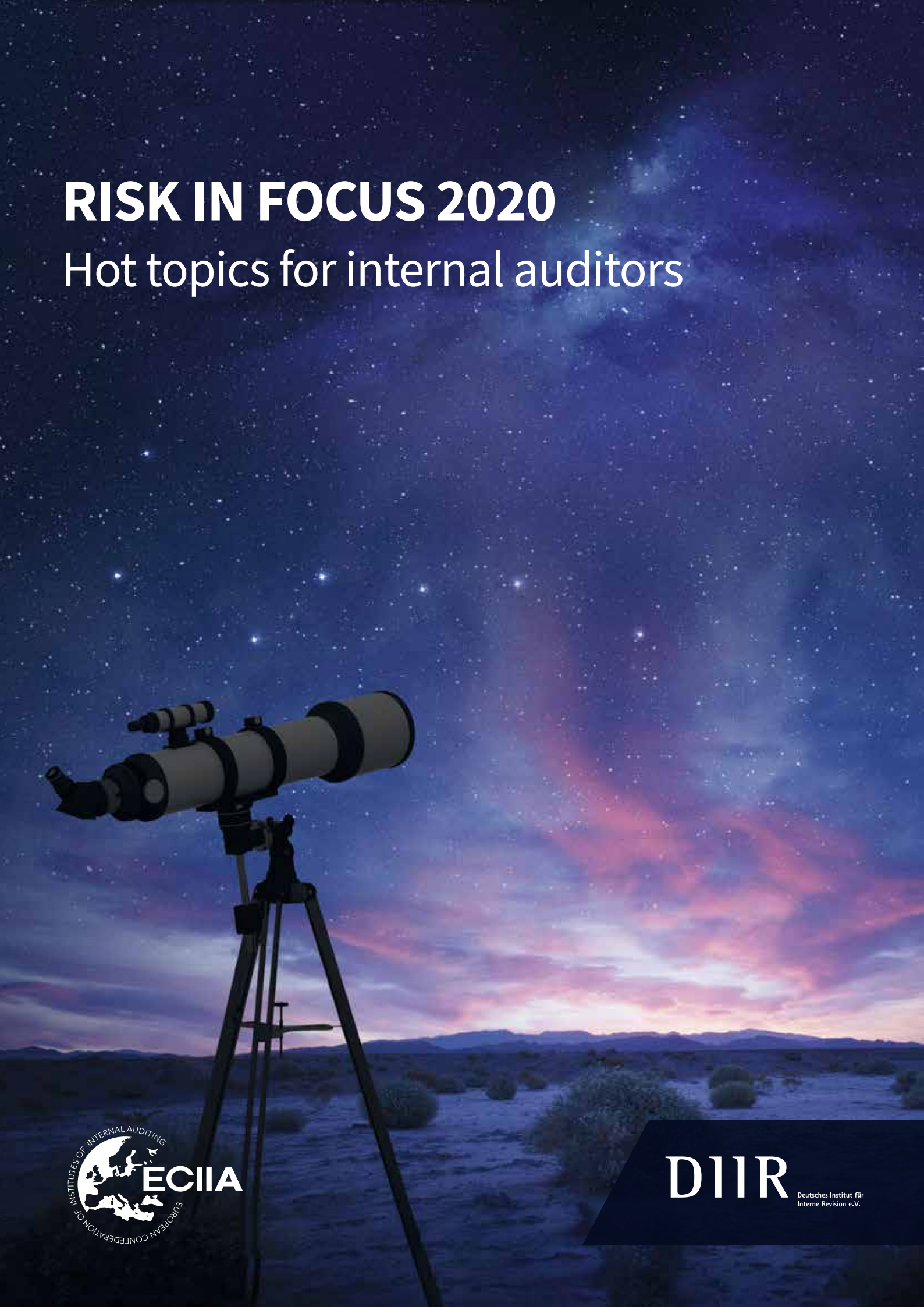
RISK IN FOCUS 2020

Hot topics for internal auditors



ECIIA
EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING

DIIR
Deutsches Institut für Interne Revision e.V.

Risk in Focus 2020 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 Spain, IIA Sweden, Institut Français De L'audit Et Du Contrôle Interne (IFACI) and the Italian Association of Internal Auditors.

Contents

Foreword

Welcome to Risk in Focus 2020. For four years now this report has sought to shed light on key business risks as identified by Chief Audit Executives (CAEs) across Europe.

This ongoing research study continues to go from strength to strength. When it was launched in 2016 it was a collaboration between three institutes of internal auditors. This latest edition is the result of a working partnership between no fewer than eight European institutes of internal auditors and draws upon qualitative interviews with 46 CAEs in Belgium, France, Germany, Italy, the Netherlands, Spain, Sweden and the UK & Ireland working in a range of industries.

In the previous edition we introduced a quantitative survey to the report for the first time. The report is becoming a more data-rich offering, with a full 528 responses to this year's CAE survey compared with 311 for Risk in Focus 2019. This is a resounding endorsement of our engagement with CAEs in the field, providing vital day-to-day assurance, advice and insight to their organisations.

The European institutes of internal auditors would like to thank all interviewees and survey respondents who contributed to the making of this year's report. We are grateful for your professional input and insights, without which it would not be possible to produce this research study.

September 2019

Introduction

This report is an annual barometer of what CAEs perceive as their organisations' risk priorities and what is preoccupying their thinking as they prepare their forthcoming audit plans. We see Risk in Focus as a vital point of reference for the internal audit profession, not just in Europe where the annual surveys and interviews are carried out, but worldwide.

Risk is not solely the domain of internal audit, of course. Therefore, while the report may serve as a valuable document for CAEs and internal auditors in helping to shape and challenge their own audit plans for 2020, we hope it serves as an important benchmarking and consultation tool for a wide stakeholder group. Indeed, this report is as relevant for boards and audit committees as it is for risk managers and other assurance providers.

Inevitably risk assurance is an idiosyncratic exercise that meets the specific needs of an organisation. Rotational audits should now be a thing of the past, internal audit instead striving to be risk based and agile, responding to and pre-empting emerging risks and stepping into its trusted advisor role whenever called upon. For this reason, the following topics should serve as a resource for CAEs to inform, challenge and sense-check their next audit plan, and provide context for discussions with senior management and the board.

You can find a rundown of this year's and previous years' hot topics in the table below to get a sense of how they have developed over time.

2018	2019	2020
1. GDPR and the data protection challenge	1. Cybersecurity: IT governance & third parties	1. Cybersecurity & data privacy: rising expectations of internal audit
2. Cybersecurity: a path to maturity	2. Data protection & strategies in a post-GDPR world	2. The increasing regulatory burden
3. Regulatory complexity and uncertainty	3. Digitalisation, automation & AI: technology adoption risks	3. Digitalisation & business model disruption
4. Pace of innovation	4. Sustainability: the environment & social ethics	4. Looking beyond third parties
5. Political uncertainty: Brexit and other unknowns	5. Anti-bribery & anti-corruption compliance	5. Business resilience, brand value & reputation
6. Vendor risk and third party assurance	6. Communication risk: protecting brand & reputation	6. Financial risks: from low returns to rising debt
7. The culture conundrum	7. Workplace culture: discrimination & staff inequality	7. Geopolitical instability & the macroeconomy
8. Workforces: planning for the future	8. A new era of trade: protectionism & sanctions	8. Human capital: the organisation of the future
9. Evolving the internal audit function	9. Risk governance & controls: adapting to change	9. Governance, ethics & culture: the exemplary organisation
	10. Auditing the right risks: taking a genuinely risk-based approach	10. Climate change: risk vs opportunity

Cyber and data security has firmly established itself as a top-of-mind issue for the majority of audit executives. Formerly a business continuity, financial and reputational concern, cybersecurity has now also taken on a compliance dimension as companies continue to make efforts to stay on the right side of the General Data Protection Regulations (GDPR).

Once again, regulatory matters remain a chief concern for a majority of CAEs, who stress the need to remain compliant with antitrust, anti-bribery and corruption, anti-money laundering laws and sanctions. This coincides with authorities in various jurisdictions, including within Europe, showing a willingness to issue record fines as a deterrent.

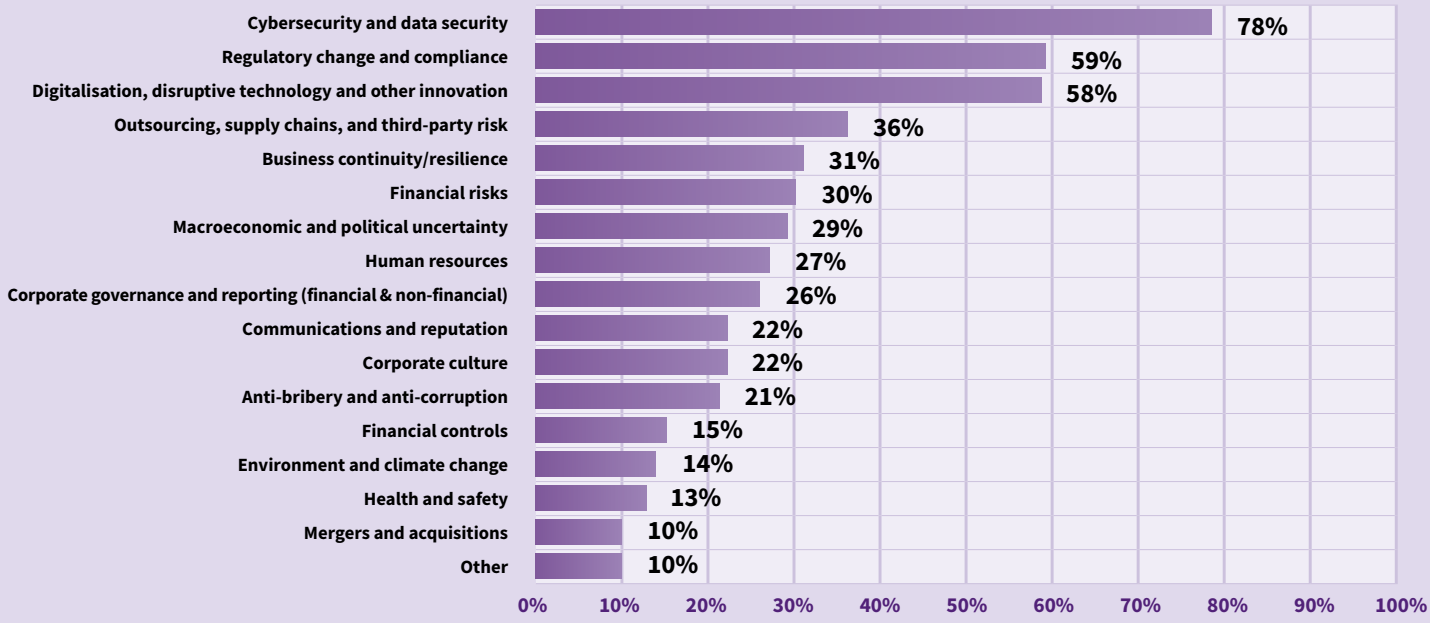
There is also a persistent concern about the effects of digitalisation, which is of course a clear source of both risk and business opportunity. As established companies face heavy competition and sectors undergo rapid evolution and convergence, CAEs are rightly questioning what digitalisation means for the future of their organisations' business models.

Political uncertainty is showing signs of gaining prominence when compared with the results from 12 months ago. This might be expected since the weaponisation of trade policy for economic and diplomatic ends has never before dominated the news flow like it has in recent months. In this sense, the economy and politics can be viewed through the same lens, each closely impacting upon the other.

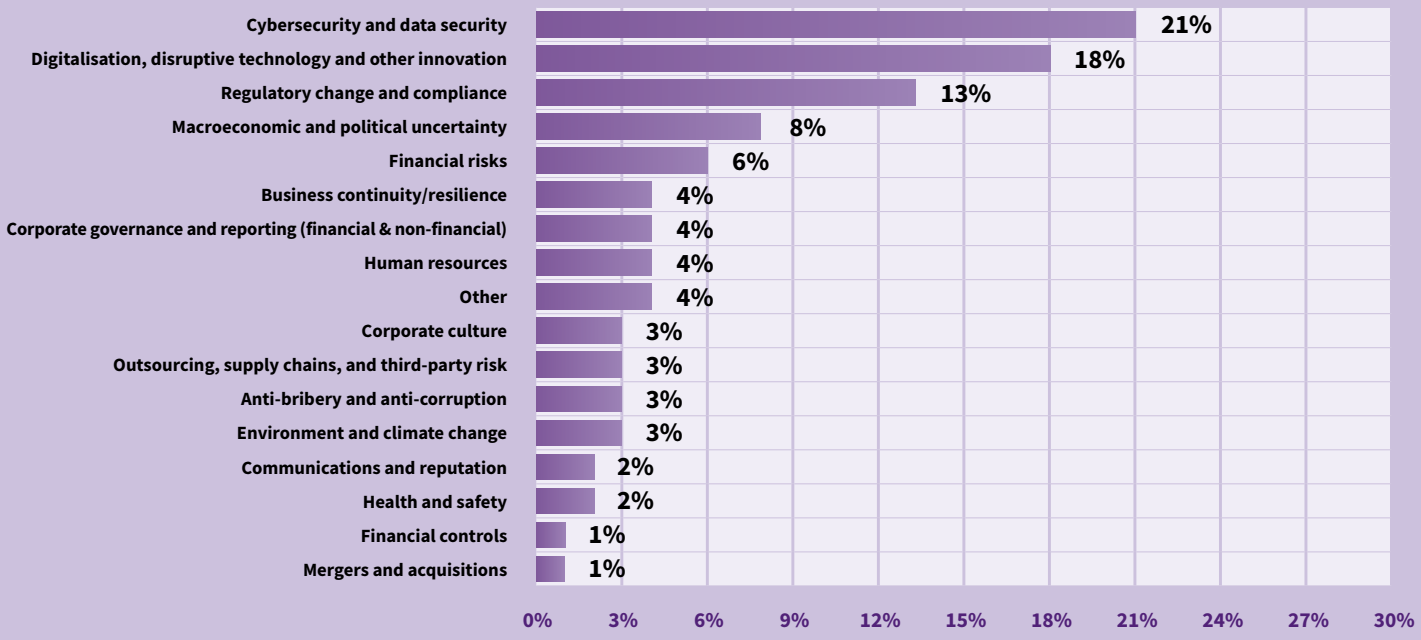
Perhaps most striking of all, we see that climate change and the environment is rising up the internal audit agenda. While still only seen as a top five risk by a minority of CAEs, there is a notable annual increase in the number of audit executives who say this is front of mind and a significant risk to their organisations. As corporations begin to grasp the nettle on climate change and their impacts on the environment, we see internal audit as a valuable ally to the board and senior management in assessing the management of risks and opportunities related to a topic that defines our times.

Learn why this year's topics have been shortlisted by reading on. Once again, we hope you find value in this fourth edition of Risk in Focus.

What are the top five risks to your organisation?



What is the single biggest risk to your organisation?



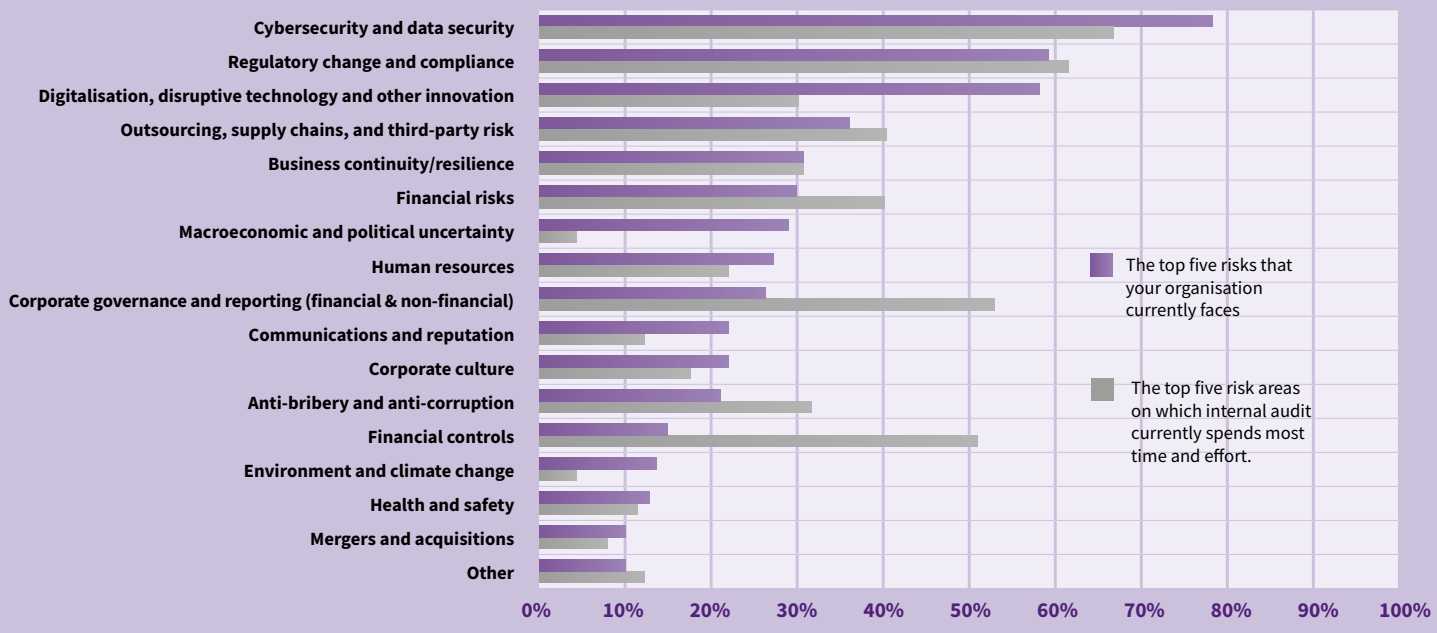
The risk-audit gap: risk priorities vs time spent auditing

In our survey of European CAEs, we not only asked what they saw as the top five risks their organisations face, but also the top five risk areas on which their internal audit functions spend the most time and effort. We have contrasted these results in the graph below. A positive takeaway from this is that there are few risks that are mismatched (i.e. with a differential of more than ten percentage points after rounding). That is to say, higher priority risks are typically given more audit time and focus and vice versa.

There are, however, some exceptions. 'Financial controls' are seen as a top five risk by only 15% of CAEs, yet 51% say this is one of the top five risk areas on which internal audit spends the most time and effort; similarly, 'Corporate governance and reporting (financial & non-financial)' is a top five risk for 26% of the cohort but 53% say this is where most time is spent auditing. This indicates that too much time is being spent on these 'traditional' audit domains relative to their level of priority.

Conversely, a full 29% cite 'Macroeconomic and political uncertainty' as a priority risk to their organisation, but only 4% say this is where most audit resources are spent. We believe this is partly a symptom of the external nature of this risk type. As we explain in the report, the economy and politics are not internal corporate risks, but outside conditions that have a knock-on effect on other risks, whether financial, operational, strategic or otherwise. Again, we see that 58% of CAEs report 'Digitalisation, disruptive technology and other innovation' as a top five risk, but just over half (30%) of this proportion of CAEs say it is in the top five risk areas that are audited the most. Unlike economic and political forces, digitalisation is very much an internal process. This indicates that internal audit should be allocating more time to auditing the risks (and opportunities) associated with their companies becoming digital-first and their ability to innovate, disrupt and, ultimately, lead their sectors. Resources permitting, CAEs should analyse any such gaps and discuss them with the board.

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



Top risks: the direction of travel

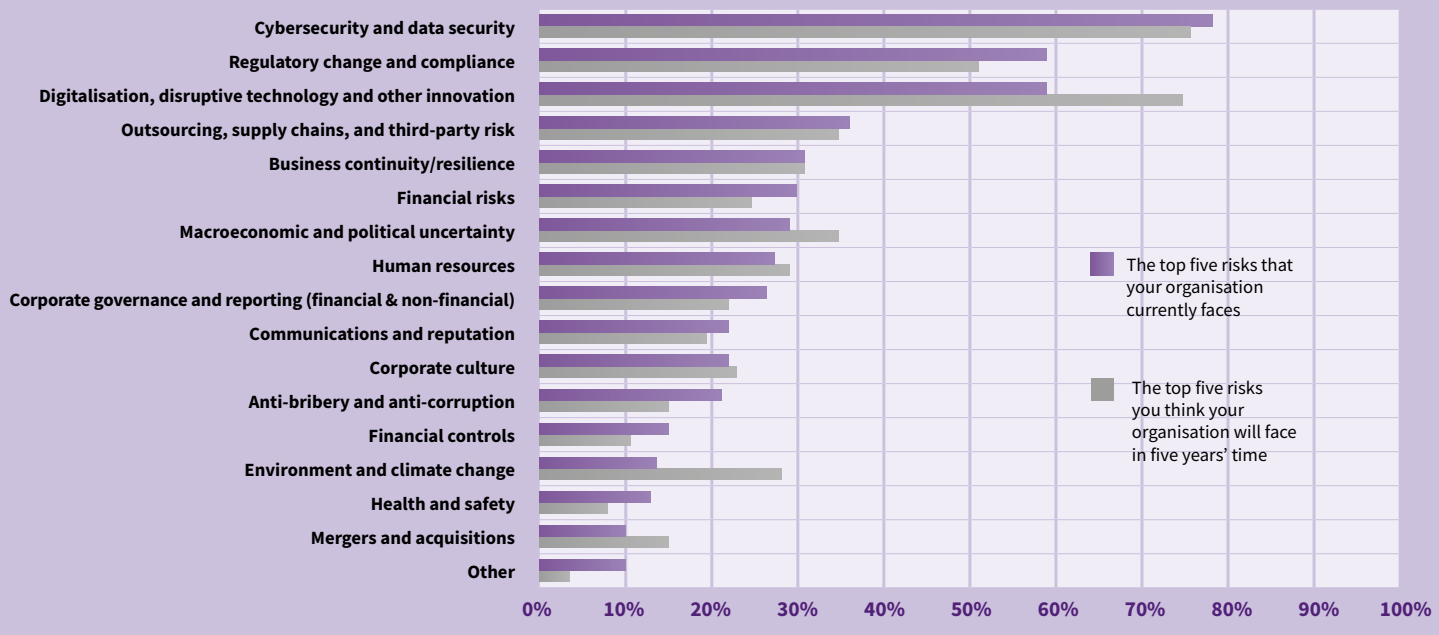
Our survey findings also show the way in which CAEs anticipate the risk profiles of their organisations developing over time. For the most part, there is a consistency between what are considered the top five risks today and what the priority risks are expected to be five years from now. There are two notable outliers, however, both of which have a differential rate of more than ten percentage points.

The first of these is 'Environment and climate change', which 14% of CAEs said is currently a priority risk their organisation faces; this surges to 28% of CAEs who anticipate this being a top five risk by 2025. This clearly demonstrates the rising prominence of this issue and suggests that internal audit should now be preparing itself to deliver relevant assurance on the risks and opportunities related to climate change.

Secondly, 'Digitalisation, disruptive technology and other innovation' is today a top five risk in the eyes of 58% of CAEs, rising to 75% who foresee it being a priority risk in five years' time. This would put digitalisation on a roughly even footing with 'Cybersecurity and data security' (76%) by 2025.

The profession should take heed of these findings. Forward-looking CAEs are advised to reflect on what these findings mean for their own organisations and audit teams. Will your function be ready and able to deliver relevant assurance over the coming years in these two separate but related domains?

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



Cybersecurity & data privacy: rising expectations of internal audit

A string of cybersecurity incidents kept the topic on the top of the corporate agenda in 2018 and 2019. Notable examples include the discovery of the Spectre and Meltdown vulnerabilities affecting virtually all Intel processing chips, which have had to be patched enmasse, the exposure of 50 million Facebook users' personal information and a "mega breach" of hotel chain Marriott that compromised the details of 500 million customers.

Cybersecurity is undoubtedly the perennial risk of the modern era; it should therefore come as no surprise that year in, year out it features prominently in the minds of CAEs and in their audit plans. We found that 78% of CAEs in the survey cohort for Risk in Focus 2020 cited 'Cybersecurity and data security' as one of the top five risks that their organisations face and 21% singled it out as the top risk, making it more widely referenced than any other risk area. Similarly, 78% of CAEs that were interviewed for this report anticipated including cybersecurity assessments in their forthcoming audit plans.

Already a well-established item on board agendas and in the minds of senior executives, there is no room for complacency in managing and mitigating cybersecurity/information security risk. Internal audit may have to dedicate time and resources to this area indefinitely given that it is a constantly moving target. Encouragingly, we see that 68% of CAEs report that cyber and data security is one of the top five risks on which internal audit currently spends most of its time and effort.

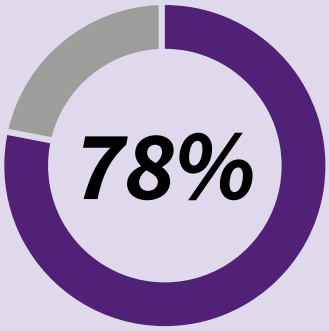
There is a need for organisations and their audit functions to remain diligent because 1) the methods by which actors attempt to breach their targets are constantly evolving and increasing in sophistication, and 2) organisations are not fixed or static entities — their so-called "perimeter" is fluid and continuously growing, as IT infrastructure migrates to the cloud, businesses move into new geographic markets and integrate merger and acquisition (M&A) targets and align their internal control systems, employers agree to "bring your own device" policies, and Internet of Things (IoT) and other digital capabilities are developed and expanded.

Regarding the sophistication of the threat (see 'Emerging cyber risk considerations' box-out on page 16), one emerging technique is for cyber criminals to compromise customer service chatbots. In our interviews with CAEs of customer-facing businesses, many report that one of the initiatives of their ongoing digitalisation/automation programmes has been to introduce such bots as a means for gaining cost efficiencies. We therefore recommend that any audit work, as part of an evaluation of the entire IT infrastructure, includes an assessment of how these chatbots are fortified against such breaches. Similarly, the security of cloud services and supply chains continues to be a focal point for internal audit and should remain a priority (see 'What's new?' box on page 16).

Internal audit, specifically IT/information security auditors, should keep up-to-date with new and emerging threats in order to challenge the first and second lines on how these specific risks are being managed. However, while new methods of attack are always being developed by adversaries, the majority of successful attacks exploit well-known and easily addressed vulnerabilities.

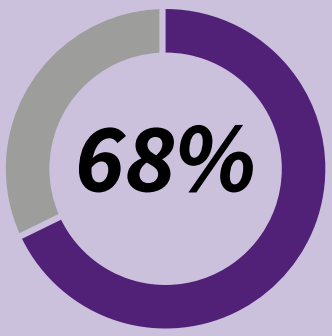
"Cybersecurity and data protection. I put all of that together because cybersecurity encompasses both aspects - protection against attacks but also protection against data leakage. For me that is about the customer experience and how they view our organisation. So it is not just a compliance risk but also a commercial risk and opportunity. It is something that can set us apart from our competitors."

CAE, German multinational insurer



*of CAEs in the survey cited '**Cybersecurity and data security**' as one of the top five risks that their organisations face.*

21% *singled it out as the top risk.*



*of CAEs report that '**Cybersecurity and data security**' is one of the top five risks on which internal audit currently spends most of its time and effort.*

"We have internal audit resources dedicated especially to information and cybersecurity audits. We follow two approaches. One is internal controls audits related to information security, which means auditing processes. Then we have third party cyber analysts that do intrusion tests. They carry out ethical hacking on a black-box basis. So, not knowing anything about the company, trying to attack the company using different vectors to see if the information security controls are working properly. The information security department has its own cyber analysts and they carry out the same kind of exercises, but it is not the same approach. They are doing it knowing the internal controls of the company. That is not as realistic as the ones we do in internal audit but is complementary to our activities."

CAE, Spanish multinational clothing company

One estimate suggests that 93% of breaches can be avoided by taking simple steps such as regularly updating software, blocking bogus emails and using email authentication, and training people to recognise phishing attacks. [1]

There is also the upside risk for businesses and their CAEs to consider. Cybersecurity should not only be seen as the potential for business continuity to be disrupted and data to be compromised, but an opportunity to deliver value. Those companies that are seen to be putting in place the best defences and that are able to respond to cyber breaches swiftly and effectively can build trust with customers and other stakeholders, which in turn creates shareholder value.

Cybersecurity and data protection converge

The topic of cybersecurity/information security risk is all the more pressing for the fact that the GDPR has just had its first anniversary. Authorities have begun to issue their first fines in a number of key European jurisdictions including France, Germany, Poland and Denmark, the most significant being a €50m penalty from the French data authority against Google for its covert collection of consumer data.

That GDPR fines totalled only €56m in their first year signals the tentative approach that regulators are taking. Authorities have so far exercised restraint, allowing time for the full force of the data privacy and protection rules to take effect. The potentially ruinous fines that can be imposed under GDPR have already prompted companies to change how they harvest personal data, as evidenced by the ubiquitous use of personal data notifications on websites' landing pages.

However, businesses cannot afford to be complacent as regulators are expected to bear their teeth in due course. The focus of authorities thus far may have been on data harvesting polices but a core component of GDPR is how secure businesses are as the guardians of personal data. Therefore, businesses should expect authorities to be increasingly willing to level fines against them for security breaches that expose personal data, as Germany's State Commissioner for Data Protection and Freedom of Information Baden-Wuerttemberg did against social media company Knuddels.de in November 2018, requiring it to pay €20,000 when 330,000 customers' data were compromised. There were an estimated 59,000 personal data breaches reported across Europe in the first eight months since the introduction of the GDPR, with 15,400, 12,600 and 10,600 breaches in the Netherlands, Germany and the UK respectively.[2] This suggests that a wave of security-related GDPR enforcement could be approaching.

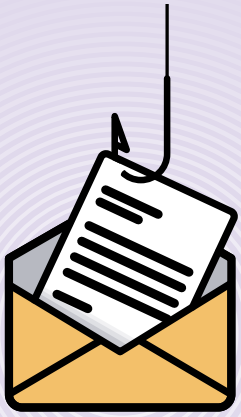
*"**Expectations** of internal audit are increasing and internal audit must rise to this challenge by **improving its skills**, capabilities and understanding of the threat."*

This represents an ongoing convergence between cybersecurity and data protection/privacy risk. Compliance and internal audit functions are having to expand their technical knowledge, while IT security teams must understand the compliance burden that comes with heavy and potentially punitive regulatory oversight. This will require closer collaboration between technical security experts on the one side, and compliance and assurance expertise on the other. GDPR compliance should be factored into all information security control modelling and IT assurance provision.

Internal audit: rising to the challenge

The persistence of the cyber threat — and the financial and reputational costs associated with periods of prolonged downtime, stolen data assets and negative press coverage — requires that internal audit remains vigilant and attentive. Even if the business's efforts to mitigate information security risk are highly mature, there is a need for the third line of defence to track these efforts, assess the ongoing evolution of the organisation's perimeter wall and stay on top of organisational and operational changes that impact upon the business's information security risk profile.

1. Online Trust Alliance's 2018 Cyber Incident & Breach Trends Report https://www.internetsociety.org/wp-content/uploads/2019/04/2018-cyber-incident-report.pdf
2. DLA Piper GDPR data breach survey: February 2019 https://www.dlapiper.com/en/uk/news/2019/02/dla-piper-gdpr-data-breach-survey/



“We have hired very good people into internal audit who are not really auditors but people who understand the cybersecurity risks and controls and then have become good cyber risk auditors. These people have a great understanding of where the greatest risks lie and where breaches will cause the biggest issues. The challenge now is these auditors have become so valuable for the bank that the second line of defence is trying to attract them away from the third line. We have also created an ethical hacking programme within internal audit, performed by professionals. We have to learn how to do that ourselves because those hacks have to be made without forewarning. It’s an interesting dual approach. We are still trying to fix the technical issues rather than the human, behavioural weaknesses at this stage.”

CAE, Spanish multinational banking group

93%

of breaches can be avoided by taking simple steps such as regularly updating software, blocking bogus emails and using email authentication, and training people to recognise phishing attacks.

Source: Online Trust Alliance

There were an estimated

59,000

personal data breaches reported across Europe in the first eight months since the introduction of the GDPR.

Source: DLA Piper

“We have almost doubled our IT auditor headcount in recent years in order to be able to thoroughly audit cybersecurity. There is a big cyber programme underway that we are also involved in. I’m a member of the oversight board for the cyber programme and we are constantly auditing that programme. The company uses external providers to carry out penetration testing on a regular basis. This is very specialised knowledge that you need for this exercise and we don’t believe it is efficient to do that either in-house or in the internal audit department.”

CAE, German transport group

Expectations of internal audit are increasing and internal audit must rise to this challenge by improving its skills, capabilities and understanding of the threat. The aforementioned effectiveness of low-level intrusions and easily mitigated attack vectors indicates that businesses are still falling short of expectations.

CAEs are therefore strongly advised to equip their departments with the necessary technical resources, either by sourcing temporary external expertise, recruiting permanent information security auditors, or taking an expertise-first approach by recruiting a technical security specialist who can then be trained to audit. Given the demand for such skills, hiring talent will be costly and this best-practice approach may not be feasible for smaller internal audit functions with limited funding. Nonetheless, the value of developing in-house information security audit resources should be clearly communicated to the board/audit committee.

In the majority of cases, third line penetration testing (i.e. pen testing that is independent from other internal hacking efforts by the first and second lines) is likely to be carried out on a co-sourced or outsourced basis. This is an intelligent approach: ethical hacking requires specialists with the requisite up-to-date expertise to replicate real-world attacks.

There is some debate over whether pen testing should be a task of the third line of defence at all. As an independent assurance provider, internal audit can verify the credibility of ethical hacking carried out by the first or second line of defence by reviewing the quality of the process, including partly re-performing their tests.

Bringing in outside expertise to test the organisation's defences is good practice, however cybersecurity assurance itself should, ideally, not be fully outsourced. In-house resources that understand the changing nature of the organisation's IT architecture, operations and internal security control environment, and the unique security challenges associated with those operations, will result in a greater breadth and depth of assurance.

Questions for internal audit

- **What evidence is there that the organisation has got the basics covered? These basics include malware detection, regular software updates, staff awareness training and access rights management.**
- **Is the organisation aware of the changing profile of its cyber risks given the changing nature of its operations, particularly as the company digitalises?**
- **Is the IT security function staying up-to-date with evolving information security threats?**
- **Does internal audit need to add staff and expertise in order to bolster its cyber/information security capabilities? Is the function over-reliant on third party service providers for cyber risk assurance?**
- **Does the internal audit function verify that penetration testing by the second line of defence is robust and comprehensive, including reperformance to obtain evidence of that?**
- **Additionally, is the third line of defence expected to provide independent hacking, in addition to reperforming first and second line pen testing? Is it doing this?**
- **To what extent is the organisation compliant with GDPR? What progress has been made in the last 12 months? Is the business fully aware of the company's obligations under GDPR and are the IT security function and the compliance function familiar with the security aspects of GDPR?**

Emerging cyber risk considerations

The most common cyber attack vectors involve financially motivated actors deploying ransomware, either by exploiting security holes in companies' networks or using phishing emails to harvest credentials and gain entry. Once breached, the company's files are encrypted, and ransom is demanded. A robust IT control environment can easily prevent these common attacks. Internal audit should nevertheless be aware of these increasingly significant information security risks.

Public cloud misconfigurations

Too often public cloud services such as Amazon Web Services (AWS) and Microsoft Azure are not configured correctly by the end user. Oversights can include insufficient access restrictions, using a single default password for the entire organisation and not utilising built-in logging features that show log-in activity, for monitoring suspicious activity.

AI as a tool and a threat

Machine learning techniques are beginning to be deployed in network intrusion detection and prevention, malware detection and secure user authentication. But cyber attacks are also expected to be increasingly AI-powered. Darktrace, an AI cyber defence company, predicts that in the future attacks will be autonomous and self-propagating, learning the target's network environment rather than relying on known or common vulnerabilities.

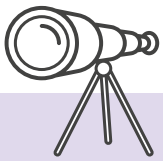
The increasing surface area

The increase in the number of third party relationships and expanding networks leaves an organisation exposed. The use of software as a service/cloud solutions, outsourcing partners and the addition of personal devices to networks all increase a company's entry points. In retail, an attacker could potentially access the Wi-Fi network in-store and, exploiting poor access rights management, reach the top of the organisation. Is the organisation fully aware of all of its vulnerabilities? Is the IT security team covering all bases?

Data theft to data manipulation

Having sensitive or personal data stolen is one of the most harmful consequences of a cyber attack. But there are growing examples of attackers interfering with data. Last year a disgruntled Tesla employee manipulated the company's manufacturing operating system in an attempt to disrupt its factory lines. Such subterfuge is expected to become increasingly common.

What's new?



'Cybersecurity: IT governance & third parties' was the theme of last year's cyber-focused hot topic, with CAEs then expressing particular concern over their organisations' expanding and fractured IT architecture, and migration to cloud platforms in particular. This should be no less of a concern in 2020 and into the future. Outsourcing IT to the cloud shows no signs of abating and the same security misconfigurations that are made internally are now being made in the cloud. While public cloud providers must be vigilant in how they protect their data centres and apps, responsibility for securing access to those services lies with organisations themselves.

This year, however, the emphasis of Risk in Focus is on the need for internal audit to step up to meet the assurance demands of organisations. Co-sourcing and outsourcing IT security audits is a valuable means for acquiring know-how, especially ethical hacking expertise. However, relying solely on third-party assurance is not enough. Given the financial and reputational costs of cyber breaches and data leaks, CAEs have a strong case to make with their boards and audit committees for increased budget allocations to address this interminable risk. Internal audit must also be cognisant of the new reality that data privacy and protection principles need to be embedded into cybersecurity controls.

The increasing regulatory burden

European regulation had a banner year in 2018. The GDPR went live, prompting businesses big and small across all sectors to evaluate how they collect, process and secure personal data, improve transparency with customers and put in place reporting procedures in the event of said data being leaked. In the financial services sector, institutions had to contend with the introduction of the Markets in Financial Instruments Directive II (MiFID II) and the Payment Services Directive 2 (PSD2), which overhauled the legal frameworks for investment services and online payments.

The challenges of complying with these specific requirements are part of a broader theme: the increasing regulatory burden that companies must shoulder in their day-to-day operations while achieving their growth strategies. One estimate shows that in 2008 there were 8,704 financial regulatory publications, changes and announcements globally; by 2016, this figure had surged to 52,506.[3]

Against this backdrop, more than half (59%) of our survey participants said that 'Regulatory change and compliance' is a top five risk to their organisation, putting it in second place behind cyber and data security, with over one in ten (13%) saying it is the single biggest risk. In keeping with these quantitative findings, more than half (52%) of the CAEs interviewed for Risk in Focus 2020 cited regulatory compliance as being one of their organisation's primary risks and an area that will require internal audit's attention in 2020.

Encouragingly, we also see that internal audit's attention and efforts to provide assurance around compliance are commensurate with its level of priority, a signal of strong risk-based internal audit in action; 61% of survey respondents said that 'Regulatory change and compliance' is a top five risk area on which it spends most of its time.

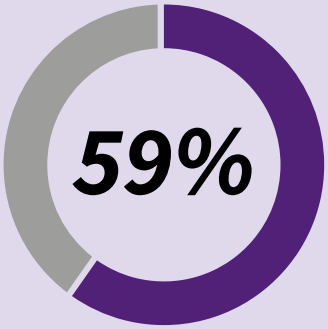
The "antis" and sanctions

Not only was 2018 a big year for the introduction of core pieces of regulation and legislation, but also for enforcement. Anti-money laundering (AML) fines in Europe, for example, reached a new record, after €775m was levied against ING for failing to spot money laundering. In the UK, Standard Chartered was ordered to pay £102m in penalties for AML breaches that included shortcomings in its counter-terrorism finance controls in the Middle East — the second-largest fine ever imposed by UK regulators for AML failures. This was part of a bigger case that cost the bank $947m in penalties to US authorities for violating sanctions against a number of countries, including Iran.

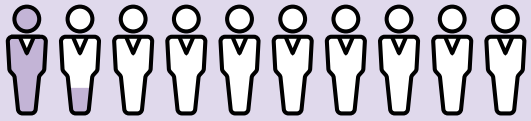
This heightened enforcement of AML rules in the financial-services sector comes as firms prepare for the forthcoming transposition of the Fifth EU Anti-Money Laundering Directive (5AMLD) into national laws by January 2020. In a clear example of the pressure that organisations are under to keep up with the pace of changing regulation, 5AMLD came into force only a year after its predecessor. The update expands the scope of the rules to include certain service providers such as electronic wallet firms, virtual currency exchange providers, and requires enhanced due diligence measures to monitor suspicious transactions involving high-risk countries such as Afghanistan, Iraq, Iran, Syria and the Democratic People's Republic of Korea, among other stipulations.

EU competition authorities have been similarly punitive. Google was hit with a record €4.3bn fine in 2018 for using its Android smartphone operating system to block handset manufacturers from installing competing search engines on their devices. Other sectors have also been the subject of strenuous enforcement. In May 2019, Anheuser-

3. Thomson Reuters: Cost of Compliance 2018 https://legal.thomsonreuters.com/content/dam/ewp-m/documents/legal/en/pdf/reports/cost-of-compliance-special-report-2018.pdf



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



13% *saying it is the single biggest risk.*

"If we look at the number of hours we allocate for mandatory regulatory and compliance audits, it amounts to about 20% of the total number of hours and it is increasing every year. But our resources are not increasing in line with that. That's a real challenge."

CAE, Swedish bank

"There is an overlap of extraterritorial laws. There are laws in the US, Europe, Russia, China, in the end everybody wants their laws to apply everywhere and in the end I'm not sure it's even possible to comply with everything at once. I'm concerned that all of these external constraints are not manageable."

CAE, French international manufacturing company

"There is an enormous number of compliance initiatives coming from the EU, the US and also locally and meeting those requirements is a real challenge for the business. We have had GDPR, the UK Anti Bribery Act, and things that take the focus away from the long-term strategic issues such as the rapid IT developments and the need to audit that. We have quite a sizeable operation in the UK and the Anti Bribery Act is extraterritorial legislation, so whatever connection there is to the UK we have to abide by that. New laws are cropping up all over the place. Some of them are easy to fix and can be addressed locally, but somehow, we in internal audit are always involved."

CAE, international Swedish construction group

30%

*of interviewees in this year's report referenced **AML, anti-bribery and corruption (ABC)** and **antitrust related compliance** as areas of particular concern.*

Busch InBev, the world's largest brewer, was hit with a €200m EU antitrust fine for a deliberate strategy to restrict cross-border sales between the Netherlands and Belgium.

All of this coincides with nearly one-third (30%) of interviewees in this year's report referenced AML, anti-bribery and corruption (ABC) and antitrust related compliance as areas of particular concern.

Sanctions compliance and enforcement is another regulatory pain point for businesses. In 2018 and into 2019, the US continued to expand its sanctions programme and increase enforcement, and is seen to be increasingly motivated by its geopolitical goals. This was evidenced in January 2019 when the country blocked dealings with Venezuela's state-owned oil company Petróleos de Venezuela in an effort to force socialist president Nicolas Maduro out of power.

US embargoes extend to foreign subsidiaries of American businesses and, what's more, the country has been active in imposing so-called "secondary sanctions", which have an extraterritorial application. For instance, secondary sanctions were reimposed on a number of sectors in Iran following America's withdrawal from the nuclear agreement last year, including banking, energy and oil and gas to name a few. The effect is that even European and other non-US companies found to be breaching these embargoes can be subject to US government sanctions.

In the largest sanctions-related fine of last year, Société Générale agreed to a $1.3bn settlement in a coordinated enforcement between multiple US agencies in relation to the French bank's violation of multiple US extraterritorial sanctions against Cuba, Iran, Sudan and Libya.

A robust due diligence programme is paramount to avoid falling victim to what is an increasingly complex sanctions regime. Companies can be caught out even if they are not dealing directly with a sanctioned party or country. If a business exports a component, for example, with knowledge that it will be re-exported to a blacklisted nation through its integration into a product, it could be liable. Similarly, doing business with a sanctioned company that is indirectly owned by a prohibited party can still result in action.

More generally, extraterritoriality is proving to be a real challenge to companies' compliance efforts. Not only has the number of rules imposed on businesses escalated in the last decade, their extraterritorial application and the sometimes conflicting priorities of different national policymakers can make it all but impossible for global operations to reconcile all of this regulation.

Then there are the costs. Record fines are easy to measure and have an obvious impact on business profits, in addition to the potential revenue loss that comes with negative press coverage. The inhibiting effect of regulation is often difficult to see and quantify but the increased workload and financial cost is ever present.

Investing in expanding compliance functions, combined with the organisational fatigue that comes with constant change to processes and controls and the persistent threat of huge fines, are all a drain on companies. Larger organisations typically have more compliance requirements owing to their international presence, but they benefit from economies of scale. All things being equal, this makes compliance disproportionately challenging for mid-sized and smaller companies.

Benchmarking total compliance spend is difficult, especially for the largest firms as their activities are so broad and can be bound by rules relating to everything from AML to data security. One poll, however, found that financial services firms spend up to 10% of their annual revenue on compliance, a conservative estimate putting this cost at $780bn globally. [4] This cost is so high because companies have to contend with a global system of divergent regulations, which requires investing in separate systems and compliance staff. Sometimes even a common standard can be interpreted differently depending on the jurisdiction.

An internal audit perspective

Compliance is a clear priority risk and internal audit should be taking a risk-based approach to key pieces of incoming regulation, for example prioritising those with the highest financial penalties and potential for reputational damage and business disruption. It is important to note, however, that internal audit is not responsible for the company's compliance. Rather it should seek evidence that the compliance function (second line) is managing this risk effectively by staying on top of key regulations, and ensuring that controls and processes are updated to align with changing regulations and laws.

4. International Federation of Accountants: Regulatory Divergence: Costs, Risks and Impacts https://www.ifac.org/publications-resources/regulatory-divergence-costs-risks-and-impacts

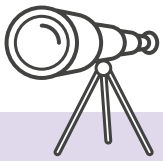
There is a risk of a blurring of the second and third lines. In some cases CAEs assume the responsibilities of compliance and risk management, especially in smaller organisations with limited resources. In such cases internal audit must be clear to senior management and the board of the inherent conflict of interest of assuming both a second and third line remit. Safeguards should be put in place to ensure that internal audit can maintain its independence and objectivity in order to verify whether the first and second line compliance activities cover all compliance requirements in an effective and efficient manner.

There is also scope for internal audit to assess the extent to which the business is effectively managing regulatory change and complexity. If a company struggles to adapt its control system on a regular and timely basis, is unable to reconcile conflicting regulatory expectations or is becoming fatigued from all of this, this should be reported to the board. As well, there is a legitimate assurance risk that internal audit's capacity is being absorbed by mandatory compliance audits. The audit function may have to disproportionately address what regulators see as the biggest risks rather than what the board and internal audit view as the priorities, undermining a true risk-based approach.

Questions for internal audit

- **Is the increasingly extraterritorial and sometimes conflicting nature of regulations and laws magnifying the organisation's compliance risk?**
- **Is the organisation responsive and taking a sufficiently forward-looking approach to regulatory changes (e.g. does it keep a regulatory implementation calendar?) and does it follow a risk-based approach to compliance?**
- **Are all different compliance activities in the first and second lines sufficiently coordinated to ensure all relevant regulations are complied with and in an efficient manner?**
- **Are lessons learned from past regulatory breaches to ensure they are not repeated? Does the business look at past compliance breaches by direct competitors and companies in adjacent sectors in order to avoid making the same mistakes?**
- **To what extent can the organisation cope with regulatory change and adapt to compliance-related internal control change?**
- **Is regulatory pressure preventing internal audit from taking a genuinely risk-based approach by preoccupying it with mandatory audits? If so, what can be done to address this?**
- **Is internal audit maintaining its independence by ensuring that it is not responsible for compliance or, if it is, creating controls to maintain its objectivity in providing third line compliance assurance?**

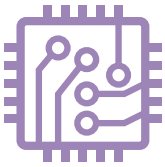
What's new?



Regulatory pressure shows no signs of easing. The banking sector, already one of the most heavily regulated industries in the world, has had to contend with a myriad of laws and regulations since 2008, as authorities have sought to de-risk the economy. Following Basel III, the EU has rolled out a string of directives, latterly PSD2 and MiFID II.

Bribery, corruption and money laundering have become prime targets of the regulatory and legislative clampdown of recent years, driven by rising examples of white-collar crime and terrorist financing. The growing complexity of the US sanctions programme and the extraterritorial application of so-called secondary sanctions threatens to trip up multinationals if they do not remain vigilant. All of this is compounded by record fines for wrongdoing. Authorities are making it clear that regulations and laws are in place for a reason and are not afraid to enforce them.

Digitalisation & business model disruption



Digitalisation risk (and opportunity) is at the forefront of internal audit's thinking. Not only did 58% of CAEs in this year's survey report that 'Digitalisation, disruptive technology and other innovation' is a top five risk to their organisation, 18% singled it out as their number one risk, putting it in second place behind cybersecurity. There is, however, a mismatch that is worth noting: only 30% of CAEs reported that this is one of the top five areas on which it spends most of its time and effort.

Technology adoption risk is pervasive. Not only is there the possibility that new technologies will underperform and therefore fail to deliver return on investment (ROI), they can radically change business processes. This may cause unforeseen disruption to organisations' long-embedded internal control environments. There may also be unanticipated downstream impacts of newly introduced technologies, such as cascade effects that result from poor or corrupted data inputs. There are also softer aspects to consider, including the cultural resistance in the workforce to new technologies that may be viewed as a threat to job security.

These are some of the risks associated with digitalisation, a process that virtually all organisations are undergoing to improve their operations. Indeed, digitalisation represents an opportunity for businesses to improve their customer/client service delivery, make back office processes more efficient, reduce their environmental impact and, ultimately, improve profit margins. Internal audit should be mindful of the upside risk associated with digitalisation and consider whether it needs to report to the board whether the company is effectively harnessing this opportunity. Is the business digitalising too slowly or too hastily, or does it lack the capabilities to harness these opportunities, for example?

Mass disruption

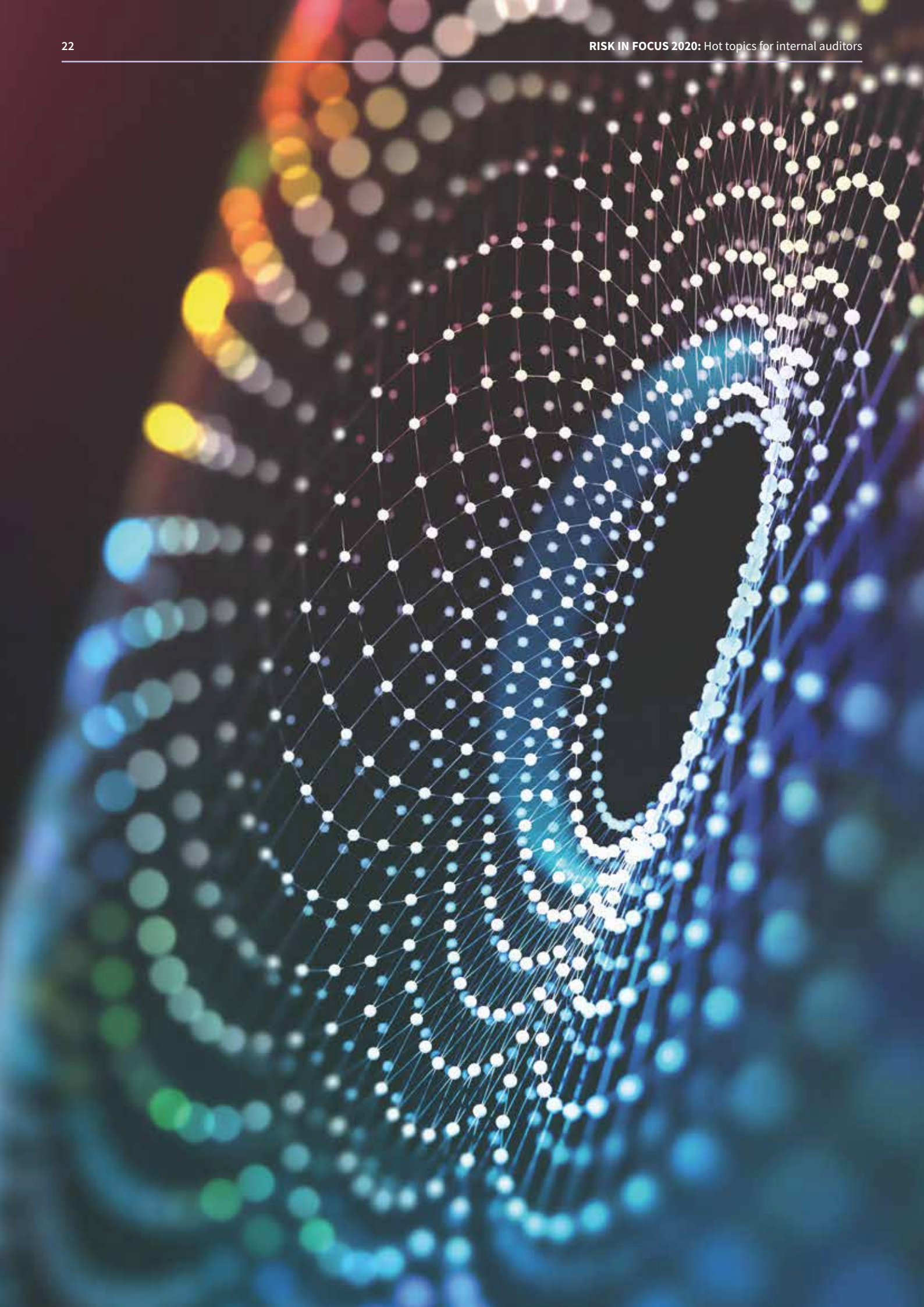
Digitalisation is disrupting business models in countless sectors and it is important for companies, and their internal audit functions, to understand how this works. Disruption refers to a process whereby disruptor companies, often start-ups with new and highly relevant business models or well-resourced big tech firms, challenge established, incumbent businesses.

The primary objective of incumbents is to improve their products and services for their core, highest-margin customers, honing and developing their offering based on what has made them successful to date.

Disruptors, meanwhile, typically seek to address the needs of overlooked pockets of the market, often at attractive prices. Incumbents may identify these new entrants early on but choose to ignore them because the size of the market that they cater to is not sufficient to justify pivoting strategy to compete against them.

The disruption occurs when disruptors begin to shift their attention, scaling up their now-established product or service, catering to the mainstream market with an offering that is better and/or cheaper than what the incumbent currently delivers.

Netflix is a prime example of a successful disruptor. Starting out as an online DVD delivery business in 1997, its core customers were both early adopters of the internet and film aficionados for whom the immediacy of renting in-store was not a priority. Technology enabled this strategy, and the improvement of internet bandwidth



eventually allowed the business to stream content, allowing it to scale up rapidly. Netflix's success signalled the end for then-incumbent Blockbuster Video. Latterly, it has also undercut the content delivery services of established telecoms/network bundle providers, who have been forced to meet the demand of its customers by distributing Netflix, with thin margins.

Disruption drivers

Technology is the great enabler of business model disruption. Since all major industries are digitalising in some form, tech disruptors have a vast scope. There are few major commercial companies that do not face the threat of being made obsolete by innovative, and often young and nimble, technology-enabled companies.

They possess other advantages. One is that they tend to be asset-light compared with incumbents. Fixed assets that were once high barriers to entry – landline networks, bricks-and-mortar retail estates, bank branches – have become a hindrance that technology businesses do not have to fund. As well, tech start-ups are highly sought after by venture capital (VC) funds with deep pockets. Companies perceived to be the next disruptors, such as WeWork and Uber, are backed by mega VC funds such as Softbank, which manages a record $100bn fund. This strong demand is pushing valuations in funding rounds to unprecedented highs, the upshot being that many disruptors have billions of dollars in funding despite not yet turning a profit – a luxury not afforded to incumbents (although history tell us that this mega funding is likely to be a cyclical phenomenon).

Technology is not the only contributing factor to mass business model disruption. Globalisation too is a disruptive force, softer economic borders mean that asset-light businesses can scale up and out at a pace that was not seen in past decades. This is compounded by ever increasing internet speeds and the ubiquity of smartphones, initially in developed markets but increasingly so in less advanced countries. The forthcoming advent of high-speed 5G will accelerate this further.

Demographic shifts also play an important role. Both younger and older generations influence business models through their behaviours as customers. More than half of the global population is now under 30 years of age,[5] with a massive bias towards emerging markets in Africa and the Middle East as child mortality has improved. In Organisation for Economic Co-operation and Development (OECD) countries, nearly one-quarter (22%) of the population is 60 or older, and by 2050 this ratio is expected to rise to around one-third (32.5%) — and this generation has greater spending power than its predecessors. This generational split is influencing demand trends in different geographies.

Disrupting the disruptors

The challenge for incumbents is in balancing growth, or at least maintaining earnings, in their core businesses while funding innovation. Abandoning a still profitable business will not be rewarded by shareholders and in many instances will not be desirable; however, as Netflix CEO Reed Hastings has said: "Most successful organisations fail to look for new things their customers want because they're afraid to hurt their core businesses."

> *"**Technology** is the great enabler of business model disruption."*

There is a tendency for incumbents to protect their core, even when they are aware their industry is being disrupted. As financial performance falters, budgets are tightened and companies scale back peripheral, innovative activities, doubling down on this core.

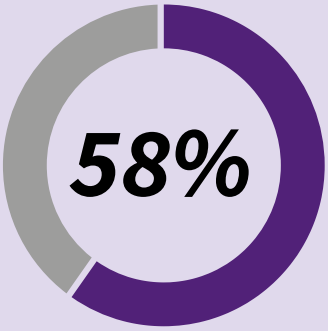
Understanding how, why and when to disrupt (or counter-disrupt) is a challenge, especially in the face of conflicting demands and expectations of diverse stakeholder groups. Success depends on a strong, prescient senior management that is bold enough to pre-emptively sustain innovation and/or pursue a forward-looking M&A strategy.

Researchers at Harvard Business School conclude that the success of innovation functions typically

5. UNESCO: Statistics on Youth
http://www.unesco.org/new/en/unesco/events/prizes-and-celebrations/celebrations/international-days/world-radio-day-2013/statistics-on-youth/

"I'm thinking about how digitised our competition and the industry is becoming and how we need to develop in order to keep up. Are we going to make those changes as rapidly as our competition, because in our world there can be a start-up that enters the market with 40 people, beats your price range and blows you out of the water? These companies can take on chunks of market share in less than a month. It's not that we want to become that, because we can't become that - we operate a network. The question becomes - if that same disruption comes to our home market, are we prepared to defend our market share?"

CAE, German telecoms group



*of CAEs in this year's survey report that '**Digitalisation, disruptive technology and other innovation**' is a top five risk to their organisation.*

There is, however, a mismatch that is worth noting:

Only **30%** *of CAEs reported that this is one of the top five areas on which it spends **most of its time and effort**.*

"You see new entrants in various markets through digitalisation, through the internet, through different platforms. Uber and Airbnb are the famous examples, but you're seeing many more organisations where smart IT solutions are taking out middlemen, they are directly linking supply and demand. That will impact business models massively. You need to understand your business, understand its place in the market and understand technology and its power to enable. In that way, you may still be late but hopefully not too late. Why are we in business? Why do our clients pay us money? What is our added value? How vulnerable are we? What is the likelihood of disruption in our market given the technologies available today and tomorrow?"

CAE, Dutch professional services firm

relies on them being given a high degree of autonomy and being kept separate from the core business. This disruptive standalone business may even begin to cannibalise the core business, stealing customers. When these autonomous disruptive businesses reach a critical mass, they can either be incorporated into the core, or the group can shift its focus, operations and financing in the new direction of travel.

If large organisations are unable to successfully innovate, they may choose instead to acquire disrupters, or already established businesses in adjacent, higher-growth sectors. The challenge here is timing: acquiring companies with proven models without paying excessively high valuations, as competitors vie for the same disruptive business models and prices are bid upwards. Another abiding challenge of M&A is integration: incumbents must have a clear integration plan and strategic vision for the enlarged group. M&A often fails as the result of cultural clashes and the inability of the incumbent to harness the unique capabilities of the disruptor.

Industries are at different stages of digital disruption. Retail and media are obvious examples of sectors that have faced business model disruption for well over a decade already and the effects of this continue to be felt to this day. Indeed, business model disruption is an ongoing process and for this reason organisations must be prepared, willing and able to continuously adapt and pivot to new strategies.

Internal audit appears to be cognisant of the persistent nature of this challenge: 75% of CAEs in our survey said they anticipate digitalisation and its disruptive effects being a top five risk five years from now. On a forward-looking basis, therefore, it should be expected that this will increase in priority as both a strategic threat — but also an opportunity.

An internal audit perspective

Advances in established and emerging technologies (AI, blockchain, quantum computing) mean that digitalisation will become an increasingly pressing theme for businesses. Internal audit should anticipate greater expectations from boards to support these digitalisation efforts. This may include offering its unique risk-control perspective in the development of digital initiatives in its trusted advisor role. In particular, as processes are reshaped and restructured, internal audit has a key role to play in advising on (although not taking accountability for) the design of new internal control systems and procedures. What's more, there is scope for internal audit to assess the ability of the organisation to exploit digitalisation opportunities and whether digital applications are being overlooked or underutilised. This should be viewed from both an operational (digitalising processes) and strategic (business model disruption) perspective.

It is typically advised that innovation projects are afforded a high degree of independence and this may mean they are subject to lighter (or entirely separate) controls than the core corporate activity, to avoid them being stifled. For instance, agile developments activities may not need to deliver progress reports as systematically as established parts of the business, although such projects do involve frequent, periodic monitoring of quality and progress and often daily discussions to address potential problems and pitfalls. Even if agile activities are subject to controls that are lighter or separate from the core business, the third line of defence can add value by assessing the validity and functioning of the agile controls. This can be achieved by seeking evidence, for example by being present at the periodic reviews, that the backlog of activities is in line with the strategy and goals, that quality is being discussed frequently and appropriately, that risks for the coming period (sprint) are defined and budgets are capped as expected.

Disruption and its influence on the strategic direction of a company has the potential to create conflict between the board and senior management. In representing the interests of shareholders, who may take a different view on the future of the company to the CEO, the board may call into question management's strategic thinking. It is not for internal audit to determine whether top management has the "right" strategy, but it can assess the processes and inputs that led to the chosen strategy. It can also challenge the strategy by putting it into context, looking at what is happening in the external business environment, and putting forth "what if?" scenarios.

"The competitive environment is always changing and new companies get into the picture and the old industry structures develop rapidly. We are currently providing TV content services but in the end that will all go over the top so I'm not sure if we will continue to deliver that service in 10 years' time. In the end people will no longer watch linear TV anymore and so that business model definitely has a finite life for us. Netflix has been very successful and that is a product that we resell but the margins on that are very thin."

CAE, Dutch telecoms group

75%

of CAEs in our survey said they anticipate digitalisation and its disruptive effects being a top five risk ***five years from now****.*

"All of the digital initiatives that require limited bureaucracy, flexible controls, rapid time to market are really contesting the expectations of internal audit. We don't want to inhibit those initiatives but we need to learn and understand how to engage with those and make sure that digitalisation doesn't come with too little control and therefore too much risk."

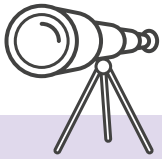
CAE, Spanish multinational banking

Advances *in established and emerging technologies (AI, blockchain, quantum computing) mean that* ***digitalisation*** *will become an increasingly pressing theme for businesses.*

Questions for internal audit

- **Does management know how the business and its sector could be disrupted and does senior management have a strategy in place to pre-empt or respond to this threat?**
- **Is the company's business model likely to exist in five to ten years from now? If not, what is being done to address this?**
- **Does the business have sufficient capacity and capabilities to innovate, and are projects and development processes (e.g. agile) sufficiently controlled and ROI appropriately measured?**
- **How effective is the company's M&A strategy? Is it learning from past mistakes with regard to things like cultural and operational integration?**
- **Are the board/shareholders and senior management aligned on strategy? Is senior management resistant to change or do shareholders disagree with management's new strategic direction?**
- **How is digitalisation affecting the business and is it harnessing emerging technologies to best effect? Is technology working as expected and are there any unforeseen downstream risks that are being created by its use?**
- **How is digitalisation affecting the internal control environment and are new technologies implemented with a risk-control mindset?**
- **Is the business a disrupter or is it being disrupted?**
- **How are the business's efforts to digitalise its processes and to disrupt impacting upon its internal control environment?**

What's new?



In last year's report the focus was on technology adoption risk, which is inherent in all digital transformation projects. Digitalisation remains a key risk as companies transition from traditional, analogue methods of operation in favour of digital processes. Automation and cloud migration in particular represent chief sources of efficiency gains and value creation, the "low-hanging fruit" of digitalisation.

At the mature end of the digitalisation spectrum, emerging technologies such as artificial intelligence (AI) and blockchain will increasingly be adopted.

The emphasis here, however, is on digitalisation as a threat to established business models and an opportunity to develop new, high-growth ones. Technology is a primary component of disruption and businesses must understand how they can defend against this external threat, mitigating the effects of business model disruption and even becoming disruptors themselves.


SATA

Looking beyond third parties

'Outsourcing, supply chains and third-party risk' continues to figure highly in the minds of CAEs; 36% of audit executives in this year's survey reported it as one of the top five risks to their organisation, putting it in fourth place.

The outsourcing trend has been in train for a number of years already, with virtually each and every business operation, process or function having the potential to be handled outside of the organisation. Offshoring non-core operations such as customer services and IT to countries with then-low labour costs exploded in the 1990s, India being a primary beneficiary of this trend owing to its supply of highly educated English-speaking workers.

This trend has begun to reverse itself. Rising wages in developing markets combined with unsatisfactory service standards are increasing the attraction of onshoring/reshoring, i.e. bringing activities either back in-house or back to a company's home nation, or nearshoring, relocating these activities to a nearby country. For instance, Ukraine's IT outsourcing industry, recognised for its inexpensive high-level technical expertise, has grown its share of the country's GDP 50-fold in the five years from 2013 as European businesses bring their back office networks closer to home.

While companies have begun to view in-housing certain activities as a more attractive, less risky option, the fact remains that business activities are spread far and wide outside of an organisation's own borders. Recent protectionist, nationalist trade developments notwithstanding, supply chains have lengthened as the world has become more globalised over the long term, meaning that third-party risk may not even apply to third parties at all, but fourth, fifth, sixth etc. parties, also known as nth parties.

'Nth' party liability

Back office operations are a primary candidate for outsourcing. Such operations must be carried out efficiently to ensure the success of the business, but these services do not fall into the core customer-facing operations of the firm. Migrating data entry, payroll, IT support and even the finance function can allow a business to focus on its core efforts and at the same time reduce costs and lessen the HR burden of staff acquisition and retention.

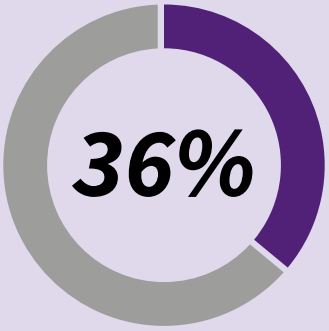
"Business activities are spread far and wide outside of an organisation's own borders."

But the risk/reward profile of doing so has changed in light of heightened regulatory oversight of data security. 'Nth' party risk, third parties outsourcing to their own sub-contractors, makes this an even more pressing consideration given that the first party has no legal contract in place with the nth parties that are indirectly servicing them. It is important to keep in mind that fourth parties may not be subjected to the level of scrutiny and oversight that the organisation has over the legally contracted third party. This calls for businesses to take even greater care in managing supplier risk.

A popular trend in outsourcing is for critical IT infrastructure and data assets to be migrated to

"**Auditing public cloud providers** is a challenge. They won't open their doors to auditors individually, but they will understand that, given the market position that they have, they must come up with a solution to provide **assurance to their clients**, the quality of their processes, the way they deal with data and so forth. They will not be eager to open their doors to 500 organisations but will be open to a consortium of very important clients **in a coordinated way** to provide assurance on the quality of their processes. **That's beginning to happen**."

CAE, global Dutch banking group



*of CAEs in this year's survey reported '**Outsourcing, supply chains, and third-party risk**' as one of the top five risks to their organisation.*

"To be able to service our **global clients**, we act through a **network of partners**. That's an area in which our own customers are demanding more and more. We receive requests from our customers about how we are **managing our own suppliers and partners**. Our clients have their own **third-party risk** by involving us in their internal processes, and there are additional steps as we outsource ourselves using our **own partners**."

CAE, Belgian software service company

*Internal audit can **add value** by taking an inventory of **core processes** and functions that are **outsourced** and reviewing the governance around procurement and contract management.*

"We audited **third parties** some time ago but looked more at the oversight model. You've got to go and inspect what's on the ground, but there are a lot of issues around whether you can even do that - **will third party organisations allow you access?** We are now revisiting third party risk in light of the **new regulation** that is coming through, acknowledging that we need to do far more of that. A desire to do it versus boots on the ground and coming up with **real findings** is still a few steps away, steps that could be quite difficult."

CAE, UK banking group

the cloud, in some cases private clouds, but often those provided by big tech firms such as Google and Amazon. This brings with it considerations around information security and fundamentally challenges risk-based auditing, i.e. how can internal audit take a risk-based approach to assurance if it is difficult or impossible to gain access and verify the security and governance controls that are in place at major tech firms? Businesses may choose to assume with a high degree of confidence that these highly advanced big tech service providers, which have huge budgets and hire the best and brightest in security, have even stronger controls than themselves; nonetheless, this is something of a black-box scenario and companies should be particularly mindful when outsourcing to smaller cloud providers that lack the same best-in-class security resources of the likes of Amazon and Google.

Financial services: a template for other sectors

US and European financial regulators continue to home in on supply chains and the risks posed not only by third party suppliers, but their own sub-contractors. The US Office of the Comptroller of the Currency (OCC), the country's banking regulator, issued guidance in 2017 challenging the financial services industry to raise its game. Among its expectations, it called on banks to monitor and review fourth and other significant nth parties with nearly the same level of scrutiny as third parties, as well as have in place third-party relationship and risk management strategies that apply to all of their relationships.

In the regulator's Spring 2019 Semiannual Risk Perspective it reiterated its concerns: "Operational risk is elevated as banks adapt to a changing and increasingly complex operating environment. Key drivers for operational risk include... [the] increasing use of third parties to provide and support operations that are not effectively understood, implemented, and controlled."

These concerns are being shared by European regulators. The European Banking Authority (EBA) published its recommendations on cloud outsourcing in June 2018, again emphasising the risks around what it calls the "sub-outsourcing" by service providers of critical functions. The EBA highlighted the additional risks associated with fourth parties being based overseas from the service provider and the inherent oversight challenges that come with long, complex value chains.

The European regulator expects internal audit to play a key assurance role here, by independently reviewing outsourcing and sub-outsourcing arrangements with a risk-based approach. This means assessing those core relationships underpinned by critical functions and should include reviewing the appropriateness of data protection and business continuity measures.

Pooled audits

Regarding critical cloud outsourcing specifically, the EBA requires that banks ensure they have the right to physically access the premises of service providers. The purpose of these rules is to ensure high levels of supervision and access to data and relevant personnel in outsourcing environments. This, it says, can be achieved through the use of "pooled audits", whereby multiple companies arrange audits of their service providers' premises to take place at the same time or through the same third party auditor, to help reduce the cost and time burden for both institutions and providers. This approach has also been adopted outside of financial services, for instance in healthcare and the public sector.

In its guidance, the EBA has set certain criteria for pooled audits, such as the scope of the audit including key systems and controls identified by the bank and within the regulations, ongoing reviews to ensure pooled audits do not become obsolete, that the auditing party is qualified and capable, and that there is a contractual right to expand the scope of the audit if necessary.

Notably, even though the EBA's guidance has only just come into play, it intends to replace it with broader recommendations on outsourcing that apply to all services, not just cloud services. Banks should expect the more generic guidance to place just as much emphasis on managing nth party risk as the current recommendations do.

An internal audit perspective

It does not matter if the business is not a financial institution, the EBA's guidance should be seen as best practice for businesses in all sectors. Regulated or not, companies need to understand the extent to which they are exposed to nth party risk in their extended supply chains.

Internal audit can add value by taking an inventory of core processes and functions that are outsourced and reviewing the governance around procurement and contract management. Audit rights should always be written into supplier contracts and internal audit should look for evidence that regular due diligence (not just at the onboarding stage) is carried out on key suppliers.

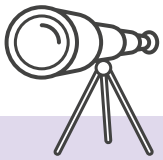
Nth party risk management requires understanding the extent to which key third parties rely on sub-outsourcers. Internal audit should assess how far the business understands its exposure to nth party risk and what controls key third parties have in place for the management of their own suppliers.

Things to consider, besides monitoring the effectiveness of the services provided and their commercial viability, include data security, i.e. how key suppliers keep the organisation's data safe and whether it is shared with other partners; as well as concentration risk, i.e. whether the organisation is over-reliant on a small number of suppliers, and whether suppliers have their own concentration risk. How easily the business can switch suppliers without being disrupted should also be reviewed.

Questions for internal audit

- **Does the business review the appropriateness of its outsourcing programme? Is it confident that the cost benefits outweigh any additional risks associated with outsourcing?**
- **Do contracts with third parties include audit rights and can internal audit, if required, gain physical access to these third parties?**
- **Is the business trying to understand its nth party risk exposure by asking third parties how they use sub-outsourcing? Are critical processes handled by nth parties and is there an inventory of these?**
- **Is due diligence carried out on third parties and their nth party suppliers, both at the onboarding stage but also on an intermittent basis?**
- **How do third/nth parties manage data and data security risk? Are these controls up to the same standards as the organisation's own controls as dictated by GDPR?**

What's new?



Given the rapid uptake of cloud services in recent years, coupled with the rise in prominence of data security risk, it is not enough to stop at auditing third-party risk management.

For core services and processes, internal audit should be asking whether the business understands nth party risk deeper into supply chains. This can be as simple as contract managers asking key third parties what processes they themselves outsource and seeking evidence of how priority risks are controlled, such as those related to data security. Financial services regulators are paying increased attention to nth parties; companies in all sectors should view high standards of nth party risk management in this sector as best practice.

Business resilience, brand value & reputation

'Business continuity/resilience' was cited as a top five risk by nearly one-third (31%) of our survey respondents, putting it in fifth place. The first few months of 2019 have provided plenty of cause for businesses to reflect on and review their ability to respond to crises and bring their operations back online after ruinous events.

In one of the worst corporate health and safety failings of recent times, an Ethiopian Airlines aeroplane crashed six minutes after take-off on 10 March. The incident was caused when an erroneous reading from the Boeing 737 Max's flight path angle sensor triggered an automated control system that automatically pushed the nose of the aircraft down. This was not an isolated incident. Five months prior, the very same Boeing model operated by Indonesian carrier Lion Air had gone down, and for the same reason. The two crashes killed 346 people.

This double tragedy led to the worldwide grounding of all 371 operating 737 Max aircraft, at an estimated cost to Boeing of $5bn. Inevitably this also led to a slowdown in the manufacturer's production output, by 19%, as deliveries of the circa 4,500 new jets it had on order were halted, a clear business continuity issue for the company. But it is not the only party to be impacted. Suppliers and airliners have felt the effects of the mass grounding, with China's three largest carriers — Air China, China Southern and China Eastern — filing for compensation for lost revenues.

Business crises are on the rise, with such incidents increasing by 25% in 2017 to reach a new peak.[6] Companies that are able to respond to such incidents, or avoid them in the first place, can better preserve financial value. This is why business continuity plans are so essential. At a basic level, organisations should have in place preventative measures, detective alerts, and corrective actions and capabilities.

In the above example, preventative measures were not acted upon. While investigations into the exact cause of the two accidents are ongoing, by its own admission Boeing was aware months before the Lion Air crash that a cockpit alert system did not work in the way that it had told airliners it did, but deemed the issue to be low risk. The aeroplane's operating manual was only updated after this first crash and neither the Lion Air or Ethiopian Airlines jets were equipped with the optional alert system.

Reputation is everything

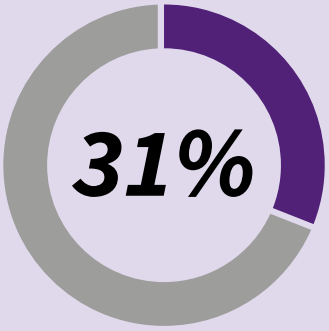
Crisis situations such as fatal accidents or major cyber attacks not only disrupt continuity and require a swift response to get business operations back online, they can have a lasting impact on a company's reputation and the value of their brands in the eyes of the public and other stakeholders. Risks rarely exist in isolation and business continuity risk and reputational risk are closely related; with this in mind, 22% of respondents to our survey said that 'Communications and reputation' is one of their organisation's top five risks.

A key part of any strong business continuity plan, therefore, is appropriately responding to a crisis to regain the trust of the public, customers and regulators. Boeing has faced widespread criticism for its mishandling of this important step. Good crisis public relations (PR) requires engaging with the media and being open, transparent and honest — and, in the event of a tragedy, showing empathy. The manufacturer is seen as having not followed these principles, instead defensively maintaining in public statements and tweets from its CEO, Dennis Muilenburg, that its planes were safe, even as they were grounded.

6. Institute for Crisis Management: Annual Crisis Report https://crisisconsultant.com/wp-content/uploads/2014/11/ICM-Annual-Crisis-Report-for-2017.Issued-April-17_2018_print.pdf

"Reputation is a real priority risk and it is linked to three things in my company: the quality and security of our products, because obviously if you are developing software for aircraft and it crashes because of the software than that will kill our business; reputation is also ethics because if the CEO is in the press because they have paid bribes for contracts then that is a serious problem; and the third one is information security — at the end of the day we are selling technology and hackers can take pride if they are able to successfully hack the system of a company such as ours."

CAE, Spanish information technology and defense systems company



*'Business continuity/ resilience' was cited as a top five risk by nearly **one-third** (31%) of our survey respondents.*

*Business crises are on the rise, with such incidents increasing by **25%** in 2017 to reach a new peak.*

Source: Institute for Crisis Management

"There is a potential risk in the way that we communicate if there is a brand issue that emerges on social media or with regard to crisis management. We need to take care of that. There may be some countries that are on the periphery, outside of France, who communicate externally and the way they present the brand and the platform is not in line with what we expected and deliver in our home market. That can be a local problem that creates a global problem. We are a big company with 350,000 staff so of course we have to take care in monitoring this risk."

CAE, French international retail group

It was not until 29 May, nearly three months after the second crash, that Muilenburg acknowledged the company "clearly fell short" in dealing with the 737 Max's implementation problems and that it had not adequately communicated with regulators.

Boeing is not alone. Awareness of reputational risk has risen in the last decade with the widespread adoption of social media. Facebook and Twitter have become platforms for both positive and negative interaction with businesses and a means for sharing customer service failings, big or small, with the world.

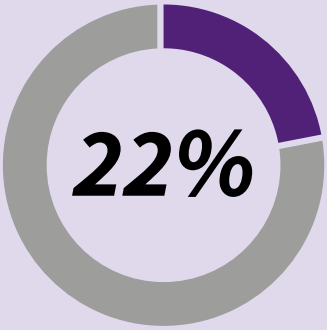
When a passenger on a Ryanair flight was racially abused by a fellow traveller in October 2018, a video of the incident was uploaded to Facebook, the consensus being that attendants failed to handle the matter appropriately. While the company was quick to condemn the incident, refer the matter to authorities and vow to ban passengers for such behaviour, the episode clearly highlighted the importance of robust staff training in an age in which a camera is never far away. In May 2019, a group of 30 drunk males were filmed chanting a racial slur on a Ryanair flight and were said to be inappropriate to female passengers while boarding, yet they were not removed. This shows that while effective PR strategies are important, they are not a substitute for the robust enforcement of policy. Saying the right thing in the public domain is undermined if companies do not keep their word.

There are countless examples of companies mishandling crises in the public domain, but there are just as many instances of companies getting it right. When the majority of the 870 KFC restaurants in the UK and Ireland ran out of chicken in 2018 due to a logistics issue, the PR team responded to the mishap in exemplary fashion. Rather than ignoring the incident, a social media and press ad campaign was swiftly rolled out rearranging the brand's letters to spell "FCK", the company staying on top of the news by issuing live updates on the matter. By being transparent, responsive, "owning" the event and addressing the incident with the appropriate level of sincerity, the company averted what could have been lasting reputational damage.

It is also important that organisations not only focus on reputational risk in times of crisis or in the years following a major incident. In being reactive rather than proactive, organisations miss the opportunity to build reputational resilience. Successful reputational risk management and resilience requires a front-foot approach of monitoring the press and social media, and assessing and responding to threats (and opportunities) early.

*"While **effective PR strategies** are important, they are not a substitute for the **robust enforcement of policy**."*

Reputational risk may appear more abstract than financial or cyber risk, but it is no less of a threat. Negative sentiment among stakeholders and the general public can have a harmful impact upon a company's share price and its revenues. As businesses increasingly recognise the significance of brand value, and as the number of examples of brand damage increase, it is becoming possible to calculate the costs of the risk. For instance, insurers are beginning to offer cover for reputation. Often this is included in broader corporate insurance policies, but it is increasingly being offered in standalone policies that cover balance sheet losses due to a sales drop based on a reputational incident. In this sense, reputational risk is calculable.



*of respondents to our survey said that '**Communications and reputation**' is one of their organisation's top five risks.*

"How we behave and operate as a business can have a major impact on reputation. I'm of the opinion that is more than just reputation, it is brand value. Reputation is more between an organisation and its regulatory authority. Brand value is for everyone and without it you cannot exist."

CAE, international German insurer

"We manage the public's money and resources and we need to focus on reputation because citizens demand more transparency. We have some KRIs to measure this risk and we are going to audit whether these are valid and the controls in place to mitigate reputational risk. We will assess how the organisation builds a complete picture of reputation, looking at its clients, the media and so on."

CAE, Spanish public sector organisation

Reputational risk may appear more abstract than financial or cyber risk, but it is no less of a threat.

An internal audit perspective

Business continuity is of the utmost importance and companies should have controls in place to mitigate risks that may impact on the continuity of operations. These preventative measures can range from cybersecurity controls to measures to ensure the safety of products and services. Internal audit should carry out, or re-perform, a risk assessment to understand what the biggest threats to business continuity are and how these are being managed. In addition, all organisations should have a documented business continuity plan (BCP) in place that not only addresses how to bring the company back online in the event of certain incidents, but how to manage any ensuing reputational blowback.

There is a genuine value-add role for internal audit to play in assessing what efforts are being made by the business to understand how it is perceived by stakeholders and the general public, and what steps are being taken to build trust and brand value to help the company better withstand the shock of future incidents.

The company should be placing just as much emphasis on reputational risk management as it does on brand management. Internal audit can assess the extent to which the company's brand (how the company aims to be perceived) and its reputation (how it is actually perceived in the real world) match up as evidence of how effectively reputational risk is being managed. Any gap between the two should be flagged up with board and senior management. Those companies that build such capabilities can identify potential risks and opportunities early, evaluate their impact and make better decisions about how to act upon them.

Questions for internal audit

- **Is the organisation aware of key business continuity risks and have they been codified? Do these risks look relevant and are they reviewed and kept up-to-date?**
- **Does the risk register capture a single or multiple business continuity risks, and are they split by business division?**
- **Is a comprehensive BCP in place to follow in the event of incidents occurring? Has the BCP been tested?**
- **Who is accountable in various business continuity situations — and are these managers aware of their responsibilities and accountability?**
- **Does the business have an adequate PR/communications damage control strategy in place in the event of an undesirable incident occurring? Is it linked to an operational resilience statement?**
- **How well does the business understand its reputation and is this in keeping with its brand? Does it understand that a poor/good reputation can damage/enhance the brand's value?**
- **Is the business monitoring its reputation using social media and press analysis and then responding to those findings to build brand resilience?**

Financial risks: from low returns to rising debt

'Financial risks' scored highly in this year's survey, 30% of CAEs reporting it as a top five risk to their organisations, putting it in sixth position, and 40% saying this is one of the top five risk areas on which internal audit focuses most of its time and effort.

Some risks are highly specific and are mostly uniform from company to company (even if the management of those risks varies widely), e.g. cyber/information security risk which largely concerns keeping baddies out of the organisation and data safe and secure. The nature of financial risk, though, greatly depends on the sector and business model in question. This high ranking in the survey therefore reflects, at least in part, the fact that financial risk is a broad category compared with certain other priorities, encompassing everything from working capital management and cost controls to debt management and oversight of the treasury function.

Financial returns risk

Insurance firms in our interviews noted recent capital market volatility and the challenge of achieving adequate returns in what continues to be a persistently low-interest rate environment.

This is inherently linked to outside risks such as central banks' loose monetary policy, the macroeconomic picture and the sensitive relationship between financial markets and politics. This latter point has become especially acute in recent years; a number of studies have identified a new phenomenon, that the US President's tweets have a direct influence on stock prices, increasing short-term volatility. In some cases, individual company prices become depressed (and inflated) over the long term as a direct result of investors reacting to Trump's Twitter feed.

The broader point here, however, is that financial markets are proving challenging. For example, the Euronext 100 and S&P 500 indices delivered a 0% return in the 12 months to 1 June 2019. This financial risk is not only a concern for insurance firms and other companies whose business model relies on market returns. Many companies manage multi-billion euro pension schemes and any underperformance in these portfolios raises the risk that the company will have to fund the shortfall themselves to meet their defined targets, reducing profits.

*"The nature of **financial risk** greatly depends on the **sector** and **business model** in question."*

The impact of accounting standards

Beyond the markets, recent accounting developments are having an impact not only on reporting, but in some cases may affect the strength of companies' financial positions. From January 2019, IFRS 16 requires that payments made on operating leases must for the first time be reported as a liability on balance sheets, in the same way that finance leases already were. In other words, under IFRS 16, operating and finance leases are now treated equally for accounting purposes.

The standard is far reaching given the ubiquity of building, vehicle and other asset leasing by businesses. The worst affected companies

"One of the top risks to our company is currency risk. We are based in the EU so we report in euros but we buy a big part of our merchandise in countries that are pegged to the US dollar. So the fluctuation between the dollar and the euro is very relevant for us and other currencies are also relevant.
For example, the Turkish lira and the Chinese yuan. So the way they fluctuate against the euro is always relevant for our P&L account. Unexpected volatility can affect our gross margins."

CAE, Spanish multinational clothing company

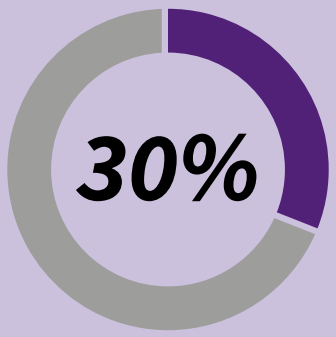
At the end of 2018 there was

$13 trillion

*of **non-financial corporate debt** on balance sheets worldwide, a new record.*

"What is becoming more important is financial performance. We face the pressure of low interest rates and volatile financial markets; that's of particular concern for the insurance industry. The biggest indicator for us is financial markets, central banks' approach and monetary policies. This is impacting exchange rates and we have been in a persistent low-yield environment. All of these indicators are interrelated."

CAE, multinational German insurer



*'Financial risks' scored highly in this year's survey, 30% of CAEs reporting it as a **top five risk** to their organisations.*

"One of the biggest external factors for us is the size of our defined benefit pension scheme. We have an in-house fund management business with £13bn in assets under management. When we look at equity and bond markets, they are all struggling for a variety of reasons. That's a factor that plays into funding because if the pension scheme is not delivering the targeted level of returns, we have to put more money in. And if the bond markets wobble then we cannot finance projects as effectively as we would like to."

CAE, UK food retailer

are expected to include retailers, airlines and professional services firms, which all make heavy use of property and equipment operating leases. Other asset-heavy sectors such as telecoms and transport may also feel the effects depending on the extent they use operating leases versus finance leases (the difference between operating and finance leases is that lessees assume legal responsibility and share in the economic upside/downside in the value of the asset in the latter instance).

The reason the changeover can weaken businesses' financial standing is that by being recognised as liabilities on balance sheets, net debt will have increased overnight for those most exposed to the new standard. This will be a concern for businesses already carrying heavy debt burdens as it increases their risk of default. As leverage ratios increase, businesses that rely on operating leases may find themselves unwittingly breaching their loan covenants. This may require renegotiating loan terms with banks or refinancing existing debt obligations.

More broadly, companies should be mindful of their debt positions after years of cheap and readily available financing. At the end of 2018 there was $13trn of non-financial corporate debt on balance sheets worldwide, a new record. This means diligence is required in ensuring that companies are able to cope with servicing this debt and are not prone to defaults and costly capital restructurings, calling for an assessment of the treasury's risk management efforts.

Many companies, especially those in highly mature sectors and those most exposed to fierce competition are also dealing with one of the most fundamental financial risks: falling profits. This is a knock-on effect of competitive pressure. As revenues contract, there is a need for expansive cost-cutting balanced with the launch of new services in order to maintain earnings and bring revenues back to positive growth.

This is a persistent challenge in telecoms, where maintaining earnings margins amid falling revenues is a chief priority and requires increased oversight of the treasury function. This is being compounded by the introduction of IFRS 15, which came into play in January 2018. The standard dictates that a business cannot recognise all revenues up-front; if a contract has been signed, revenue can only be recognised in the financials when it is collected. The effects of this change are now beginning to show. In January 2019, Vodafone reported that its turnover had fallen by €800m, blaming both competition and the effects of IFRS 15.

All companies should prioritise the effective management and oversight of working capital expenditure, but especially those businesses whose revenues have come under pressure in recent times. The efficient management of working capital required for operational expenditure purposes can offer significant advantages, such as boosting the available funds for capital expenditure to help the company grow over the long term through strategic investments in assets and operations. More generally, a robust, well-governed treasury function that is on top of not only working capital management but cashflow forecasting, banking, debt and funding, investments, and risk-manages currency and interest rate movements will enable the long-term success of the company.

*"Companies should be **mindful of their debt positions** after years of cheap and readily available **financing**."*

An internal audit perspective

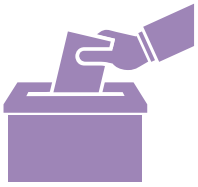
Expectations of internal audit have increased dramatically over the past decade. Once a function preoccupied with providing assurance around financial risk management, internal audit is now an essential tool in assessing more pressing risk areas with a lower risk-management maturity. Nevertheless, finance-related business challenges are evergreen and, depending on the company and sector, the board may require that more traditional assignments are carried out.

Where appropriate, internal audit can assist in carrying out an independent assessment of the potential impact of new accounting standards on the financial position of the company, or seek evidence that this has been carried out and evaluate the validity of that assessment. It may also be expected to review how effectively working capital is being managed, monitored and reported, and provide an independent view on the efficacy of the treasury's financial risk management. Well-functioning treasuries should be able to demonstrate how they are keeping the cost of debt financing to a minimum, putting in place dynamic foreign exchange hedging mechanisms to reduce the effects of market volatility and managing the company's capital requirements.

Questions for internal audit

- **How mature is the company's financial risk management and is there a need for an assurance to be provided on the efficacy of the financial controls?**
- **To what extent are market volatility and low returns affecting the business's ability to finance its operations and fund its pension obligations?**
- **Is the organisation compliant with the new accounting standards? Importantly, how are these standards affecting revenue and debt calculations?**
- **Does the business make significant use of operating leases and what is the likely impact of IFRS 16 on the balance sheet? If it is significant, what is the company doing to remedy this?**
- **Does the board require an audit of the treasury function to assess currency hedging strategies in the face of heightened geopolitical tensions?**
- **What evidence is there that working capital is being managed as effectively as possible in order to free up financial resources for non-operating expenditure purposes?**

Geopolitical instability & the macroeconomy



Political risk has loomed large in the last three years since the UK's decision to leave the EU and Donald Trump was elected to the US presidency. Since then the political landscape has polarised further. In Latin America's two largest economies, Brazil and Mexico, respective far-right and far-left governments have taken power in the last 12 months and nationalist sentiment is rising.

Meanwhile, hopes that the US and China would resolve their ongoing trade standoff, which is in part seen as being politically motivated, have not been met; instead the situation escalated further in May 2019 when the US raised tariffs on $200bn of Chinese goods from 10% to 25%, China responding with tariffs on $60bn of US imports. China is not the only target of a protectionist US trade policy. In a like-for-like response to the US imposing levies on steel imports, the EU retaliated with its own tariff hike last year and has tabled a further response if the US goes ahead with a proposed round of taxes on $11bn worth of European imports. In May, President Trump said: "The European Union treats us, I would say, worse than China. They're just smaller... They send Mercedes-Benzes in here like they're cookies."

This is the macro background against which CAEs of Europe-headquartered, and in many cases multinational, organisations participated in this year's Risk in Focus quantitative survey and qualitative interviews. Nearly one-third (29%) of those surveyed in this year's report said that 'Macroeconomic and political uncertainty' is a top five risk to their organisation, putting it in seventh place. Meanwhile, more than half (63%) of the CAEs interviewed for the report said that the political and macroeconomic outlook is preoccupying their thinking as they prepare their audit plans for 2020, a likely symptom of global politics, trade and the world economy dominating headlines in the past year.

The future of Europe

After more than 30 years of centre-right and centre-left parties governing most EU countries, with broadly equivalent policies and visions of the future, populist parties have found a strong voice and support. European parliamentary elections in late May 2019 resulted in the "grand coalition" of centrist parties losing their decades-long majority.

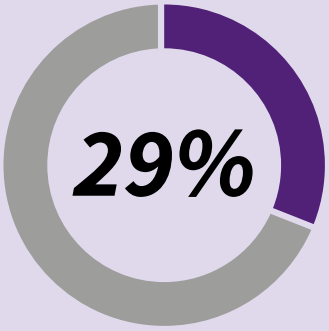
There are legitimate concerns over the future stability of the EU. If and when the UK does leave the single market it could set a precedent for other countries to follow. Nationalist, anti-immigration, anti-EU political rhetoric and campaigning from ruling parties has become the norm in countries such as Italy and Hungary, an obvious cause for concern. If nations were to secede from the bloc it would have significant, far-reaching long-term economic, legal, regulatory, and political consequences.

However, it is important to note that while much has been made of the future of Europe in the mainstream media, these concerns may be somewhat overstated, a natural consequence of the media reporting on the political shift away from the centre. The main anti-EU parties

*"There are **legitimate concerns** over the **future stability of the EU**. If and when the UK does leave the single market it could set a precedent **for other countries to follow**."*

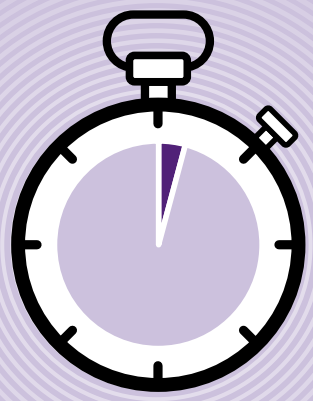
"National tariffs, political tensions coming from one country or another and the level of political populism in the respective governments is all loaded with a high level of uncertainty. I truly believe we might not have yet seen the peak of these political movements. Internal audit can assess the level of flexibility or adaptability in the organisation to react in a meaningful way to these disruptive changes. This might be a little bit hard to address with a traditional audit approach, but in essence this is where the true value of internal audit lies with these issues."

CAE, German multinational industrial conglomerate



*Nearly **one-third** of those surveyed in this year's report said that **'Macroeconomic and political uncertainty'** is **a top five risk** to their organisation.*

*But only **4%** say this is a **top five domain** on which internal audit **spends the most time and effort.***



"The advertising business is cyclical so is very much linked to GDP. When the economy grows, our industry does well and vice versa. We don't know what will come tomorrow with the situation between the US and China, it may slow down global economic activity. There is a sense that we are in the latter stages of the business cycle. Will the downturn be in 2019, 2020, 2021? Nobody knows for sure but it will come eventually and in advertising we are on the front line of any recession."

CAE, French multinational advertising and public relations firm

of the UK, France and Italy — the Brexit Party, the Rassemblement National Party, and Lega Nord Party respectively — all led the European elections results of their respective countries. But, overall, the European Parliament remains overwhelmingly dominated by pro-EU MEPs (Members of European Parliament).

Further, the European Commission's spring 2019 Eurobarometer found consistently high levels of support for the bloc. The survey of 27,973 Europeans showed that 68% of EU citizens believe member states benefit from being part of the EU, the highest result for the question since the survey began in 1983; further, 61% of respondents said that their home country's membership of the EU was overall "a good thing", matching the result of the previous barometer, which showed the highest level of EU approval since the 1989 fall of the Berlin Wall. Similarly, a recent Kantar poll showed support for remaining in the EU stands at well over 80% in the majority of member states.

Politics and the global economy

Politics and the economy are intrinsically linked and this has become especially apparent in recent years. Brexit (again, if it goes ahead) is expected to cause an economic drag not only in the UK but Europe as a whole, the region already showing close to flat growth.

Ongoing tensions between the US and China are being closely watched by investors and are already having a dampening effect on the world's two largest economies. World GDP growth will slow to 3.2% this year, from 3.5% in 2018, the OECD identifying continuing trade tensions as the principal factor weighing on the world economy. Trade headwinds are being felt in Europe already, with Germany — the continent's so-called economic engine — contracting in the second quarter. The Netherlands too has forecast an annual drop in GDP growth from 2.7% to 1.7% in 2019, reducing further to 1.5% in 2020, as exports and investments are hampered by US trade policies. The OECD has said that if a sharper slowdown in China were to emerge, it would have a ripple effect around the world.

This global slowdown coincides with the current business/credit cycle entering its tenth year of expansion, the average cycle lasting no more than seven years. The longer the growth span from the global financial crisis and ensuing worldwide recession in 2008, the closer we are to the next widespread economic contraction.

A number of amber warning signs have been flashing in recent months. One signal widely cited by economists and investors is the inversion of the "yield curve". This refers to riskier long-term treasury bonds offering a lower rate than lower-risk short-term bonds, a sign that financial markets anticipate an imminent contraction — a reliable predictor of oncoming recessions. Some believe this is a function of unprecedentedly loose monetary policy (low interest rates and quantitative easing by central banks); others believe it is a sign that an economic contraction is due within the next six to 24 months. The economist who first correlated the yield-curve inversion to economic declines, Campbell Harvey, pinpoints the three-month versus five-year curve as a key recession indicator once it inverts for a full quarter. That has now happened.

*"**Politics** and the **economy** are **intrinsically linked** and this has become especially apparent in recent years."*

Another point of concern is the massive accumulation of corporate, sovereign and consumer debt. Global debt issued by non-financial corporates alone had reached $13trn by the end of last year, more than double the figure in the last credit bubble that preceded the 2008 global financial crisis. Leveraged debt, loans on the balance sheets of companies with the highest chance of default, has also peaked.

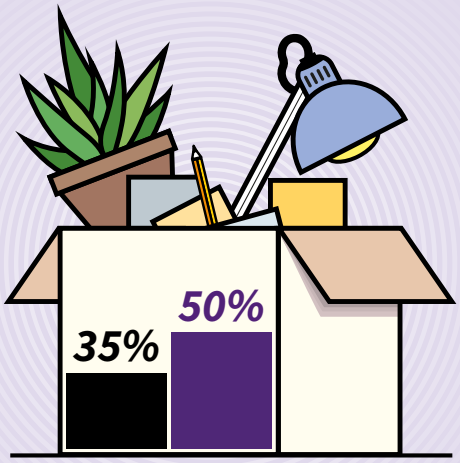
Policymakers such as the US Federal Reserve have begun to monitor these indicators with concern. While predicting recessions with accuracy is all but impossible, one forecast in Q2 2019 estimated there is a 35% chance of the US falling into recession in 2019, rising to 50% for the euro area.[7]

7. Vanguard: Known unknowns: What are the odds of a recession? https://www.vanguardinvestor.co.uk/articles/latest-thoughts/markets-economy/known-unknowns

"There is lots of uncertainty in Europe if you look at France, Italy and the UK. Is Europe still relevant for its citizens? What will the long-term impact of Brexit be for Europe? All those concerns make the economic context really uncertain and we intend on auditing how prepared the company is for these macroeconomic uncertainties in our next audit plan."

CAE, global German insurance group

*There is a **35%** chance of the US falling into recession in 2019, rising to **50%** for the euro area.*



Source: Vanguard Investor

World GDP growth will slow to **3.2%** *this year*

from **3.5%** *in 2018.*

"The US yield curve has inverted, with long term rates dropping below short term rates. That has got people sparked up recently, although the rest of the data's been pretty positive coming from the US. Generally there's a nervousness among my board members around markets and that's what everyone seems to be concerned about."

CAE, UK manufacturing group

There are few organisations that would not feel the impact of a recession. A fall in business investment and spend in the economy would harm the private sector as revenues and profits drop and unemployment rises. This would have the knock-on effect of lowering countries' tax bases and lead to a significant pullback in investment in the public sector as sovereign debt has ballooned since Western governments bailed out their banking systems in 2008. The need to understand how organisations are managing risks associated with the economic environment will persist as the latter stage of the business cycle unfolds and geopolitical risk, which is now closely linked to the global economy, remains high.

An internal audit perspective

Economic and political risks may not be interpreted as "true" corporate risks, but external forces that are beyond the control of the organisation. In other words, geopolitics and the economy are macro conditions outside of the organisation that lead to certain direct corporate risks increasing in priority (i.e. potential severity and probability). For example, protectionist policy from a new government may introduce new customs duties (external), the knock-on effect being that the price of materials rise causing working capital costs to increase (internal).

This may explain the disparity between the proportion of CAEs who say macroeconomic and political risk is currently significant for their organisation (29%) and the small minority (4%) who say this is where internal audit spends the most time and effort — because economic risk itself is not technically auditable. However, given their potential impact, these external forces cannot be ignored. Internal audit must understand the root causes of internal risk by looking at the external environment. In order to mitigate external risks, the organisation should have the capacity to foresee — to identify and envision trends and future developments — so that it is not caught off guard. This can be achieved through open dialogue and methods such as scenario planning and war gaming. The business should also be ready and able to react when external forces lead to internal risks manifesting.[8]

Trade policy is one area of geopolitics that is being felt by businesses and internal auditors may choose to respond accordingly. For instance, Harley-Davidson, Coca-Cola, Ford and General Electric have all reported that raised tariffs are inflating the cost of input materials, namely raw metals, that will either erode their profit margins or result in higher costs to their customers, or both.

Boards/audit committees may therefore require an independent assurance from internal audit that the financial risks associated with higher input costs are being effectively managed. For example, are the goods manufactured by the company, or are the raw materials used in the manufacture of those goods, affected or likely to be affected by trade tariffs? Is the business aware of proposed tariffs and their potential impact on the business — and does it have an appropriate strategic response in place, e.g. adapting its supply chain?

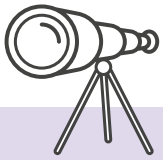
Looking at the stage of the business cycle, there may be a role for internal audit to play in assessing the extent to which the business is forecasting economic risk and is prepared to withstand a downturn. For example, is the ROI of major expansion projects predicated on sustained economic growth? Would such projects fail to complete if financing conditions materially weakened? A major recession may also cause third-party bankruptcies for key business partners in the supply chain, causing indirect disruption. Another consideration is financial leverage — if the business has accumulated significant debt in the low-interest environment it will be at higher risk of default if earnings fall.

8. Managing Risks: A New Framework, by Robert S. Kaplan & Anette Mikes
https://hbr.org/2012/06/managing-risks-a-new-framework

Questions for internal audit

- **Is the business aware of how political risk affects it and its unique operational footprint?**
- **Does the business have a monitoring system in place to identify the development of slow and fast political and economic risks and the need for action?**
- **Does the business have a contingency plan in place in the event of a hard Brexit?**
- **Is the business aware of proposed tariffs and their potential impacts not only on the business's exports, but the inflationary effects of rising import costs on raw materials and other inputs? Does the procurement function have a tariff register and is it kept up to date?**
- **Is the organisation making investment decisions that are commensurate with its stated risk appetite? Do base case investment scenarios account for the potential for a recession?**
- **Are contingency plans and insurance policies in place in the event of third-party/supply chain insolvencies?**
- **Is the company's balance sheet over-levered, putting it at risk of default in the event of a downturn?**

What's new?



Last year 'Political uncertainty' was cited as a top five risk by 23% of CAEs. This year 'Macroeconomic and political uncertainty' was reported to be a priority risk by 29% of CAEs. When we canvassed the opinions of audit executives for Risk in Focus 2019, the trade war between the US and China was just getting started. A year on and the weaponisation of trade policy for economic and diplomatic motives has dominated the news cycle for months. It is abundantly clear that economics has become political and it is difficult to view one risk without also considering the other.

What's more, in our interviews with CAEs, a full 63% said the economy and politics were external factors preoccupying their thinking as they think about their next audit plans, with Brexit and trade tensions frequently referenced. The rise of protectionism and nationalism are symbolic of a politically fractured world in which globalisation is beginning to show signs, albeit very early signs, of reversing.

Human capital: the organisation of the future

Over one-quarter (27%) of CAEs said 'Human resources' (HR) is a top five risk to their organisation, putting it in eighth position in this year's quantitative survey. More than one-third (37%) of interviewees, meanwhile, referenced HR-related issues as priority risks or areas of concern, including talent management and skills shortages and the development of future organisational models.

This theme represents a confluence of factors including technological developments, demographic shifts and changing paradigms over what an organisation can and should look like.

Technological developments

Emerging technologies are already disrupting the nature of work in certain industries by rendering some tasks obsolete while simultaneously creating new ones. Automation capabilities and early applications of artificial intelligence (AI) are transforming jobs, contributing to efficiency, cost reduction and opportunities for scaling.

Forecasts on the impact of technology on the human workforce vary, from a conservative estimate of 75 million jobs to be lost to automation and other technological advances, up to as many as two billion jobs by 2030 if futurist Thomas Frey is to be believed.

Further, around half of current work activities are technically automatable by adapting currently demonstrated technologies,[9] with a large variance in different sectors and for different tasks. Mobility, transport and logistics is one area likely to be deeply impacted. Tesla anticipates fully self-driving cars by the end of 2019, although regulatory approval and trials are expected to delay industrial adoption for some time. This alone has major implications considering that driver jobs constitute 2% of the US economy and is the biggest source of work for the country's male population.

Few occupations, however, consist entirely of activities that can be fully automated. While that could change over the next decade with advances in AI, humans are not expected to be replaced wholesale by robots. Rather, we are entering an era in which people begin to work side-by-side with technology, using it to augment existing tasks. Indeed, one estimate suggests that technological developments have the potential to create up to 133 million new roles, [10] at the same time that other jobs are lost.

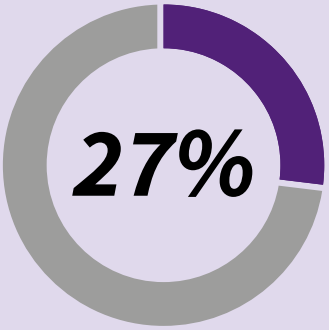
Companies face existential questions such as how humans will work alongside technology and how to train and upskill their workforces to fill new roles that enable the organisation's long-term strategy. If this is not managed effectively, skills gaps at all levels, from the factory floor up to senior management, may hamper the adoption of emerging technologies and therefore growth.

Areas of demand in the skill base include technology design and programming, reflecting the increasingly central role that technology plays in organisations' operations. As manual and repetitive tasks continue to be handed over to algorithms, an emphasis will be placed on human skills and traits that cannot be replicated by software, such as creativity, originality, initiative, critical thinking, persuasion and negotiation, complex problem-solving and emotional intelligence. Companies must already be working to understand what skills they will require in the coming years, aligning this with the forward-looking strategy of the business and how technology will, or is likely to, enable that strategy.

There is already a skill/talent mismatch in Europe. On a year-on-year basis, a majority of countries had a rise in the rate of unfilled vacancies to employment in 2018, with the biggest increases seen in the Czech Republic (38%), Italy (32%) and

9. McKinsey: Jobs lost, jobs gained: workforce transitions in a time of automation https://www.mckinsey.com/~/media/mckinsey/featured%20insights/future%20of%20organizations/what%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/mgi-jobs-lost-jobs-gained-report-december-6-2017.ashx

10. World Economic Forum: The Future of Jobs 2018 http://reports.weforum.org/future-of-jobs-2018/



*Over one-quarter (27%) of CAEs said '**Human resources**' (HR) is a top five risk to their organisation.*

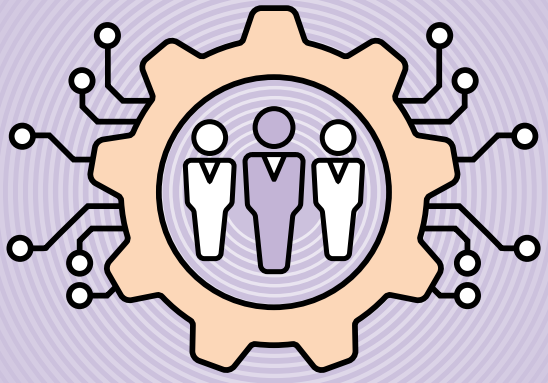
"Partly linked to digitalisation is the strong emergence of agile HR models. I believe this is something that up until now was more restricted to young start-up companies or to project management. I believe this is a development that will much more strongly affect larger organisations and not just the management of projects but the overall structure of organisations. Businesses have to ask themselves - how do we organise ourselves? The traditional hierarchical model that is familiar will have to become more and more flexible; smaller parts of our organisation are innovating with very lean hierarchies, if not working without hierarchies entirely."

CAE, German transport group

"Due to the digitalisation of the business, the development of the market and society, we will need new people skills and a significant change in management approach. It's a very soft kind of risk but very significant. My bank needs to be ready to manage the skills of our people, and if we are not able we will see significant damage to our company. That's very important considering we are a financial institution with a 48-year-old median age. That's very high."

CAE, multinational Italian banking group

*Over **37%** of interviewees, meanwhile, referenced **HR-related issues** as priority risks.*



Austria (28%).[11] This gap is likely to persist and possibly widen with the rapid adoption of enabling technologies.

Companies are under pressure to make themselves more attractive to prospective employees by demonstrating a clear vision. HR recruitment and retention programmes should be put in place to meet that vision and the future needs of the business. As well, since filling skills gaps will be an ongoing challenge for virtually all organisations over the next phase of automation and technology adoption, it should be expected that high-demand technological skills may be in short supply.

Organisational structures

Companies are also faced with the challenge of adapting their structures to keep pace with changing societal expectations and to foster innovation. The traditional hierarchy model has served industries well for the last century, but there is little desire among large, established businesses to increase bureaucracy and add further layers of management. In the face of competitive disruption, businesses are looking to the playbooks of start-ups to see how flatter structures and agile project delivery can deliver improved results.

Concepts such as hierarchy-less organisational models and "intrapreneurship" — the promotion of entrepreneurship within large, established businesses — are gaining traction as a means of improving productivity and the development of fresh ideas, but also to remain competitive in an innovative, fast-changing world. Another defining trend of recent years is for employees not to be located within the company at all, e.g. working from home.

Research is conflicting on the productivity gains than can be achieved through remote working and, for one, IBM decided to partially reverse its homeworking policy in 2017 by asking 2,600 marketing staff to either relocate on-premise or leave the company. This followed decisions in prior years by Yahoo and Reddit to do the same.

The evidence suggests that remote working improves personal productivity — employees already have clear goals and are left to work uninterrupted. But if a company's mission is to innovate or change strategy, then working shoulder-to-shoulder is the better option as it allows for collaboration, problem solving and the sharing of ideas. Of course, a single organisation may benefit from a combination of the two. After all, 40% of IBM's 386,000-strong workforce worked from home prior to its decision to bring a minority of these staff back on site.

Demographic pressures

This workforce strategy is not only about achieving the company's goals. It is important for organisations to meet the wants of today's workforce, the rise of home working in recent years being tied to the entry of younger generations (Millennials and Generation Z, those born after the 1980s) entering the labour force with specific expectations. In order to attract the best talent, companies may have to rethink their social contracts with employees, such as flexible working hours, new incentive and benefit schemes, worker-friendly parental leave, mental health support and agile working.

The theme of putting workers' interests first is reflected in regulation, too. The UK's recently revised corporate governance code stresses the importance of the need for boards to understand the views of the company's staff and describe in the annual report how their interests have been considered in board discussions and decision-making. It recommends achieving engagement with the workforce by, either alone or in combination, appointing a director to the board from the workforce, establishing a formal workforce advisory panel, or designating a non-executive director responsible for worker interests.

This introduces a concept that is already well-established in Germany. Since 1952, companies with 500 to 2,000 employees have been required to have a one-third representation of workers on their boards, rising to half for companies with more than 2,000 staff. While this is a country-specific legal obligation, the recent inclusion of worker representation in the latest iteration of the UK's corporate governance code confirms that adopting the approach innovated by Germany represents best practice.

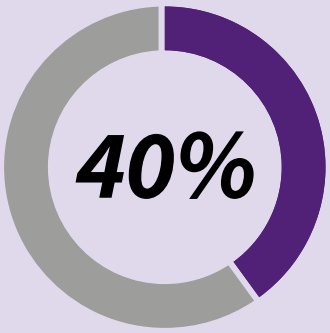
An internal audit perspective

Internal audit has a key role to play in assessing how the organisation is addressing its HR needs. Companies that fail to recruit and retain staff that enable it to realise its forward-looking strategic goals will struggle to achieve adequate growth and meet the needs of their customer base. This is why

11. The Hays Global Skills Index 2018
https://www.hays-index.com/wp-content/uploads/2018/09/Hays-Global-Skills-Index-2018-Report.pdf

"There's a lot going on in the people space, whether it's the gender pay gap, minimum wage, labour unions or the changing economy. How do you develop a more flexible working model for a generation of people who are used to or want two or three jobs? You get guys who want to do certain hours in-store, also want to be an Uber driver and do other things. Are we flexible enough to accommodate that when we've got a fairly rigid and historical model that is based around working 9-5? That's changing. There's a lot of press about employers enforcing that on people, but we're finding that our staff are pulling on that."

CAE, international UK retailer

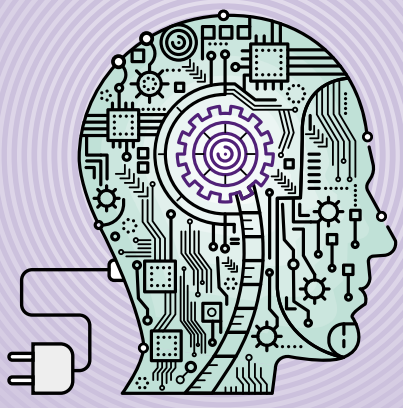


*of IBM's **386,000**-strong workforce **worked from home** prior to its decision to bring a minority of these staff **back on site**.*

Technological developments have the potential to create up to

133 million

new roles at the same time that other jobs are lost.



Source: World Economic Forum

"There is a technical skills gap in certain areas such as data and the way we manage and govern the data. We need to attract more data talent. And the other risk is how to retain that talent once it has been hired into the company. That's not only linked to how we manage salaries, although that is a clear point, but the governance of the company, the way we work, the way we follow our key people and develop key talent is a big issue in retaining people."

CAE, French international retail group

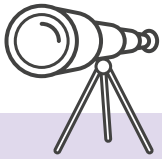
it is so important that recruitment is aligned with strategy and for internal audit to query the extent to which HR initiatives aimed at addressing skills gaps are fully aligned with the strategy set by senior management. In large companies this may require the adoption of "people analytics", i.e. data analytics applied to HR that help businesses to make smarter, more strategic and more informed talent decisions.

Undoubtedly, digital skills related to automation and emerging technologies will become increasingly central to the future success of commercial companies. So internal audit should assess the company's ability to identify any current or future skills gaps, what is being done to fill those gaps and if the audit function itself can attract the necessary talent to meet the organisation's assurance needs.

Internal audit can also play a supporting role in companies' transition to new organisational models and methods of working. Audits can be directed at evaluating whether the existing organisational model still fits with the strategy and demands from the environment in which the organisation is operating. It should also assess whether any shift to a more innovative, less hierarchical model is being implemented effectively, productivity is being tracked and, in its advisory role, give a risk-control perspective; this is because adapting to new working models is likely to fundamentally impact existing control environments. As a follow-up to this, it can offer an independent view on the success of any changes to the organisational model.

Questions for internal audit

- **How effective are the organisation's recruitment, talent development and career progression initiatives?**
- **Are the business's recruitment efforts addressing any skills gaps? Is the business hiring the right talent and is it attractive enough to meet its medium to long-term strategic goals?**
- **What are the likely impacts of automation and other digitalisation on the workforce, and is the business ensuring it has the skills required to enable that technology?**
- **Is the current organisational model effective or is it hampering the strategic goals and are efforts being made by the organisation to evaluate and address this?**
- **If the company has transitioned to a new model or style of working, or if it is in the process of doing so, to what extent have those transitions also incorporated necessary changes to control processes?**



What's new?

HR risk is a common priority and has featured in previous editions of this report in some form. Over one-quarter (27%) of CAEs in our surveys said that HR is a top five risk to their organisation, representing a 36% year-on-year fall on the 42% who said the same last year.

Further, 37% of interviewees referenced workforce-related and organisational issues as priority risks or areas of concern, such as talent management and skill shortages or adapting to future organisational models.

The reality is that organisations, especially private sector companies, are under pressure to stay relevant as new technologies emerge and are rapidly adopted. The most innovative companies will attract the best talent, exposing others to skills shortages, in the digital field especially. The challenge is not only in attracting the right people with the required skills and expertise, but in structuring organisations in ways that deliver increased productivity and innovation. This will require businesses to reconsider their operating models and whether they need to be overhauled.

Governance, ethics & culture: the exemplary organisation

'Corporate governance and reporting (financial & non-financial)' was cited as a top five risk by 26% of CAEs in this year's survey, broadly in line with last year's findings (22%). While this puts this risk down in ninth place, governance is receiving considerable attention from internal audit. We found that 53% of CAEs said corporate governance was one of the top five risks on which their functions spend most time and effort, behind only cybersecurity (68%) and regulation/ compliance (61%).

Europe is in the process of bringing its governance standards up to date with the introduction of the Shareholder Rights Directive II (SRD II), which had a transposition date of 10 June 2019. The purpose of the directive, an amendment to SRD I which was introduced in 2007, is to strengthen the position of shareholders and ensure that business decisions are made with long-term stability and sustainability in mind.

Corporate governance concerns how responsibly a company is run, the appropriateness and effectiveness of decision-making, and the accuracy of reporting — the interests of shareholders being central to maintaining high standards of governance. Corporate social responsibility (CSR), meanwhile, is a form of corporate self-regulation that aims to align the company's impact and objectives with the interests of the wider stakeholder community, factoring society into the equation. Regulation plays its part in driving CSR, specifically with regard to transparency. For instance, the EU Non-Financial Reporting Directive, applicable since January 2017, although still being transposed into member states laws (Spain for instance went live at the beginning of 2019), mandates that listed companies report on their CSR efforts — but not that CSR efforts are made. However, by increasing transparency with compulsory disclosures, companies are being motivated to take action.

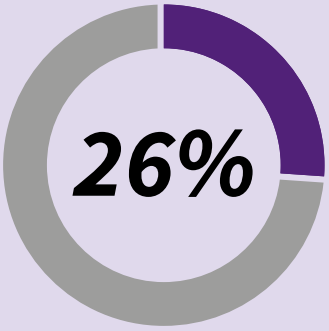
Traditionally, corporate governance and CSR have been seen as representing conflicted interests: profit maximisation for shareholders not being aligned with efforts to meet the interests of society. Increasingly these two concepts are occupying the same territory, with CSR now considered as falling under the umbrella of corporate governance. Rather than simply maximising value for shareholders, companies are expected to maximise value for the wider stakeholder community. Accordingly, the core CSR principle of long-term sustainability is being woven into updated corporate governance codes and legislation. This convergence has paved the way for corporate governance to be driven by high ethical standards and the need for accountability, to the public as well as investors.

The "exemplary organisation" therefore is one that is both well governed in the traditional sense and makes determined efforts to prevent harm to individuals, society and the environment and live up to its publicly stated standards (although, for emphasis, environment-related risk has been given its own topic, as sustainability does not account for the exogenous impacts of climate change. See page 61).

Regulators and governments in Europe have pushed to improve corporate governance and CSR standards in recent times. Since 2018, French companies and multinationals with more than 10,000 staff in the country have had to comply with the Le devoir de vigilance (the Corporate duty of vigilance law), which has bound companies to publish vigilance plans with the goal of preventing environmental harm, human rights abuses and corruption in their own operations and those of their subsidiaries, sub-contractors and suppliers.

"We are feeling more and more vulnerable in the court of public opinion with issues related to human rights. We expect increased scrutiny and therefore we want to be much more prepared in making sure that we are compliant with our own policies. In a way it is linked to the fact that we have been much more explicit in the last few years about our values in our policies - our intentions are totally transparent. There need to be controls to make sure those strategies are supported by actions, otherwise the numbers in the report are arbitrary. It's not just financial analysts and investors, it's also the employees and consumers who are paying attention to this."

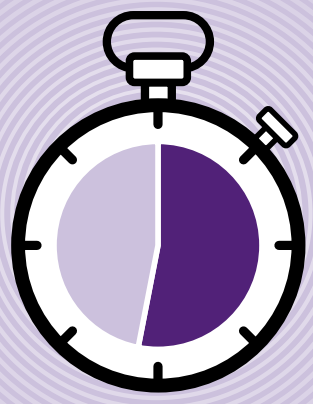
CAE, multinational Dutch consumer goods group



*'Corporate governance and reporting (financial & non-financial)' was cited as a **top five risk** by 26% of CAEs in this year's survey.*

53%

*of CAEs said **corporate governance** was one of the **top five risks** on which their functions spend most time and effort.*



"Managers, board members, everybody is more personally accountable today and so we need to be sure that the way the bank is organised and the efficiency of the governance allows managers to get the right information at the right time to be able to make the right decisions. That means auditing the governance. We may need to reinvent the methodology of how we audit that area, but I am personally convinced that is a new risk area."

CAE, French international banking group

The introduction of the 2018 UK Corporate Governance Code, effective since January 2019, expanded the scope of existing "comply or explain" rules to take a more CSR-centred approach. While the code does not explicitly define social responsibility requirements, it stresses the importance of strong culture and dialogue with a wide range of stakeholders in promoting long-term, sustainable business success. Similarly, the latest Dutch Corporate Governance Code, effective since January 2018, places an emphasis on serving the interests of external stakeholders outside of the shareholder base, in accordance with its central theme of "long-term value creation".

Corporate conduct and culture

As mentioned earlier in this report, risk topics do not exist in a vacuum — they overlap and impact upon each other. Culture is intrinsically linked to corporate conduct, governance and ethics. The culture of an organisation is the living, breathing manifestation of its ethics and principles. Regulators have come to understand this — this is why culture figures highly in the modernised Dutch and UK corporate governance codes.

We found that 22% of CAEs reported that 'Corporate culture' is a top five risk in this year's survey. Again, this is broadly in keeping with last year's findings (25%); however, while CAEs reported spending significant time auditing corporate governance, only 17% of them said that culture is one of the top five risk areas on which it spends most of its time and effort.

There are a number of possible explanations for disparities between organisations' primary risks and where internal audit's assurance resources are focused; it does not necessarily mean that internal audit is not adopting a sufficiently risk-based approach. For instance, bandwidth may be allocated to compulsory regulatory audits, taking the attention away from non-compulsory priority areas; or assurance may be provided by the second line of defence or other functions of the business (all the while ensuring that the business and internal audit are clear as to who is providing assurance for what risk areas).

There is a possibility, however, that internal audit is still getting to grips with how best to approach auditing culture. Given its significance to corporate governance, behaviour and ethics, CAEs should think carefully about whether they are falling short by failing to deliver an assurance on corporate culture.

Ethics — an ever broader scope

As an area of corporate risk, ethics has an increasingly broad scope. Gender equality and diversity in the workplace have become central to the topic in recent years as there is an expectation that businesses' workforces, including senior management and boards, are representative of diversity in the outside world. This is reflected by the EU's non-financial reporting requirements on diversity.

*"**Risk topics** do not exist in a vacuum — they overlap and impact upon each other."*

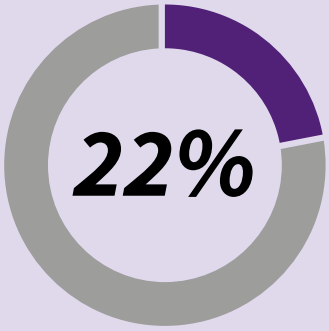
Some business models such as payday lending or discount alcohol retailing are overtly at odds with today's social ethics. Then there are business models which are not inherently bad as long as they are well governed and non-exploitative, such as manufacturers using credible suppliers with high standards in low-labour-cost countries.

But there are other, more subtle considerations for businesses in today's more socially aware environment. For instance, a clothing company may carry out robust due diligence on it suppliers and be confident that it is not causing social or environmental harm internally or in its supply chain; however, if it releases clothing designs that offend cultural or religious sensitivities, this could cause the business considerable reputational and financial damage. Multinationals with operations far away from their corporate headquarters, where centralised product and marketing decisions are made, have to be increasingly mindful of such missteps.

Data too has become a point of contention. Attention is turning to big tech firms and their use of personal data for commercial gain. Companies such as Google and Facebook have inevitably

"A new risk we are facing all over the world is to what extent the design of our clothes are culturally appropriate. We do not want our products to be culturally offensive. Last year H&M had issues in South Africa after the design of its clothes were deemed offensive. You're now seeing issues at Gucci with designs being seen as racially offensive. We have had some issues in the past. In China we have a different perspective. There are geographical and territorial issues that are very sensitive, such as we cannot refer to Hong Kong or Taiwan as countries. There are issues with the government there because of that."

CAE, Spanish multinational clothing company

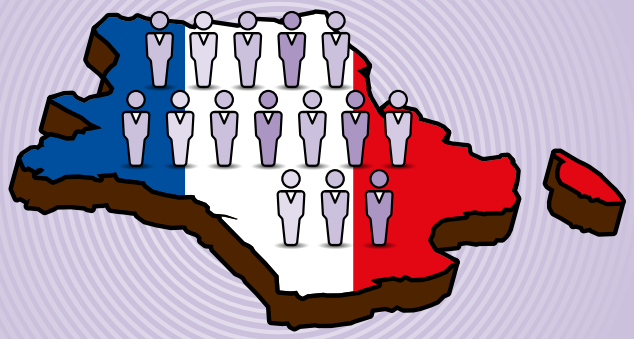


22% of CAEs reported that 'Corporate culture' is a top five risk in this year's survey.

Since 2018, French companies and multinationals with more than

10,000 staff

in the country have had to comply with the Le devoir de vigilance (the Corporate duty of vigilance law).



"There is considerable negative sentiment around companies and data ethics if buying patterns and behaviours online are reflected in their ads being presented to us online. People are starting to feel that they are being surveilled and that their data is being misused. That's something that companies are concerned about."

CAE, Swedish professional services firm

been the first port of call for authorities enforcing the EU's new GDPR rules. But deeper concerns are emerging. Legislators, regulators and society are beginning to question data ethics, including the intrinsic value of their personal data and how companies should be licensed to use it. This has rapidly become a matter of priority. For instance, Facebook has been heavily criticised for being unwilling to accept accountability for the downstream effects of content and advertising on its platform, which has been blamed for eroding democracy and fuelling political polarisation. As companies pursue digitalisation initiatives that include data analytics, machine learning and AI, the governance and unbiased processing of such data will become an increasingly significant ethical consideration that needs to be addressed.

An internal audit perspective

Corporate governance has long been an area of focus for internal audit and this remains the case. Shareholders deserve for the companies they own to be well run and internal audit can augment governance by assessing the extent to which internal reporting is effective, i.e. do the right people receive the right information at the right time in order to make the right decisions? Moreover, it is increasingly expected that companies are well run in the interests of a wider stakeholder group that includes employees, customers, regulators and the society as a whole.

As corporate governance and CSR converge, and with the introduction of regulatory requirements to disclose non-financial performance, there is a need for businesses to understand how they impact the world around them. Is the business sustainable and does it live up to today's ethical standards with regard to its social impact? Importantly, is the company as sustainable as it claims to be in its annual reports? In the first instance, internal audit may choose to check that the company is reporting everything that is required of it. In due course, internal audit may choose to go further by assessing the robustness of controls that underpin the sustainability strategy and enable the organisation to reach its goals, including assessing non-financial reporting inputs and metrics to determine whether sustainability disclosures are accurate.

As it has come to be accepted that culture is a critical ingredient of strong governance, there will be a desire among boards to understand the true nature of this culture. Internal audit can be the board's barometer for this, assessing the extent to which the tone at the top filters through the organisation, the way decisions are made and implemented, and problems are discussed openly to learn from them. An organisation may strive to be exemplary, holding itself to a high standard, but there is a risk that its core values, ethics and virtues are not reflected in the culture and everyday behaviour of middle management and other staff.

Questions for internal audit

- **How mature is the organisation's governance and what evidence is there to support this?**
- **Is the company fully compliant with non-financial reporting requirements?**
- **Are the processes behind non-financial reporting robust and do they support the accurate reporting of sustainability metrics?**
- **To what extent are the business's claims with regard to sustainability reflected in the operations of the business, i.e. is the business what it says it is?**
- **Are the company's stated values and ethics aligned with those of the society and are they reflected in the culture of the organisation?**
- **Is the organisation's culture in line with the strategy and specified core values of the organisation?**
- **Is the company aware of cultural/religious sensitivities in its products and marketing?**
- **Are the business' personal data strategies likely to be seen as exploitative, even if they are compliant with GDPR? Is the business aware of changing ethical expectations?**

Climate change: risk vs opportunity

More than one in ten (14%) CAEs in this year's survey cited 'Environment and climate change' as one of the top five risks to their organisation (although only 3% reported it as being their organisation's single biggest risk). While this is relatively low, it represents a 75% annual increase on the 8% of CAEs who referenced the environment and climate change as a priority risk last year. What's more, a full 28% of internal audit chiefs foresee this being a priority risk by 2025.

Climate change and its downstream impacts, from extreme weather events to forced migration, is a more significant business risk today than ever before and there is little evidence of this abating in the short or even medium term. Government efforts to curb human-made impacts on the climate are only in their earliest stages and are likely to persist for decades to come.

Once again, the World Economic Forum's Global Risks Report was unequivocal in this regard. Canvassing the perceptions of business, government, civil society and thought leaders, for the third year running environmental threats dominated. Of the number one most likely risk to impact the world, extreme weather events topped the list with other closely related risks heavily represented.

Last year proved that climate change is not a looming phenomenon: 2018 saw unprecedented heatwaves in Japan and Oman, California's worst wildfire on record, Typhoon Mangkhut devastate the Philippines and Hong Kong, Hurricanes Florence and Michael hit the east coast of the US, and a new peak in carbon emissions of 37.1 gigatonnes.

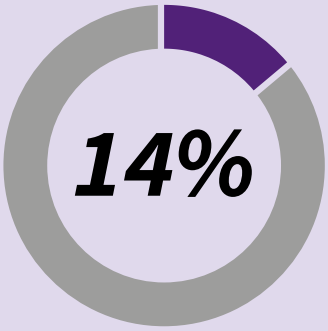
While governments have begun to take tentative steps to tackle climate change, activists are demanding more urgent action. Protest group Extinction Rebellion brought parts of central London to a standstill for 11 days in April 2019 and says it has more acts of civil disobedience planned, including a proposed global workplace strike on 20 September. Inspired by Nobel Peace Prize nominee Greta Thunberg, the 16-year-old who protested outside Sweden's parliament last year, young students have begun to stage worldwide school strikes and vowed to continue boycotting classes on Fridays until their countries adhere to the 2015 Paris Agreement, which aims to prevent global temperatures from rising 1.5C above pre-industrial levels.

What this means for business

From a business perspective, risks related to the environment are both endogenous and exogenous. The endogenous perspective concerns sustainability issues. Businesses must think about the outward impact their operations have on the environment, such as air pollution, water contamination, the manufacturing of disposable un-recyclable plastics, or draining resources in the making of their products.

*"**Climate change** and its downstream impacts, from extreme weather events to forced migration, is a **more significant business risk today** than ever before."*

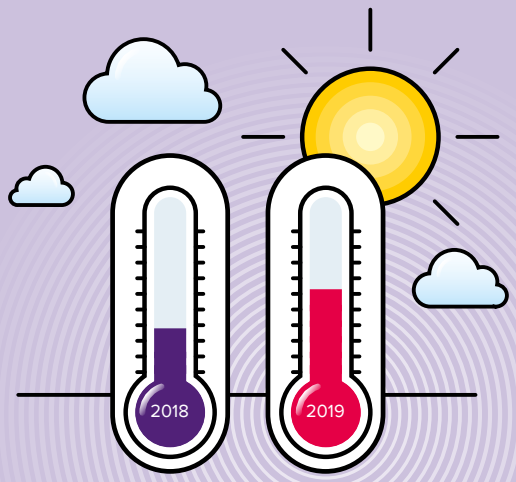
Climate change risks meanwhile are exogenous and refer to forces outside of an organisation's control that have an inward impact, such as rising sea levels and wildfires. Like politics and the economy, this may not be seen as a risk in itself, but a causal force that can lead to the emergence of numerous other risks. These external forces themselves may not be under a company's control, but how a company responds to and



*of CAEs in this year's survey cited '**Environment and climate change**' as one of **the top five risks** to their organisation.*

"There are limited resources, so in the future will there be enough water? Will there be enough electricity? How do we source those fundamental resources that any business needs? What do the 10-20 year plans look like? I would like to see internal audit looking into how companies maintain their security in the future and what the long-term plans are, in the same way that HR plans are being looked at. I don't see that happening. Companies are working in three-year cycles. They are too short term."

CAE, Swedish professional services firm



It represents a

75% annual increase

*on the 8% of CAEs who referenced the **Environment and climate change** as a priority risk last year.*

"The other area we will do more on this year is around environmental and sustainability risks. That's a very real issue and speaks to a number of angles. At some point there will be a tipping point for investors and if you're not doing everything you can do regarding sustainability, your share price will be harmed. It also speaks to business resilience and success going forward. If you're not thinking three to five years ahead then you'll find yourself paying more for goods and that becomes a success issue. Another really big factor will be transport. At what point will the government stop you delivering in diesel lorries and have we planned enough and are we prepared enough to upgrade the fleet? The whole environmental transport piece will be a big issue in five years."

CAE, international UK food retailer

steels itself against these forces is very much within its powers.

Companies are not exposed to the same number or severity of environmental-related risks. Depending on their sector and geography, climate change — as an external, causal force — precipitates an array of direct business risks, including: physical and operational (e.g. business continuity and supply chain disruption from weather events), reputational (e.g. negative customer and investor sentiment), regulatory and legislative (e.g. China, India and various European governments placing bans on future fossil fuel car sales), strategic (e.g. the existential threat to fossil fuel producers or consumer companies that ignore shifting customer preferences), financial (e.g. the potential for carbon pricing initiatives to be rolled out worldwide) and so on.

Real-world impacts of climate change in the business world are fast emerging. Last year's Camp Fire, California's largest wildfire on record which claimed 86 lives and destroyed 14,000 homes, was caused by a power line owned by Pacific Gas and Electric coming into contact with nearby trees. Facing billions of dollars in claims, California's largest utility filed for bankruptcy protection in January 2019 citing as one of its reasons "significant increase in wildfire risk resulting from climate change". The media have dubbed this "the first climate change bankruptcy".

The business impacts of climate change are not always so dramatic. Water shortages are putting pressure on beverage groups, which require multiple litres of water produce a single litre of their products. Asset-heavy industries such as telecommunications, meanwhile, are feeling the effects of attrition, network infrastructure having to be more frequently maintained to bring it back online after freak weather events and upgraded to be more resilient to the elements.

In the financial services sector, insurance firms are having to pay out higher volumes of weather-related claims. It is estimated that natural disasters and extreme weather caused around $160bn worth of damage in 2018, only $80bn of which was insured against.[12] The agricultural sector continues to be hit by droughts, causing food shortages and increasing default risk for banks lending into the industry.

Capitalising on climate change

Money talks and when investors speak, businesses listen. In his most recent annual letter to corporate leaders, Larry Fink, CEO of BlackRock, said: "Your company's strategy must articulate a path to achieve financial performance. To sustain that performance, however, you must also understand the societal impact of your business as well as the ways that broad, structural trends... [including] climate change affect your potential for growth."

BlackRock, the largest asset manager in the world, with $6.5trn under management, is not the only major investor calling for action. The Institutional Investors Group on Climate Change, a consortium of more than 400 investors representing more than $32trn in assets, in December 2018 urged both governments and businesses to take action "with the utmost urgency" to fulfil the goals of the Paris Agreement, saying companies that "enact strong climate and low carbon energy policies will see significant economic benefits and attract increased investment that will create jobs in industries of the future".

*"Real-world impacts of **climate change** in the business world are **fast emerging**."*

Calls to action are being acknowledged by the most forward-thinking companies. The Alliance of CEO Climate Leaders, a group of CEOs with collective company revenues of more than $1.5trn, have already reduced their aggregate emissions by 9% since 2015 and are committed to further cuts. In addition to advocating for improved analysis and reporting of climate-related financial risks, the alliance has and continues to set science-based carbon emissions targets, reduce energy use, switch to renewable forms of power and work with partners in their supply chains to dial back on emissions.

12. Munich Re: Extreme storms, wildfires and droughts cause heavy nat cat losses in 2018
https://www.munichre.com/en/media-relations/publications/press-releases/2019/2019-01-08-press-release/index.html

Natural disasters and extreme weather caused around

$160 billion

worth of damage in 2018. Only $80bn of which was insured against.

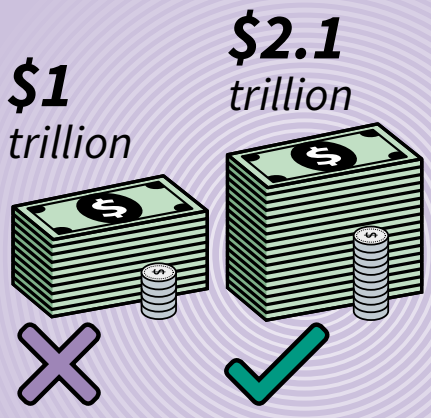
Source: Munich Re

"**Renewables** are at an inflection point. It now **costs less** to deliver a unit of energy from solar than it does from coal. When you have got that tipping point, where it's actually cheaper to produce energy from renewables, then obviously the market's going to move away from fossil fuels. And if you're **not strong** in those markets then that becomes a risk."

CAE, UK manufacturing group

"Climate change is becoming **more prominent** but for our organisation it is an **opportunity** rather than a risk, as we are offering **energy efficient solutions** to run solar farms or use green energy with wind turbines and the like. We have elements in our portfolio that help our clients to **address challenges** related to climate change. So that is looked at less from a risk perspective and more through an opportunity lens."

CAE, German multinational industrial conglomerate



*215 of the world's largest companies have valued **climate risks** to their businesses at almost **$1trn**; these same companies calculated that **climate business opportunities are worth some $2.1trn**.*

Source: CDP

"A really strongly emerging risk is **climate change**, which is especially relevant for our networks. We used to be able to spend a good part of the summer months maintaining and developing networks, but we are now spending most of that time repairing them because of all the **floods** and tempests that are **damaging the infrastructure**. You can really see the effects of climate change in action. That links with another risk which is **business continuity**. The way we do our risk management, a lot of these things we would have as causes. So in the past climate change has been a **cause of business outage**."

CAE, international French telecoms group

Firms that pay attention to stakeholders and take a stand on sustainability and climate resiliency and adaptation are in a better position to retain and win customers. In this sense, climate change should be seen not only as a risk but a commercial opportunity. For instance, a group of 215 of the world's largest companies have valued climate risks to their businesses at almost $1trn; these same companies calculated that climate business opportunities are worth some $2.1trn, nearly all of which are highly likely or virtually certain.[13] Long-term government efforts to decarbonise the economy will create new growth sectors and sub-sectors, such as electric mobility and other energy-efficient technologies. Climate-related opportunities include increased revenue through demand for sustainable products and services and increased capital availability as institutional investors favour low-carbon companies. Progressive businesses can secure their future success by aligning their strategic goals with those of governments, investors and society at large.

This can be as simple as setting and meeting sustainability targets such as reducing energy consumption and carbon emissions, to the more ambitious objective of remodelling the business's product or service offering itself. Toyota's launch of its hybrid Prius, for instance, was a risk that paid off. Between 1999 and 2014 the company sold 1.5 million of the fuel-efficient cars in the US alone, taking more than a 50% share of the hybrid vehicle market. As a first-mover, the Japanese company capitalised on changing attitudes towards climate change and carbon emissions. It hopes to repeat that success with Mirai, its new model powered by hydrogen fuel cells whose only emission is water. Companies whose products and services are future-proofed in this way stand themselves in good stead to grow and succeed.

An internal audit perspective

As a component of CSR, companies need to think carefully about how their operations impact upon the environment. There is a compliance dimension in that companies need to be operating within the boundaries of environmental and sustainability laws, as mentioned in the previous topic. More fundamentally, senior management must be aware that companies with strong environmental sustainability credentials are favoured by major institutional investors, a key source of financing, and customers alike. There should be a clear understanding that climate change is not only a risk, but one of the biggest business opportunities of this era.

Long-term efforts to phase out fossil fuels, bring down carbon emissions, reduce plastic waste, and conserve water and other resources pose an existential threat to all manner of sectors including energy production, transportation, manufacturing, agriculture and food production. But equally this long-term trend represents an opportunity to take action and meet society's needs. Internal audit can evaluate how such considerations are factored into senior management's strategy development and seek evidence for how climate-conscious operational and strategic decisions are being linked to growth forecasting.

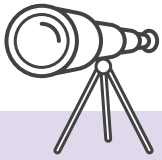
Climate change may not feature on the organisation's risk register, but senior management needs to be thinking about the extent to which the downside knock-on effects of climate change affect the risk profile of the organisation. Internal audit should consider whether any risk assessment has been carried out to determine these potential impacts and, if not, should report this to the board who can request that management take action. Climate change and the increasing frequency of extreme weather events is affecting business continuity and there is a role for internal audit to assess whether the monitoring systems to identify this impact are working, and if the organisation's insurance policies and operational contingency plans are fit for purpose.

13. CDP (formerly the Carbon Disclosure Project): Global Climate Change Analysis 2018

Questions for internal audit

- **Is the business aware not only of how its operations impact upon the environment, but also how climate change impacts upon the business's operations and its long-term strategy?**
- **What is the correlation between the organisation's efforts to address environmental sustainability, its reputation among investors and customers, and its growth?**
- **Is senior management mindful of the increasing expectations of major institutional investors with regard to green credentials? Is the business communicating with the markets effectively on this matter?**
- **Does the business model leave the company prone to activist intervention and public shaming?**
- **Do insurance policies cover physical damage caused by the effects of climate change? Do these policies need to be reviewed and updated?**
- **Does the long-term target of reducing carbon emissions, reducing waste and conserving resources pose a threat to the current business model and, if so, what is the company doing to adapt?**
- **Are innovation and product development programmes aligned with the long-term climate goals of governments and society?**
- **Do societal changes initiated by climate change offer the organisation opportunities for new business and, if so, what is the business doing to utilise these (before others do)?**
- **Can internal audit support any strategic transition by reviewing how any strategic change has affected the operations of the business, either positively or negatively?**

What's new?



In the previous edition of this report, 8% of the CAEs we surveyed cited 'Environment and climate change' as a top five risk; this has nearly doubled to 14% this year. Environmental and social ethics was featured as a hot topic last year, with CAEs' focus being on the regulatory aspects of environmental sustainability, such as integrated reporting. This year, however, we find that audit executives are paying attention to the action of climate change itself, with 17% of our interviewees highlighting such issues alongside environmental sustainability.

Concerns vary. Banks with exposure to the agri-food sector are seeing issues in their portfolios related to weather conditions. For instance, agricultural debtors in Australia are facing the hottest drought in their lifetimes, weakening their ability to repay loans. In telecoms, infrastructure is being physically affected, requiring higher capital expenditure allocations for maintenance purposes. From a strategic point of view, businesses are increasingly being forced to evaluate their futures in a changing physical environment and as governments come under heavy pressure to avert catastrophe.

Sources

1. Online Trust Alliance's 2018 Cyber Incident & Breach Trends Report

   https://www.internetsociety.org/wp-content/uploads/2019/04/2018-cyber-incident-report.pdf

2. DLA Piper GDPR data breach survey: February 2019

   https://www.dlapiper.com/en/uk/news/2019/02/dla-piper-gdpr-data-breach-survey/

3. Thomson Reuters: Cost of Compliance 2018

   https://legal.thomsonreuters.com/content/dam/ewp-m/documents/legal/en/pdf/reports/cost-of-compliance-special-report-2018.pdf

4. International Federation of Accountants: Regulatory Divergence: Costs, Risks and Impacts

   https://www.ifac.org/publications-resources/regulatory-divergence-costs-risks-and-impacts

5. UNESCO: Statistics on Youth

   http://www.unesco.org/new/en/unesco/events/prizes-and-celebrations/celebrations/international-days/world-radio-day-2013/statistics-on-youth/

6. Institute for Crisis Management: Annual Crisis Report

   https://crisisconsultant.com/wp-content/uploads/2014/11/ICM-Annual-Crisis-Report-for-2017.Issued-April-17_2018_print.pdf

7. Vanguard: Known unknowns: What are the odds of a recession?

   https://www.vanguardinvestor.co.uk/articles/latest-thoughts/markets-economy/known-unknowns

8. Managing Risks: A New Framework, by Robert S. Kaplan & Anette Mikes

   https://hbr.org/2012/06/managing-risks-a-new-framework

9. McKinsey: Jobs lost, jobs gained: workforce transitions in a time of automation

   https://www.mckinsey.com/~/media/mckinsey/featured%20insights/future%20of%20organizations/what%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/mgi-jobs-lost-jobs-gained-report-december-6-2017.ashx

10. World Economic Forum: The Future of Jobs 2018

    http://reports.weforum.org/future-of-jobs-2018/

11. The Hays Global Skills Index 2018

    https://www.hays-index.com/wp-content/uploads/2018/09/Hays-Global-Skills-Index-2018-Report.pdf

12. Munich Re: Extreme storms, wildfires and droughts cause heavy nat cat losses in 2018

    https://www.munichre.com/en/media-relations/publications/press-releases/2019/2019-01-08-press-release/index.html

13. CDP (formerly the Carbon Disclosure Project): Global Climate Change Analysis 2018

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 umfassende 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

info@diir.de
www.diir.de

DIIR Deutsches Institut für Interne Revision e.V.