RISK IN FOCUS 2021

Hot topics for internal auditors

EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING
ECIIA

DIIR Deutsches Institut für Interne Revision e.V.

Risk in Focus 2021 has been published by a consortium of institutes of internal auditors that includes the Chartered Institute of Internal Auditors (UK & Ireland), Deutsches Institut für Interne Revision (DIIR), IIA Belgium, IIA Nederland, IIA Luxembourg, IIA Austria, Instituto de Auditores Internos de España, IIA Sweden, Institut Français De L'audit Et Du Contrôle Interne (IFACI) and the Italian Association of Internal Auditors.

Contents

4 **Foreword: Risk in Focus 2021 in context**

5 **Introduction**

6 **Methodology** 

7 **Data breakdown: the survey results** 

13 **Information security in the expanded work environment** 

17 **Regulatory forbearance and the return to normal** 

19 **Strategic relevance and the digital imperative** 

23 **Liquidity risk and cost-cutting amid depressed demand** 

27 **Managing talent, staff wellbeing and diversity challenges** 

31 **Disaster and crisis preparedness: lessons from the pandemic** 

35 **Rising nationalism and social tensions amid unprecedented economic volatility** 

39 **Supply chain disruption and vendor solvency** 

43 **Fraud and the exploitation of operational and economic disruption** 

47 **Climate change: the next crisis?** 

Foreword:
Risk in Focus 2021 in context

Without question, 2020 was defined by the global coronavirus pandemic (GCP). By March, as the research for Risk in Focus got underway, Europe had become the epicentre of the biggest public health crisis in living memory. This caught most countries and businesses off guard, despite the fact the World Economic Forum and others had already been sounding the alarm on global health security and the probability of a pandemic event.

Not only has the virus had huge public health consequences, social distancing and lockdown measures have had profound economic impacts. The GCP is the most significant and far-reaching event for businesses since at least the global financial crisis of 2008, and is expected to cause a deeper recession, higher rates of unemployment and bigger increases in public debt.

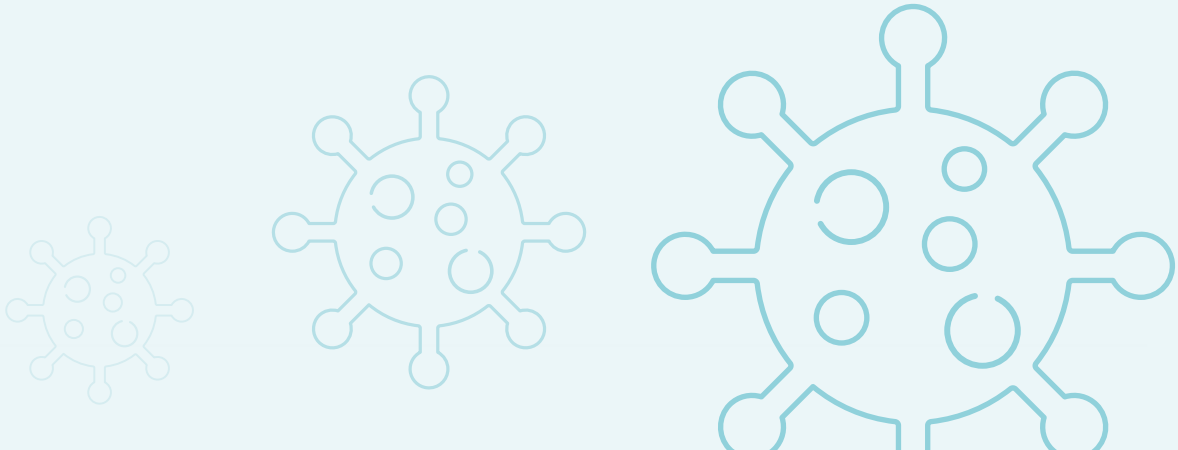
Businesses and their risk profiles have been significantly affected by coronavirus. The safety of workers has been a priority, with staff sent home to work in the first half of 2020 under orders from governments and employers. Lockdowns inevitably caused immense operational disruption as companies were forced to rapidly adjust and sectors including manufacturing, construction and industrials had to reduce output in order to maintain distancing measures within their core business.

The beginning of summer 2020 was marked by an easing of restrictions as governments managed the delicate balance of kickstarting their economies with resurgences in infections. It is expected that this challenge will have to be managed throughout 2021. Although the exact course of the pandemic's development is uncertain, it was continuing to accelerate in the second half of 2020.

The longer-term implications of this exceptional scenario are less clear. Lessons will be learned over the coming months and years by governments and businesses. Internal audit can and should assist in this regard. Its unique 360-degree view of the business and risk-control mindset can help organisations identify their blind spots and opportunities to improve their operations. Looking ahead to 2021, internal audit's enterprise-wide perspective has never been more necessary. Boards and executive management teams will depend on this independent top-down viewpoint for insights into the business and its risks during what remains a significantly challenging period.

This is the exceptional backdrop against which this year's Risk in Focus is set.

September 2020



Introduction

For the past five years Risk in Focus has sought to highlight the key risk areas identified by Chief Audit Executives (CAEs). The purpose of this is to help the internal audit profession prepare its independent risk assessment work, annual planning and even audit scoping by sharing the insights and learnings from the research.

Unlike previous years, the unprecedented circumstances of the GCP, the biggest global risk event in recent memory, have undoubtedly shaped the outlook for 2021. However, coronavirus itself is not a principal risk. Rather than posing new threats, the novel coronavirus has exacerbated existing risks, putting them in a new light and forcing organisations to think about them from different angles or assign to them new levels of priority.

A case in point, cyber and data security is a perennial front-of-mind risk for board members, Audit Committee Chairs and CAEs. Widespread homeworking has meant that cybersecurity has taken on a new dimension, as the IT infrastructure and perimeter wall of the business had to be adapted in record time. Inevitably, phishing attempts and social engineering incidents have soared as bad actors attempt to exploit security weaknesses following the decampment of staff into their homes.

Well-established risk management and internal control systems have been upheaved amid large-scale operational disruption. Internal audit has had to question how the disciplines, procedures and protections embedded in the DNA of the company have changed – intentionally or unintentionally – to ensure the ongoing operation of the organisation. Workplaces gradually reopened mid-year, but it is expected that a significant degree of remote working will remain in place indefinitely. This has implications for the strength and integrity of the internal control environment.

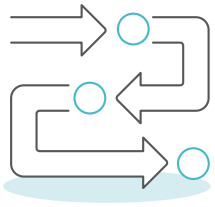
For its part, internal audit has had to rapidly evaluate what it can deliver in 2020-2021. Agreed audit plans have been revisited to determine what is a priority and what fieldwork can, where necessary, be performed remotely. Data analytics has reaped rewards for internal audit during the initial phase of remote working and some have used the downtime wisely to finally embed long-planned digital and continuous auditing capabilities. Analytics and continuous auditing have never been more relevant given limited access to the business and international travel restrictions.

Some audit leaders have been putting together half-year or quarterly plans or working off-plan altogether, knowing that annual proposals will quickly become outdated. In some cases internal audit support has been short, sharp and provided in real-time and CAEs anticipate maintaining this more nimble approach indefinitely. The third line has also been called upon to adopt the role of trusted advisor with an urgency that has not been required of it in recent years, if ever.

Internal audit must be forward-looking, proactive and continue to stay as close to the business as possible to understand both its risks and its needs. Increasingly, this involves not only operational considerations but strategic risks and factors in the external environment acting upon the organisation.

Now is the time for internal audit to prove its worth.

Methodology



The research for Risk in Focus 2021 once again combines both a quantitative survey and qualitative interviews with CAEs, this time from across 11 European countries and 10 institutes of internal auditors in Austria, Belgium, France, Germany, Italy, Luxembourg, the Netherlands, Spain, Sweden and the UK & Ireland.

For the first time this year the process included interviews with Audit Committee Chairs to give a broader perspective on where key business risks lie. This interview cohort comprised 42 CAEs and Audit Committee Chairs (29 CAEs and 13 Audit Committee Chairs) and the quantitative survey saw 579 respondents, a 10% annual increase and the highest response rate since this research study began five years ago.

In another first, this year included three rounds of interviews with subject matter experts using the Delphi method. This added a new dimension and provided up-to-date insight on how key risks are developing and how internal audit should be investigating these areas. A total of 51 experts participated and the number of experts per risk area varied from two to seven.

This research process was started in Q1 of 2020 and completed in Q2, amid the virus spreading across Europe. The timing of this influenced how the CAEs and Audit Committee Chairs we interviewed perceived their businesses' short to medium term risks, especially with regard to health and safety and financial liquidity. Further, this timing is likely to have influenced the scoring of the key risks by our survey respondents, as outlined in the following pages breaking down the quantitative results.

The results of this three-tiered research approach were combined to produce the topics shortlisted for the report.

Once again, we are immensely grateful to everyone who participated in this year's Risk in Focus, especially at what was such a challenging and uncertain time.

42
CAEs and Audit Committee Chairs interviewed

579
survey respondents
+10% annual increase

51
experts interviewed

Data breakdown: the survey results

Comparing last year's survey data with this year's data we can see which risks have become more or less of a priority in the eyes of CAEs across Europe. A number of risk areas appear to have been impacted by the GCP, including *Health and safety, Financial, capital and liquidity risks* and *Human capital and talent management*, all three of which have shown notable annual increases.

Supply chains, outsourcing and 'nth' party risks has fallen substantially. One reason for this may be that what started out as a supply-side concern at the beginning of 2020 soon became a demand issue, the emphasis shifting to companies' ability to continue as a going concern and remain solvent as the world entered a recession.

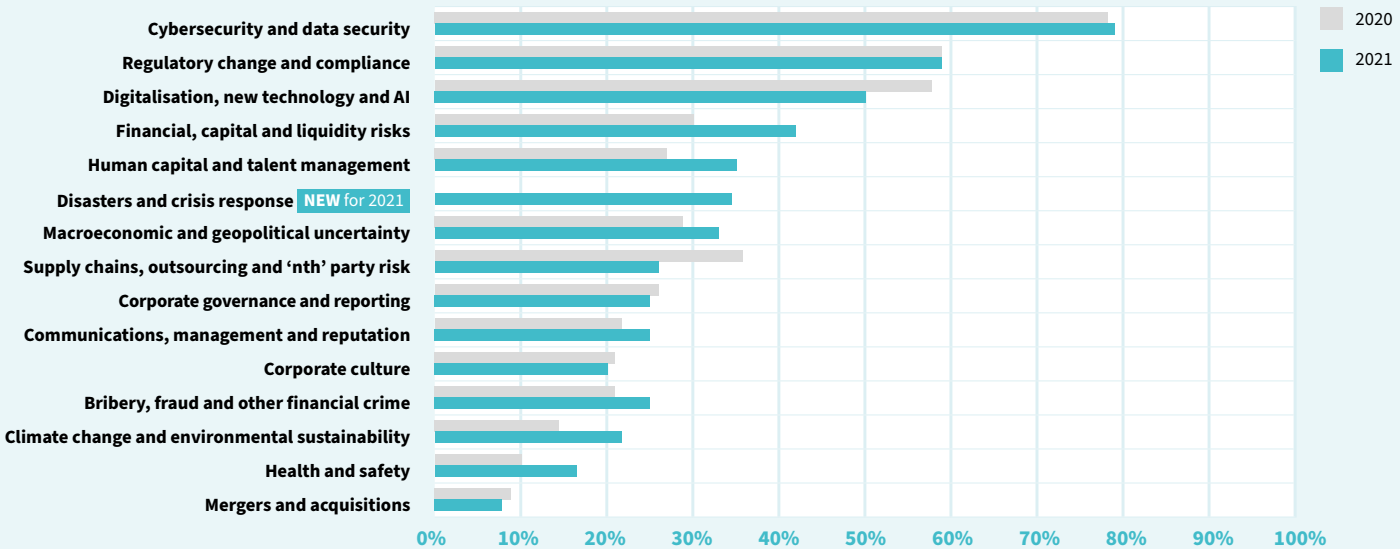
However, resurgences in coronavirus remain a threat to companies and their suppliers and it should not be forgotten that the financial and liquidity risks that rise in a downmarket apply to key vendors too. Businesses and internal audit should be mindful of the solvency of core suppliers and outsourcing partners, and the ongoing ability to stock appropriate levels of inventory to meet demand.

This latest edition of the survey for the first time includes *Disasters and crisis response*, which 34% of CAEs cited as among their top five risks, putting it in sixth place just behind *Human capital and talent management*. Audits of the business's response to the GCP have clearly been a matter of priority in recent months and most, if not all, organisations will need to undertake lessons-learned exercises and update their crisis continuity protocols.

Climate change and environmental sustainability, meanwhile, has shown a significant increase since last year's survey, continuing a positive trend seen last year. In our inaugural survey for Risk in Focus 2019, only 8% of CAEs said it was among the top five risks to their business, rising to 14% the following year and now to 22%. Climate change and sustainability issues have been part of the public discussion for many years already and are steadily, if not swiftly, becoming areas of actionable strategic focus and risk mitigation for companies.

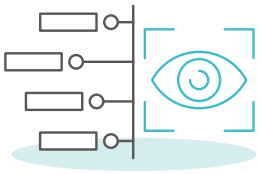
One year on: 2021 vs 2020

What are the top five risks that your organisation faces?



"With climate change becoming an increasingly pressing issue for businesses to finally address, especially as the world's largest investors demand urgent action, there is a notable lack of attention from the third line on this risk area."

Risk priorities vs. audit's focus

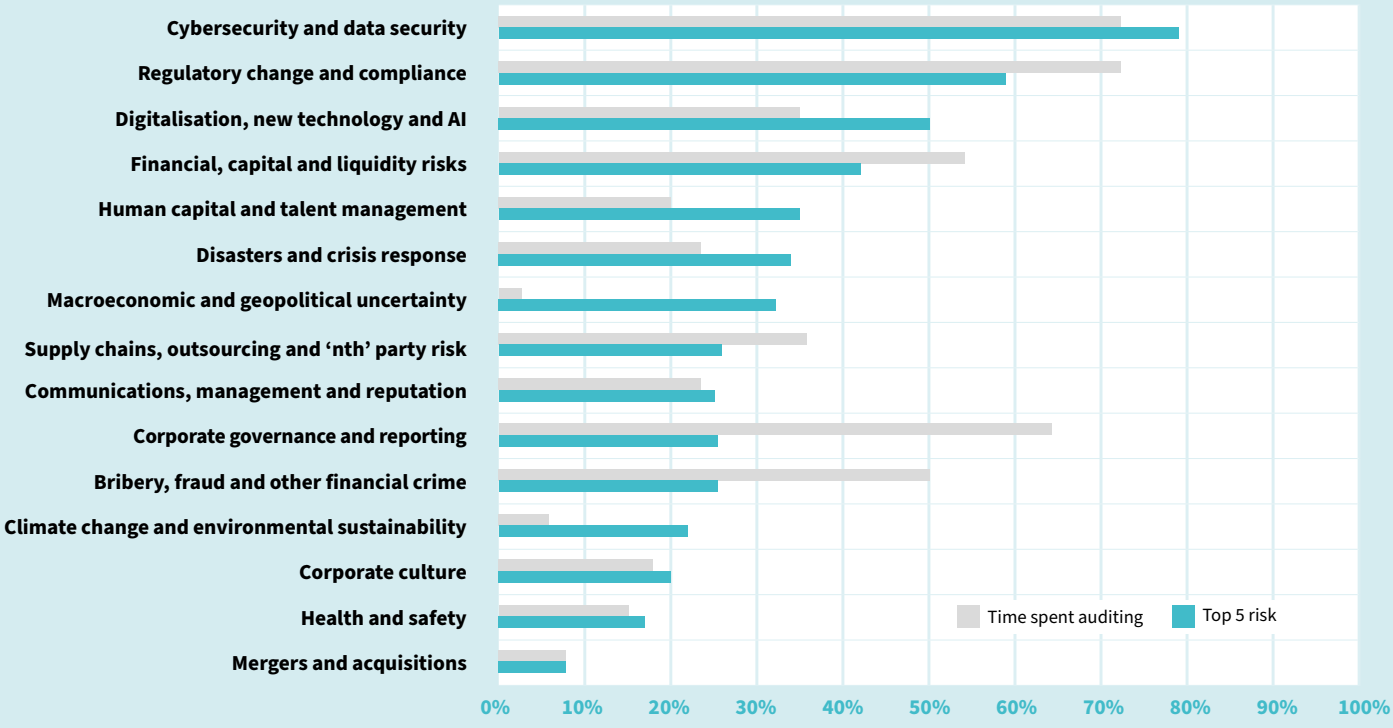


By asking CAEs both what they currently view as the biggest risks to their organisation and what risk areas they spend the most time and effort auditing, we develop a picture of how well aligned the third line's assurance work is. Any mismatch does not necessarily mean that internal audit is not taking a sufficiently risk-based approach. For instance, within regulated firms internal audit is obliged to dedicate resources to compliance assignments even if it does not see compliance risks as the biggest real-world threats to the organisation.

Also, areas with high audit engagement may have a lower risk priority as a consequence of internal audit's risk mitigation efforts, i.e. the third line is having its desired effect.

However, these results do give reason to reflect and have conversations with the board or audit committee about whether internal audit's time and resources are being spent wisely and if they need to be reallocated to overlooked risk areas. With climate change becoming an increasingly pressing issue for businesses to finally address, especially as the world's largest investors demand urgent action, there is a notable lack of attention from the third line on this risk area. *Macroeconomic and geopolitical uncertainty* and *Digitalisation, new technology and AI* also receive minimal audit attention compared with their level of risk priority. If this is true in your organisation, is there justification for why these are not areas of focus for the third line?

The top five risks that your organisation currently faces vs. the top five risks areas on which internal audit currently spends most time and effort.



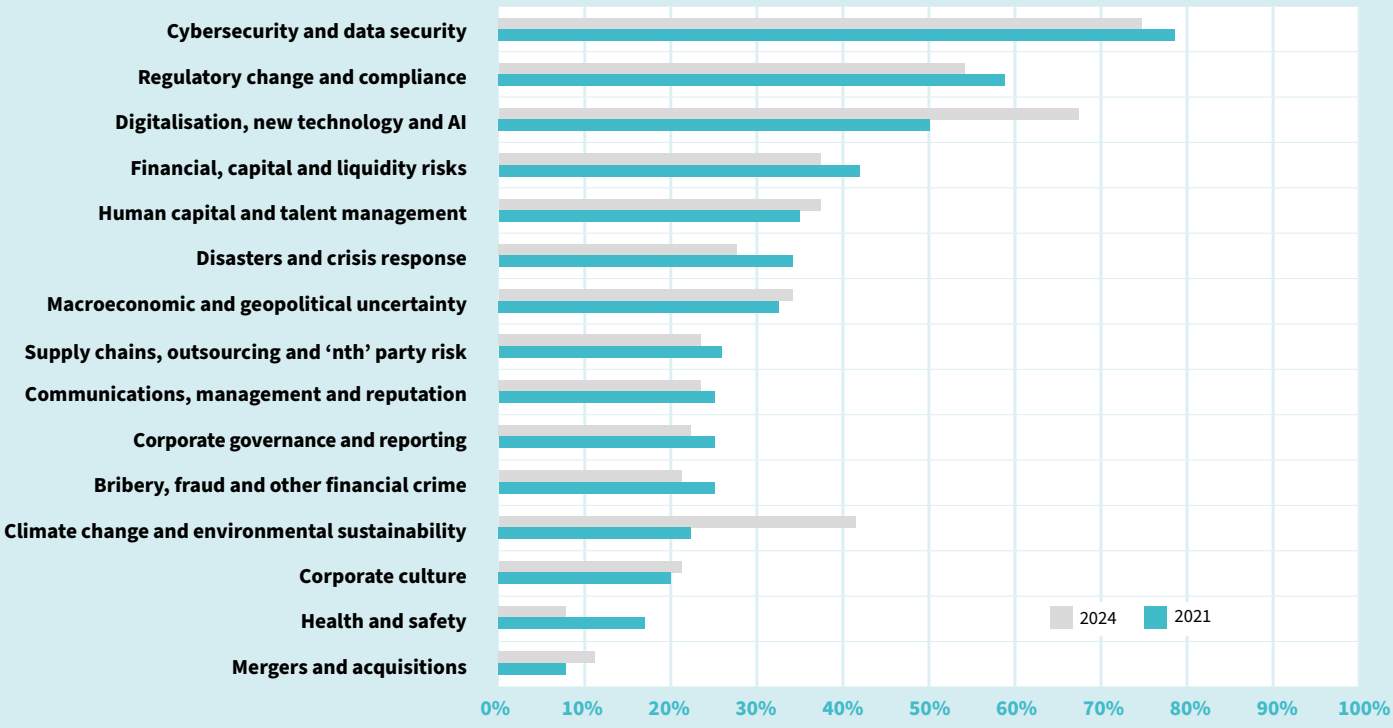
Risks today vs. tomorrow

In addition to asking CAEs what they see as the biggest risks to their organisation, we asked what they expect the biggest risks will be in three years' time. This shows how audit leaders anticipate the risk profiles of their organisations developing over time. Notably, we see that both *Digitalisation*, *new technology and AI* and *Climate change and environmental sustainability* are expected to significantly increase in priority in the near future.

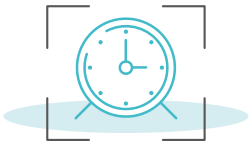
Technology and innovation is intrinsically linked to sustainability. The application of advanced hardware and software will help to mitigate climate change impacts and improve sustainability. Companies will need to innovate their core products and harness new and emerging technologies such as long-term battery storage and advanced smart metering to minimise emissions as well as big data analytics to reveal operational efficiency gaps that can be closed, among countless other approaches, in order to achieve their ambitious sustainability goals.

*"Notably, we see that both **Digitalisation, new technology and AI** and **Climate change and environmental sustainability** are expected to significantly increase in priority in the near future."*

The top five risks that your organisation currently faces vs. the risks that you think your organisation will face in three years' time.



Audit's focus over time



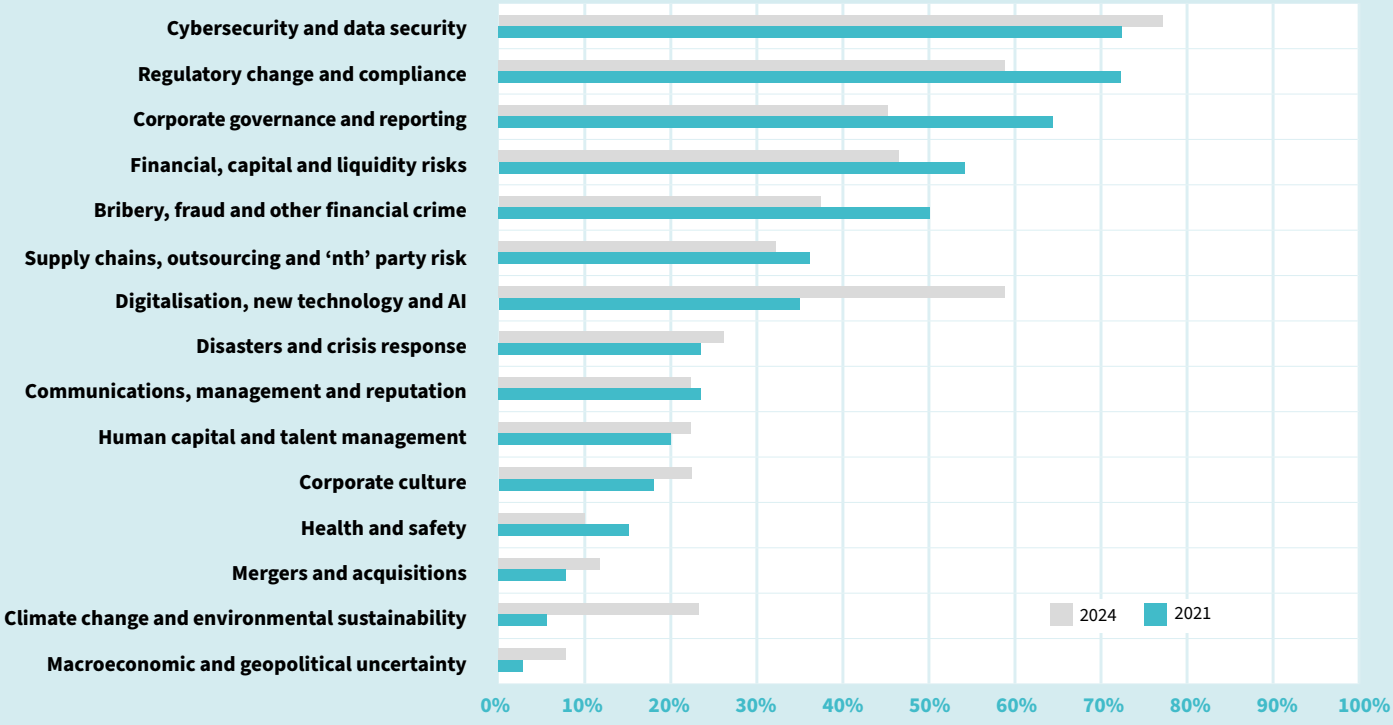
We can also see where internal audit's time and efforts are expected to be directed over time. As the risk management of areas such as *Corporate governance and reporting* and *Regulatory change and compliance* matures, there is an indication that internal audit will focus more on less traditional areas such as *Macroeconomic and geopolitical uncertainty, Climate change and environmental sustainability, Digitalisation, new technology and AI* and *Human capital and talent management.*

We are also able to compare this with what CAEs perceive businesses' risk priorities to be three years from now.

There is strong alignment in this regard, with numerous identical matches. This can be explained by optimism among audit chiefs that internal audit's resources will be directed where they are most needed. Notable mismatches include *Digitalisation, new technology and AI*, which 67% say will be a top five risk but only 59% anticipate being a priority audit area. This may suggest that internal audit needs to improve its skills, innovate its practices and source greater expertise to successfully bring this risk area under its focus in future.

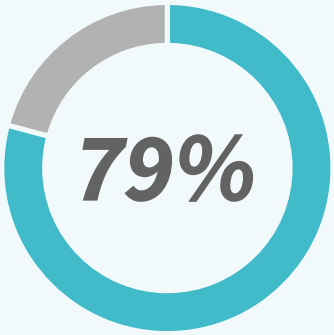
In contrast, while regulatory-driven areas (*Corporate governance and reporting, Bribery, fraud and other financial crime* and *Regulatory change and compliance*) are expected to receive less attention from internal audit in the near future, the time and effort paid to these risks is anticipated to significantly exceed their risk priority in three years' time. This may call for a constructive conversation with the audit committee about how the third line should be resourced over the coming years, and whether attention should be shifted away from already well-controlled risk areas so that the third line can take a more effective risk-based approach.

The top five risk areas on which internal audit currently spends most time and effort vs. the top five risk areas on which you think internal audit will spend most time and effort in three years' time.



"The cybersecurity threat depends on the weakest link in the organisation and the weakest links are always the people. As long as you work in the secure environment of your organisation, you know that the security people can deal with the situation and that it's probably close to 100% secure. With everybody working at home, the situation is completely different. So how can we on one hand open the firewall so that people can work remotely, but on the other hand be sure that hackers are not taking advantage of the current situation? That's a challenge."

Audit Committee Chair, Flemish local government, Belgium



'Cybersecurity and data security' *came out on top in this year's survey, with 79% of CAEs saying it is a* ***top five risk****.*

Worldwide

*4.5 billion**

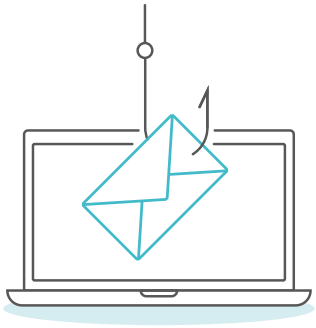
people were living under social distancing measures at the height of the first wave of the pandemic in Europe.

**Estimated*

Source: BBC

"Digital communication and the ability to steer the company remotely using digital means will increase. Information exchange in times of crisis and in the new environment, and the reliability of those mediums for communication, will be one of the main risks. One of the major lessons will be how can we maintain effective and secure communications if a disaster happens? How sustainable are those channels of communication? If the internet is down what are we going to do? Use walkie-talkies?"

CAE, DAX chemicals company, Germany



Information security in the expanded work environment

Data and information – whether customer credentials or intellectual property – are economic assets on which all organisations depend. Until that changes, data security will remain one of the highest-priority items on the corporate agenda. Once again, *Cybersecurity and data security* came out on top in this year's survey, with 79% of CAEs saying it is a top five risk and 27% singling it out as the number one risk their organisation faces.

The rules of the game, however, have changed. The wide-scale shift to homeworking arrangements in rapid time during lockdowns increased the vulnerability of organisations to cyber-attacks. It is estimated that worldwide at least 4.5 billion people – more than half the global population - were living under social distancing measures at the height of the first wave of the pandemic in Europe.[1] Workers had to access critical infrastructure and data via personal devices or open, internet-facing channels. Overnight, work laptops were forced to share home WiFi networks en masse, making the attack surface of companies less clearly defined and more permeable. Few if any business continuity plans (BCPs) had accounted for such massive upheaval in such a short space of time. Companies' Security Operations Centres (SOCs) set up to monitor and analyse potential anomalous activity on networks, servers and databases under normal circumstances were impaired by having to detect outlier behaviours in a modified IT environment.

Information security functions have needed to ensure they are mitigating the risks of remote access to sensitive data by securing homeworking devices with patch updates, maintaining network segmentation and managing access rights to ensure an acceptable level of security.

The human behavioural element is critical to cyber and data security risk. Lacking personal interaction, staff can be more susceptible to social engineering ploys as they cannot immediately sense-check emails with nearby co-workers. There is also greater potential for controls and safety measures to soften or be circumvented when workers are not being watched, as they are overlooked and ignored to save time. One report shows that 52% of office workers believe they can get away with riskier behaviour when working from home, such as sharing confidential files via email and using personal devices to conduct company business. Reasons for not following security controls include feeling that these protocols impede productivity (51%) and not being watched by IT departments (48%).[2]

All means of digital communication, not just email, must also be stable and operationally resilient as well as secure from outside interference and possible espionage by cybercriminals, competitors and nation states. There have been numerous incidences of rogue infiltrations on videoconferencing software platforms, which became the primary means of communication as lockdowns commenced. Another concern is the integrity of certain platforms. Intelligence agencies have warned governments to avoid the use of Zoom over concerns it is vulnerable to backdoor state surveillance, the company's research department being stationed in China.

1. Coronavirus pandemic: Tracking the global outbreak | BBC
2. The State of Data Loss Prevention 2020 | Tessian

Adjusting to securing the homeworking environment is not expected to be temporary. Companies that have maintained productivity through the lockdown and whose staff have successfully adapted to working remotely may dispose of office space permanently, especially as revenues come under pressure and businesses seek ways to reduce their fixed cost base.

One estimate indicates that 74% of companies plan to shift to more remote work post coronavirus.[3] This will require companies to flex and adapt while maintaining the highest information security standards, both on-site and in the newly expanded home-based work environment.

A group of experts surveyed for Risk in Focus ranked several cyber threats companies will face in the next year in order of likelihood. Phishing attempts and malware infections are seen as the most likely threats to arise, which shows the criticality of staff behaviour, training and awareness in mitigating cyber risk.

Cyber threat	Most likely to be faced in the next year (order of importance: from more to less likely)	Challenge for organisations
Phishing		To reduce timeframe between security events and responses.
Malware infection		
Intrusion into the company's network		
DoS/DDos attacks		
Information security breach		
Cyberespionage activities/spyware		
Software vulnerabilities		
Data and information extraction		

The internal audit perspective

Internal audit can offer its view on the extent to which any relaxing or adaptation of controls has increased the risk of data leakage or security breaches. The real question is - what has changed? That applies externally (e.g. a rise in phishing attempts) and internally (e.g. lack of staff cyber awareness training post crisis or security patching of homeworking devices not being managed as effectively as on-site). By understanding where the most disruption lies as well as where the highest-value data assets reside, internal audit can determine the impact of any change on the organisation's information security risk and the control environment that is in place to mitigate it.

Staff awareness and understanding of information security risk is absolutely essential. This applies to protocols around the use, management and storing of confidential data to prevent data leakage, and applies to ensuring workers know how to spot cybercrime to avoid people succumbing to phishing and spear phishing (targeted at a specific individual) attempts which can result in costly malware and ransomware attacks and fraud by deception. Internal audit can and should check whether cybersecurity awareness is being sufficiently fostered and whether staff training has been updated in light of changes to the working environment and IT infrastructure. It should also attempt to provide assurance that staff are not circumventing processes to save time and effort.

Internal audit can also be a sounding board for information security teams that may be forced to adapt the IT control environment to keep the business operational and as efficient and productive as possible in the face of shock events. Any high-risk control changes will need to be reported to senior management to check that they are within the organisation's cyber-risk appetite.

3. CFO Actions in Response to COVID-19 | Gartner

*"A group of experts surveyed for Risk in Focus ranked several cyber threats companies will face in the next year in order of likelihood. **Phishing attempts** and **malware infections** are seen as the most likely threats to arise, which shows the criticality of staff behaviour, training and awareness in mitigating cyber risk."*

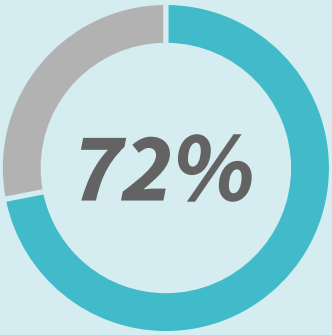
Questions and considerations for internal audit

- How has the newly expanded work environment impacted the IT controls system in different parts of the business and what risks does this pose?
- Has the business performed a risk assessment to identify possible network weaknesses and data assets whose susceptibility to attacks and theft has increased in the last 12 months?
- Is the first line raising staff awareness of key cyber threats and telling them what they should look out for?
- Are security patches on personal devices being updated and managed to the same standard as on-premise devices?
- How have the company's Security Operations Centre's monitoring capabilities been hindered or disrupted over the last 12 months?
- Does the first line truly understand the perimeter of the business? For instance, are absolutely all devices with connectivity and network access (e.g. Internet of Things devices) secure?
- Have new software applications (e.g. videoconferencing software) adopted to ensure operational continuity been adequately vetted for potential security flaws and vulnerabilities?
- Is the first or second line testing staff awareness with friendly phishing attempts? Should internal audit test IT defences independently, perhaps with the assistance of a co-sourcing partner?

"Are we taking shortcuts or are we taking the appropriate measures in compliance with all the relevant consumer protection regulations? Are we behaving in a way that might undermine some categories of customers, and if that is the case, is that putting us at risk within the regulatory environment in which we operate?"

CAE, FTSE 100 online payments provider, Luxembourg

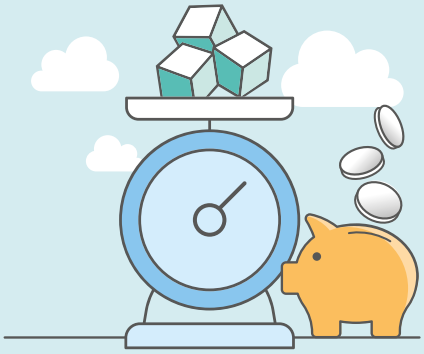
*of CAEs in our survey said **'Regulatory change and compliance'** is a **top five risk** to their organisation.*



*Nearly **three quarters** (72%) of audit chiefs also say that this is one of the **top five areas** on which internal audit spends **most of its time and effort**.*

"It feels like we are becoming more regulated with more tax burdens, whether it's sugar tax, which we already had. The taxes are coming in to drive consumer behaviour. The other direction goes off into climate change, there are plastic taxes coming in, carbon taxes. We anticipate this becoming more and more onerous."

CAE, national supermarket chain, UK



Regulatory forbearance and the return to normal

The regulatory burden was eased in the first half of 2020 to give companies room to manoeuvre. The European Securities and Markets Authority (ESMA) advised national regulators across the EU to apply forbearance powers towards listed companies to delay publication of financial reports by two months.

In the financial services sector, banks have come under unprecedented regulatory pressure in the years following the global financial crisis, the primary focus being to boost capital buffers to cushion them against any future shocks to the financial system. Those buffers were precisely for times like now. Consequently, the European Central Bank (ECB) made a temporary and partial reduction to banks' capital requirements in 2020 to free up financing to ensure access to funds in the economy. The European Banking Authority (EBA), meanwhile, postponed its EU-wide stress test exercise to 2021 to allow banks to attend to their customers and manage their credit risks.

Forbearance in the banking sector comes amid state-guaranteed loan schemes as governments and regulators recognised the need to stand out of the way of banks mid-crisis and encourage them to lend into the real economy. While there is some degree of regulatory clarity around coronavirus loan programmes – for example customers' credit ratings are not allowed to be impacted by their seeking of payment breaks and loan extensions – a major grey area is the criteria with which banks decide the financial terms of restructured loans, which remains at their discretion. Once the pandemic has passed, banks may have to justify the decisions that were made, their treatment of customers and the risks that were assumed during the height of the pandemic.

In the broader regulatory context, there is also evidence of data watchdogs having modified their approach to the enforcement of GDPR in light of the pandemic. Both the UK's Information Commissioner's Office and France's Commission nationale de l'informatique et des libertés have taken into account the practical challenges faced by the companies they regulate. They have stood down audit work and issued fewer fines against organisations struggling to meet data protection standards as a result of the pandemic. While GDPR laws clearly remain in place, it is recognised that companies' operating capacity has been constrained and many have seen revenues collapse.

To an extent, then, the pandemic represents a partial regulatory easing. Regulations are imposed by the state and governments are less inclined to penalise companies amid one of the biggest economic crises in history, potentially putting jobs at risk. But regulatory forbearance is only temporary and is by no means absolute. Existing regulations remain in place even if they have not been as aggressively enforced in recent months. There may also have been a temptation among companies to take their eye off the ball in 2020, causing them to fall behind now that postponed timelines for forthcoming regulations have to be met in 2021.

For 59% of CAEs in our survey *Regulatory change and compliance* is a top five risk to their organisation, exactly matching the result from last year, a clear indication that compliance is an evergreen risk. Indeed, 53% say that it will remain a top five risk three years from now.

Nearly three quarters (72%) of audit chiefs also say that this is one of the top five areas on which

internal audit spends most of its time and effort (an annual rise of 11 percentage points) and over 19% say this is the single risk area on which audit dedicates most of its focus – ahead of any other risk area apart from *Cybersecurity and data security* (also 19%).

In all companies, regardless of sector, there should be an awareness of the need to behave to the highest possible standards amid the disruption. Compliance functions may have had their resources stretched and should therefore be taking an appropriately risk-based approach to their work, by mapping and prioritising key compliance risks. This should apply to laws and regulations that are already in place, e.g. GDPR, as well as forthcoming and potentially postponed rules and other regulatory oversight. In 2020, the European Commission (EC) launched two public consultations on revisions to the Non-Financial Reporting Directive, which is seen as having fallen short in improving the disclosure of consistent and actionable climate and environmental and diversity data by companies for investors to make informed decisions. The aim is to standardise this reporting and the EC's review is now expected to complete in the first quarter of 2021, having been postponed by the pandemic.

An internal audit perspective

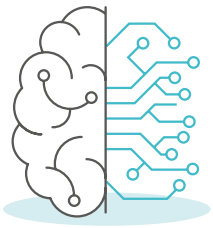
It is not internal audit's remit to ensure that companies are compliant, but, as our survey results show, the third line spends much of its time and effort ensuring that compliance functions are on top of regulatory risk. One major consideration for internal audit is the extent to which the business has been capable of maintaining acceptable standards of compliance amid the shake-up of operations and control systems. The third line should consider what impact recent operational disruptions have had on the work of the compliance function and the ability of the business to remain compliant. This also applies to the reorganisation of the business as staff return to the office and working arrangements are adjusted to whatever "new normal" the organisation has decided best suits it and its workforce.

There may be a temptation for the business to de-prioritise regulatory requirements that have been postponed. The business should have an eye on what regulatory developments are coming down the pipeline, understand what actions need to be taken and when, and be able to show how it is managing regulatory timelines and priorities by taking an appropriately risk-based approach. It may be that work to ensure compliance with postponed rules has been delayed; if so, there should at the very least be a clear case for why that decision has been taken.

Questions and considerations for internal audit

- To what extent has the pandemic and the organisation's efforts to remain operational amid the disruption impacted its compliance risk? Have staff been taking shortcuts that pose possible conduct and other regulatory breaches?
- How have the compliance function and its capabilities been impacted by the coronavirus pandemic in both the short and medium terms?
- What evidence is there that the compliance function has been able to support the first line adequately on new and forthcoming developments and maintain its oversight of the first line with regard to existing rules and regulations?
- Is the organisation prepared for regulators to roll back any forbearance and increase their oversight in 2021?
- Does the first line pay appropriate attention to compliance and understand its accountability for compliance risks?
- Has the compliance function taken an appropriately risk-based approach to its work, by mapping and prioritising key compliance risks and departments?
- Has the compliance function updated its regulatory calendar to account for postponed regulations and rules that have been paused? Is the function prepared for the new deadlines for these?
- Should internal audit conduct an independent regulatory risk assessment and see how closely it matches the second line's assessment?

Strategic relevance and the digital imperative



The need for companies to press ahead in meeting their digital goals has been laid bare. Numerous sectors have had no choice but to transition to digital service provision during mass lockdowns. For instance, e-commerce was no longer an option for retailers but a necessity. Companies that were further ahead in their digital evolution were at a significant advantage amid the coronavirus outbreak.

On the one hand, the pandemic has magnified the digital imperative, making such transformations a more pressing priority. On the other hand, the pandemic has in many cases temporarily made digital progress and transformation initiatives more complex and challenging. Lockdown and distancing measures have atomised organisations, potentially hindering the collaboration efforts of companies not used to operating under remote conditions. Companies have had to concentrate their efforts on managing crisis-related challenges such as the health and safety of their staff as workers are gradually and carefully brought back on-site, and the integrity and continuity of supply chains. Such core business considerations may have drawn attention away from vital longer-term digital goals on which the strategic relevance and therefore future of the company may depend.

Half of CAEs (50%) see *Digitalisation, new technology and AI* as one of the top five risks their organisations face, down from 58% a year ago. This fall may reflect the shift in attention to the shorter-term impacts of the GCP as digital transformation projects were slowed or put on hold. This is further supported by the fact that 67% of audit chiefs expect this to be a top five risk to their organisation in three years' time, indicating an only temporary lull of this risk priority.

There is a process of creative destruction at work whereby the life expectancy of large companies is shortening as innovators replace the old guard. It has been estimated that by 2027, 75% of S&P 500 companies will no longer exist, their average age having fallen from 61 years in 1958 to just 22 years.[4] This illustrates the need for companies to innovate in order to lead their markets or face becoming extinct. It remains to be seen whether this will reverse as today's big tech innovators maintain or grow their existing lead, or whether the crisis will accelerate this trend by causing further digital and market disruption.

Digitalisation typically has two goals: to enable the strategy of a company and to enhance its operations. From an operational standpoint, technologies such as automation, machine learning and artificial intelligence speed up processes, increase efficiency and reduce costs over the long term (i.e. once investment costs have been recovered) while removing the need for manual processing. Companies can also disrupt existing markets or create new ones by innovating digital and physical new technologies, ensuring their strategic relevance and securing their existence.

The most forward-looking businesses will use digital transformation both to accelerate their growth out of the 2020/2021 economic recession and to build operational resilience to the current and future pandemics. This may be one of the biggest risks/opportunities in the current climate. In mid-March, immediately prior to COVID-19 sweeping through Europe and the US, innovation was on nearly every corporate agenda. Just 8% of Chief Executives said they were not planning to invest in this area. Only a month later and that figure had jumped to 25%. Delaying or cancelling

4. Corporate Longevity Forecast: Creative Destruction is Accelerating | Innosight

"The current coronavirus situation puts even more pressure on the optimisation and digitalisation of processes because there will be more need for things to be automated to keep organisations running with people working remotely. There are more and more complicated automated processes and a big question for internal audit is how to audit those processes."

Audit Committee Chair, research and technology organisation, Austria

"It is estimated that 70% of digital initiatives do not reach their goals."

Source: Forbes

*Half of CAEs (50%) see **'Digitalisation, new technology and AI'** as one of the **top five risks** their organisations face.*

"The imperative to be strategically relevant is especially critical in this sector. That is our long-term risk, that change management is not agile enough and it takes too long to innovate and bring new products and services to market, whether it's new apps or new mobile financial services. And I think that's where more of internal audit's focus will go, away from the compliance areas. Then you're looking at things like change management, like how does the company measure consumer behaviour and how does the company monitor what the competition is doing?"

CAE, Nasdaq-listed telecoms company, the Netherlands

innovation projects is among the top financial responses to the GCP, alongside layoffs and other cost savings — 28% of Chief Executives have said they are planning innovation cutbacks.[5]

This poses its own risks. Certainly, many businesses will need to control their costs through 2020 and 2021, depending on how severely their cash flows have been impacted and the health of their balance sheets (see *Liquidity risk and cost-cutting amid depressed demand* on page 23). But cost-cutting is not a long-term strategy. By paring back on innovation, companies are ignoring the lessons from the global financial crisis, during which those that invested emerged from the crisis stronger than their rivals and with greater long-term viability. A tendency towards caution may be understandable, but companies that already excel at innovation are expected to use the crisis to cement their competitive advantage.

There is a double-sided risk of not digitalising and innovating fast enough to compete and doing so in an unfocused or haphazard manner. It is estimated that 70% of digital initiatives do not reach their goals, equating to $900bn of the $1.3trn invested in digital transformation in 2019.[6] This is why it is important that management understands the who, what and how of the various digitalisation projects that are planned and underway. A fundamental question is whether the business understands what projects are a priority and why they are really necessary to ensure the company's future.

> *"By paring back on **innovation**, companies are ignoring the lessons from the **global financial crisis**."*

An internal audit perspective

Internal audit can support strategic digital objectives in a number of ways. These include confirming that the business understands how digital and other innovation initiatives are aligned with and enable the overall corporate strategy, i.e. what their purpose is and why they are important. Internal audit can also assess the governance of these projects, including appropriate accountability for their success or failure and clear objectives that are aligned with the corporate strategy. In the case of projects being derailed by disruption associated with the pandemic, internal audit can help the board to understand these issues in order to bring projects back on track through closer oversight and input from senior management.

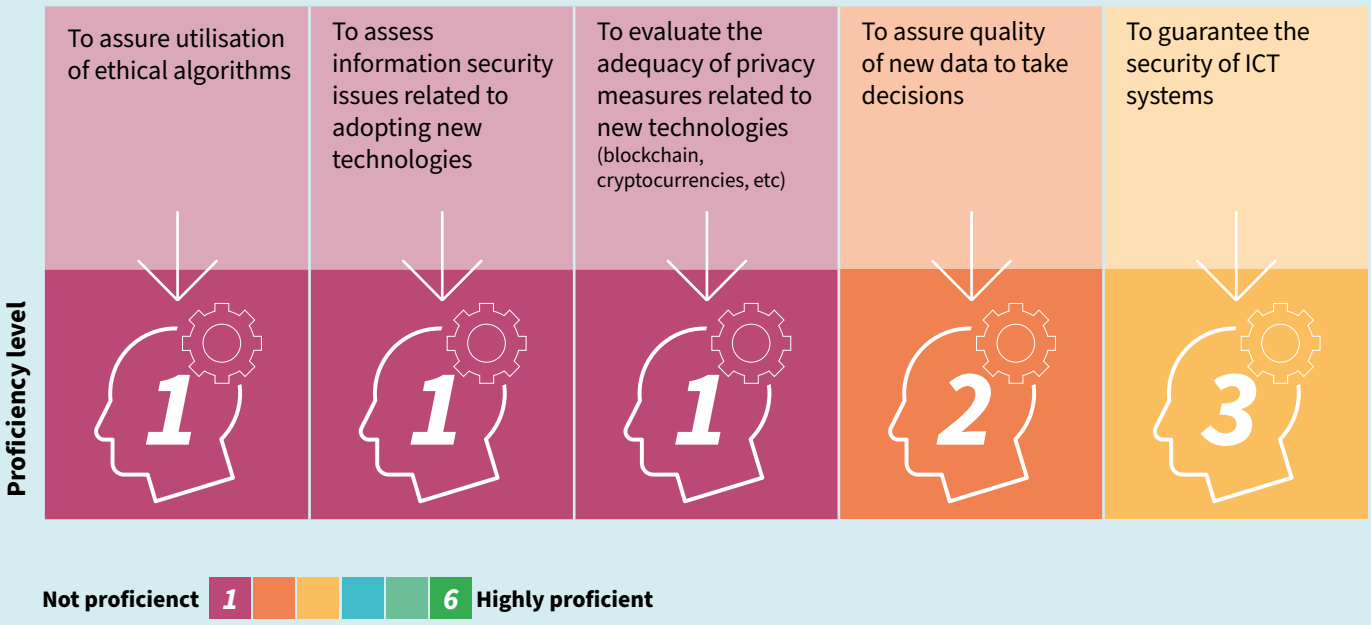
At the more granular level, internal audit can involve itself early in projects as an advisor. It can consult on digitalised processes in the development stage before they are rolled out by providing its unique risk-control perspective. Full independence must of course be ensured in these circumstances, i.e. internal audit is never accountable for designing controls, only advising, and the auditor that advises should not be involved in any formal audit of these processes or projects at a later date. In the case of agile product development, internal audit should be present for sprint reviews when stakeholders complete a new iteration of the project to assure whether risks and controls have been accounted for and logged.

There is also scope for the third line to audit technologies themselves. All digital processes depend on accurate, high-quality data. Internal audit may assess the governance around business-critical data, including how it is sourced, managed and cleaned. Third line assurance work may also apply to algorithms that are powered by this data – internal audit may check that algorithms parse data as expected and deliver the desired outcomes. These algorithms will need to be documented, explainable and ethical. Human biases can be intentionally or inadvertently programmed into machine learning and anything that unfairly prejudices demographic groups may have serious legal, regulatory and reputational ramifications.

5. Why crises call for innovation, not hibernation | Rainmaking
6. 100 Stats On Digital Transformation And Customer Experience | Forbes

Perceived internal audit skills and knowledge gaps

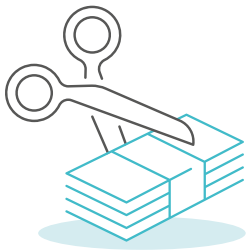
Based on the proficiency of internal audit, subject matter experts in our research considered that the "average" audit function could have difficulty in performing the following engagements:



Questions and considerations for internal audit

- Does management have a clear view on which innovation projects are critical to ensuring the strategic relevance and future viability of the company and have they been appropriately resourced?
- Have opportunities been identified by management to invest in innovation during the economic lull while competitors are distracted and side-tracked?
- Is the governance aligned with the development framework e.g. Waterfall, Agile, hybrid models? Are project development frameworks used for the right purposes and has this been justified? Are management roles, tasks and accountability aligned with the chosen method of development?
- Is the expected governance around projects in place, including overall project ownership and accountability? Does each digital transformation project have a single owner who is accountable for its success?
- Can the business successfully manage projects and change? Have lessons been learned from the success or failure of past projects? What evidence is there of this? Are any competency gaps understood by the first line?
- Does the company have a well-managed and authoritative system of record to track innovation investment, progress and results?
- Does the technology and data that is fundamental to enabling the company's operations and strategy work as expected? Are algorithms ethical and unbiased for instance?

Liquidity risk and cost-cutting amid depressed demand



Some industries have financially benefitted from recent events, technology being a clear winner in this crisis as the stock prices of Facebook and Amazon rebounded well above their pre-COVID highs. Most have not been so fortunate. What started as a supply-side issue when China was stemming the outbreak with its lockdown between January and March quickly shifted to a demand-side concern. A collapse in demand forced many companies into survival mode as cash flows evaporated.

CAEs we interviewed for this year's Risk in Focus at non-financial services companies spoke of liquidity being one of three urgent risks amid the immediate impact of the pandemic (alongside the health and safety of staff and cybersecurity in the homeworking environment). More than two in five (42%) CAEs in our quantitative survey, meanwhile, cited *Financial, capital and liquidity risks* as being among the top five risks their organisation faces, a 40% increase on the 30% of audit leaders who said the same just 12 months prior. This is likely a consequence of the timing of the survey in March, when the coronavirus outbreak reached Europe and short-term liquidity risk spiked for most companies.

Notably, financial services CAEs highlighted that the GCP has so far had limited impact on liquidity in the sector as there has been no run on the banks. While the pandemic, like the global financial crisis, has precipitated a major worldwide recession, 2008 started as a banking failure. In 2020, the financial sector remained in robust shape, having shored up balance sheets and allocated regulatory capital in prior years. Nevertheless, capital risks will rise if loans in hard-hit sectors such as consumer discretionary, dining and leisure default in vast numbers, which will depend on the depth and duration of the recessionary environment.

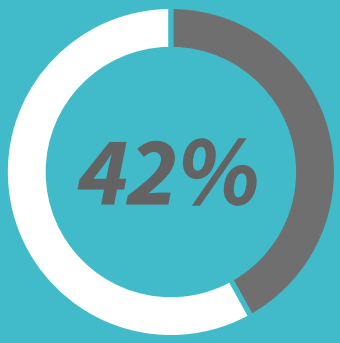
Companies' priority in 2020 has been to assess liquidity risk by taking an enterprise-wide view of receivables, payables, inventory, taxes and – perhaps most important of all - cash and cash equivalents. The primary objective has been to stem financial outgoings and secure income, to the extent that is possible when vendors and customers are all doing the same.

Like other risk impacts related to the pandemic, this can be split into short-term and longer-term effects. Even companies with strong balance sheets (i.e. high levels of assets, especially cash, versus low liabilities) will have to consider their financial sustainability in a potentially challenging trading environment through 2021. The International Monetary Fund (IMF) has said the world is likely to be facing the deepest recession since the 1930s Great Depression and warned that the recovery may take longer than initially hoped. Others point to the sharp decline and recovery of stock markets and unprecedented monetary and fiscal stimulus as reasons to expect a V-shaped economic recovery.

Whichever side is correct, many businesses will now be reviewing their working capital costs and margins on underperforming business lines to secure their long-term financial sustainability. Indeed, 30% of Chief Executives have said that

"Financial resilience is a very hot topic because we are missing a lot of revenue and income. I don't know how we are going to cope in relation to project management and infrastructural investments. Do we have a plan? Do we have a strong enough cash position? Has our investment capacity been impacted? I want to know how financially resilient we are and what has been put into place in terms of changes to processes, projects, investments and so on. In relation to audit, what I want to know is how well controlled the important processes are – the budget process, the cost management process, budget defining, budget responsibility."

CAE, hospital, Belgium



More than two in five (42%) CAEs in our quantitative survey cited ***'Financial, capital and liquidity risks'*** *as being among the* ***top five risks*** *their organisation faces.*

improving operational efficiencies will be a financial action taken in direct response to COVID-19.[5] Cost-saving may include postponing planned capex-intensive innovation projects (although this may be inadvisable – see *Strategic relevance and the digital imperative* on page 19), capping or freezing pay rises, using contract labour rather than fully employing staff and choosing not to renew office leases. This requires a holistic assessment of enterprise-level operations such as manufacturing, sales, advertising and marketing activities to reveal areas to significantly improve efficiencies and bring down costs.

This is not without risk, of course. Taking resources out of the business will cause disruption, could reduce the flexibility necessary for business resilience and may limit future growth potential. Cutting costs is not a long-term growth strategy. This is a trade-off that businesses must pay close attention to.

An internal audit perspective

Short-term financial risks may have abated by 2021, although the board/audit committee could seek treasury audits to confirm that liquidity risks are being managed amid what may be ongoing depressed levels of demand – or that cash flows, working capital and investments are being closely monitored within companies experiencing elevated demand for their products and services.

The medium-term need to rein in costs is where internal audit can add significant value, supporting the business by analysing business operations for gaps and inefficiencies that can be closed to deliver savings. There is also an assurance role to play in assessing whether management's cost-cutting initiatives have clear goals and have been fully thought through. Relatively modest disruption to operations can be achieved by making cross-department savings; sweeping operational restructurings or jettisoning full business units are likely to have a greater disruptive impact but may deliver commensurately larger savings. The business may choose some combination of the two but should be able to show evidence of the rationale for whatever action it plans to take. Internal audit can assess whether the knock-on effects - the disruptive costs and not just the cost savings - are accounted for in management's calculations.

Questions and considerations for internal audit

- How successful have the treasury and CFO been in their efforts to manage the company's liquidity risks?
- If demand for the company's products or services has fallen dramatically, have the root causes been identified and steps been taken to adapt the business model, if necessary? Have these been justified and documented? To what extent have any such urgent operational or strategic pivots impacted the risk profile of the business and its control environment?
- Can internal audit help the business identify operational efficiencies and gaps that can be closed to make long-term cost savings? Is this required by key stakeholders including senior management? What steps has internal audit taken to maintain its independence if supporting the first line in this capacity?
- Has senior management made or proposed cost-cutting measures? If so, to what extent are these likely to cause disruptions and has this been accounted for? To what extent do cost-cutting measures or a focus on operational efficiencies pose a risk to the organisation's operational resiliency, growth and strategic plan?
- Have longer-term liquidity and financial risks been addressed, such as access to necessary refinancing when loan and bond terms expire?

*"More than one in three (35%) CAEs cited **'Human capital and talent management'** as a **top five risk**, compared with 27% who said the same a year ago."*

Managing talent, staff wellbeing and diversity challenges

New ways of working and organising personnel were already underway in recent years, with a trend towards more flexible working arrangements and greater autonomy as generational attitudes to work shifted. By forcing remote working almost instantaneously, the pandemic accelerated that gradual evolution.

Among the other major business trends fast-tracked by the health crisis is the competitive advantage afforded to companies with exemplary digital capabilities, heightening pressure on competitors to raise their game. This will mean hiring from an already highly competitive digital talent pool. Meanwhile, social equality and diversity issues were at the centre of public debate in 2020, which has brought companies' ethics, staffing policies and racial and gender representation into sharper focus than ever.

More than one in three (35%) CAEs cited *Human capital and talent management* as a top five risk, compared with 27% who said the same a year ago; the magnitude of this risk is also increasing - 37% said they anticipate it being a priority three years from now.

All businesses should have some degree of skills mapping and forecasting capability to understand and anticipate the organisation's human capital requirements. This will not only provide insight in advance as to what skills and candidates need to be sourced from the outside world – and the steps that need to be taken to attract those people - tracking and developing existing skills within the business help organisations to nurture and retain talent by filling positions internally.

In the near term, sourcing in-demand talent will be made more complicated by the need to maintain safe working environments and the health of staff. Companies are deciding between phasing in a return of staff with restricted capacity to maintain social distancing, or offering homeworking on a permanent basis. Interviewing, onboarding and training people may need to happen remotely and employers face the prospect of creating a sense of unity, common purpose and belonging amid disparate and distanced working conditions, which will be especially challenging for new joiners. Candidates may also be reluctant to move roles, giving up the security of their current position within a team they know to join an unfamiliar organisation amid economic uncertainty.

Employers will not be inclined to force staff to return on-premise and precautionary measures will have to be taken to ensure the physical wellbeing of staff (masks, hand sanitiser, Perspex dividers) until this health risk has receded. Another major safety consideration is the potential for a second or more waves of the virus. Heeding the warnings of health experts

*"All businesses should have some degree of **skills mapping** and forecasting capability to understand and anticipate the organisation's **human capital** requirements."*

and scientists, 77% of large US companies (i.e. those with more than 1,000 employees) are incorporating this potential scenario into their return-to-workplace strategies.[7] Businesses must also be mindful of the psychological impacts that months of isolation may have had on their workers. The bottom line is that without a healthy staff, the operations of an organisation can be seriously impaired. And companies that do not take sufficient care of their people may struggle to retain talent over the long run.

These considerations have put *Health and safety* under the spotlight; 17% of CAEs in our quantitative survey said this is a top five risk, a 70% year-on-year increase on the 10% of audit leaders who said the same a year ago.

The diversity agenda has taken on renewed significance and this has human capital implications. The Non-Financial Reporting Directive, which operates on a "comply or explain" basis and has been under consultation in 2020 to help standardise reporting, has encouraged transparency of diversity and inclusion. Since it was rolled out to member states in 2018, disclosure on diversity and inclusion in the region has improved and this is expected to increase further.

Businesses need to be more conscious than ever of how their personnel practices align with and reflect the cultural values of society as the awareness of diversity and equality issues rises. Hiring policies, working cultures and ethics will be under the microscope like never before. Racial equality was at the centre of public debate in 2020 after the Black Lives Matter (BLM) movement called for an end to police brutality and racist law enforcement practices. Many corporations and institutions have shown solidarity with BLM, including the European Parliament which passed a non-legally binding resolution to denounce racism and white supremacy. Major firms that publicly champion diversity and condemn social inequity and yet under-employ people of colour or who have gender pay gaps could face public censure. The reputational damage of this should not be underestimated.

An internal audit perspective

The business, its corporate strategy and personnel management must be closely aligned. Internal audit should look for evidence that the business understands and is forecasting what skills, competences and attitudes are required to secure its market position and long-term strategic relevance. Boards may seek assurance that specific skills and worker profiles are being matched to planned innovation projects that will determine the future success of the company. This will be made more complicated by the accelerated shift to more homeworking, a challenge the business will need to demonstrate it is overcoming from a human capital perspective.

The diversity challenge can also be addressed with the assistance of internal audit. For one, there is scope for the third line to deliver assurance on the effectiveness of HR practices designed to avoid biases and ensure the fair treatment and representation of staff - and analyse the root cause of any biases that do exist or reasons why diversity is not achieved. Internal audit can give the board/audit committee an impartial view on how effectively the company is meeting its diversity goals or uncover any weaknesses in procedures or policies that result in inconsistencies in the treatment and career progression of staff. There is scope here for culture audits, or cultural elements of HR audits, to show how the everyday life of the organisation and the behaviour of its staff reflect its espoused values.

7. 77% of organizations are planning for a second wave of Covid-19 infections | I4CP Survey

Questions and considerations for internal audit

- How does the business define and manage its human capital and talent management needs and risk?
- Is the HR/workforce strategy aligned with the corporate strategy, culture and values and do they inform each other?
- How does the business intend to attract and retain the skills it requires, e.g. digital skills? What will make talent decide to work at the company versus its competition (e.g. salary, job satisfaction, flexible arrangements, culture and values of the company)?
- Does the business have any skills forecasting capability and is there an understanding of what hiring will be needed over the short, medium and long-term?
- Are the skills that are present in the business mapped and are gaps identified? Is there evidence that the business develops skills in order to meet its strategic requirements?
- Is there a clear return-to-work strategy that prioritises the health and safety of staff?
- How effective is the business in ensuring the physical and mental wellbeing of its staff, both in the office and in the homeworking environment? Has this had to be adapted since the GCP and how?
- Does the organisation's workforce diversity reflect its publicly espoused values?
- What processes and policies are in place that ensure the fair treatment of staff? Are there any biases that result in the unequal treatment of workers, especially with regards to race, gender, religion and sexual orientation?

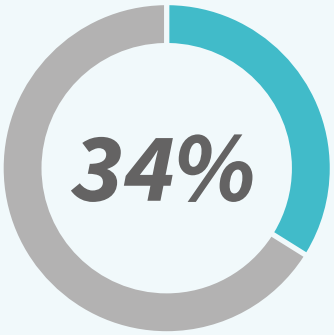
Priority areas in HR for internal audit

The following were ranked by subject matter experts as the most important factors to be audited, in descending order.

- **Capacity to attract new talent**
- **Retention rates of key staff**
- **Level of diversity**
- **Level of burnout**
- **Speed of decision making**
- **Flexibility of operations**
- **Absenteeism**
- **Employee engagement**
- **Continuous personal improvement and education**

"This coronavirus outbreak is like a mass experiment in operational resiliency. It's important that a business understands its end-to-end customer journeys, the systems and processes and teams that support those. And then have appropriate resiliency arrangements so that, as and when certain components fail, whether technology or people, there are swap-ins to keep key services live. It's beyond disaster recovery."

CAE, Euronext-listed banking group, Ireland



*of CAEs put **'Disasters and crisis response'** among their organisation's **top five risk** priorities.*

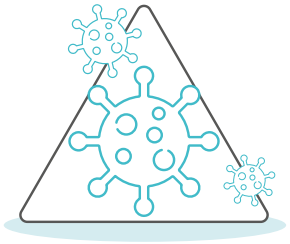
1 in 4

*(25%) CAEs say that **'Communications, management and reputation'** is one of the **top five risks** their organisation currently faces.*

"It's an opportunity to update the protocols and BCP because we have now had a worst-case scenario forced upon everyone. We know exactly what happened, what went wrong and it's the perfect opportunity to improve the crisis management. It's one thing not being prepared for something like this. But the worst thing is to not learn any lessons from this experience and fail to be better prepared for something like this happening again.
This is a good opportunity for the company to be more resilient and adaptable than before. We can rethink the production model and the way the production is organised to be more operationally resilient and flexible. This is not the last crisis unfortunately."

CAE, defence contractor and industrial group, France

Disaster and crisis preparedness: lessons from the pandemic



One of the biggest lessons to take from the pandemic is the importance of crisis preparedness and operational resiliency. All companies will have had business continuity or crisis response plans in place. But these are more likely to have accounted for short-lived events like power or network outages, earthquakes and data breaches. Few would have included a major pandemic scenario and likely none planned for an almost simultaneous global lockdown. The pandemic has set a new precedent in crisis management.

Organisations will be conducting post reviews on how effective their business continuity plans (BCPs) were, to what extent they were followed and the robustness of the governance around crisis time decision-making. Crisis management and planning will have to be updated in light of the potential for a second or more waves of the coronavirus, not to mention other possible pandemics that follow a similarly rapid contagion path.

For the first time this year, *Disasters and crisis response* was included in our quantitative survey and 34% of CAEs put this among their organisation's top five risk priorities; 10% of CAEs highlighted it as the single biggest risk behind only *Cybersecurity and data security* (27%), and broadly on par with *Financial, capital and liquidity* (11%) and *Regulatory change and compliance* (also 11%).

Before the pandemic struck, greater attention was already being paid to the concept of operational resiliency, which is subtly distinct from business continuity management. Where the latter concerns the company's response to disruptive scenarios, such as outages or extreme weather events, operational resiliency takes a broader view of the ability to maintain integrity and keep the lights on whatever the circumstances. Resilience focuses not just on how to get back to business after a specific event arises, but on how businesses can identify their most valuable assets, services and processes and pre-emptively protect their resources, staff and brand equity from threats.

The UK Financial Conduct Authority is developing guidance in this area for financial firms. Formal guidance is expected to be finalised towards the end of 2020 with oversight commencing in the second half of 2021, the pandemic having caused delays to the regulator's public consultation. In addition, in March 2020 the European Commission closed a public consultation to explore how an enhanced cross-sectoral digital operational resilience framework for the EU financial services sector could be set up. This has a specific focus on improving IT security in the industry across Europe.

With these regulatory developments still in motion and more complete guidance to follow, the initial thinking is that firms can take four core steps to build greater operational resiliency. It is proposed that organisations:

- Identify their most important business services that if disrupted could cause the most harm and instability to their operations and customers (and, for financial services firm, the financial system and markets).
- Set impact tolerances for each important business service, which would quantify the maximum tolerable level of disruption.

- Identify and document the people, processes, technology, facilities and information that support critical business services.
- Stress test their ability to remain within their impact tolerances through a range of severe but plausible disruption scenarios, which now should clearly include the impact of pandemics and other global shock events.

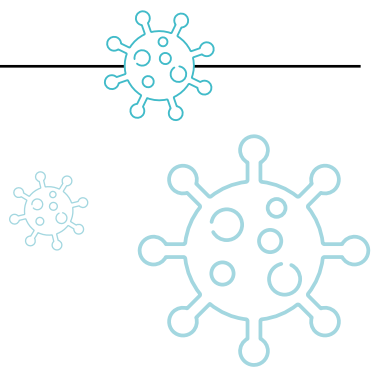
At the most fundamental level, businesses need to consider and understand the chain of activities that make up the business service or product they deliver to customers and clients, including all necessary third parties they depend upon. The company can then test various scenarios and assess the impact on staff, systems, operations and customers to see if any weaknesses emerge that require immediate attention. The pandemic represents the ideal opportunity for all organisations to review their resilience in the face of what has been a real-life crisis scenario. The opportunity to learn from and improve upon that response should not be wasted.

Integral to the crisis response in any major organisation is the assembly of a pre-determined crisis/emergency committee. The coronavirus pandemic has shown that crises have the potential to touch all corners of an organisation and so these emergency committees should be cross-functional and include heads of HR, communications, legal, compliance, customer services, risk management and internal audit and be headed by a senior management member. This crisis team should meet regularly and frequently (at least weekly if not daily, depending on the severity of the crisis) to discuss how the business should respond operationally and strategically in real-time to what may be a rapidly evolving and uncertain situation.

Another factor to consider in crisis situations is the treatment of customers and what this means for the business's reputation. Banks, utilities, telecoms firms and other companies that provide services on credit are having to think carefully about their customers' ability to meet their financial obligations as unemployment rates have surged. Crises bring scrutiny and consumers will remember how companies behaved during this time and will vote with their wallets when conditions improve. Reputations are at stake and those businesses who assist and support customers can turn the pandemic to their advantage by fostering long-term relationships. One in four (25%) CAEs say that *Communications, management and reputation* is one of the top five risks their organisation currently faces, a small increase on last year (22%).

External crisis communications should be part of every BCP so that the business has protocols for providing status updates and information to key clients and other stakeholders. These should be used to openly and honestly outline how the business is responding to and proactively mitigating the effects of disruption. These should be tailored to the specific audience they are addressing, whether customers or the media. Managing a crisis is only one part of the equation; managing communications in the wake of a crisis can make or break a company's reputation and trust in its brand.

*"The pandemic represents the **ideal opportunity** for all organisations to review their **resilience** in the face of what has been a real-life crisis scenario."*



An internal audit perspective

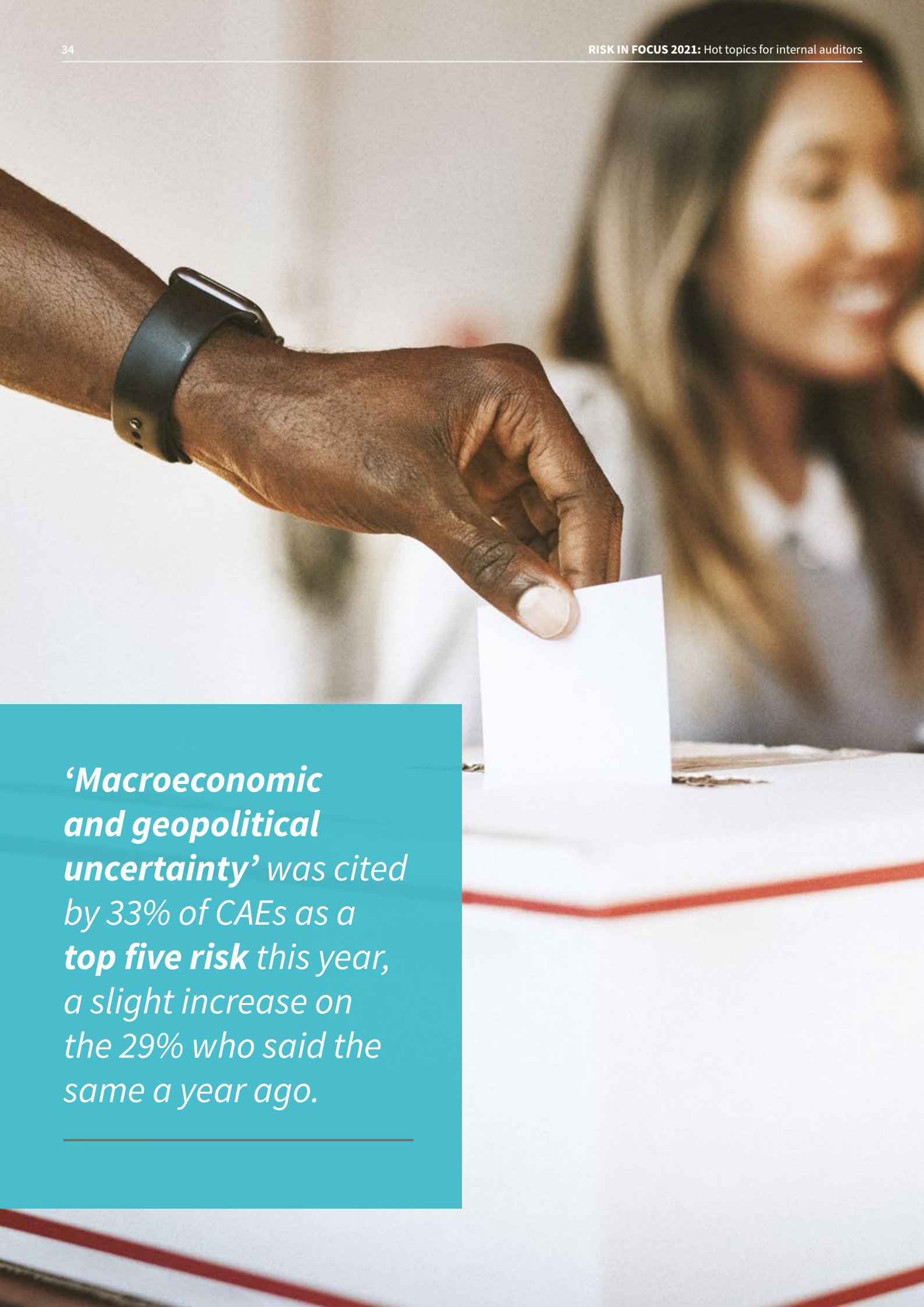
The third line can review whether the business has carried out a post-mortem to determine how well it coped with the pandemic crisis and whether the business continuity or crisis response plans were fit for purpose, were followed and whether they require updating. It may even choose to carry out an independent post-mortem of its own. This can help test the integrity of the conclusions drawn from the first line's own assessments.

The most mature approaches will go further than simply updating and adding global lockdown scenarios to BCPs. True operational resiliency will require that businesses identify and map key people and business units, set impact tolerances and test response and recovery actions based on those tolerances. Internal audit can highlight to the board any gaps in the maturity of the organisation's approach to resiliency.

Internal audit should seek evidence of the governance around crisis decision-making and the integrity of data and information reported to crisis committees. The CAE may have a seat in the crisis committee in an advisory capacity to give its view on how decisions might impact upon the business and its risk exposure. If this is the case, internal audit's independence will need to be maintained given the audit head's proximity to the crisis management decision-making body. The third line can also check the preparedness of the company to communicate with customers, the public and the media swiftly and effectively in crisis situations. There should be evidence of clear responsibilities and reporting as it relates to crisis management and damage control in the public domain and internal audit can assess the adequacy of controls designed to ensure correct interactions on social media, such as who can use these platforms and what they are permitted to say.

Questions and considerations for internal audit

- How effective was the organisation in responding and adapting to the pandemic? Was this consistent across territories? If not, why?
- Has the business continuity plan been updated to include a global pandemic scenario and its related challenges? Does the plan now include and cover all possible external risk events? Are the various scenarios and BCP arrangements tested?
- Has the business carried out a lessons-learned exercise since the pandemic scenario to improve its response to future crises? What lessons were learned?
- Has internal audit independently carried out a post-mortem, rather than examine the business's work in this regard? Does the board/audit committee require the third line to carry out an independent post-mortem?
- Was crisis decision-making aligned with the specific circumstances and was it fast and effective enough? Was the governance of these decisions as would be expected and based on sound and consistent data and assumptions? Did management monitor the effects of the first decisions it took and act upon the outcomes of those decisions?
- Are crisis communications procedures set out in the BCP that apply to both staff and external stakeholders such as customers, suppliers and shareholders?
- Does senior management understand its brand value and reputational risk? Has this been impacted by its response to the pandemic and the ensuing economic crisis?



'Macroeconomic and geopolitical uncertainty' *was cited by 33% of CAEs as a* ***top five risk*** *this year, a slight increase on the 29% who said the same a year ago.*

Rising nationalism and social tensions amid unprecedented economic volatility

Macroeconomic and geopolitical uncertainty **was cited by 33% of CAEs as a top five risk this year, a slight increase on the 29% who said the same a year ago, while 8% say it is the single biggest risk their company currently faces. Yet only 3% say this is an area on which internal audit spends significant time and effort, a disconnect also present in last year's results (4%).**

At the beginning of 2020 UN Secretary-General António Guterres warned that geopolitical tensions are at their highest level this century as the world's two biggest superpowers, the US and China, vie for position. Against a backdrop of elevated nationalism and radicalisation that has been bubbling already for a number of years, he said that trade and technological conflicts were fracturing world markets and that more and more countries were taking "unpredicted decisions with unpredictable consequences", carrying with it a risk of miscalculation.

This was before the spread of coronavirus was recognised as a global pandemic. Since then nationalist fractures have exacerbated further. Border restrictions were put in place through 2020 and questions have been asked about the risks posed by the reliance of Western industry on Chinese manufacturing and technology. The US and Chinese technology sectors have already begun to decouple, impacting strategic industries such as semiconductors, cloud computing and 5G. Governments are becoming more protective of innovation industries as they introduce greater restrictions on foreign investment.

On March 25 2020, in direct response to the GCP, the European Commission issued guidelines on the protection of European strategic assets. The general principles relate to the screening of investments in member states' critical assets and technologies to prevent them from being controlled by foreign investors whose interests run counter to the EU. The concern is that overseas actors may seek to exploit market disruption caused by the pandemic to acquire and control not only sensitive technologies but critical healthcare-related assets. Recent months have witnessed a more united front against China among Western countries including in Europe, not just the US. For instance, the UK decided to ban Huawei from its 5G infrastructure as a matter of national security, following in the footsteps of Australia, New Zealand, Japan, Taiwan and the US.

A number of developments in 2019-2020 widened the diplomatic gap between the West and China, including the Hong Kong protests that concluded in China passing a controversial security law in the territory, further evidence of the persecution of Uighur minorities and obfuscation surrounding the coronavirus outbreak. All of this suggests that even if the US administration changes over following the November 2020 US presidential elections, political and trade tensions may remain high.

January 2021 will see the end of the UK's Brexit transition period after the deadline for an extension passed in June. If no trade deal has been agreed and ratified by the end of 2020, then the UK faces the prospect of tariffs on imports and exports via the EU and vice versa. This will ultimately add more cost for businesses and will be of particular concern for UK companies. More than 100 UK Chief Executives have warned that they do not have time or capacity to prepare for big changes in trading rules by the end of 2020 — especially in light of the upheaval caused by coronavirus.[8]

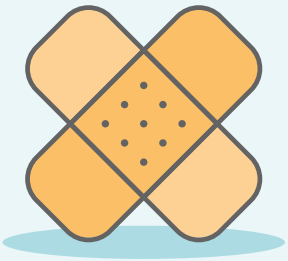
Widening inequality is also causing social tensions. Real wages have stagnated over the last five decades at the same time that productivity (the value a company gains per unit of labour) has

8. Johnson warned by business on 'hugely damaging' no-deal Brexit | Financial Times

"A lot of measures have been taken to mitigate the effects of the virus and have come at an enormous cost, so how do we manage that in the future and what has to be changed? There will be a lot of pressure on governments for the next few years now with all of the expenditure, the public debt it has created and the speed of the economic recovery."

CAE, public sector audit agency, Belgium

The US spent $700bn in 2008 rescuing its financial system *compared with* ***the $3trn*** *it has earmarked for its coronavirus response under the HEROES Act.*



In June 2020, the IMF cut its ***global economic growth*** *forecast to* ***-4.9%*** *from -3%.*

"Various countries are very sceptical of China right now and they're thinking about whether they should have their supply chain so dependent on China. I think you're going to see a lot of repatriation of manufacturing back into home countries and more nationalisation and as with the Golden Power rule in Italy we've already seen countries become more strict about foreign investment with rules to block certain deals. There could be a greater aversion to foreign investment and obviously that's a problem when global companies are looking to expand and improve their margins."

CAE, NYSE-listed telecoms group, Italy

increased.[9] The pandemic is expected to further widen the wealth gap as low-skilled labour disproportionately bears the brunt of economic volatility. In June 2020, the IMF cut its global economic growth forecast to -4.9% from -3% and said the crisis is causing a steeper recession and a slower recovery than initially expected. Riots sparked by racial injustice in 2020 are a related symptom of the persistent and growing socioeconomic divide that, combined with the public health crisis, has been destabilising civil society. At the same time, unprecedented economic stimulus packages (for perspective, the US spent $700bn in 2008 rescuing its financial system compared with the $3trn it has earmarked for its coronavirus response under the HEROES Act) are adding to already historically high levels of public debt, a hangover from the bank bail-outs during the global financial crisis.

A return of the sovereign debt crises of the 2010s looks almost inevitable for some EU states contending with ageing populations and fiscal problems. This poses a fundamental question: who will pay down this public debt and who will address the growing wealth gap? This represents a significant looming tax threat for businesses. Coupled with rising nationalism, foreign companies are prime targets for bridging these public deficits and restoring a degree of economic equality. Any such actions by governments to tax foreign businesses typically result in retaliatory political actions such as trade tariffs and other levies, increasing the financial burden on companies.

An internal audit perspective

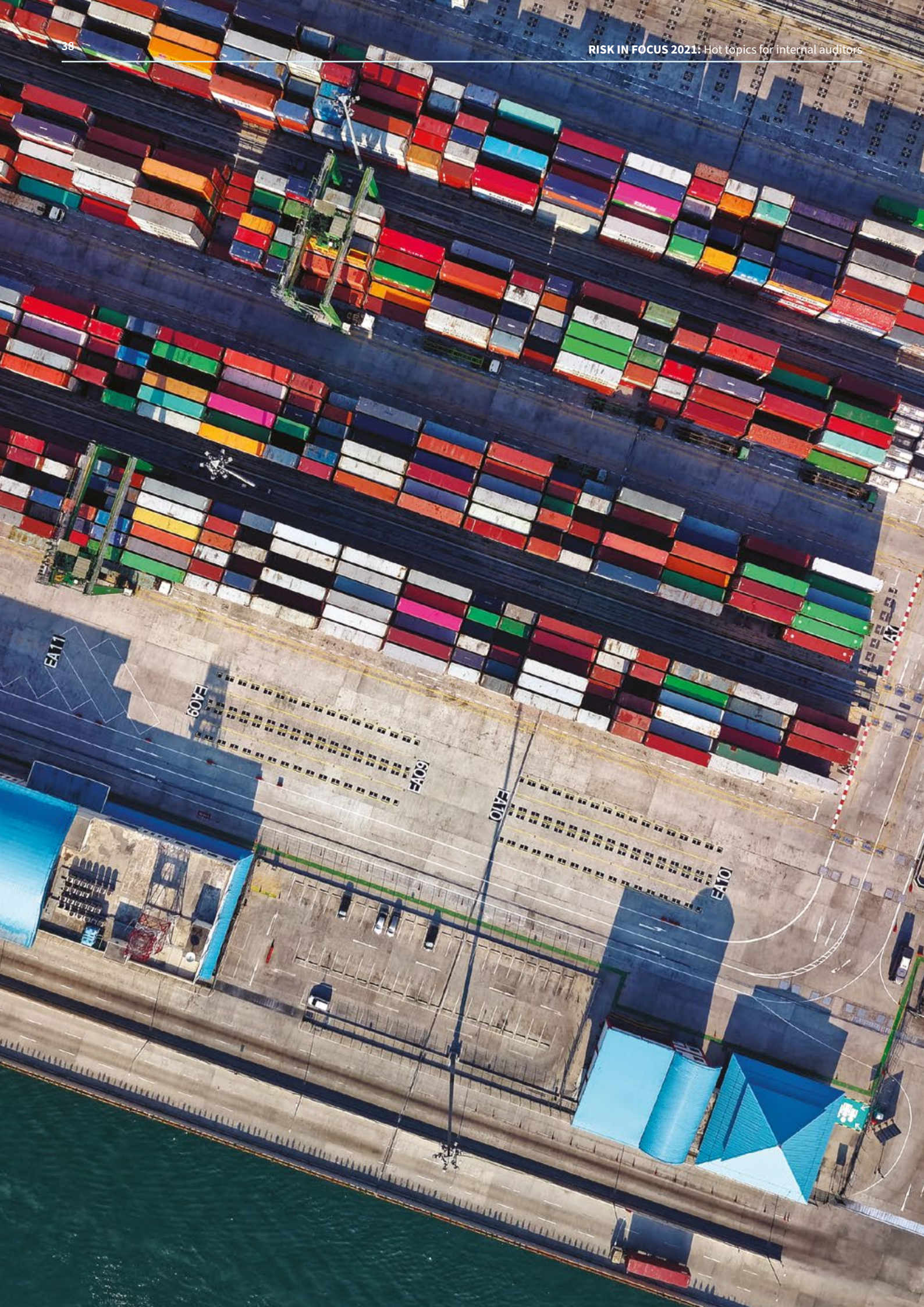
Currently audit work in this area is a priority for a tiny minority of internal audit departments (3%); however, 8% of CAEs anticipate *Macroeconomic and geopolitical uncertainty* to be one of the top five risk areas on which internal audit spends most time and effort three years from now. Organisations need to know they can rapidly adapt to changing circumstances and internal audit can provide assurance on this ability to strategically and operationally pivot in a timely manner. Macroeconomic and political "what if?" risk scenarios should be included in BCPs and, ultimately, a company's ability to be fluid and adapt to changes in the external environment outside of its control come down to its operational resiliency (see page 31). The speed with which companies can adapt has never been more critical given the unpredictability of political decisions in recent years.

Internal audit can check whether the business has accounted for possible developments in the markets in which the business operates that pose the greatest political risk. This may include seeing whether peer group companies have previously been impacted by sitting governments' political decisions or if they have become tax targets. There should be an awareness among senior management that aligning with politically sensitive vendors (e.g. Huawei) could harm the company's prospects and market access, particularly in the US. Internal audit can verify that macroeconomic and geopolitical uncertainty is factored into the company's business strategy. It should also assure the existence of strategy-making processes that routinely identify, assess, monitor, update and incorporate the latest political and economic risks in key markets and that past experience is included in the strategy-making feedback loop.

Questions and considerations for internal audit

- Are macroeconomic and geopolitical risks factored into the company's business strategy and decision making?
- Does the business have preparedness committees and is macroeconomic and geopolitical scenario planning being utilised effectively?
- Are carefully substantiated continuity/resilience plans in place should politically motivated trade measures escalate?
- Is the business aware of sensitive vendors (e.g. Huawei) and customers that associating with may jeopardise future opportunities?
- Has the business accounted for a no-deal Brexit scenario and what this will mean for it?
- Has the business considered whether it is likely to become a tax target in certain jurisdictions? What, if anything, will it do if that is the case, e.g. pull out of that jurisdiction, legally restructure its operations to protect profits, engage with the government early to make its case?

9. On the link between US pay and productivity | VOX, CEPR Policy Portal


EA11
EA09
EA08
EA10
EA01
A7

Supply chain disruption and vendor solvency

Supply chains have come under immense stress. Past considerations focused on efficiency and suppliers' ethical integrity; however, the emphasis has shifted to the robustness of supply chains and concentration risk. China, the biggest supplier nation in the world by a considerable distance, overcame its first wave of coronavirus relatively quickly and initial concerns amid the pandemic's early weeks quickly turned from supply to demand. Only 26% of CAEs say *Supply chains, outsourcing and 'nth' party risk* is among their companies' top five risks compared with 36% last year, with less than 2% singling it out as the biggest risk.

The ability to meet depressed demand with available supply in the face of the GCP may have given companies a false sense of security. Resurgences in the coronavirus cases or new pandemics may cause future supply disruptions and the length and complexity of supply chains means that any delays may take many months to work their way from beginning to end. This can make the true impact of disruption hard to gauge.

Supply chains are also leaner than ever, a fact that was made obvious by shortages in PPE (personal protective equipment) when coronavirus reached Europe in Q1 2020. Inventory management techniques inspired by Just-in-Time manufacturing were adopted in recent decades to eliminate waste and align production to demand. This is achieved by having suppliers deliver smaller amounts of materials more frequently to reduce holding and storing extra stock. The crisis situation exposed the fact that global supply chains have become taught and, consequently, more fragile. Their length and leanness means that supply can be too slow to meet demand.

Major companies have also had to assess the ongoing viability of key suppliers and, where appropriate, offer financial assistance by paying upfront to ensure their own operations do not go offline. Vendor insolvencies have the potential to cause massive disruption. One blind spot that few companies accounted for is the level of outsourcing to overseas territories such as India and parts of South-East Asia and what this means in the event of a global pandemic lockdown. For instance, is it even possible to send a customer services function based in India to work from home? What happens if multiple outsourcing territories enter simultaneous lockdowns? These are questions that companies have never had cause to ask themselves until now.

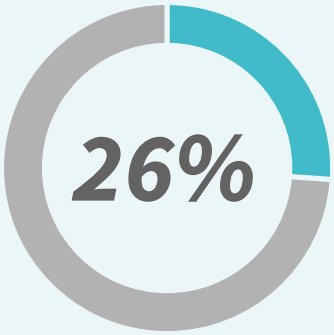
*"**Supply chains** are leaner than ever, a fact that was made obvious by shortages in PPE when coronavirus reached Europe in Q1 2020."*

"I would assume that internal audit will look at areas where there were always risks, but now they will just be a lot more serious. Bankruptcies of key suppliers that can stop production lines, for example. How do we handle such situations? Whenever we get through this crisis businesses are going to be looking at their supply chains and their dependability."

Audit Committee Chair, appliance manufacturer, Sweden

"Supplier dependency is certainly something to think about more deeply in future. We continue to depend on faraway countries in areas where information is not very transparent."

CAE, CAC 40 food retailer, France



*Over a quarter of CAEs say **Supply chains, outsourcing and 'nth' party risk** is among their companies' **top five risks** compared with 36% last year.*

Supplier risk considerations

The subject matter experts surveyed for this year's report identified the following as the most important outsourcing considerations right now:

- The need to reinforce diversified supply sources
- The need to reinforce local supply sources
- Increasing specialisation is making supply chains longer (more 'nth' parties)

The experts were also asked to judge the change in importance of supplier-related risks and their impacts on the business:

Effect/impact	Present at this moment	Change in importance
Vendor lock-in/dependency of third parties	Highly present	More important
Scalability	Highly present	More important
Over-reliance on unknown levels of control	Highly present	No real change; slightly more important
Loss of data/know how	Highly present	No real change; slightly more important
Weak assurance and traceability of controls (incl. right to audit)	Highly present	No real change; slightly more important

An internal audit perspective

The business should be aware of weaknesses, pressure points and potential bottlenecks in its supply chains, tracing all the way back to raw materials. Flexibility and agility can help to mitigate these. Indeed, while overseeing a more complex supply chain requires more effort, having alternative suppliers on standby in various geographies reduces concentration risk should shock events occur.

Internal audit can assess whether the business has paid sufficient attention to the need to remodel supply chains and outsourcing strategies to improve its operational resiliency. This remodelling may take the form of embedding contingency measures such as alternative suppliers, or permanently repatriating production and business functions to better cope with future problems. The business should understand and be able to explain the rationale behind the supply chain model and approach that it uses, including any lean inventory management practices. Internal audit can seek evidence of the quality of data and the governance of the decision-making that underpins the going-forward supply chain strategy.

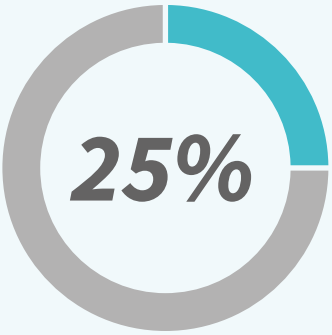
The board may also seek some assurance that key vendors are on a sound financial footing as the economy comes under stress. Depending on the value of the relationship and the risk to the business the supplier's insolvency poses, this may require offering to pay ahead of delivery or some other financing solution. Internal audit can seek evidence that vendor insolvency risk is being sufficiently managed.

Questions and considerations for internal audit

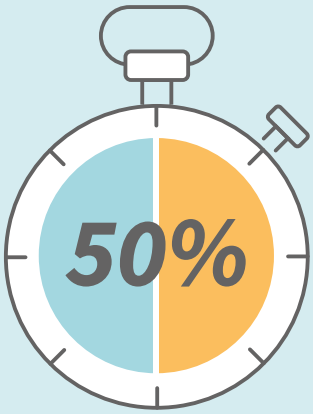
- How is the company's supply chain and outsourcing risk determined and have risk assessments been updated post pandemic? Has a recent supply chain risk assessment accounted for supplier concentration risks and dependencies?
- How has any volatility as a result of the GCP impacted the supply chain and what has the business done to mitigate these effects in future?
- What is the rationale for the current supply chain/outsourcing model? Do the benefits still outweigh the costs and potential risks? Is there reason to increase inventory to cushion against supply shocks or re-shore business functions, for example?
- Do the cost savings of sourcing materials and parts from overseas outweigh the operational risks this presents? Has this cost-benefit analysis been carried out by the business recently?
- Have alternative suppliers of key materials and components been identified and put on standby?
- Does the business have short-term contingency plans for outsourced business functions going offline? Has the business considered whether having core functions overseas still makes sense from a risk perspective?
- Does the organisation have enough insight into the governance and controls within contracted suppliers and their ability to manage their liquidity and own supplier risk? Is there a right to audit?
- Do contracts have a balanced contractual relationship between the organisation and service provider and include regular renegotiations and exit provisions to allow the company to update its supplier base?

"Certain people like trading floor staff or treasury workers do not work from home under normal circumstances. Allowing them to work from home requires far more security measures and protocols because those are the areas with higher potential and higher impact from fraud and cyber breaches. For that reason traditionally there has been a view that there's no way that we can have trading floor and treasury people working remotely. Risk management need to first accept the measures that it takes to make that possible. And then we need audit involved and looking at these high-risk areas and the robustness of the measures that have been put in place to accommodate those changes."

Audit Committee Chair, multinational Dutch bank, the Netherlands



*One in four (25%) CAEs say that **'Bribery, fraud and other financial crime'** was one of the **top five risks** currently faced by their organisation.*



*say that 'Bribery, fraud and other financial crime' is one of the **top five risk** areas on which internal audit is spending the **most time and effort**.*

"Old-fashioned concepts like the segregation of duties are a little more difficult to achieve or there are more process workarounds that people can take more easily in a remote working environment. Things just happen differently and in ways that you would not expect under normal circumstances. Certain high-risk activities lack oversight and the normal control environment around them."

Audit Committee Chair, global healthcare insurer, UK

Fraud and the exploitation of operational and economic disruption

Two forces are putting businesses at heightened risk of financial crimes. First, there is an increase in ploys to capitalise on the crisis by fraudsters using sophisticated digital techniques. Second, the efficacy of controls is likely to have been weakened in recent months. For instance, it may be more difficult to spot suspicious transactions or dubious customers given the disruption to operations and fraud monitoring activity.

The recessionary environment and increased pressure on management to remain sufficiently profitable may also raise the temptation to do business with parties the organisation would be better off not engaging with. With the main objective being to keep the business going, this same pressure may also diminish the attention paid to due diligence procedures and processes, while resources invested in compliance and conduct oversight may be reduced as priorities shift.

One in four (25%) CAEs say that *Bribery, fraud and other financial crime* was one of the top five risks currently faced by their organisation, a notable 19% increase on the 21% who said the same a year prior. Meanwhile, a full 50% say that it is one of the top five risk areas on which internal audit is spending the most time and effort, a more than 56% increase on the 32% of CAEs who said the same a year ago. There is certainly cause for paying close scrutiny to financial crime in the current climate.

The EBA warned on 31 March 2020 that new techniques and channels of laundering money are likely to emerge in the wake of the pandemic. The authority singled out international trade as a potential risk area, saying that banks processing payments linked to trade transactions should take additional measures to establish whether unexpected flows – particularly linked to customers or regions badly affected by coronavirus – are of legitimate origin.

Anti-money laundering continues to be a pressure point for banks, especially as criminals seek to exploit ongoing disruption, as firms operate remotely and then transition back into the office as the coronavirus contagion rate falls to more manageable levels. The Financial Action Task Force (FATF) has warned lenders about illicit finance crime related to coronavirus, specifically money laundering and terrorist financing.[10] A major challenge for banks has been, with offices closed, it takes time to update processes and put in controls to mitigate new risks and ensure the continuing ability to detect suspicious customers and transactions. FATF highlighted the benefit of flexible risk-based approaches in the fight against money laundering, balanced with the need to remain alert with regard to new and existing illicit finance risks which include imposter, investment and product scams, as well as insider trading related to the crisis.

Regulators have recognised that firms may need to re-prioritise or reasonably delay some activities such as ongoing customer due diligence reviews, but that they should not adjust their risk appetites or suspend transaction monitoring activities. Any reduction or delay in due diligence follow-up activity should be appropriately risk-based, with attention focused on higher-risk transactions and customers. There should also be a plan in place to return to business as usual whenever possible.

Complicating matters, amid the GCP banks have had to balance administering relief loans to businesses, and making these processes as

10. COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses | Financial Action Task Force

*"**Anti-money laundering** continues to be a pressure point for banks, especially as criminals seek to exploit ongoing disruption, as firms operate remotely and then transition back into the office as the coronavirus contagion rate falls to more manageable levels."*

smooth and as timely as possible, with the potential for these loans to be abused by criminals. Some due diligence measures such as customer verification have had to be simplified under government assistance programmes to make funds available as quickly as possible. In some cases, this may require ongoing due diligence or reviewing loans if risks are detected at a later stage.

An internal audit perspective

Internal audit can help management and the board gain an up-to-date view of the business's fraud and money laundering risk by identifying the potential effects of any recent disruption to the business's operations. The control framework and monitoring of potential criminal activity may have become weakened due to reduced headcounts and remote working, leaving gaps in fraud detection and creating opportunities for malicious customers and staff. Attention should also be paid to the company's ability to keep up with the increasing sophistication of fraudsters' use of advanced digital techniques.

Internal audit can check that the organisation is aware of hotspots, such as those highlighted by regulators including trade transactions and the misuse and misappropriation of domestic and international financial aid and emergency funding, for example. The third line should think about how customer due diligence measures may have softened and how criminals may have found ways to bypass such measures. Crucially, any due diligence or monitoring activities that were de-prioritised to ensure the operational agility of the business mid-crisis will need to brought back in line with previous standards when the firm returns its operating status to some degree of normality. The business should also be able to provide evidence that it has followed an intelligent risk-based approach to any adaptive measures it has taken.

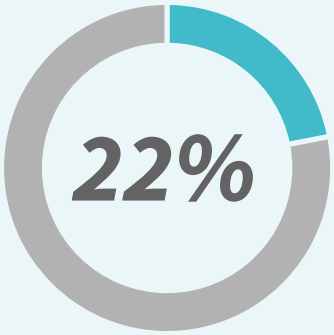
As the organisation contends with the pressures of a potential recessionary environment in 2021, internal audit should think about whether this has increased the potential for bribery as a means for securing vital contracts and meeting financial targets. Economic challenges may have averted the business's attention away from financial crime risks as it seeks to be as competitive as possible and ensure its survival in a challenging trading environment. Internal audit should therefore consider how both operational and economic disruption is impacting upon risks related to financial crime perpetrated by insiders and criminals outside of the organisation.

Questions and considerations for internal audit

- Do the highest ethical standards continue to be promoted from the top down throughout the organisation? Is senior management leading by example?
- Has the state of the economy and its impact on the business caused a weakening of bribery risk mitigation efforts as the organisation shifts its focus and priorities to remaining profitable?
- How has any destabilisation of the business operations impacted the organisation's ability to manage fraud and money laundering risks? In what ways?
- Are the established controls for preventing and recognising fraudulent behaviour and financial crime still in place and working? These may include hard controls such as transaction monitoring and customer due diligence through to softer controls such as staff awareness and compliance training.
- Are these controls updated to cope with the increase of sophisticated digital techniques used to commit fraud and other financial crime?
- Has the business taken a sufficiently risk-based approach to customer due diligence? What was changed in response to the pandemic, was this risk-assessed and documented and have any measures that were relaxed been restored?
- Has the monitoring and follow-up of suspicious transactions changed in any way? Has full monitoring capacity since been reinstated or is there a plan to do so?

"In the sense of opportunity, something that should be on the company's agenda is everything around the circular economy, sustainability and how do we make sure that we manage our ecological footprint. We consistently have a position on the Dow Jones Sustainability Index and we produce sustainability annual reports and we're active and explicit supporters of the UN's goals. But are our businesses sufficiently working on products that are entirely circular, that are taken from the market and redeployed? I think there is more work to be done. That is to a large extent a strategic opportunity. But it won't take long before that becomes a requirement of doing business in the very first place."

CAE, Euronext-listed health technology company, the Netherlands



*of CAEs cited **'Climate change and environmental sustainability'** as one of their company's **top five risks**, a more than 50% increase on the 14% who said the same in last year's Risk in Focus survey.*

Changes forced by the pandemic have offered a glimpse of what a cleaner and quieter future might look like. Nevertheless, dramatic falls in emissions will have little to no impact on the level of atmospheric CO_2, which remains at its highest level for two million years.

Source: Met Office

"The company is not going to survive in the long-term if we don't do things the right way. We have to be sustainable. For internal audit, we have audited some of the sustainability indicators in the past and the processes that are affected by the changes in sustainability including transport, purchasing of merchandise, research activity etc. So we know very well the processes that will be affected by the company's new sustainability commitments."

CAE, IBEX 35 retailer, Spain

Climate change: the next crisis?

Internal audit increasingly recognises the challenge and risks companies face in achieving their sustainability goals and minimising their contribution to climate change. Nearly one-quarter (22%) of CAEs cited *Climate change and environmental sustainability* as one of their company's top five risks, a more than 50% increase on the 14% who said the same in last year's Risk in Focus survey. This direction of travel is expected to continue, with a full 41% of CAEs anticipating it being a top five risk in three years' time. No other risk area is expected to gain more in priority over this period.

The pandemic will cause the largest ever annual drop in carbon emissions in history in absolute terms and since World War II in relative terms, a consequence of reduced industrial activity, air travel, work commuting and energy consumption through much of 2020. Satellite data compiled by the European Space Agency and NASA showed NO_X levels falling by as much as half in some major European industrial centres during lockdown.[11] Changes forced by the pandemic have offered a glimpse of what a cleaner and quieter future might look like. Nevertheless, dramatic falls in emissions will have little to no impact on the level of atmospheric CO_2, which remains at its highest level for two million years.[12]

If anything, 2020 has exposed the magnitude of the climate challenge that lies ahead and the need for big, lasting change in order for the European Union to meet its net-zero emissions target by 2050. The hoped-for economic recovery in 2021 could lead to a surge in carbon emissions. As the urgency of the coronavirus crisis abates, companies will have to balance their commercial imperatives with a new focus on their commitment to carbon neutrality and the sustainability of their operations and strategies for the future.

In January 2020 Larry Fink, CEO of BlackRock, the world's largest asset management firm, heralded the "edge of a fundamental reshaping of finance" and said that, "In the near future – and sooner than most anticipate – there will be a significant reallocation of capital." Companies coming out of the recession without a clear plan and commitment to environmental sustainability risk higher long-term financing costs or being priced out of capital markets entirely as investors increasingly scrutinise companies' plans to minimise climate risk.

But climate and sustainability risk is not only a matter of financing costs. Extreme weather and environmental shifts are reshaping supply chains. From a demand perspective, customers are also striving to decarbonise their consumption, gravitating to companies that are putting sustainability at the heart of their mission. The global coronavirus pandemic may heighten people's awareness of the human impact on the world and what they can do to minimise the damage caused by their behaviour by adjusting their consumption habits. Therefore, there is a commercial imperative for companies to deliver sustainable products and services that are aligned with changing consumer values.

In December 2019 the EU agreed on a landmark "Green Deal" to make its economy and society climate neutral by 2050. The EC has proposed the European Climate Law to legally enshrine this

11. Air pollution sharply falls worldwide on COVID-19 lockdowns | Balkan Green Energy News
12. Coronavirus will impact the atmospheric CO_2 record – but not enough to slow global heating | Met Office

policy ambition. Since then the pandemic has wrought huge economic damage and prompted governments and central banks to deliver their most ambitious stimulus packages in history.

A consortium of 180 researchers, non-governmental organisations, ministers from 10 European countries and business leaders including the Chief Executives of Ikea, L'Oréal and Unilever wrote an open letter stating that Europe's economic recovery from the coronavirus crisis should go hand in hand with the EU's climate objectives via a raft of green stimulus packages. Research shows that projects which cut greenhouse gas emissions as well as stimulating economic growth deliver higher returns on government spending than conventional stimulus spending, over both the short and long-term.[13] Recognising the need to make Europe's recovery green and compatible with its democratic principles, the EU agreed a landmark €750bn stimulus in July 2020 that will be distributed between member states with oversight from the EC; 30% of the recovery fund, or €225bn, will be used for climate-related purposes such as greener transport, cleaner industry and energy and renovated homes. This is not to mention similar allocations in future EU budgets. It is possible, then, that 2020-2021 will mark a watershed moment when European governments and businesses led the charge by taking decisive action on the climate crisis.

An internal audit perspective

There is a disconnect between the urgency and severity of climate change risk – as recognised by businesses, their executive teams, boards and CAEs - and the time and resources spent auditing this area. Only 6% of audit chiefs say that *Climate change and environmental sustainability* is one of the top five risk areas on which internal audit spends most of its time and effort, though this rises to 23% who say this will be a prime focus three years from now. This reflects findings from the 2020 North American Pulse of Internal Auditors, which found that 90% of audit leaders do not plan to devote any part of their annual audit plan to sustainability.

*"How well prepared are we for the **climate crisis** and what are we doing to ensure we are turning it to our advantage rather than contributing to it?"*

This large disconnect may be explained by the perceived limited scope for audit at this time given the relative immaturity of the risk management around climate and sustainability risk. It may also be explained by the choice to reduce overlaps with the independent review of sustainability reports carried out by external auditors.

However, internal audit has much to offer here. One of the biggest lessons businesses can take from the coronavirus crisis is the extent to which they were prepared. Now is the time for organisations to be accelerating their response to the present and increasing risks posed by the mounting climate change crisis. The GCP showed that companies were caught by surprise by a global pandemic. There will be no excuses for being similarly unprepared for climate change risks, for which companies have been given fair warning.

Therefore, internal audit can help companies to answer the question, how well prepared are we for the climate crisis and what are we doing to ensure we are turning it to our advantage rather than contributing to it? This is not simply a case of assessing the business has crisis contingency measures in place, for example for extreme weather events taking suppliers offline. It is a matter of the longevity of the business strategy and whether climate change and sustainability are integrated into the company's objectives. Internal audit can assess the executive decision-making processes for evidence that these issues are gaining enough attention, to give its view on whether this risk is being managed at the most fundamental strategic level.

13. Will COVID-19 fiscal recovery packages accelerate or retard progress on climate change? | Oxford Smith School of Enterprise and Environment

Internal audit can examine this area at an operational level too, given its deep view into the processes that are related to and impacted by sustainability, from materials sourcing to transport and logistics and waste management. The third line can help senior management to identify the first steps that can be taken to close any sustainability gaps and improve inefficiencies that will reduce the company's carbon footprint and environmental impact.

Boards will need to know that the business is living up to its environmental claims and investigative audit work can show how clean and green operations are in reality. This can include reviewing governance around environmental data, sense-checking the reliability of carbon emissions reporting and independently assessing the methodologies and data inputs used at both the ground-level operations and executive-level strategy making to spot any gaps and possible errors.

There is also a compliance dimension to climate change and sustainability and the legally binding obligations are set to increase. In 2020 the EC launched public consultations as it works to improve upon the Non-Financial Reporting Directive. Internal audit can provide assurance that the business has factored in any changes required by the EU when the new-look directive is brought in. Among the limitations of existing non-financial reporting are the inclusion of unquantifiable data that is inconsistent between companies. The third line can examine whether the company delivers measurable and standardised sustainability key performance indicators (KPIs) that achieve greater transparency for investors and the public.

Questions and considerations for internal audit

- Have climate change and sustainability risks been identified by senior management and factored into the strategy-making process of the business? Are these risks periodically reviewed?
- If the business takes no action, is its strategic relevance under threat from decarbonisation goals and increasing consumer awareness of environmental issues? What is being done about that risk?
- Is senior management sufficiently aware of the commercial opportunities available to it in leading the charge on climate change e.g. disrupting the market, winning new customers, cutting financing costs?
- Are climate change, environmental and sustainability risks factored into the supply chain management processes along with human rights and ethics?
- Does the business have the appropriate culture required to become a green company and fulfil its sustainability ambitions? Is there buy-in at all levels of the company to achieve these goals?
- Does senior management have incentives linked to tackling climate change or are bonuses counterproductive to the sustainability goals?
- Who in the business is accountable for climate risk? Is there a Chief Sustainability Officer, or plans to hire one, or has the decision been taken to leave that accountability with the Chief Executive? Is there a clear rationale for that decision?
- Is the third line's 360-degree view of the business being applied to help it mitigate its sustainability risks?
- Is the compliance function aware of all existing and forthcoming environmental laws and regulations that apply to the business in the various jurisdictions in which it is present?
- Does the company have clearly articulated sustainability goals? How do they compare with its peer group companies?
- Have the goals and objectives been translated into internal management processes and controls, including KPIs that indicate progress against the objectives?
- How does the company measure and report its progress in reaching its sustainability goals and reducing its environmental impact? Should internal audit review the reliability of these reports?

Sources

1. Coronavirus pandemic: Tracking the global outbreak | BBC

   https://www.bbc.co.uk/news/world-51235105

2. The State of Data Loss Prevention 2020 | Tessian

   https://www.tessian.com/research/the-state-of-data-loss-prevention-2020/

3. CFO Actions in Response to COVID-19 | Gartner

   https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

4. Corporate Longevity Forecast: Creative Destruction is Accelerating | Innosight

   https://www.innosight.com/insight/creative-destruction/

5. Why crises call for innovation, not hibernation | Rainmaking

   https://discover.rainmaking.io/hubfs/Why%20crises%20call%20for%20innovation.pdf

6. 100 Stats On Digital Transformation And Customer Experience | Forbes

   https://www.forbes.com/sites/blakemorgan/2019/12/16/100-stats-on-digital-transformation-and-customer-experience/#7124f5e93bf3

7. 77% of organizations are planning for a second wave of Covid-19 infections | I4CP Survey

   https://www.i4cp.com/coronavirus/i4cp-survey-77-of-organizations-are-planning-for-a-second-wave-of-covid-19-infections

8. Johnson warned by business on 'hugely damaging' no-deal Brexit | Financial Times

   https://www.ft.com/content/e4da78ae-a428-4466-9721-d3841cc0e005

9. On the link between US pay and productivity | VOX, CEPR Policy Portal

   https://voxeu.org/article/link-between-us-pay-and-productivity

10. COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses | Financial Action Task Force

    https://www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html

11. Air pollution sharply falls worldwide on COVID-19 lockdowns | Balkan Green Energy News

    https://balkangreenenergynews.com/air-pollution-sharply-falls-worldwide-on-covid-19-lockdowns/

12. Coronavirus will impact the atmospheric CO2 record – but not enough to slow global heating | Met Office

    https://blog.metoffice.gov.uk/2020/05/07/coronavirus-will-impact-the-atmospheric-co2-record-but-not-enough-to-slow-global-heating/

13. Will COVID-19 fiscal recovery packages accelerate or retard progress on climate change? | Oxford Smith School of Enterprise and Environment

    https://www.smithschool.ox.ac.uk/publications/wpapers/workingpaper20-02.pdf

Über das DIIR – Deutsches Institut für Interne Revision e.V.

Das DIIR – Deutsches Institut für Interne Revision e.V. wurde 1958 als gemeinnützige Organisation mit Sitz in Frankfurt am Main gegründet. Hauptanliegen ist der ständige nationale und internationale Erfahrungsaustausch und die Weiterentwicklung in allen Bereichen der Internen Revision. Heute zählt das Institut 3.000 Firmen und Einzelmitglieder aus allen Sektoren der Wirtschaft und aus der Verwaltung. Das DIIR unterstützt die in der Internen Revision tätigen Fach- bzw. Führungskräfte u. a. mit der Bereitstellung von Fachinformationen und durch um fassende Aus- und Weiterbildungsangebote. Weitere Ziele und Aufgaben sind die wissenschaftliche Forschung sowie die Weiterentwicklung von Grundsätzen und Methoden der Internen Revision.

DIIR - Deutsches Institut für Interne Revision e.V.
Theodor-Heuss-Allee 108
60486 Frankfurt am Main

email **info@diir.de**
www.diir.de

DIIR Deutsches Institut für Interne Revision e.V.