on organisations and the communities they serve. They need to secure from the board the resources and remit to tackle the most pressing risks with urgency.

If there was ever a time for the profession to step up and deliver on its full potential, it is now.

Venn Diagram Illustrating the Perfect Storm of High-Impact Interlocking Risks



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

METHODOLOGY

In the first half of 2022, a quantitative survey was distributed among chief audit executives (CAEs) by 14 European Institutes of Internal Auditors, spanning 15 countries including Austria, Belgium, Bulgaria, France, Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Slovenia, Spain, Sweden, Switzerland, and the UK. This survey elicited 834 responses, an all-time high for this research project.

Simultaneously, four roundtable events were hosted with 39 CAEs and 9 subject matter experts were interviewed, including CAEs, Audit Committee Chairs and industry experts from a range of countries to provide deeper insights into how these risks are manifesting and developing.

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 format of this report differs from previous years. Instead of giving each of the top ten risk areas relatively equal prominence, it was decided that a deeper look into areas of pressing importance to internal audit and their stakeholders would prove to be more useful. That is why the qualitative material has been used more prominently to contextualise the survey results, providing colour and up-to-the-minute

considerations for CAEs, with priority given to new issues and emerging themes that warrant attention.

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.



Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

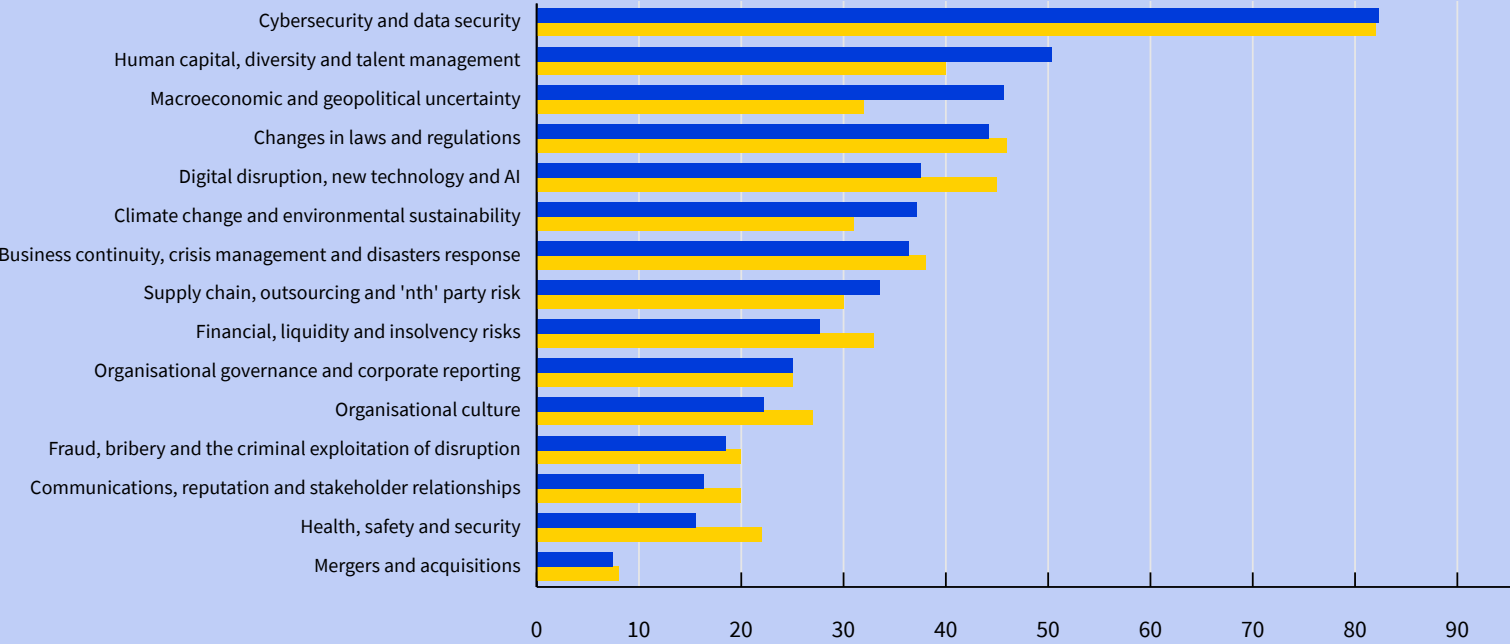
Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

Key survey findings

What are the top five risks your organisation currently faces?

Human capital risk moves into second place this year followed by macroeconomic and geopolitical uncertainty.



Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

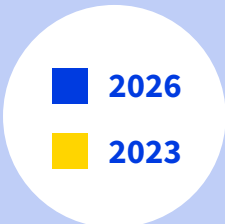
Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

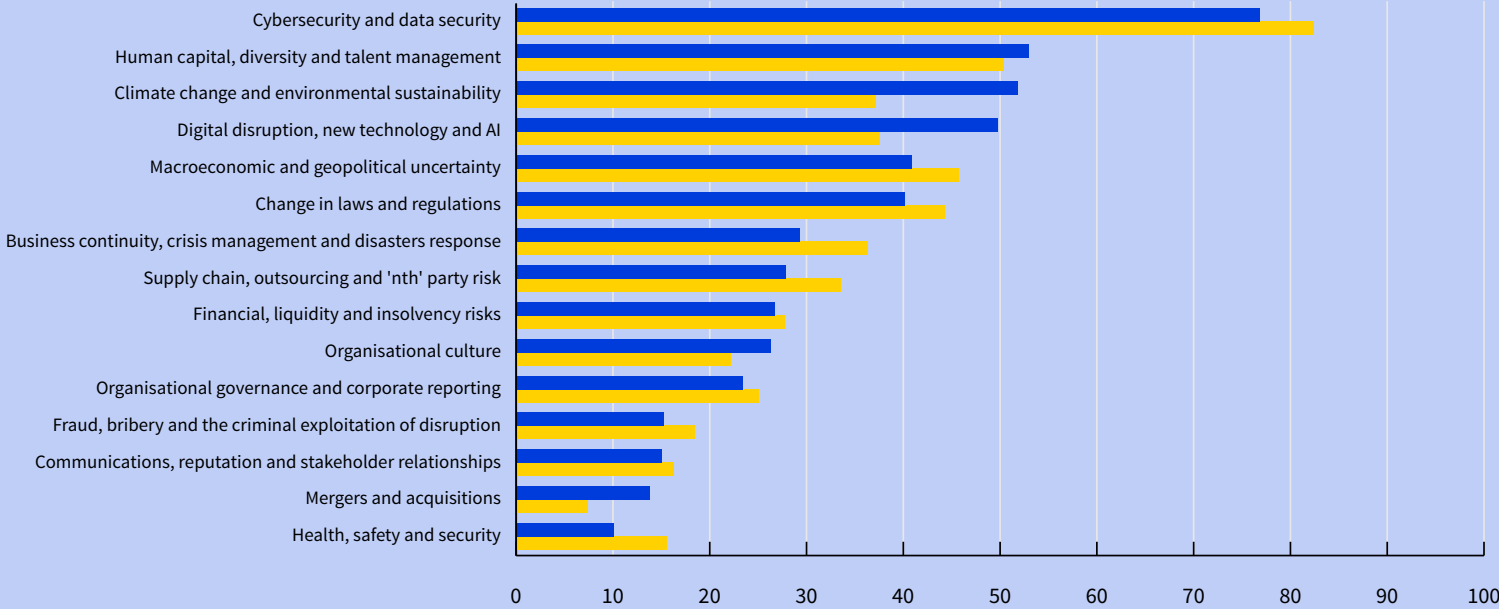
Digital disruption and new technology: Switching to automatic

Looking ahead

What are the top 5 risks that your organisation will face three years from now?



Cybersecurity and data risk is set to remain the number one risk to organisations.



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

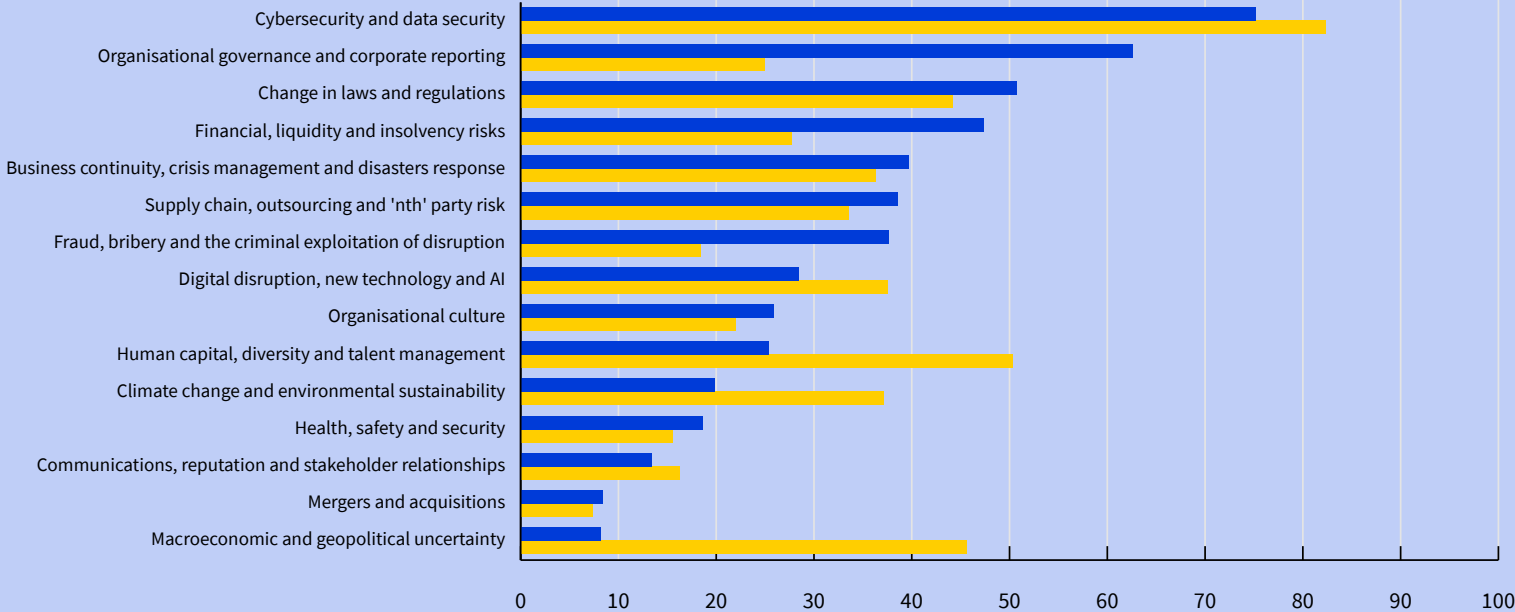
Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

Risk priorities vs. audit's focus

What are the top 5 risks on which internal audit spends most time and effort?



Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

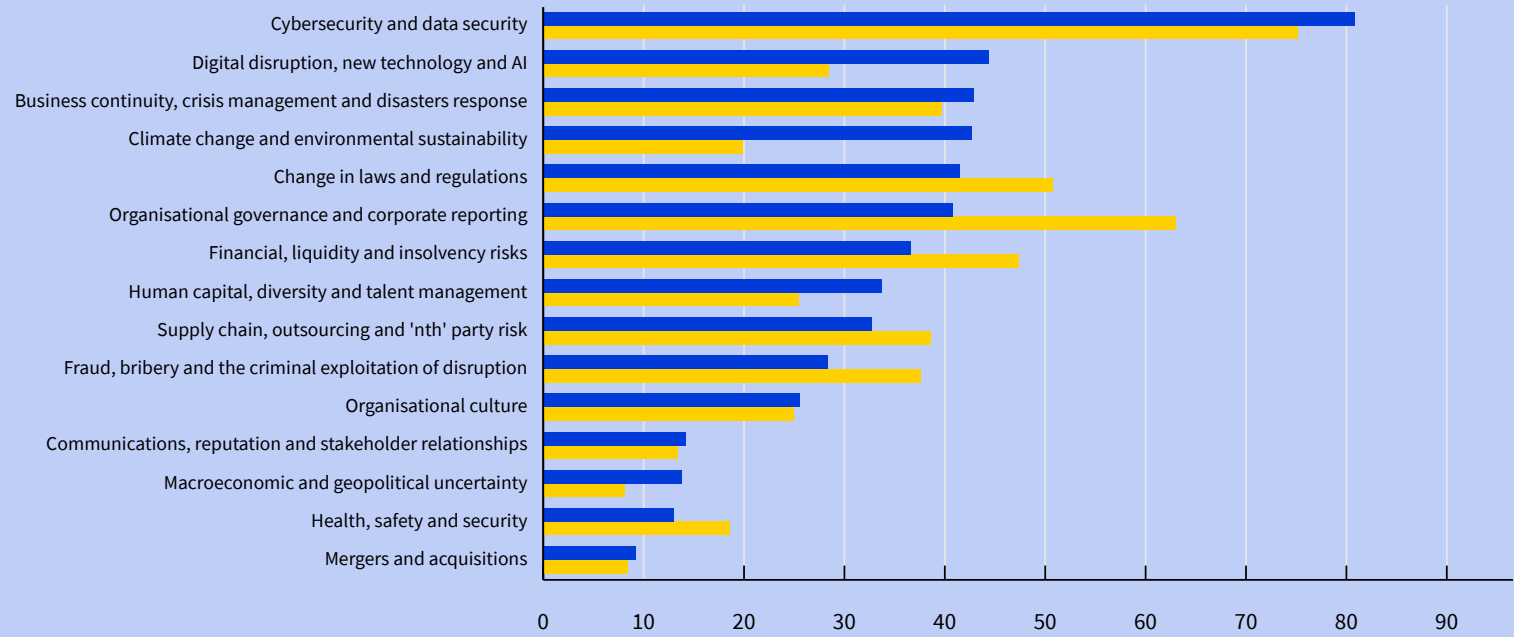
Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

Looking ahead

What are the top 5 risks you expect internal audit to spend the most time and effort addressing 3 years from now?



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

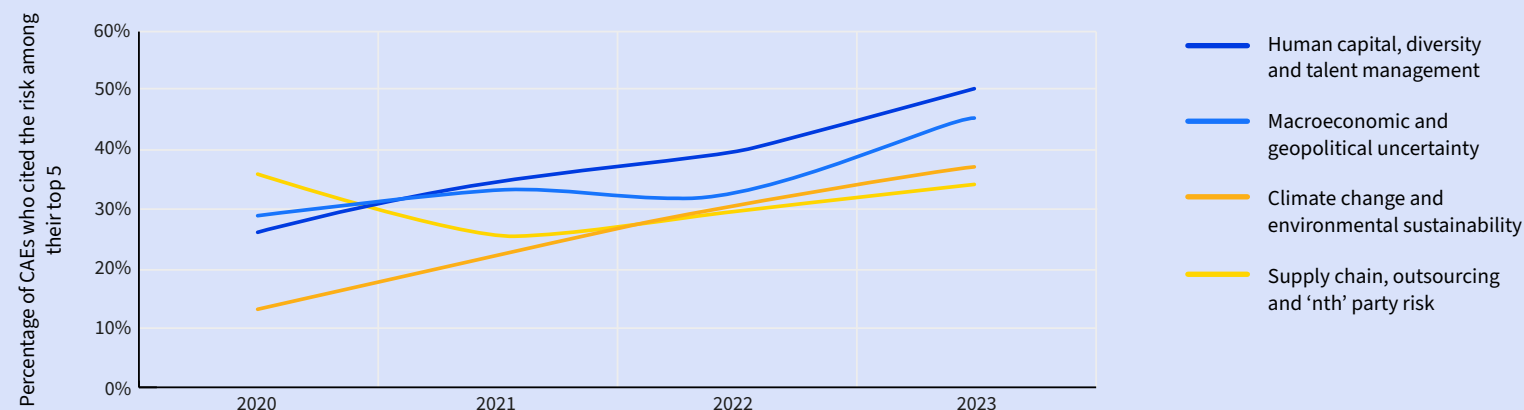
Digital disruption and new technology: Switching to automatic

Key survey findings



While cybersecurity continued to hold its top place in the Risk in Focus 2023 survey as the number one risk businesses face, human capital risk moved into second place (up from fourth in 2022) followed by geopolitical risk in third (up from seventh). The shortage of skills and labour has become more acute as behaviours engendered during the pandemic have started to play out.

Risk trends over time



Even as the risk of business continuity failures and financial, liquidity and insolvency risk that the pandemic had boosted in 2021 faded in 2022, the war in Ukraine helped to push geopolitical uncertainty risk higher. Rapid changes to the sanctions' regimes for Russian

businesses, as well as long-running developments in regulation over a wide range of issues, meant that changes in laws and regulations are still seen as a major threat (down to fourth place in 2023 from second in 2022).

Climate change is becoming a more persistent theme in the Risk in Focus surveys, rising this year to sixth place from eighth in 2022 and is starting to be a key area of internal audit activity as respondents expect the risk to rise to third place in three years' time. In contrast,



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

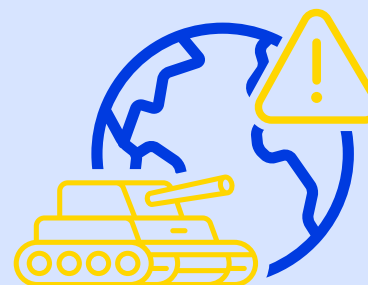
Digital disruption and new technology: Switching to automatic

Key survey findings

digital disruption fell from third to fifth place in 2023 with respondents also ranking it as low in the threat hierarchy three years from now. For example, last year respondents said it would rank second place in three years' time – in 2023, they say it will rank fourth place in three years' time.

If the risk rankings are changing rapidly, the areas on which internal auditors spend their time appears to be relatively static – raising the question of whether some functions need to be more agile to meet the changing needs of their organisations. Human capital, for example, moved up from 11th place in 2022 to 10th this year in terms of time and effort spent on this risk area, despite the huge pressure organisations are under to attract, retain, train and protect the well-being of staff. Organisational governance and corporate reporting, on the other hand, held its position as the second biggest area that

received internal audit's attention. How well internal audit departments continue to align their efforts to the needs of their organisations is likely to become more of a pressing issue as large-scale interconnected risks continue to rise with unprecedented speed in the years to come.



Geopolitical risk has risen to third, up from seventh in 2022



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

MACROECONOMIC AND GEOPOLITICAL RISK, EMERGING AND STRATEGIC RISK

Auditing in a time of crisis

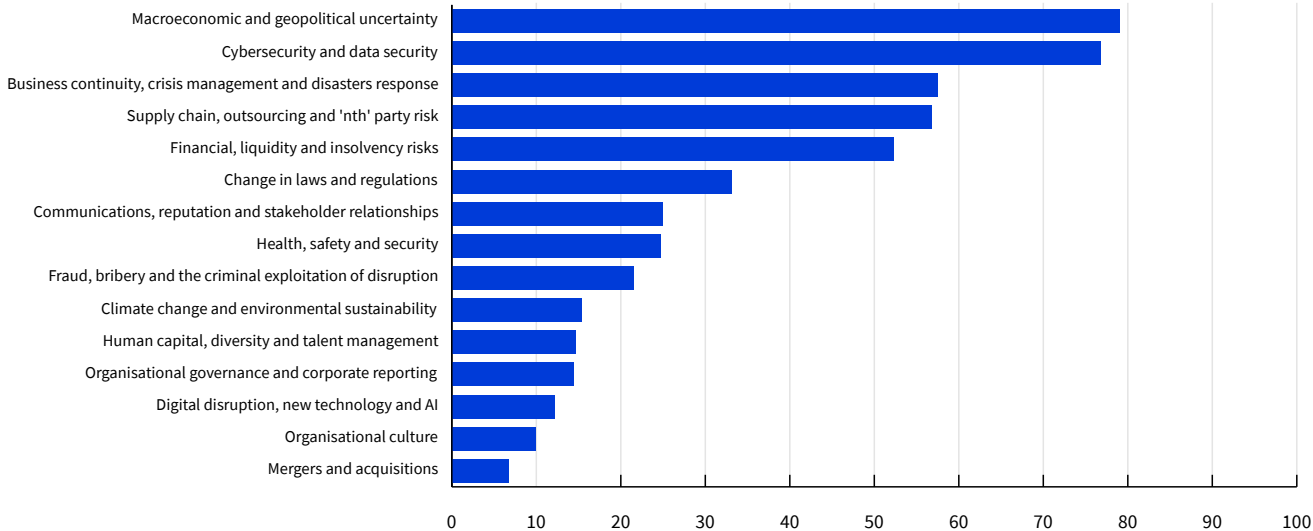
Macroeconomic and geopolitical uncertainty has jumped up the risk rankings in 2022, but such recent events could indicate a permanent change in the nature of emerging risk. Internal auditors must adapt to provide relevant assurance to their organisations.

The war in Ukraine took many organisations by surprise, including those with deep commercial interests in the region. As the Risk in Focus 2023 survey took place during the first quarter of 2022 when the conflict was just beginning, the crisis helped to push macroeconomic and geopolitical uncertainty into 3rd place in the survey, up from

seventh just a year ago. With 46% citing it as a top five risk this year, compared to 32% last year.

In a special question on the war, internal auditors said that the event's immediate impact on their risks included most prominently macroeconomic and geopolitical uncertainty.

What top five risks has the War in Ukraine had the most impact on?



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 13 OF 48

MACROECONOMIC AND GEOPOLITICAL RISK, EMERGING AND STRATEGIC RISK

Yet, internal auditors also said in the response to the general questions in Risk in Focus 2023 that risks associated with macroeconomic and geopolitical uncertainty ranked only 15th in terms of their time and effort – and was only likely to rise to 13th place on this metric in three years' time. As the extended ramifications of the conflict continue to unravel, this lack of attention to such a key risk seems either short-sighted or untenable.

The conflict has forced businesses into swift, often large-scale action. Organisations with ties to Russian businesses and the government severed them. Some organisations sold Russian subsidiaries at rock-bottom prices while others scrambled to source supplies of goods and services from outside the country. In response to sanctions by the European Union, the United Kingdom and the United States, Russia cut its supplies of oil to Bulgaria, Finland and Poland – pushing up prices. At the time of writing this report, the situation is highly volatile.

The war has also impacted financial liquidity and insolvency risk. While ranked ninth considered as the top risk facing organisations in the Risk in Focus 2023 survey (down from sixth last year), the risk scored fifth when considered as a direct impact of the conflict in Ukraine. The crisis comes at a time when Europe is winding down its unprecedented €2.3 trillion¹ aid package for businesses and governments across the zone and inflation – stoked by a cocktail of rising energy costs, wages and food prices – is on the rise. Not only are businesses readjusting to a changing customer landscape following the pandemic, but the war has also helped push the eurozone into becoming a lower growth, higher inflation region². Coming into the winter of 2023, these tensions are likely to intensify, especially if food and gas shortages worsen.

Further pressure on corporate finances is likely during 2022 and 2023 as the European Central Bank looks set to end 8 years of negative interest rates to deal

“Chief audit executives should re-examine their audit planning process to see if it is fit for the 2023 risk landscape”

with inflationary pressures. But perhaps surprisingly, the perceived impact of financial liquidity risk and insolvency risk dropped from sixth place in 2022 to ninth in the Risk in Focus 2023 survey, suggesting that many organisations that had survived the depth of the pandemic felt more confident about their prospects. Yet the speed at which high-impact change can impact organisations raises the uncomfortable question over whether internal auditors have given this risk enough prominence.



¹ COVID-19: the EU's response to the economic fallout, European Council of the EU, June 2022

² Spring 2022 Economic Forecast: Russian invasion tests EU economic resilience, European Commission, May 2022

Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 14 OF 48

MACROECONOMIC AND GEOPOLITICAL RISK, EMERGING AND STRATEGIC RISK

Rapid changes to sanctions

If a major area of focus in last year's survey was environmental regulation, this year it is the sudden acceleration of sanction risks. Internal auditors said dealing with changes in laws was the 3rd biggest risk in terms of the time and effort for their departments – the same as last year. While not a new threat, the scale and intensity of sanctions imposed on Russia by the European Union, United Kingdom and the United States has been unprecedented. Not only does it target Russian commercial and political interests, but individuals associated with the regime too.

It is a risk that is likely to grow in 2023 and beyond, partner at BDO specialising in economic crime Angela Foyle says. She warns that sanctions will increasingly become a weapon of choice for countries as they continue to wage economic war against opposing regimes. Tackling the fallout could force internal auditors and risk professionals to allocate more time to business continuity, supply chain and liquidity risks - all identified

by Risk in Focus 2023 survey respondents as impacts of the crisis.

Agility of risk assessments

“Sanctions of this scale and complexity are a nightmare to police,” Foyle says. Since they originate from different jurisdictions and apply to both organisations and individuals, simply keeping risk assessments up to date can be challenging. Businesses must map the restrictions imposed by all countries across their global enterprise - including those relating to sources of funding. Tracking the money trail when assets can be held by family members of those individuals who have been sanctioned can be difficult, time-consuming and costly.

Just as the quantity and depth of measures are altering, penalties are rising too. In 2022, for example, the UK introduced strict liability for sanctions breaches for both corporate entities and, potentially, directors, as well as name-and-shame procedures for those caught on the wrong side of the line³. Foyle says internal auditors should support their

organisations to both maintain up-to-date risk assessments in this area and strengthen controls for screening those with whom they do business, including both suppliers and shareholders. Having easy access to such data may mean beefing up data governance to increase transparency.

This is a key area where internal auditors must seek to work in co-ordination with first and second lines – especially legal, compliance and risk management. While many chief audit executives participating in Risk in Focus roundtables said they worked with other parts of the business, the practice of combined assurance is not as widespread as it might be – despite being the topic of IIA Standard 2050⁴.

³ The UK government passed the Economic Crime (Transparency and Enforcement) Act 2022 on 15 March 2022, which included these provisions

⁴ Combined Assurance: One Language, One Voice, One View, Sam C. J. Huibers EMIA, RO, CRMA, The IIA Research Foundation, 2015



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

MACROECONOMIC AND GEOPOLITICAL RISK, EMERGING AND STRATEGIC RISK

Emerging risks changing in nature

For Greg Schlegel, founder of the Supply Chain Risk Consortium in the US and Adjunct Professor for teaching enterprise risk management for Villanova University's EMBA programme, first the pandemic and now the conflict in Europe have underlined a fundamental shift in the nature of emerging risks.

Instead of being siloed into the kind of categories that appear on most risk registers, such threats cut across all business areas and are fundamentally outside of the organisation's control. Low-probability, high-impact events such as natural disasters, political upheaval, inflation, pandemics and wars may turn out to be more common than people think. Supply chains not only face disruptions from geopolitical tension, but from shortages of raw materials and components – from grain to computer chips – and from a lack of workers following the pandemic and events such as Brexit. In fact, Schlegel says the strategic threats posed by

supply chain disruption are often existential either to lives or organisations.

Too many assurance professionals overlook their importance, he says, or perhaps some boards set different priorities for them. While internal audit priorities may not always map onto strategic risks, a recurring issue flagged by the Risk in Focus 2023 survey (as well as in the 2022 survey) is a persistent mismatch between what internal auditors identify as their organisations' key risks and where they spend most of their time. For example, respondents rated human capital and macroeconomic risks in 2nd and 3rd place in the biggest risk ranking - but 10th and 15th place for the time allocated to deal with it. By comparison, behind cybersecurity, internal auditors spend most time on organisational governance and corporate reporting, and changes in laws and regulations.

“When auditors see one of these low-probability, high-impact strategy risks, they tend to kick the can down the road,” Schlegel says. It is a trend he sees among his manufacturing clients where many spend the

most time on tactical and operational risks which have minimal impact on the business. If chief audit executives find themselves in this situation, he urges them to re-examine their audit planning process to see if it is fit for the 2023 risk landscape. “Auditors have to get executives involved in this process,” he says, “by putting together a compelling, forward-looking business case that clearly spells out the risks and rewards.”



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 16 OF 48

MACROECONOMIC AND GEOPOLITICAL RISK, EMERGING AND STRATEGIC RISK



Supply chain disruption

In particular, Schlegel predicts that stress on supply chains will be a constant feature over the next few years, especially since the European Commission's Proposal for a Directive on Corporate Sustainability Due Diligence seeks to further tighten environmental and human rights protection in law⁵. In this year's survey, supply chain, outsourcing and "nth" party risk ranked eighth in terms of its potential impact (up from ninth in 2022) and respondents said it ranked sixth in terms of the areas where internal audit functions spend most time and effort.

The nature of extended enterprises means that organisations are increasingly exposed to high-impact events directly and through their supply chains. The answer? "Get clear visibility of your supply chains then digitise them," Schlegel says. That means taking the entire supply chain structure and putting it into a digital model so that internal auditors can do "what if scenarios?"

for their businesses. Once management sees how the supply chain reacts and what the potential cost of such events are, they will be able to begin building risk mitigation plans grounded in reality. It will also help build the case for better funding for the second and third lines.

Yet over and above these systemic risks that cut across many areas of the business, operating in a permanent state of emergency poses its own challenges.

Crises now systemic

"It is more than three years now since we have been in a state of emergency, including most recently from the situation in Ukraine, and we can see that these crises are becoming systemic," Stanislas Martin, chief risk officer at the French energy company EDF who is responsible for crisis management at the business, says.

Every sector has its own story. As well as the pandemic, a storm-induced, winter energy outage in Texas in 2021 triggered

concerns in the industry that exceptional worsening weather conditions could lead to more frequent shutdowns elsewhere in the world. Energy systems are generally designed to withstand peaks in demand during cold snaps - but not if they happen in all parts of the system (or across inter-connected countries) at the same time. It sparked a global rush in energy businesses to understand which lessons could be learnt from the Texas storm and to ensure that they could manage such risks in future. Then, from September 2021 - and set to continue into 2023 - energy shortages started to send prices high, a situation that has spiralled into a full-blown global crisis because Russia is a key supplier of gas in Europe.

"These crises are becoming systemic"

⁵ Just and sustainable economy: Commission lays down rules for companies to respect human rights and environment in global value chains, European Commission, February 2022

Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

MACROECONOMIC AND GEOPOLITICAL RISK, EMERGING AND STRATEGIC RISK

Crisis management systems broken

Martin agreed with Schlegel that while in the past, crises generally were contained in one or two areas of the business, now they infuse all aspects of an organisation with urgency and a heightened sense of threat – but enterprises that are not properly trained through global crisis management exercises find it difficult to resolve issues quickly because of the scale and complexity of their potential impact and the fact they have no control over their causes.

Traditionally, an operational crisis management team would help the part of the business affected deal with the event and attempt to bring it under control. If several crises arose in a year, people would be rotated in and out of the team because of the intense nature of the work. These types of arrangements have been fundamentally broken by recent events because it is beyond the scope of a crisis management structure to cope with non-stop emergencies. Internal auditors responding to the Risk in Focus 2023 survey rated business continuity, crisis

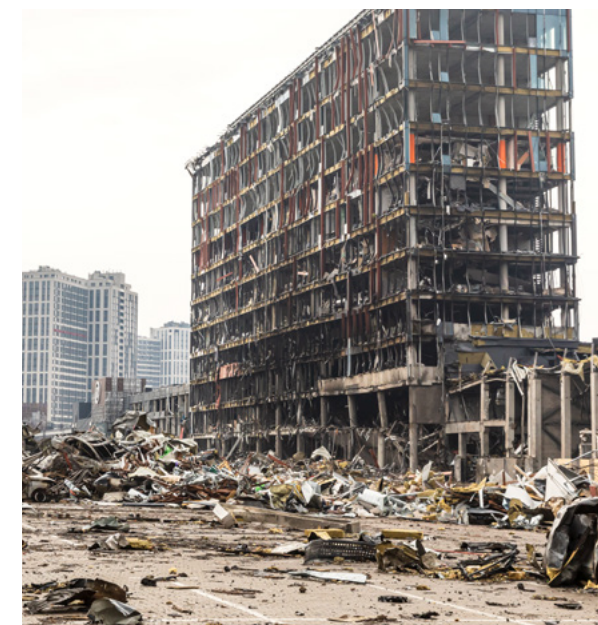
“How do you think through a scenario when it is a potential issue and before it gets to the stage of crisis?”

management and disaster response fifth as the risk area where they spent most time and effort – compared with fourth in the 2022 survey.

In many industries, the entire enterprise has effectively become the crisis management team whether they have been prepared for it or not. In addition, says Martin, the impact of such threats can jump unpredictably from one area of a business to another within days, weeks and months - in effect creating sub-crises of differing intensities - in a way that makes resource allocation critical.

“The cumulative level of fatigue and employee burnout has also to be taken into consideration,” he says. Additional pressure on staff from waves of colleagues falling ill during the pandemic, or key posts remaining vacant, have added to a sense of exhaustion, not just in front line services such as health and retail, but more generally in all sectors where rolling crises have become the norm.

Given that businesses are already struggling to retain and attract staff, risk managers and internal auditors need to push training and well-being centre stage in 2023 to help both organisations and their departments improve their resilience (see Human capital chapter, defining better controls).



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

MACROECONOMIC AND GEOPOLITICAL RISK, EMERGING AND STRATEGIC RISK



Reassessing global risk

The conflict in Ukraine has revealed that the interconnected global energy systems that were established to ensure stability of supply can become a cause of vulnerability and risk, says Ken Marnoch, Executive Vice President, Internal Audit and Investigations, Shell International. Not only are the energy implications of reducing Europe's reliance on Russian energy complex, but could take years to play out.

"The situation is similar to what happened with the COVID-19 pandemic. Based on experience with dealing with other virus outbreaks, for example severe acute respiratory syndrome, or SARS, there was initially a belief that the COVID-19 pandemic would be a localised problem," he says. "That meant that very few people asked the question, 'what happens if our global supply chains get disrupted because of a pandemic?', much less prepared for it."

Risk mitigation plans often missed the possibility of global demand for the same

pieces of medical equipment at the same time as a global disruption to supply chains. With the benefit of hindsight, the assumptions and the natural tendency to 'hope for the best' did impact the response to such a large-scale event.

Over the last couple of years, Shell businesses have rethought 'risk management'. The kinds of credible worst-case scenarios that used to be relatively confined to the crisis management team have now become much more readily disseminated and discussed within the businesses as part of everyday risk management. In addition, business continuity planning is now reframed to think with a local or regional focus as well as discussing what could happen if all parts of the organisation were affected by the same or linked events - such as the switch in energy usage patterns and IT network loads when working from home became a global phenomenon.

"How do you think through the range of scenarios, including the credible worst case, when those scenarios are still only a potential issue and not yet a crisis?" he says.

"From a practical point of view, that can entail consciously encouraging critiques to be actively raised and considered."

Clarifying risk appetite

Marnoch and his team are engaging in what he calls "stronger conversations about risk appetite". He says having a clear understanding of how much risk each business can take on in specific areas is most useful during a dilemma - where all choices may have potential upsides and downsides. Then, clarity on the appetite for the risks associated with the different choices can act as a guiding light through the problem.

Historically, Shell's internal audit had focused on operational, culture and conduct-based risks. The internal audit group has now set up a specific team to focus on the risks and control framework associated with the delivery of strategic objectives.

"If you break strategic objectives down to measurable goals, the related risks, the explicit controls, and an understanding of



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



MACROECONOMIC AND GEOPOLITICAL RISK, EMERGING AND STRATEGIC RISK

how business leaders know that the controls are working, then you have the scope for an internal audit,” he says. “Part of the role of the new team is to help people move away from fixed thinking around the correctness of assumptions they made at the beginning of a project, or strategy, when so much in the

world is changing dramatically. How to be actively inquisitive, to find information that tests the beliefs and the fast feedback on the current reality are required to navigate an uncertain future.”

“If you let go of the need to be right and acknowledge it was a decision made with the best information at the time, you will be more open to looking for information that challenges your thinking. That opens up a lot more power in managing a key risk in the delivery of your strategic objectives.”

Key questions for internal audit in evaluating the risks of the organisation

1. In terms of the time and effort spent on internal auditing assignments, how is internal audit aligned to the organisation’s strategic objectives – including on geopolitical risk and climate change?
2. How strong is the support for internal audit activities in areas such as strategy and crisis management and what can be done to improve that support where it is lacking?
3. How far is internal audit able to leverage resources of other lines to provide proper coverage and minimise the duplication of effort?
4. How do you know whether the assumptions the organisation (and the internal audit function) have made about the nature of key risk areas are still valid today and fit the circumstances likely to arise in 2023?
5. Does the organisation have up-to-date risk assessments for sanctions risk and robust controls for screening third party ownership and company shareholders?
6. How far does the organisation take advantage of digital tools to model key risks and to run “what if” scenarios?
7. Have you reassessed the relationship between the organisation’s business continuity, crisis management and risk management teams to ensure they are fit for purpose?
8. Does the organisation seriously consider critical voices and those of external experts in their assessment of risks?



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 20 OF 48

CLIMATE CHANGE AND ENVIRONMENTAL SUSTAINABILITY

Transition to climate change auditing

Auditors are beginning to get to grips with auditing environmental sustainability, but helping organisations achieve their objectives requires a holistic approach.

While internal auditors have had climate change on the agenda for some time, chief audit executives taking part in this year's Risk in Focus 2023 roundtable on the topic agreed that it was moving higher up their agendas. "Last year we were starting to wake up to the issue with training and seminars; this year we are getting into the detail and starting to implement environmental issues in every audit," said one participant.

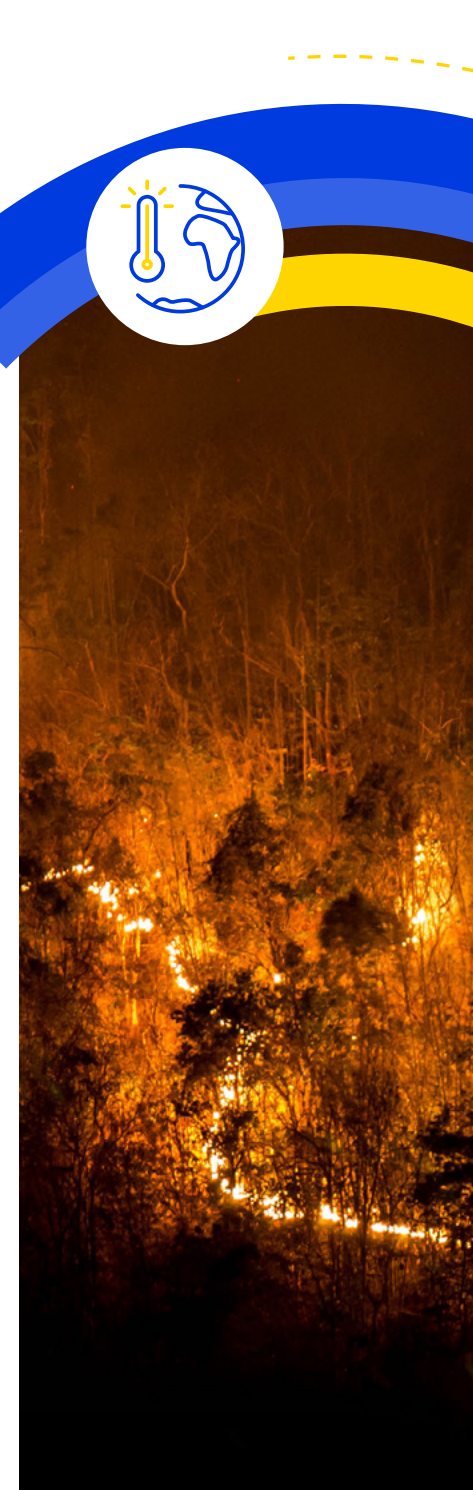
In the Risk in Focus 2023 survey, internal auditors said that climate change was the 6th most important risk they faced, up from 8th from last year. With 37% citing it as a top five risk compared to 31% last year. And they expect it to move up to 3rd place in the risk rankings and 4th in terms of the amount of time they spend in three years' time – that makes it one of the most dynamic, fast-moving risk areas for the profession.

As temperatures soared to unusually high levels across Europe at the time of writing, the

evidence of unpredictable change is clear – yet unless internal auditors get a firm grip on the issue now, the risk could become the next big crisis that organisations are unprepared for. While internal auditors are shifting more resources into climate change assignments, they do not yet give it the priority it deserves. Today, it ranks only 11th place in terms of where they say they spend their time and effort. If internal auditors want to move it to 4th place, they need to step up their efforts in this area today.



37% of internal auditors cited climate change as a top five risk compared to 31% last year.



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 21 OF 48

CLIMATE CHANGE AND ENVIRONMENTAL SUSTAINABILITY

COP26's stretching goals

The Conference of the Parties (better known as COP 26) set fresh climate goals that organisations may struggle to help meet. Key targets included securing net global emissions by 2030 to keep warming to 1.5 degrees within sight⁶. In addition, in 2022 the European Financial Reporting Advisory Group released the Exposure Drafts for European Sustainability Reporting Standards, a key component of the Corporate Sustainability Reporting Directive. These are due to be finalised by the end of 2022, as are the International Sustainability Standards Board's own financial rules on climate and sustainability-related disclosures⁷.

In key sectors, the impact of COP26 will be huge. "For Shell, Powering Progress sets out our strategy to accelerate the transition of our business to net-zero emissions by 2050. Shell's current operating plans do not reflect our 2050 net-zero emissions target. In the future, as society moves

towards net-zero emissions, we expect Shell's operating plans to reflect this movement. However, if society is not net zero in 2050, as of today, there would be significant risk that Shell may not meet this target. This is a global challenge and one where we also need to work with our customers and across sectors to accelerate the transition to net zero. We can learn from the experiences from the response to the pandemic and the conflict in Ukraine," Ken Marnoch, Executive Vice President, Internal Audit and Investigations, Shell International, says. The world needs more and cleaner energy solutions to power progress, and this requires fast learning, complex decision-making and effective risk management at Shell.

Climate change framework

Shell is developing its management frameworks to enable it to make the transition to net zero, and Marnoch wants his team to be part of the assurance around

the frameworks as they are being built. Shell Internal Audit is therefore asking questions on the business objectives, the risks associated with those objectives, what controls would be appropriate and how assurance around those controls can be integrated as the frameworks develop.

He says that internal auditors should make sure that they can be involved during the carbon transition journey. They can provide timely feedback and provide assurance to the Audit Committee about how it is developing and how risks are being managed instead of coming in a couple of years down the line and raising concerns.

"The energy transition to renewables has very similar dynamics to the pandemic and the conflict in Ukraine"

⁶ COP 26 goals, UN Climate Change Conference UK 2021, 2021

⁷ NEW PROPOSALS FOR EUROPEAN SUSTAINABILITY REPORTING STANDARDS, Accounting for Sustainability, May 2022



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

CLIMATE CHANGE AND ENVIRONMENTAL SUSTAINABILITY

Internal audit's role

Because organisations are at different levels of maturity in their journey to achieving environmental sustainability, internal audit's role can be hard to pin down with certainty. Those who are unsure should consult Chartered IIA UK and Ireland's paper, *Harnessing internal audit against climate change risk*, which urges boards to give functions the authority to work at a strategic level on the issue⁸. IIA Netherlands paper *Climate change and environmental risk*⁹ advises to centre efforts around assurance on reporting, the risk management of sustainability goals and (or) climate-related consultancy where needed. (This risk can be tackled by internal auditors in five ways outlined in the Risk in Focus 2021 special supplement.¹⁰)

Chief audit executives at the Risk in Focus 2023 roundtable agreed that, as well as helping management shape strategies and goals, internal auditors must lead the way in helping raise awareness and drum up meaningful support for environmental initiatives. "Some people will want to just chase the key performance indicators, but others at all levels of seniority really believe in the climate agenda," said one chief audit executive. "Get those people involved and set goals from the bottom as well as the top of the business to create a full process that is driven by those who want to see change happen."

Chief audit executives should also ensure that those team members who are most committed to helping address climate change issues are assigned key roles in assignments where feasible. They are more likely to challenge management and push for internal audit recommendations to be completed. Assessing the attitudes of internal audit team members on the issue can be tested in staff evaluations.



⁸ *Harnessing Internal Audit Against Climate Change Risk*, Chartered IIA UK and Ireland, October 2021

⁹ *Climate Change and Environmental Risk - challenges and tools for Internal Audit*, IIA Netherlands, 2021

¹⁰ *RiF 2021 Practical guidance on climate change and environmental sustainability*, European Institutes Research Group, January 2021

Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 23 OF 48

CLIMATE CHANGE AND ENVIRONMENTAL SUSTAINABILITY

Avoiding box-ticking and green-washing

Moving to a more practical approach has thrown up some thorny questions. For example, attendees at the roundtable agreed that there is currently too much emphasis placed on the important topic of reporting - not surprising given regulatory pressures in both the United States and Europe - a key topic in Risk in Focus 2022. But that leaves open the question of how an organisation's governance model is to work effectively to integrate sustainability goals without it being relegated to a box-ticking exercise around regulatory requirements. In addition, a separate study by IIA Netherlands found that measures taken to tackle climate change risk range from including the topic in the risk register (47%) to using KPI's (41%) – but none of the initiatives were used by over half the organisations surveyed¹¹.

Internal auditors must ensure that their organisation's basic compliance efforts do

“We can make some big improvements without overloading people as they struggle to cope with various crises”

not replicate the worst excesses of the culture created by the 2002 Sarbanes-Oxley Act over controls around financial reporting. That pushed swathes of internal auditors into low-level compliance exercises, sometimes at the expense of being able to provide more value adding services.

“It is easy to build a SOX-style system that does not help the organisation achieve its environmental objectives,” The chief audit executive at an international IT company says. “There is a risk that there will be many companies who are good at communicating on environmental risk, but poor at managing it.”

But, he says, chief audit executives must accept that it will be a long journey, not least because the activity is in its infancy. In his view, the risk of green-washing is partly an outcome of having relatively low levels of maturity in the

non-financial reporting standards currently available and in development. He sees a parallel with the development of more stringent capital adequacy requirements, particularly the self-assessment of risks, that arose in the financial services industry following the economic crisis of 2007-2008.

“From that example, it is easy to see that it will take time for KPIs around environmental reporting to make sense and become properly comparable,” he says.

¹¹ Climate Change and Environmental Risk - challenges and tools for Internal Audit, IIA Netherlands, 2021



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 24 OF 48

CLIMATE CHANGE AND ENVIRONMENTAL SUSTAINABILITY

Focus on ESG

Echoing comments made by chief audit executives during the Risk in Focus environmental roundtable, he adds that his recommended approach for internal auditors is to consider that Environmental, Social and Governance (ESG) really begins with the “G” of Governance¹². In fact, while organisational governance and corporate reporting ranked 10th as a risk in the Risk in Focus 2023 survey, it ranked 2nd in terms of the area where internal auditors spend their time – suggesting many see it as an opportunity to help their organisations manage a wide range of issues, including climate change¹³.

“You could say that governance is the mother of all concerns and all solutions,” the chief audit executive at an international IT company says. “Good governance will provide the transparency you need to protect you from green-washing. And it also provides assurance to key stakeholders that you are on the right path.”

For some organisations, such as banks, the business’ own environmental impact is relatively easy to measure in terms of its infrastructure of buildings and energy consumption. More difficult is its risk assessment of the carbon impact related to loan books, for example - a key third-party risk.

Linking controls to environmental strategy

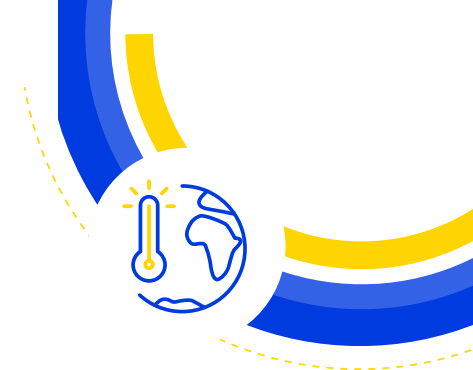
“Banks’ policies and philosophies on financing transition, who you will or won’t do business with is fundamental,” John Devine, risk committee chair for abrdn, says. “These decisions are wider than just climate change, they feed into the entire ESG agenda.”

Devine says that because the situation is fluid internal audit must adapt its approach accordingly. Irrespective of specific new developments, every organisation must have a clear strategy, which it can talk about to investors and “walk the walk.”

“Since every company is making legal, voluntary and marketing disclosures in these areas, internal auditors need to make sure that the control processes underpinning what a company is saying really resonates back to the core strategy,” he says, “because the big risk is that those statements are wrong.”

If banks are lending to coal-burning companies on the axis of transition, for example, they must have policies in place to validate that external business’ carbon transition plan. Internal audit’s role is to ensure that the bank has robust controls in place around those validation processes.

The driver that will continue to push accurate reporting beyond heavily regulated industries, Devine believes, is shareholder pressure. Proxy agencies, pressure groups and individual investors, for example, may take a relatively binary view on whether a business is meeting its environmental targets, he says. Over the past few years, that pressure has driven the need for better control processes to validate information and led, in Devine’s view, to the need for the professionalisation of non-financial indicators.



¹² Internal Audit and ESG Criteria, IIA Spain, November 2021

¹³ GLOBAL PERSPECTIVES & INSIGHTS - The ESG Risk Landscape, Global IIA, 2022

Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 25 OF 48

CLIMATE CHANGE AND ENVIRONMENTAL SUSTAINABILITY

Building skills and knowledge

Over and above the necessary technical auditing skills, the chief audit executive must understand the business, the context in which it operates, and crucially must have influence. “The chief audit executive must have a seat at the table, be able to talk to the CEO, the audit committee, and get things on the agenda and make sure audit’s voice is heard and is listened to,” he says.

While Devine accepts that outside of larger, multinational industries, chief audit executives do not always enjoy that status, he says that organisations that want to get to grips with climate change and broader ESG issues must give the function the prominence it needs to do its job.

Chief audit executives at the Risk in Focus 2023 roundtable mostly said they were taking a blended approach to auditing particular environmental issues, although some departments had yet to start full-scale, real-life auditing. A blended approach entails both conducting audits

on the specific impact of the business on the environment - using, for example, standards such as ISO14001 - at the same time integrating sustainability issues into other audits, where possible.

For those who have started environmental auditing, one of the biggest challenges has been to up-skill their teams – a difficulty for all departments given the struggle to attract and retain high-quality staff into internal auditing, an issue raised by most Risk in Focus 2023 roundtable participants under all topics covered by this year’s report. Understanding the complex global regulatory landscape and its potential significance for the business can be a major undertaking and many businesses seek help from external audit firms and global consultancies. But it is only half the picture. The other is being able to bring in engineers, scientists and other experts to help with building subject matter expertise. While some assistance can be found within the business, increasingly chief audit executives are turning to external sources for help to source such experts. Internal auditors must ensure their departments have access to the right skills

and knowledge to get on top of climate-related risk before it is too late.

“You could say that governance is the mother of all concerns and all solutions”



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

CLIMATE CHANGE AND ENVIRONMENTAL SUSTAINABILITY



How internal audit can help the organisation

1. Talk to the CEO or board to help them reflect on where the company stands on climate change and what it really wants to achieve compared with regulations, competitors and societal expectations.
2. Understand the company's goals and current maturity on climate-related sustainability and assess how far this is reflected in the business and action plans on different levels.
3. Assess how far management has both considered the organisation's impact on the environment and the environment's impact on the business – the issue of double materiality.
4. Assess the reliability of the organisation's climate-related KPIs.
5. Assess the robustness of the controls and risk management processes associated with these goals and risks.
6. Assess how well the second line monitors climate-related risk and the accuracy of climate-related data.
7. Assess the extent to which corporate stakeholder communications on climate change initiatives are supported by sufficient data to avoid the charges of green-washing and its attendant reputational risks.



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

HUMAN CAPITAL, DIVERSITY AND TALENT MANAGEMENT

The human factor

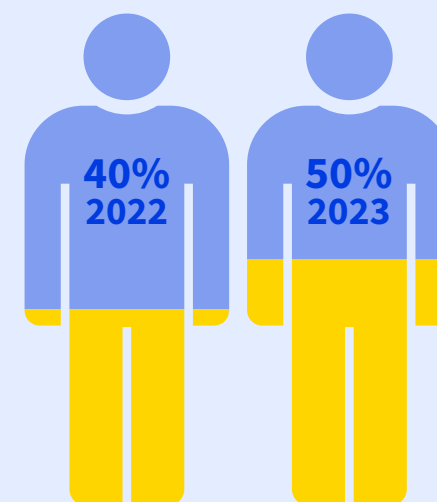
Organisations need to find their social purpose to overcome their human capital challenges, which means internal auditors must focus less on the numbers.

In the wake of an ongoing pandemic, organisational culture and talent management have become key areas of competitive advantage for organisations. Human capital, diversity and talent management ranked 2nd in Risk in Focus 2023's risk ranking, up from fourth place in 2022. With 50% citing it as a top five risk this year compared to 40% last year. Eighteen per cent of respondents said it was their number one priority. It is a risk that is firmly cementing itself among the hardest challenges businesses face and internal auditors say that it will rank as the second largest risk three years from now – with 21% saying it will be their number one priority.

Chief audit executives taking part in the Risk in Focus 2023 roundtable on the issue agreed that the pandemic had fuelled new

challenges as well as accelerated longer running trends. In 2023, the global talent shortage is likely to increase, particularly for those organisations seeking to employ people with technical expertise, because luring people back into workplaces while ensuring their psychological well-being has moved higher up the agenda. More recently, inflation has moved pay settlements and industrial action centre stage – and with the rising operational costs, some businesses will struggle more to retain staff.

“Not being able to keep pace with all of the expectations around social issues and the impact on organisational culture is a huge risk,” said one chief audit executive at the roundtable. “But companies are not quick to adapt in this area and need to speed up significantly.”



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



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

HUMAN CAPITAL, DIVERSITY AND TALENT MANAGEMENT

Adapting to hybrid working

Hybrid working styles were already on the rise before Covid, but offices are struggling to accommodate workers who want the more flexible working conditions that arose during the pandemic to continue, according to a 2022 survey by Microsoft. Almost 7 out of 10 (69%) of European managers wanted to do more to help teams meet employee expectations but said they did not have the influence or resources to do so. And 53% said their organisations were out of touch with what employees wanted¹⁴.

The greater problem, though, is that fewer people want to work at all. While in the United States, the so-called great resignation saw record numbers of people dropping out of the workplace altogether, in Europe pressure on wages has been intensified by, among other trends, a lack of skilled workers and younger people quitting work¹⁵.

“What’s really bothering us is the number of skilled, experienced, older people who are choosing to leave the workforce altogether to do something less pressurised, while at the same time younger people are staying longer in education,” Kate Shoesmith, deputy CEO of the Recruitment Employers Confederation in the UK, said in this year’s Risk in Focus 2022 supplementary report, Risk overview: human capital, diversity and talent management¹⁶.

The combination of leeching institutional knowledge, skills and personnel shortages has increased the sense of burnout in many organisations and left businesses with hard-to-fill gaps for key projects, such as digitalisation – a process that promises to alleviate staff shortages through automation. If there was one single issue that all chief audit executives that took part in the various roundtable sessions and one-to-one interviews agreed on, it was this.



¹⁴ 2022 Work trend index: annual report: Great expectations: making hybrid work work, Microsoft, March 2022

¹⁵ Why The Great Resignation is Happening in Western Europe Too, YPulse, November 2021

¹⁶ RIF 2022 Risk overview: Human capital, diversity, and talent management, European Institutes Research Group, March 2022

Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

HUMAN CAPITAL, DIVERSITY AND TALENT MANAGEMENT

Defining normal working practices

John Devine, risk committee chair for abrdn, says that organisations need to understand when they are coming out of the crisis and what it means to normalise working practices. In his experience, such events accelerate and force change – and successful organisations are quick to adapt. Businesses that expect things to go back to how things were prior to the event may be missing opportunities or, worse, not recognising challenges to their business models. Internal auditors are well placed to help the business to distinguish between what may be just cyclical trends and the deeper, more permanent changes that are taking place.

“Internal audit needs to understand what the new normal is both for the business and itself, and that is likely to entail recutting and retooling organisational culture,” he says. That can involve making changes to employment policies to create flexibility where needed around work-life balance, which will differ depending on the sector and organisation.

More fundamentally, though, whatever policies organisations have, businesses need to ask, “how do I create an organisation with a heart?” Devine says. That means creating a core that accommodates diversity but that is operational, productive and functional whether people are at home or not. But, he says, in the new emerging risk landscape, businesses will need to be open to adapt as circumstances inevitably continue to change.

Building social purpose

Younger people tend to be more interested in working in organisations whose social purpose is aligned with their own goals and beliefs. The rise of social enterprises in the past decade is just one indication of that shift in priorities. While internal auditors ranked human capital as the second biggest risk their organisations faced in this year’s Risk in Focus 2023 survey, the organisational culture that could help attract new talent only ranked in eleventh place.

In fact, there is a gap between how people at different seniority levels in organisations perceive their relationship with the business, according to a study by the consultant McKinsey, which could suggest why human capital and organisational culture may sometimes be considered as separate issues. While 85% of executives and upper managers agreed that they could live the purpose of the organisation in their day-to-day lives, only 15% of frontline managers and employees agreed.

“When employees at any level say that their purpose is fulfilled by their work, the work and life outcomes they report are anywhere from two to five times higher than those reported by their unfulfilled peers”



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 30 OF 48

HUMAN CAPITAL, DIVERSITY AND TALENT MANAGEMENT

ESG sustainability goals

Anita Punwani, who represented the UK as an expert in the development of the international standard in governance at the International Organization for Standardization, and head of the Environmental and Social Governance Group at the Institute of Risk Management, says that organisations often fail to connect their own values and purpose with changes happening in society at large.

The advent of the use of smartphones together with discussions taking place on social media has made such an attitude untenable, not least because every key stakeholder, including members of staff, now are commentators on the behaviour as well as the performance of a business.

Organisations can use the UN Sustainable Development Goals as a starting point for their ESG ambitions and work back from there to consider how that impacts their own purpose and goals. Internal auditors can use that project to speak to

“Not being able to keep pace with all of the expectations around social issues and the impact on organisational culture is a huge risk”

a wide array of stakeholders, which will help inform the company of the specific social context in which they are operating. In fact, the EU’s pandemic recovery plan – NextGenerationEU¹⁸ – represents a unique opportunity for internal auditors to underline the importance of ESG in corporate governance since it is built on the UN’s goals. NextGenerationEU is highly focused on climate change, biodiversity and gender equality to build a more equitable Europe in the wake of the pandemic.

Refreshing the governance framework could help businesses align with such initiatives. “Organisations are structured in a certain way to deliver on strategies and goals, so bringing about change is not easy,” Punwani says. “In some cases there will be the building blocks for change; in others it may need a whole change programme.”

Those in the first, second and third lines are often too focused on reporting. But internal auditors are uniquely placed to use their facilitation skills and breadth of reach across their organisations to foster a constructive discussion to help management to create a purpose that is relevant and resonates with the cultures in which they operate.

¹⁸ Recovery plan for Europe, European Commission, July 2022



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 31 OF 48

HUMAN CAPITAL, DIVERSITY AND TALENT MANAGEMENT

Creating the right metrics

Chief audit executives participating in the Risk in Focus 2023 roundtable said internal auditors should separate those areas that could be usefully dealt with by assigning clear metrics to goals - for example, achieving diversity objectives that seek to increase the representation of women and ethnic groups across the business - from less quantitative areas.

One chief audit executive said that he split his assignments on cultural issues into measurable components and issues that were less well defined. “Those assignments do not necessarily lead to concrete recommendations but help us link company values with some of the key behaviours we identify,” he said. “We may include results of our quantitative interviews with customers in an appendix to feedback to management so they can understand how the results fit into the wider context of what’s happening in the organisation.” The key is to link the right metric with identified strategic goals and risks.

Defining better controls

While human capital, diversity and talent management ranked 2nd in both the current and future risk categories in the Risk in Focus 2023 survey, the topic only scored 10th and 8th respectively in terms of how much time auditors spend on the issue. In fact, recent research by Chartered IIA UK and Ireland showed that only 37% of internal auditors integrated culture into their standard audits – and over half (52%) said they had not been asked by the board or audit committee to produce reports on the issue, suggesting many do not take the matter seriously¹⁹.

Historically, internal auditors have audited mainly procedural, hard controls, although recently there has become more attention focused on soft controls and auditing culture and behaviour. This could be one reason challenges such as organisational culture tend to receive less attention. But with issues such as human capital, it is harder to define the controls and, where there are controls in place, they

are most likely to be directive human resource controls, such as policies and procedures. These are not the controls that are driving talent management. Auditors must work harder to define those controls that align with the organisation’s strategic human capital objectives. For example, research by Google scholars²⁰ found that psychological safety was a key player in team effectiveness and affected how long staff stayed at the organisation. Internal auditors must fully understand what factors influence the creation and development of successful teams and ensure that those issues are brought to the audit committee or board for action²¹.

Chief audit executives attending the Risk in Focus 2023 roundtable said that internal audit professionals should not be looking for quick fixes, especially when trying to define the organisational

“How do I create an organisation with a heart?”

¹⁹ Cultivating a healthy culture, Chartered IIA UK and Ireland, March 2022
²⁰ <https://rework.withgoogle.com/print/guides/5721312655835136/>



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 32 OF 48

HUMAN CAPITAL, DIVERSITY AND TALENT MANAGEMENT

culture of enterprises that span different geographical zones. That is because in reality there is likely to be a wide range of business and geographical cultures to take into consideration.

“The more we invest in boosting their skills, the more we risk losing them to organisations with deeper pockets”

Internal audit's role

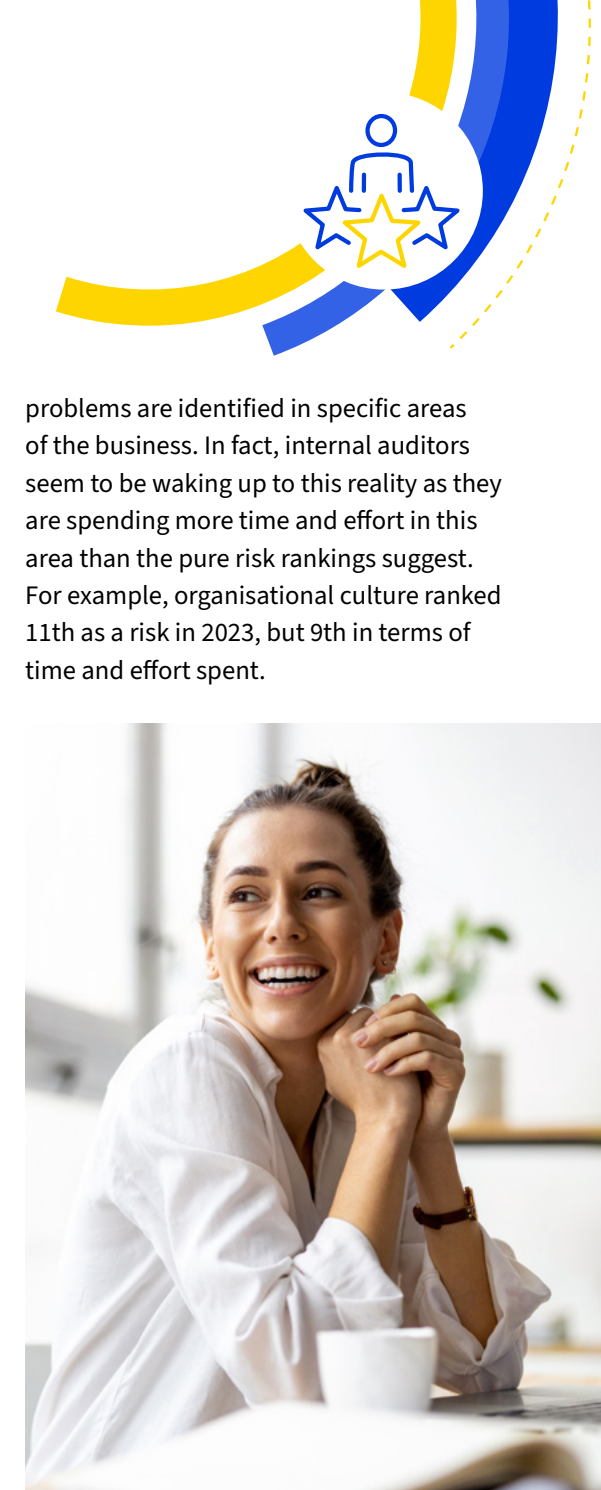
A first step can entail internal audit reviewing existing cultural norms and using the results as a catalyst to define the business' current culture. That review can be used to develop a roadmap for change. Seeking views outside of the business is key. Customers and stakeholders - such as vendors and contractors - often have a clear view of the prevailing culture based on continuous interaction with staff. When they say they feel valued and

respected and are not subjected to unfair or dictatorial behaviour, those comments can indicate that the culture is moving in the right direction.

The roadmap should also show how the desired cultural behaviours are embedded in an organisation's processes, and are aligned with clear roles and responsibilities, as well as being assigned to individual accountabilities. But chief audit executives agreed that from the outset of any cultural change programme the tone from the top was key. “Staff want to be proud of management and the organisation's ethical conduct,” said one chief audit executive. “Management can drive a big difference in behaviour.”

The organisational culture must be clearly articulated throughout the business. A well-understood set of desired behavioural attributes can then be included in talent management and training programmes, employee selection and onboarding procedures, job descriptions, and even picked up on during out-boarding interviews to make sure

problems are identified in specific areas of the business. In fact, internal auditors seem to be waking up to this reality as they are spending more time and effort in this area than the pure risk rankings suggest. For example, organisational culture ranked 11th as a risk in 2023, but 9th in terms of time and effort spent.



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

HUMAN CAPITAL, DIVERSITY AND TALENT MANAGEMENT

Coping with shortages

The acceleration of digitalisation in organisations around the world has helped to create a global shortage of people with the right skills and competencies in both businesses and their internal audit teams. Money is certainly a problem.

For a publicly funded organisation such as the World Intellectual Property Organisation (WIPO) attracting, training and retaining qualified data scientists and IT auditors is a struggle, Rajesh Singh, director of its internal oversight division, says. Singh's operation includes three elements – evaluation, investigation and pure internal audit. The internal audit team has three people and is being boosted by a data scientist and a full-time, mid-grade audit member with IT auditing expertise. But because the internal audit section is small, people tend to leave after two or three years as there are few options for promotion, even though WIPO invests heavily in training. Second line functions in the organisation suffer from the same issue for staff with IT expertise.

“The more we invest in boosting their skills, the more we risk losing them to organisations with deeper pockets,” Singh says. “It creates a loss of institutional knowledge that is hard to rebuild because turnover is relatively fast.” Like many chief audit executives, he partners with third-party suppliers, but a single assignment sometimes can cost the same as an IT auditor's annual salary, which he finds hard to stomach.

He has decided to become more opportunistic. As well as investing in the same training for all team members to ease the skills gap when someone leaves, he is setting budget aside to try to poach high-flying IT specialists who may want a sabbatical or be in between jobs. If successful, those will be shorter-term hires, young people who may be happy to stay for six months, and from whom Singh's team can learn. The longer-term plan is to continue automating routine audit assignments to free his team up to focus on more strategically relevant work.



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

HUMAN CAPITAL, DIVERSITY AND TALENT MANAGEMENT

How internal audit can help the organisation

1. Evaluate how far are the organisation's human resources strategies aligned with its vision and mission, and whether they are suitable for these times of scarcity when it is key to attract and retain employees within the organisation.
2. Assess how well those strategies are implemented at the different levels within the organisation and whether they are discussed periodically, including at board-level meetings.
3. Test whether the organisation's employment policies and procedures strike a fair balance between the potentially changing demands of employees and the preferred organisational culture.
4. Evaluate how quickly and effectively can the business' technological and physical infrastructures adapt to future changes in working patterns.
5. Assess how well and widely the organisation's social purpose is clearly defined, disseminated and lived in practice.
6. Assess how well the social purpose of the business and its organisational culture are embedded in talent acquisition and management processes.



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 35 OF 48

CYBERSECURITY AND DATA SECURITY

Auditing at the speed of crime

With hackers now able to threaten critical infrastructure and people's lives, internal auditors must move faster than ever to combat threats.

Cybersecurity and data security retained its hold as the number one threat in the Risk in Focus 2023 survey – with 82% of respondents saying it was a top five risk (the same as in 2022). It is also the area on which internal auditors say they spend most time and effort. In three years' time, internal auditors expect the risk to still rank highest as a threat to their organisations but with slightly fewer ranking it a top five risk (77%).

In fact, the threat landscape has become more dangerous – not least because of the war in Ukraine. Survey respondents said cybercrime and data security was their second biggest risk from the conflict. In addition, ransomware attacks increased by 80% in 2022, according to cyberthreat analyst Sophos²². That growth was driven in part by hackers taking advantage of the burgeoning ransomware-as-a-service

industry. The average price for recovering stolen data soared from \$170,000 per infringement to \$812,360, according to the survey. Hackers are also moving into the more ominous area of so-called “killware” to put pressure on organisations to pay up – those attacks target critical infrastructure, such as hospitals or energy supplies, which could result in actual deaths.

Chief audit executives at the Risk in Focus 2023 roundtable on cyber and data security agreed that ransomware risk continues to be difficult to mitigate and poses a potential existential threat to businesses. “A major data breach can impact on the quality of our services, trust and reputation, our financials and, if our clients lose money, we have to compensate them,” said one chief audit executive. “But the biggest threat we are scared of is that we cannot keep our business running.”

²² The State of Ransomware 2022, Sophos, April 2022



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

CYBERSECURITY AND DATA SECURITY

Cybercrime business models maturing

“The maturation of business models around cybercrime is becoming a major threat,” the chief audit executive of an international IT company says. He says that the ability of low-skilled hackers to buy sophisticated off-the-shelf attacks should be on every internal audit team’s radar. “It is now an open battlefield and auditors should ensure they keep up-to-date on the main evolutions in cyber-attack strategies.” While technicians are best placed to develop and deploy defences, he says, internal auditors should help to effectively spread new counter measures and advice from those teams throughout the organisation.

“Every day, this issue becomes more rather than less important,” said another chief audit executive at the Risk in Focus 2023 roundtable on the issue. “It has all the characteristics of an emerging risk, which are often the most difficult to tackle. This year, for example, we could face increased

Russian cyber-attacks, next year it could be something else. It is the biggest risk we have.”

Raising board awareness

Auditors must help to connect the dots between what is going on in the business and the board. A qualitative survey by the UK government earlier this year uncovered limited board understanding of cybersecurity risk²³. This had led, it said, to efforts to pass on the risk to outsourced cyber providers, insurance companies or even non-board level colleagues.

Risk in Focus 2023 roundtable participants agreed it could be difficult to find board time for IT-related topics, including cybercrime, despite the fact the pandemic had pushed digitalisation efforts further up the agenda. In last year’s Risk in Focus survey, for example, the threat from digitalisation ranked third – compared with fifth this year.



“I participate in both risk and audit committees,” said one chief audit executive at a financial services firm, “and while we talk a lot about lending, compliance and credit risk, we don’t discuss IT.” That was left to a separate meeting with the chief information officer and those in the second lines.

An internal audit presence at IT security committees, or with chief information and security officers²⁴, is effective for driving better security, but board-level engagement is key. Chief audit executives can play a major role in raising awareness of cyberthreats in board rooms. They should explain how much money their organisations stands to lose when specific risks crystallise – and avoid cloaking the topic in technical jargon.



²³ Cyber Security Breaches Survey 2022, Department for Digital, Culture, Media and Sport, UK Government, July 2022

²⁴ Cybersecurity in 2022, Part 2: Critical Partners — Internal Audit and the CISO, The Institute of Internal Auditors, June 2022

Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

CYBERSECURITY AND DATA SECURITY


Third parties create weak links

While many large organisations are relatively well-protected by strong cyber defences and regular up-to-date training, this year has seen more of a shift to hackers targeting third-party suppliers with less mature security systems. Yet European legislation such as the General Data Protection Regulation²⁵ and, more recently, guidance by the European Banking Authority, place responsibility squarely on the shoulders of the organisation that owns the data²⁶. This trend is likely to continue to grow under Europe's revised cybersecurity directive, NIS2²⁷. Like many new emerging risks, identification, control and mitigation lies partly outside of the business' remit.

Those concerns extended to cloud service providers, especially since many organisations have signed up to the

same few major businesses to accelerate their digitalisation plans. Given that the levels of service are standardised by each provider, chief audit executives said that organisations often had little negotiating power to agree or force controls on those suppliers. "Everything becomes a bit too far from our site from an internal audit point of view and it can be hard to assess and mitigate risk."

Greg Schlegel, founder of the Supply Chain Risk Consortium in the US and Adjunct Professor for teaching enterprise risk management for Villanova University's EMBA programme, says that internal auditors must focus on such third-party risks over the next twelve months – even though the time internal auditors spend on supply chain issues is likely to fall from sixth to ninth place, according to Risk in Focus 2023 survey. While he accepts that data security is a key issue in terms of protecting the organisation's digital assets and infrastructure, auditors should also



"The biggest threat we are scared of is that we cannot keep our business running"

ensure that the cloud service providers (and others who supply critical data infrastructure) are financially secure.

"The business needs some methodology to assess the financial health of third-party suppliers because the world at the moment is a very uncertain place, especially with inflationary pressures and energy supply risk increasing," Schlegel says. He also advises internal auditors to ensure that the business knows where suppliers are located physically. While software security is often framed in terms of the cloud, if the sites where those services are based become subject to power outages - such as the one at Amazon Web Services in 2021²⁸ - that could bring an organisation's critical infrastructure to a halt.



²⁵ What is GDPR, the EU's new data protection law?, GDPR EU, 2022

²⁶ GDPR and Corporate Governance: The Role of Internal Audit and Risk Management One Year After Implementation, ECIA, November 2019

²⁷ Review of the Directive on security of network and information systems in "A Europe Fit for the Digital Age", European Parliament, June 2022

²⁸ Power outage in Amazon's cloud service disrupts technology throughout the United States, World Socialist Web Site, December 2021

Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 38 OF 48

CYBERSECURITY AND DATA SECURITY

Cyber and economic crimes merging

Cybercrime taxonomies are also evolving. Cyber enabled crime involves attacks, such as phishing emails, that may lead to a hacker defrauding a company. Pure cybercrime, or cyber dependent crime, on the other hand, entails hacking to steal or ransom data. But these categories are increasingly blending because technologies now enable more sophisticated attacks to combine several elements in one infringement.

“Fraud or criminality was never traditionally included in categories such as economic crime - such as those involving money laundering, sanctions, bribery and corruption - but governments are increasingly seeing these as inter-related economic crimes,” partner at BDO specialising in economic crime Angela Foyle says.

A business’s understanding of these taxonomies has led many to segment their cyber and data security teams into separate functional departments - often

with poor communication lines. For example, a ransomware attack may be treated by the IT team as a standalone attack by many organisations. But today that approach is no longer adequate.

For instance, if a business loses some of its data from a ransomware attack and decides to pay the criminals to get it back - an increasingly common practice, according to the Sophos report - not only may the data not be returned, but the company’s exposure to regulatory action could grow. If regimes such as North Korea or Russia are behind the attack, then the business could fall foul of breaching sanctions regimes.

“It is critical that organisations make sure they have links across the different elements of the business dealing with cyber and data security, and with regulatory compliance,” Foyle says. “Internal auditors must ensure that those lines exist and that the controls ensuring fast and clear communication are in place and work.” Ideally, the internal audit team would have at least one member of staff with sound cyber skills and knowledge, she adds.



“It is critical that organisations make sure they have links across the different elements of the business dealing with cyber and data security, and with regulatory compliance”



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

CYBERSECURITY AND DATA SECURITY

Controls must be implemented

Not only did the pandemic weaken many organisations' cyber defences as staff were forced to work at home, the culture around data security also deteriorated. As online communication became the norm, one of the hacker's favourite weapons of choice – the spoof email – was less easy to detect as most correspondence moved online.

Foyle said that audit controls should include training and alerts so that people become more aware of the latest hacks. "Quite simple things, such as always hovering over email to make sure it is one that you recognise or would expect to see, can make a difference," she says.

Also, applying risk frameworks with policies and procedures, including ISO 27100, NEST and COBIT are a must. But they are not enough. "We have excellent IT policies and standards that follow best practice – but the simplest error is that people often fail to implement them," said one chief audit executive at the Risk in Focus 2023 roundtable event.

While larger organisations tend to have specialist cyber security expertise in-house, general internal auditors can make a big difference by refocusing on the basics. That includes the security culture of the organisation, which a Chartered IIA UK and Ireland study found was often a blind spot for internal auditors and businesses²⁹.



²⁹ Mind the Gap: Cyber security risk in the new normal, Chartered IIA UK and Ireland, February 2021

Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

CYBERSECURITY AND DATA SECURITY

Internal audit's role

First, internal audit can considerably reduce threats by focusing in detail on whether policies had been implemented on the ground. Ensuring that software patches are applied in a timely way and keeping on top of which staff have access to systems makes a big difference. In addition, proper back-up procedures need to be in place and should be included in routine internal audits.

Second, auditing access rights, ensuring remote parts of the business have applied software patches and helping to communicate policies and procedures are all important exercises for the internal audit team. Where those are already at a more mature stage, facilitating data breach simulations and tabletop exercises can make sure that systems designed to contain breaches work and everyone concerned knows their roles and responsibilities. That can include ensuring there is redundancy in the system

so that if a key member of the response team is unavailable it does not stop the remediation process.

Longer-term, those who work closely with in-house IT departments should build up knowledge in the internal audit team. This approach also increases risk awareness in technology departments. But in some areas co-sourcing or outsourcing with external providers is a must.

Rajesh Singh, director of internal oversight division at World Intellectual Property Organisation, has three people in his internal audit team, all of whom are certified in IT and cyber security.

On a recent cybersecurity audit, he brought in a large consultancy to lead on the project. "The certifications certainly help," he says, "but because we are not dealing with these issues every day, our skills and knowledge cannot match those of experts who are immersed in the topic on a daily basis." A recent survey said

that more organisations are turning to third party help for security because of an increasing shortage of skills in this area³⁰. In fact, human capital, diversity and talent management ranked as the second highest risk in the Risk in Focus 2023 survey and many roundtable participants agreed most internal audit departments are struggling to attract and retain the right staff.

"We have excellent IT policies and standards that follow best practice - but the simplest error is that people often fail to implement them"



³⁰ Security leaders relying more heavily on MSPs amid talent crunch, helpnetsecurity, April 2022

Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

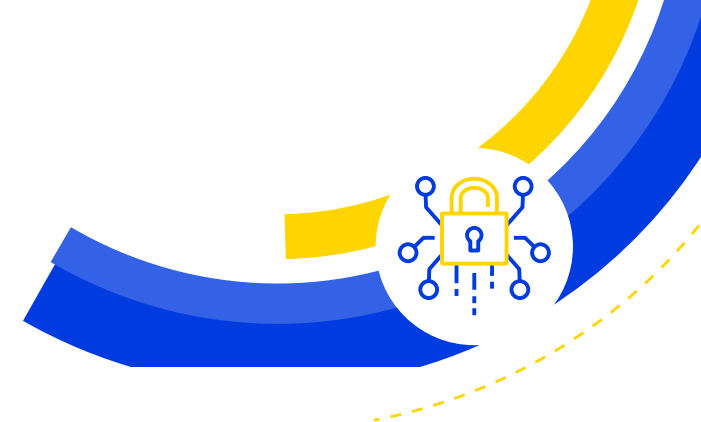
Digital disruption and new technology: Switching to automatic

CYBERSECURITY AND DATA SECURITY

Insurance hard to secure

Insuring against cyber-attacks is becoming more difficult to secure, according to Risk in Focus 2023 roundtable attendees. One hurdle is that the business' financial calculations of potential risk may not be accurate enough for insurance purposes. Where there is a specific ongoing risk, such as phishing attacks, for instance, quantifying a monthly amount for insurance purposes is often feasible. But with ransomware attacks where the future of the organisation may be in question, there may be too many variables to calculate the likely cost of cover needed.

Many organisations use a risk management process to map and cost risks, but those looking to start the process for the first time are likely to need to progress through trial and error. "It is super-complicated," said one chief audit executive at the roundtable event, "and you don't get it right first time - it is something you improve with experience." But with insurance difficult to obtain at the right price, internal auditors must work harder and smarter to defend their organisations against increasingly sophisticated cyber threats.



How internal audit can help the organisation

1. Assess whether the organisation has effective and timely mechanisms in place to spread information on new cyber threats, countermeasures, and advice throughout the business.
2. Assess whether the board has a firm grasp on the business risk cyber and data security pose to the organisation's strategy.
3. Focus on third-party technology supplier threat, including from vulnerabilities to their physical infrastructure.
4. Assess whether strong links exist between the different parts of the business involved in cybercrime, data security, fraud, economic crime and regulatory compliance.
5. Test that security practices, patches and procedures are implemented consistently in all parts and locations of the business, or ensure that the organisation (usually the second line) does perform such tests.
6. Assess whether adequate recovery plans are in place.
7. Assess whether the information underlying the business' financial calculations on assessing the potential loss from cyber-risk are valid and accurate enough to support insurance claims.



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

DIGITAL DISRUPTION AND NEW TECHNOLOGY

Switching to automatic

While internal auditors are turning their attention to artificial intelligence systems, they must also ensure that their organisations have got the basics right for digitalisation.

The pandemic pushed organisations' digitalisation efforts into third place in the risk rankings in the Risk in Focus 2022 survey as they moved staff to homeworking and shifted sales online. Not surprisingly, perhaps, this year internal auditors ranked it as the 5th biggest risk their organisations faced. With 38% citing it a top five risk this year compared to 45% last year.

Internal auditors said they expected to spend an increasing amount of time on the issue so that in three years' time it will rank as the 2nd biggest area for internal audit effort in terms of time spent, according to the Risk in Focus 2023 survey. But with rocketing inflation, pressure to increase pay and supply chain disruption, it may be that in 2023 many businesses do not have the funds to carry out these plans.

Organisations are naturally at different levels of maturity with their innovation strategies - from having basic networked computers to being digital-first businesses

built on sophisticated online platforms. Most sit somewhere in between.

Developing an innovation culture

"Perhaps more important than considering digitalisation from a technical point of view, organisations must first get to grips with the innovation culture within their businesses to succeed," the chief audit executive at an international IT company says.

"A corporate culture that fosters transparency, openness, fairness, collaboration and that has a strong customer-focus is very important," he says. That must be backed up with a clear strategic vision, the right talent and an ability to maintain a helicopter view of projects so that they continue to head in the right direction. A culture that enables people to make mistakes and try new things without fear of failure can also help develop and attract the right talent, an increasingly scarce resource in this field.

"The more siloed an organisation is and the less open to collaboration, the less harmonised the culture will be around innovation," he says.

Chief audit executives at the Risk in Focus 2023 roundtable on the issue agreed that they had a key role to help assess and foster their organisations' innovation cultures. But they also said internal auditors needed to keep an eye on those areas of the business with fast-moving, technological projects – particularly in organisations with agile philosophies – where the threat from potential data risk could be high.

It only takes a few minutes for a manager, for instance, to download a third-party app to quickly fix a bottle neck in a system. Internal audit must make itself aware of every project that, for instance, could be processing data in ways that breach legal rules such as those set out in the General Data Protection Regulation on the storage and handling of personal data.



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

DIGITAL DISRUPTION AND NEW TECHNOLOGY

Measuring innovation gains

The chief audit executive at an international IT company agrees that these can be potential problems but says that it is not for the audit team to set the balance between innovation and risk - that is the role of management. "Chief audit executives should help by bringing visibility and assess whether different types of innovation efforts are more or less productive," he says. "Or whether they are well-aligned to achieving strategic objectives."

On a practical level, auditors should help measure how much financial value innovation creates for the business. That can include calculating business gains in

"Heads of audit should help digitalisation efforts by assessing whether different types of innovation efforts are well-aligned to the organisation's strategic objectives"

areas that are digitalising and, perhaps, measuring any increase in value of its intellectual property portfolio. Overall, internal auditors must ensure that they understand the alignment of the culture of innovation with the organisation's strategic goals - a task that does not necessarily require deep technical expertise to exist in the function's team.

Valuing data

Unlike digital-first companies, many organisations have legacy systems that are poorly integrated. In practice, that can mean the same customer is often dealing with multiple departments in an organisation, but their data is spread over separate systems.

"The fragmentation of the data landscape is a key barrier to digitalisation in any large organisation that has not been built on a newer digital platform," Shehryar Humayun, audit director - applications, data and applied sciences at Lloyds Banking Group, says.

He says that culturally, organisations tend not to prioritise their data because it is costly to do so and seems less of a priority than, say, creating new business propositions. But putting monetary value on data is the key to turning this attitude

around. Internal auditors should help their organisations on this awareness and cultural journey by highlighting the opportunities and value their data assets unlock but also the risks that the lack of data focus carry. That can be through, for example, potential monetisation through personalisation, or potential loss via compliance or data breaches, or through poor customer service. Developing an enterprise-wide governance framework is a must.

Internal auditors must have clear, comprehensible understanding of all technologies in the business so that they can communicate effectively with the board - especially given the relatively low understanding of technology risk in many boards (see, cyber chapter).



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic



PAGE 44 OF 48

DIGITAL DISRUPTION AND NEW TECHNOLOGY

Focusing on strategic data risk

When the root cause is data, Humayun says, risk can manifest in many areas at the same time, including for example, reputational, regulatory, operational, financial and other risks. But unlike emerging systemic risks, businesses are in the fortunate position of being able to control the situation with the right focus and prioritisation.

For Lloyds Banking Group, the importance of focusing on data was highlighted when the Group added data risk to its risk taxonomy a few years back. Sorting out the source data can mitigate risks in multiple areas of the organisation where the risk manifests itself in various forms. This approach involves more stakeholder engagement across multiple divisions of the organisation, and is often cumbersome and more expensive to resolve, but when done right it solves the organisation's strategic data risks rather than data risk in a single business unit.

Humayun's teams within the group internal audit function include an applied sciences group to enable data-driven assurance and another team that carries out thematic audits on data risks across the business,

such as privacy, ethics, data by design, data retention, metadata and other areas. This arrangement ensures the teams have experience of both understanding the power of harnessing data and being able to highlight the impact of data challenges. "Audit has a brilliant vantage point under this arrangement to take a holistic view across the organisation and to help it on its journey to get to grips with a fragmented data landscape with legacy tech in a practical way," he says.

While other approaches are likely to be effective in different organisations, internal auditors must ensure they build skills and capabilities around data to help organisations approach data risk from a strategic point of view.

"The fragmentation of the data landscape is a key barrier to digitalisation in any large organisation that has not been built on a newer digital platform"



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

DIGITAL DISRUPTION AND NEW TECHNOLOGY

Internal audit's role

This year's emerging topic is artificial intelligence. Some chief audit executives attending the Risk in Focus 2023 roundtable event were at the more mature end of the digitalisation spectrum. They had begun not only to audit AI within the business but had begun introducing AI programs within the internal audit process itself.

Results in both of these emerging areas have been mixed. Some internal audit functions have been identifying which first and second line AI implementations can be incorporated into existing audit engagements.

It is a process that puts a heavier burden of work on the auditees because they must be prepared to work closely with the internal audit function to share knowledge. That includes details of the AI models they have deployed, which can be complex and increases the level of specialist knowledge needed within the internal audit team. One roundtable attendee said he had brought in these skills initially from an external supplier. However, as the organisation digitalised it had decided to create a dedicated team of experts in-house that internal audit could buy days

from through an internal exchange system. While that worked well, finding subject matter experts in the business areas affected by AI remained challenging.

The European Union's proposal for draft regulation on artificial intelligence, which was published in 2021, is well underway. That is likely to require certification for AI models and business areas that are considered high risk - such as those making decisions that could affect people's lives. Organisations are expected to have to register their systems with the authorities and conduct regular compliance checks. Internal auditors already said that changes in laws and regulations was the fourth biggest risk to their businesses in the Risk in Focus 2023 survey, but as digitalisation increases this focus is likely to intensify. Not only do organisations need to protect and use data ethically, but they must also ensure any artificial intelligence scripts are free from bias throughout the organisation - whether that relates to the gender and diversity of customers or employees. A bias script can have serious reputational, legal and talent management risks. Internal auditors must work with the organisation and vendors to ensure bias does not become baked into the business' decision-making processes.

AI in internal audit

While several roundtable attendees said they had trialled AI processes within their functions - such as chat bots and machine learning routines - most said those experiments had mostly served to highlight where data systems needed improvement and how AI might be used better in future. One attendee had used machine learning to carry out anomaly detection routines. That had helped the internal audit team understand where potential risk areas were in the data prior to an assignment and the results of the exercise informed the audit plan.

Making the leap from data analytics to AI is a sound strategy, provided that the jump is not too big. "It is best to get comfortable with data analytics and then move into AI," said one attendee. In fact, existing tools can help create continuous auditing systems that offer 100% data coverage and anomaly detection. Those without advanced capabilities in these techniques may be wise to wait until their analytics programs mature.

Although potential benefits include greater audit coverage, continuous monitoring and a further standardisation of audit methodologies as they become embedded



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

DIGITAL DISRUPTION AND NEW TECHNOLOGY

in AI programs, there can be a mismatch between the time it takes to train new algorithms and the typical audit cycle. If, for example, an AI routine takes six months to train and the audit cycle for that assignment is only 12 weeks, it would be impractical for most departments to begin the training process.

Creating AI routines for predictive analytics has proven to be even harder. For example, some chief audit executives attending the roundtable said they had tried to use predictive analytics to help them understand when the conditions in the business were reaching a point where risk had crystallised in the past. But the process was too complex. “It was a useful exercise,” said one chief audit executive, “but there were too many data points to accurately predict control failures.”

“There is no point in trying to reinvent the wheel if you can customise a vendor’s emerging AI tools.”

Real-life applications

Rajesh Singh, director of internal oversight division at World Intellectual Property Organisation, has a small but highly certified team and has been running advanced data analytics pilots, which he expects to launch this year. That comprises over 55 scripts that query and monitor core areas twice a year, such as procurement, human resources and ERP and financials. Recruiting a data scientist and a full-time IT auditor will help him further develop that program into the more commercial aspects of the organisation’s activities as well as moving to test controls on a continuous basis.

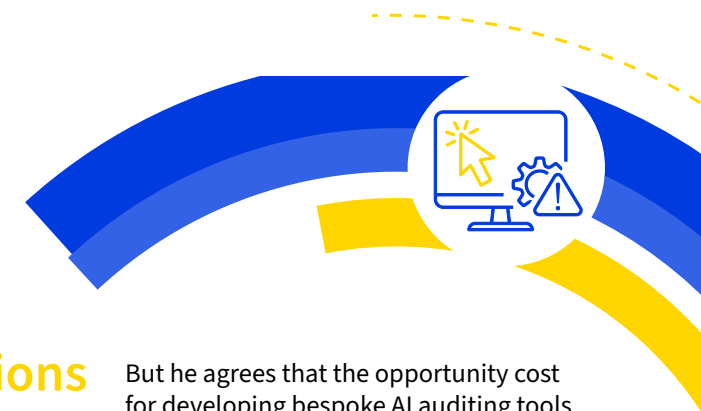
Singh secured the buy-in of the Director General, which he says was key. But he decided it would be better for internal audit to develop and run its own data analytics systems even though the in-house IT and security assurance departments had ongoing projects in those areas. “Given the mandate of internal audit, in my view some objectivity for internal audit needs to be maintained,” he says. “We don’t duplicate because I take the results of those departments and feed them into my engagements as an assurance mechanism.” But he says being independent allows him to sample those results if he feels it is worthwhile.

But he agrees that the opportunity cost for developing bespoke AI auditing tools at this stage is perhaps too stretching. Instead, in future he intends to use the AI embedded in the commercial auditing programs that are available and get the vendor’s help to enable his function to deploy what is most readily feasible. “There is no point in trying to reinvent the wheel if you can customise a vendor’s emerging AI tools,” he says.

Retaining a human point of view

More fundamentally though, too great a focus on automation and what can be audited by intelligent systems threatens to narrow the potential scope of what auditors can offer. “Putting all of our energy into automating systems that are sophisticated is okay but are we in danger of missing risks in those grey areas that are not as visible in AI applications?” asked one Risk in Focus 2023 roundtable attendee.

To provide valuable assurance to the business over AI in future, internal auditors must ensure that the right balance between human and artificial intelligence exists in the business.



Contents

Executive summary: Navigating the perfect storm of high-impact interlocking risks

Methodology

Key survey findings

Macroeconomic and geopolitical risk, emerging and strategic risk: Auditing in a time of crisis

Climate change and environmental sustainability: Transition to climate change auditing

Human capital, diversity and talent management: The human factor

Cybersecurity and data security: Auditing at the speed of crime

Digital disruption and new technology: Switching to automatic

DIGITAL DISRUPTION AND NEW TECHNOLOGY

How internal audit can help the organisation

1. Assess how far corporate culture strikes the right balance between innovation and risk mitigation.
2. Evaluate whether the organisation monitors its digitalisation and innovation initiatives in relation to its goals.
3. Assess how far the organisation has developed effective metrics to monitor and control its digitalisation and innovation efforts (such as monetary value or market share) and the quality of its data.
4. Evaluate how far the organisation considers data as a strategic risk in its taxonomies and whether the management of threats and opportunities are aligned to that strategic relevance.
5. Assess whether the organisation has a roadmap for progressing to artificial intelligence, including the risk and mitigation measures.
6. Evaluate the organisation's process for assuring the reliability and validity of its artificial intelligence tools.
7. Assess whether the selection and management of third-party vendors are adequate for the organisation's needs if it needs to customise their AI tools.



ABOUT RISK IN FOCUS

For the past seven 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 2023 involved a collaboration between 14 Institutes of Internal Auditors spanning 15 European countries which included: Austria, Belgium, Bulgaria, France, Germany, Greece, Italy, Luxembourg, the Netherlands, Slovenia, Spain, Sweden, Switzerland and the UK & Ireland. The highest number of European countries involved so far.

The survey elicited a record-breaking 834 responses from CAEs across Europe. Simultaneously, four roundtable discussions were organised with 39 CAEs on each of the risk areas covered in the report. In addition, we also conducted 9 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.

The colour scheme for this year's Risk in Focus has been chosen as the same colours of the Ukraine flag, to express European solidarity and support with the people of Ukraine.

