RISK IN FOCUS 2019

HOT TOPICS FOR INTERNAL AUDITORS

ECIIA
EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING

Instituto de Auditores Internos de España

CONTENTS

2 FOREWORD

3 INTRODUCTION

4 CYBERSECURITY: IT GOVERNANCE & THIRD PARTIES

8 DATA PROTECTION & STRATEGIES IN A POST-GDPR WORLD

12 DIGITALISATION, AUTOMATION & AI: TECHNOLOGY ADOPTION RISKS

16 SUSTAINABILITY: THE ENVIRONMENT & SOCIAL ETHICS

20 ANTI-BRIBERY & ANTI-CORRUPTION COMPLIANCE

24 COMMUNICATIONS RISK: PROTECTING BRAND & REPUTATION

28 WORKPLACE CULTURE: DISCRIMINATION & STAFF INEQUALITY

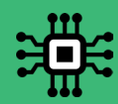
32 A NEW ERA OF TRADE: PROTECTIONISM & SANCTIONS

36 RISK GOVERNANCE & CONTROLS: ADAPTING TO CHANGE

38 AUDITING THE RIGHT RISKS: TAKING A GENUINELY RISK-BASED APPROACH

42 SOURCES










FOREWORD

Now in its third year, Risk in Focus: Hot Topics for Internal Auditors is more ambitious than ever. This edition is the result of a collaborative effort between seven European institutes of internal auditors in France, Germany, Italy, the Netherlands, Spain, Sweden and the UK and Ireland.

As previously, we interviewed Chief Audit Executives (CAEs) in all of these territories and across sectors as part of our qualitative research into priority risk areas that are expected to be addressed in audit plans for 2019 — and further into the future.

To supplement the interview process, this year for the first time we distributed a survey that received 311 responses. This quantitative research augmented the overall report by providing data on the biggest risks that CAEs believe their organisations face and where internal audit is spending its time.

The European institutes of internal auditors are immensely grateful to everybody who contributed to this report, both the 300-plus CAEs who responded to our survey and especially the 42 executives who gave up their time to be interviewed. Without their vital insights this report would not have been possible.

September 2018

HOT TOPICS FOR INTERNAL AUDITORS

The purpose of Risk in Focus is to provide a touchpoint for the internal audit profession that helps CAEs to understand how their peers view today's risk landscape. Working hand-in-hand with boards, audit committees and other stakeholders, internal audit should already have a rigorous understanding of their organisations and the greatest financial, operational and strategic risks they face. However, it is vital that knowledge and thinking is shared within the profession to reinforce risk assessments and mapping and, ultimately, to support the provision of greater assurance.

While many audit functions will be preoccupied with business-as-usual operational audits, and all should be focused on areas specific to the assurance needs of their organisations, the hot topics in this report represent themes that are relevant across industries, with an emphasis on new and emerging risks. To be clear, this list is not exhaustive and we expect internal audit to take an appropriately risk-based approach to its work by addressing organisations' greatest priorities. The topics listed herein should therefore be treated as a reference point rather than audit planning guidance.

The most sophisticated audit functions will not only test internal control systems but support their business in identifying risks looming on the horizon. We hope this report serves as a valuable resource for CAEs in evaluating risks they may not have considered, or contemplate from fresh angles risks that are already on their radar screens. Some readers may recognise themes from their own risk assessments and they should take comfort from this. It is confirmation that they are risk-aware. Others may find the highlighted topics help them to shape their forthcoming audit plans.

As last year, we interviewed CAEs from right across Europe to gauge their opinions. This time, however, a quantitative survey was also carried out. The hard data from the survey (see below) complements the qualitative research we undertook by showing, at the highest level, priority risks that organisations face, as identified by their CAEs, and quantitative results are included in the relevant topics. The interviews, meanwhile, allowed us to dig deeper and draw attention to more granular issues related to these broad priority risks.

For the most part, there was little discernible difference between CAEs' top risks in the various countries and sectors in this quantitative sample, although we did find that the Netherlands is the only country in which culture was cumulatively cited as the biggest risk facing organisations. This is consistent with the introduction of culture as a component of effective corporate governance in the country's revised Corporate Governance Code, introduced at the beginning of 2018.

Similarly, in our qualitative sample half of the Dutch interviewees raised the importance of corporate sustainability issues related to the environment and social ethics, which corresponds with the revised Code's emphasis on long-term value creation's explicit link to "the environment, social and employee-related matters". We also found that two-thirds of French interviewees underscored the need to look at anti-bribery & anti-corruption (ABC) compliance, higher than for any other country. This correlates with the recent introduction of the country's Sapin II law.

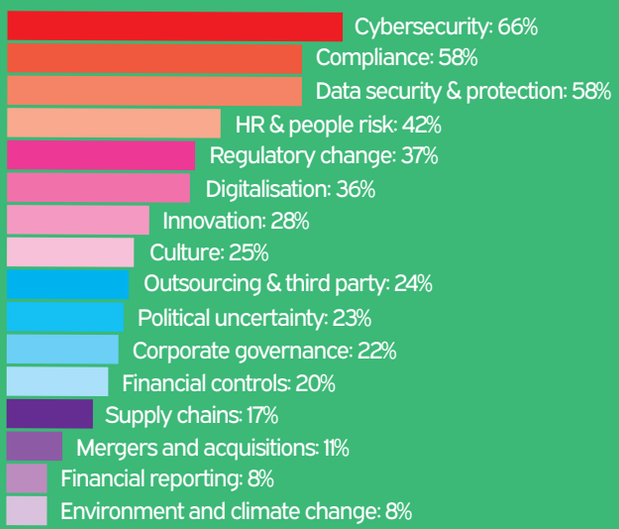
We are aware of the limits of ascribing statistical significance to the analysis of a qualitative sample of 42 executives spread over seven territories. We therefore ask readers to draw their own conclusions from these observations and we do not suggest they indicate that organisations in other countries should treat ABC compliance, culture or sustainability risks as any less of a priority.

We hope you enjoy this year's edition of Risk in Focus and, as ever, we welcome your feedback and engagement.

What is the single most important risk that your organisation faces?

- Cybersecurity: 15%
- Compliance: 13%
- Digitalisation: 9%
- Regulatory change: 8%
- Political uncertainty: 8%
- Data security & protection: 6%
- Culture: 6%
- HR & people risk: 5%
- Innovation: 5%
- Corporate governance: 3%
- Outsourcing & third party risk: 3%
- Financial controls: 3%
- Supply chains: 2%
- Mergers and acquisitions: 1%
- Financial reporting: 1%
- Environment and climate change: 1%
- Other (unspecified): 11%

Which of the following are one of the top five risks your organisation faces?



CYBERSECURITY: IT GOVERNANCE & THIRD PARTIES

Cybersecurity has been a high-priority risk for a number of years and this shows no signs of abating. Companies are pushing to move away from legacy systems and, as approaches to managing cyber risk mature, attention is turning to third-party defensibility.

In our quantitative survey of more than 300 CAEs we found that cybersecurity is considered the biggest risk to their organisations. Two-thirds said it was one of the top five risks and 15% cited it as the single biggest risk, ahead of compliance (13%), digitalisation (9%), regulatory change (8%) and political uncertainty (8%). As might be expected, our qualitative research found that all CAEs have this area earmarked for their 2019 audit plans in some form, mirroring our findings from previous years' reports.

Whether referred to as cybersecurity, IT security, information security or any other name, the need to defend networks and the data that resides on them is here to stay. The sophistication of adversaries, including nation states, and the constantly changing nature of the threat has created a race between threat actors and IT security functions.

A major obstacle to mitigating this risk is the piecemeal approach companies have taken to their IT infrastructure planning and development over past decades. Poor governance and oversight of IT functions has meant businesses have gradually built siloed systems and bolted on parts of their network over a period when cyber risk was low. Now that cybercrime is exploding, with the cost of damage from attacks expected to double between 2015 and 2021 to $6 trillion [1], it is hard to defend heterogeneous systems.

The first steps of migrating from legacy systems (e.g. Windows 98, NT and 2000 and unsupported software including Internet Explorer 7, 8, 9, and 10) and rationalising IT infrastructures are being taken and the value of penetration testing and ethical hacking is now well understood. As these systems are brought up to standard, as the management of cyber risk matures and as companies are better able to stay on top of the threat to their direct operations, attention is shifting externally.

Supply chains and cloud services

In recent times, hackers not only target organisations directly but through connections with key suppliers and technology partners. Last year's Petya strike, one of the largest attacks to date, used exactly this method by exploiting Ukrainian accounting software MeDoc as the point of entry to deploy malicious code that spread across corporate networks worldwide. This high-profile example was not an isolated case – it is estimated that incidences of malware being injected into supply chains to infiltrate unsuspecting targets increased by 200% in 2017 [2]. The interconnected, interdependent nature of today's businesses and the emerging strategy of hacking into this web of relationships is multiplying the likelihood of cyber attacks and means that organisations are only as strong as the weakest link in their supply chains.

The integrity of cloud-based services is another consideration. There is a strong business case for migrating certain services and data to the cloud — it can reduce hardware and software costs and other overheads, as well as improve the ease of remote working, collaboration and disaster recovery. Cloud service providers house mountains of their clients' data and top-tier suppliers of generic, commodity services, such as Google (Google Cloud Platform), Amazon (AWS), and IBM and Microsoft (Azure), employ the best expertise available to keep their platforms safe and secure, and use automated systems that can detect and block millions of password attacks every day.

Nonetheless, Microsoft reported in 2017 that it had seen a year-on-year quadrupling of the number of attacks on its customers' cloud-based accounts. It noted that a large majority of compromises are the result of weak, guessable passwords and poor password management, followed by targeted phishing attacks and breaches of third-party services. To illustrate this point, FedEx suffered a breach in 2017 that cost the company $300m in lost business when data was stolen from an Amazon-hosted server. Researchers later found that the cloud server was not protected with a password. This shows how crucial it is that organisations apply the same level of security controls across their IT infrastructure, whether it is housed internally or provided by external parties.

66% of CAEs
said cybersecurity is one of the top five risks their organisation faces
Source: Proprietary Quantitative Research

"We are conducting a **joint audit** with ten banks on one of our cloud providers, Microsoft Azure, to gain the assurance that we all want. This is really a **breakthrough** and will be the first time we've been involved in anything like that. There has always been difficulty with **outsourced activities** because third parties can't have all of these audit functions coming in, and it's often **not feasible** for them to deliver **tailor-made** assurance reports for all of their clients."

Chief Audit Executive,
Dutch multinational banking group

The cost of damage from cyber attacks is expected to double between 2015 and 2021 to **$6 trillion**

Source: Cybersecurity Ventures

"Given the **growth** of the company and the amount of data we hold, cyber risk is becoming **more promiment**. There's the outside threat but how do you make sure that service providers have **sufficent data** to support the business, but not so much data that it constitutes inside information? We have **great contracts**, but no one looks at them anymore. It's good periodically **to look at the big processes** and **exposures** to outsourced service providers. We haven't done much of that and one of the items for 2019 is **supplier mangement**."

Chief Audit Executive,
Dutch multinational retail group

56%

of organisations have had a breach that was caused by one of their vendors in 2017. This represents a 6% year-on-year increase.

Source: Ponemon Institute

Incidences of malware being injected into supply chains to infiltrate unsuspecting organisations increased by **200%** in **2017**

Source: Symantec

Third party cyber risk considerations are especially pertinent in the face of the EU's General Data Protection Regulation (GDPR). The GDPR provides that both 'data controllers' and 'data processors' are jointly and severally liable where they are both responsible for damage caused by their processing of data. Therefore, if the personal data of EU citizens is held in the cloud and the cloud provider, a data processor, suffers a breach, then the controller can be held liable provided the processor has adhered to the controller's requirements, as detailed in the data-sharing agreement/contract. What's more, while the punitive fines that regulators can issue under the GDPR are what has drawn the most attention and concern, regulators also have the power to halt any processing in the event of a breach. This has the potential to freeze a company's operations all because of an incident at the cloud provider level, regardless of which party is liable, with such disruption likely to cause a significant loss of value.

"Companies like Amazon provide good cloud storage solutions, but from a controls and vendor mangement perspective, there are constraints in getting access to audit those providers compared with other vendors. After the data leak at Facebook, this is a really big concern. From an internal audit perspective, we are trying to get back to basics by reviewing the inventory of vendors, the vendor risk management programmes and how well defined they are. How the organisation executes vendor monitoring will be a focus of our audit plans in future."

Chief Audit Executive,
Spanish multinational banking group

An internal audit perspective

Cybersecurity risk is here to stay and the third line of defence will be expected to provide assurance on the internal management of this risk for the foreseeable future, if not indefinitely. Getting the essentials of firewalls, secure configuration, patch management, access control and malware protection right will continue to be of the utmost importance and these controls will likely need to be periodically assessed. The same is true for penetration testing, although given the likelihood that a breach will occur at some point, continuous monitoring and detection by the IT security function will be equally important.

Evaluating governance in this area will also be hugely valuable. Often IT is seen as independent of the business and in the past may have been given too much autonomy in constructing the organisation's network and systems, which can lead to significant security challenges over the long term. Internal audit may choose to bring this to senior management's attention and, if necessary, recommend greater oversight of purchasing decisions and that the IT function take a more strategic, forward-planning approach to developing the organisation's information systems to avoid a fragmented infrastructure with a greater number of vulnerabilities and potential entry points. The European Confederation of Institutes of Internal Auditing and the Federation of European Risk Management Associations last year published a joint report, 'At the Junction of Corporate Governance & Cybersecurity', which highlights the need to align cyber risk management strategies with the business strategy and objectives. The report can be found here: bit.ly/ECIIAcyber

With the aforementioned rise in attacks on premium cloud-service providers such as Microsoft, internal audit should ensure that cybersecurity risk in the third party environment is being controlled to the same standards as it is internally, including basics such as password management. This may involve identifying parties which deliver the most critical IT services and ensuring that they are monitored and evaluated more frequently than others, checking that cloud providers are GDPR-compliant and exercising auditing rights to test the robustness of their controls, assessing the due diligence processes followed when engaging with new suppliers, as well as conducting independent research into how key third parties are viewed in the marketplace.

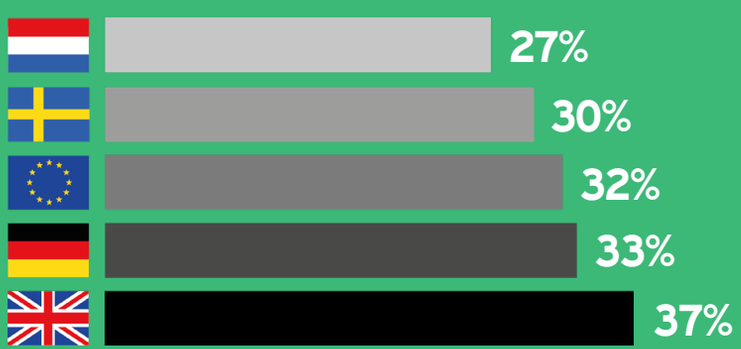
Key questions

- Has the organisation moved or is it moving away from legacy systems to a more homogeneous, harmonious system that is easier to defend?
- Are security considerations central to the IT plan and network development?
- Is there strong governance in IT and oversight of procurement and development of networks and infrastructure?
- In addition to having robust defences to keep attackers out, does the organisation deploy effective monitoring capabilities to detect when a breach has occurred?
- Is internal cyber risk management sufficiently mature to direct attention towards connected parties?
- What cloud services does the company use and how is the organisation sure these providers maintain high security standards and robust controls?
- Are the same password management standards applied internally also applied to cloud services?
- How strong are the procurement function's cybersecurity due diligence processes when bringing on board suppliers and connecting with business partners?

"There's a **clear trend** towards the **cloud** and the virtualisation of servers, but I don't think many heads of audit really know where IT functions have got to with that and what the real controls are. Most IT functions are still **governed too low down**; there's not good governance oversight of IT in most organisations. As CAEs we co-source pieces of work but don't really understand how that fits with the business. There needs to be **more oversight** of significant IT changes, and a better understanding of where the controls between the organisation and its cloud-based providers really lie. More broadly, it still seems unclear **what good looks like** from an IT capability perspective."

Chief Audit Executive,
UK public sector

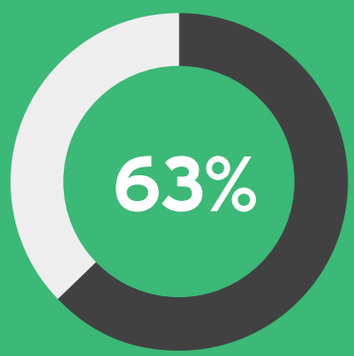
Percentage of businesses that experienced a data breach in 2017



Source: Thales Security

Microsoft reported a quadrupling of cyber attacks on its cloud services in 2017

Source: Microsoft Security Intelligence Report



63% of cybersecurity breaches can be traced back to third-party vendors

Source: Soha System

"Our IT has been developed over the past 20 years, when there was **no cyber threat** so there is a lack of security in these **integrated systems**. If a ransomware attack was targeted at our organisation it could take a long time to get our physical **infrastructure assets** functioning again and that could cause a threat to people's safety. Internal audit's focus has gone from operations and efficiency to **basic safety** and security."

Chief Audit Executive,
Swedish public sector

DATA PROTECTION & STRATEGIES IN A POST-GDPR WORLD

The deadline for the EU's General Data Protection Regulation has now passed and internal audit functions have either performed readiness audits or will imminently look at this area for the first time. But there is more to consider than simply ticking the GDPR compliance box.

The talk around GDPR over the last 18 months has been loud, which should come as no surprise given the pervasive nature of the regulation (it applies to all companies processing EU citizens' personal data), its sector-agnostic application and the heavy fines that come with non-compliance. The challenge of obeying this sweeping regulation was included in last year's report and, similarly, we found that every interviewee in our qualitative research this year raised GDPR compliance or the broader issue of data security, governance and strategies as an area of focus for 2019 and further ahead. Supporting this, our quantitative survey revealed that 58% of respondents put compliance and 58% put data security and protection each as one of their top five risks, behind only cybersecurity (66%).

Europe is not the only territory to tighten its rules — on 1 May China published its Personal Information Security Specification, which provides detailed guidance for compliance with the country's Cybersecurity Law, passed in 2016. The GDPR was largely used as a template for this guidance, therefore European companies are likely to meet China's standards if they are already compliant with the GDPR, but should conduct a gap analysis against the Specification if they are concerned about their use of Chinese citizens' personal data.

Reputation matters

The GDPR has had a significant ripple effect. Facebook, one of the most data-rich companies in the world, asked all of its 2.2 billion users to review their privacy settings once the law went live on 25 May, despite not being required to do so. That this followed a significant breach of trust at the social media site is likely no coincidence.

The backlash towards Facebook in early 2018 was severe when it emerged that political consulting firm Cambridge Analytica harvested in excess of 87 million users' data in support of its mandate to promote Donald Trump's presidential bid in the run-up to the 2016 elections.

In the wake of the news, $70bn of the company's market value was wiped out in ten days. While the company's share price recovered, there is now heightened scepticism towards the ethical use of personal data for commercial and even political purposes, and demands from lawmakers in various countries for greater accountability. An estimated 60% of Germans said they fear that Facebook and other social networks are having a negative impact on democracy [3] and less than half of Americans now trust Facebook to obey US privacy laws [4]. This illustrates that data security is more than just a compliance issue, but one of trust and reputation.

The EU-US Privacy Shield

The GDPR has a number of requirements regarding the transfer of personal data out of the EU. One of these is that data must only be transferred to countries deemed as having adequate data protection laws.

Currently, the US has weak data protection laws and does not meet this requirement, although a programme known as the EU-US Privacy Shield allows certified US companies with appropriate controls to receive personal data from businesses based in the EU.

However, a group of Members of the European Parliament have called for the Shield to be suspended, claiming that it does not offer adequate safeguards, and should only be reimplemented once weaknesses in the programme have been fully addressed. European companies sharing personal data with US partners should keep a watching brief on developments.

For more information, visit www.privacyshield.gov

Strategy and governance

Abiding by the GDPR is undoubtedly a primary concern but it is not enough to reach full compliance with the law on day one and then ignore it. Data, both personal and operational, is not only hugely valuable but proliferating exponentially. It is estimated that

58% of CAEs say that data security and compliance are each one of the top five risks their organisation faces

Source: Proprietary Quantitative Research

"**GDPR** will be on the schedule for a long time - it's affecting all businesses. It requires more **data privacy** and better management of data, not only from a **regulatory perspective** but to ensure the **trust of customers**. Also, if we have a lot of data, what can we use it for? What kind of business can we do commercially using that data?"

Chief Audit Executive,
Swedish telecoms group

"You see **more visibility** of the management of data privacy, not just regarding the GDPR, but privacy and **data management** as a whole. This will be an ongoing issue, particularly with what's going on with the social media firms. That's **morphing** into something more **all-encompassing** around how organisations manage data, and particularly the use of **third party data** and the risks associated with that."

Chief Audit Executive, UK financial services firm

50%

Less than 50% of Americans trust Facebook to obey US privacy laws in the wake of a scandal over its handling of personal information

Source: Reuters/Ipsos

27%

Only 27% of businesses in the EU reported being compliant with GDPR one month after the enforcement date of 25 May 2018

Source: TrustArc

74%

However, 74% expect to be compliant by the end of 2018 and 93% by the end of 2019

Source: TrustArc

60%

of Germans say they fear that Facebook and other social networks are having a negative impact on democracy

Source: Bild am Sonntag

"GDPR is a compliance area where we will focus our attention. We have audited that this year already in terms of GDPR-readiness of the organisation internally but also our products. Our customers expect our products to be compliant. There are similar laws being established in other countries. You have the cybersecurity law in China, and in Russia you have the same. So this continues to be a focus area on the audit side. It's not just GDPR but data protection in general, in all its forms in various locations."

Chief Audit Executive, German multinational software corporation

internet traffic surpassed one zettabyte in 2016, the equivalent to streaming 150 million years of high-definition video, and this is expected to nearly triple by 2021 [5]. The more advanced that analytics become and the deeper the insights that companies can draw from their analysis, the more value data will hold. At the same time, because the ways in which businesses collect and harness data is continuously developing, GDPR compliance will be a moving target that will need to be revisited as new applications and uses of personal data emerge. The ability to manage and model these torrents of information is critical to a company's success. Organisations must therefore develop clear data strategies and governance that support the broader corporate strategy and the company's value-enhancing objectives, all the while maintaining high standards of security and compliance.

This may require employing a Chief Data Officer, a role that has become more common in the last five years, and building a data management function that can strive towards standardising unstructured data and improving the governance of how data is managed. Once the laying of these foundations has reached maturity, companies can then focus more on data analysis and modelling techniques to maximise the value of the data they own, all the while keeping it safe and secure.

An internal audit perspective

If internal audit has not already provided assurance that the organisation is GDPR-compliant, the time to do so is now. For many companies, particularly those for which personal data is central to revenue generation, this will require periodic reviews, especially as new data points are harvested and by new means, e.g. collecting personalised customer behaviour data through geolocated advertising that interacts with people's smartphones.

More than this, there is scope for internal audit to assess the extent to which the organisation has established a data strategy and governance standards. This will involve considering how data is managed, the extent to which it successfully drives value (revenues and profits) and supports the company's objectives and corporate strategy. This data strategy should be closely aligned with the organisation's cybersecurity strategy, as any loss of data to hackers or internal actors will result in a loss of value.

Becoming a data-led organisation involves significant change, a process that can be supported by the third line. There may not be pre-defined standards to audit against and the specific changes may be unfamiliar, however internal audit should stick to core principles applied to project management, such as identifying clear objectives for change, ownership and accountability, the alignment of the data strategy with the overarching corporate strategy, the validity of key performance indicators (KPIs) used to measure the success of change, and how change will impact upon existing controls, processes, risks and the structure of the business.

Key questions

- Is the organisation compliant with GDPR and, if necessary, China's Personal Information Security Specification?
- Are US companies that share the organisation's personal data certified under the EU-US Privacy Shield scheme?
- How is personal and operationally/strategically sensitive data shared with third parties and how do you know these parties are keeping it secure?
- Are senior management and the compliance function aware of the need to remain compliant as the company and the ways in which it collects and uses personal data evolves?
- Is the compliance function in close communication with the data management function so that the former is aware of how any company changes may impact upon GDPR compliance?
- Is there a data strategy for how the organisation uses data, personal or otherwise, to its advantage? Is this aligned with the corporate strategy?
- How does the strategy envisage data being used in the future? Is this clear and well articulated?
- Is the internal audit function prepared to advise the Chief Data Officer and/or data management function with any changes to the organisation's use of data by providing a risk control perspective?

Only **12%** of Fortune 1000 corporations employed a Chief Data Officer in 2012...

...by 2018 **63%** had created this role in their organisation

Source: NewVantage Partners

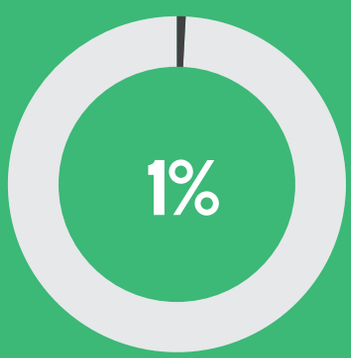
"It is **not only** a **regulatory concern**. When you're talking about data leaks, the most important thing to us is our customers and we are very involved in data privacy. We want to monitor this risk not only because we could be **fined** but because we are managing more and **more data** and we need to make sure it is being protected effectively. It is a **continuous process** to remain compliant, not only **today** but also **tomorrow**."

Chief Audit Executive,
French media conglomerate

44
zettabytes

By 2020, the accumulated volume of big data will increase from 4.4 zettabytes to roughly 44 zettabytes

Source: Dell EMC



Less than 1% of the unstructured data that companies own is analysed or used at all

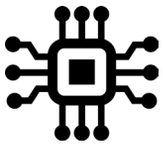
Source: Harvard Business Review

"The recent developments we have seen with **Facebook** mean that organisations need to think about being more open about what they do with data and how they protect it. This is broadly covered by GDPR, but **regulation** is always **behind** developments in the real world. Internal audit must look at the **long-term value** creation of the organisation. That means looking at its values, the **values of society** and considering whether the organisation is doing things that might **not** be **acceptable** even if they are legal. There is no book or regulation for that but internal audit should be raising the **red flag**, otherwise who else in the organisation is going to?"

Chief Audit Executive,
Dutch professional services firm

80%
of analysts' time is spent discovering and preparing data rather than analysing it

Source: Harvard Business Review



DIGITALISATION, AUTOMATION & AI: TECHNOLOGY ADOPTION RISKS

The cost and efficiency benefits of automation and other digital processes can be transformative, if harnessed to their full potential. But organisations must also consider the risks associated with such transformation.

Our research shows that 36% of CAEs believe digitalisation is one of the top five risks facing their organisation and nearly one in ten (9%) said it is the single biggest risk, behind only cybersecurity (15%) and compliance (13%). Of the cohort who were interviewed for our qualitative research, 66% said that risks related to digitalisation and the adoption of technology would be an area of focus for their work in 2019 and beyond.

The pace of innovation and organisations' ability to keep up with their competitors was included in last year's report. This will remain a concern, particularity in sectors most impacted by technology, such as media, telecoms, retail banking and other consumer-facing industries. For those companies that are already making progress in their digital journey, there may be a tendency to focus on the benefits without fully accounting for how incorporating technology is exposing them to risk.

But what is meant by digitalisation? It is a broad term that refers to everything from installing enterprise resource planning (ERP) and customer relationship management (CRM) systems such as SAP and Salesforce that centralise core data and processes, all the way through to automated technologies.

The basic steps of adopting ERP and CRM systems can be hugely beneficial. For example, the uptake of these core technologies in the UK is lower than it was in Denmark in 2009, and this has been linked to the country's productivity gap (UK productivity has not grown since 2008). It is estimated that adopting tools such as ERP and CRM could add £100bn to the UK's annual economic output.

At the advanced end of the spectrum are technologies such as robotic process automation (RPA) and artificial intelligence (AI). RPA can be understood as software that automates a process according to programming instructions, without learning. AI, meanwhile, refers to self-learning systems that can process unstructured data inputs and improve over time.

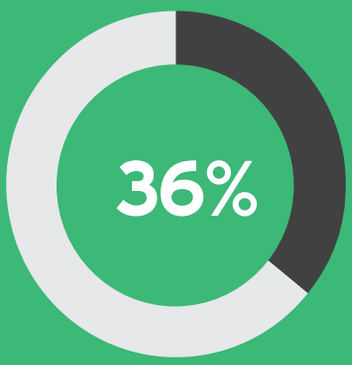
Factoring in risks

Automation is already a reality for many organisations. Chatbots are increasingly being introduced in business-to-consumer companies to handle customer queries, and algorithms are used to quickly and automatically underwrite financial products in the retail banking and insurance markets. The cost and efficiency benefits of such applications are obvious, but what about the risks?

To give one example, if an error exists in an algorithm that determines the creditworthiness of loan applicants, even if a tiny percentage of applications are miscalculated, this could have catastrophic consequences for the quality of a bank's loan portfolio over time when applied to thousands or millions of loans.

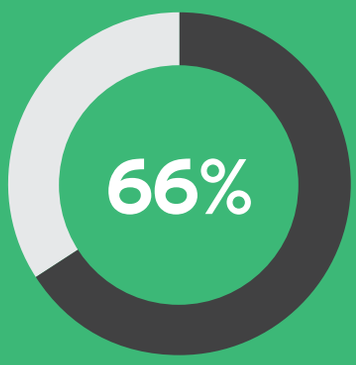
RPA and AI systems are programmed by humans and compute datasets selected and refined by people, which creates a margin for error. Financial institutions therefore run the risk of their algorithms inadvertently making biased decisions at scale or taking actions that discriminate against certain customer demographics. This would make them accountable even if the discrimination is unintended. In this financial services scenario, both an accurate risk-based approach to underwriting financial products and one that treats customers objectively and fairly is crucial. This is recognised by the GDPR, which requires that data subjects are offered simple ways to request human intervention or challenge a decision based on an automated process, and that regular checks are carried out to make sure that systems are working as intended.

Rolling out technology also has implications for the culture of an organisation. It can drive uncertainty and resistance in



36% of CAEs said digitalisation is one of the top five risks their organisation faces

Source: Proprietary Quantitative Data



66% of CAEs said that risks related to digitalisation and the adoption of new technologies would be an area of focus for their work in 2019 and beyond

Source: Proprietary Qualitative Data

"**Automation**, robotisation, AI, this drives a lot of **uncertainty** in organisations. If jobs are due to be filled by robots, that affects the **behaviour** of the people working in the organisation at the moment. How are they behaving and is it influencing the organisation's **culture**? Are they ignoring these developments because they are afraid of them? There's a **human element** to technology risk that is really important. If people don't feel secure, that drives certain behaviour. Organisations are operating with **increased risk** when they decide to do something new, especially in areas in which they are **less mature**."

Chief Audit Executive, Dutch professional services firm

40%

More than 40% of business leaders anticipate that AI will start displacing humans from some jobs in their industry by 2021

Source: Economist Intelligence Unit

"We are pretty **agile** in **responding** to **innovation**. We've begun to adopt artificial intelligence, robotics, analytics and more digital interfaces. What is less well understood is what are the **risks associated** with that innovation and what might we be letting ourselves in for. What are the risks that are introduced as a result of things like AI, robotics and being more digitalised organisations? That is **not well understood**."

Chief Audit Executive, UK financial services firm

the workforce. Swathes of personnel may have to retrain or face the prospect of eventual redundancy, so it is important to understand how such initiatives are affecting the morale and behaviour of staff. This may be out in the open or suppressed and, since it will impede the successful adoption of new technology, any resistance in the workforce must be recognised and managed accordingly.

It is also important to remember that, for the time being at least, technology is largely a supplementary tool. It is less a case of staff being replaced wholesale than them working in tandem with technology, using it to augment existing tasks. Companies that relinquish too much control to technology can unintentionally increase their risk exposure, and there is a need to understand how the workforce will interact and engage with things like automation and articial intelligence in order to maximise its benefits and effectiveness.

Company-wide transformation requires buy-in and sponsorship from key stakeholders, especially middle management. It is not enough for a Chief Technology Officer alone to champion such projects from the top, lower tiers of management must demonstrate commitment to the new way of working in what they say and do. Without this buy-in from all layers of management, projects may lack the momentum necessary for successful delivery and completion.

All technology adoption, whether upgrading to ERP and CRMs in the back office, launching apps and integrating mobile functionality for consumer markets or developing RPA and AI to expedite operations, will cause an element of disruption and possible business continuity issues, especially at the implementation stage. Keeping this disruption to a minimum and achieving a seamless, or as smooth as possible, transition is paramount.

An internal audit perspective

Senior management and the board should be aware of the risks associated with adopting new technologies. Tech evangelists within the organisation may have made a strong business case for digitalisation without fully highlighting the potential issues that can arise, and the second line of defence should seek to identify, assess and communicate to senior management and the board what these risks are — e.g. a lack of cost-benefit analysis, weak beta testing, algorithm errors and human biases, workforce resistance, organisational change. Internal audit should seek evidence that associated risks have been identified, ensure there are plans to manage these risks and call out any potential weaknesses in the risk framework.

Ambitious projects such as adopting AI on a wide scale may expose the organisation to excessive risk that outweighs the benefits. For this reason, pilot projects and step changes are typically an appropriate, risk-adjusted approach. Once these projects have been proven and successfully integrated, then the organisation can scale up adoption of the technology. There may also be value in the organisation assessing how direct competitors are adopting new technologies, how successful this has been for them and why, and whether the market has reacted positively to such development.

Adopting technology should ultimately help the organisation to achieve its goals and so internal audit should assess whether projects are aligned with the corporate strategy. This should be documented and specific, not conceptual. It should address the exact processes that will be improved, how they will be improved and include KPIs to measure the new technology against to gauge its success once it is operational, as well as appropriate key risk indicators (KRIs) that will raise red flags if key controls fail or are likely to do so. Internal audit should look for clearly articulated goals and rationales, as well as acknowledgement of how processes will be affected and what this means for risks and controls. There is also an assurance role to play in checking that technology works as expected and this may require testing the accuracy of data inputs, the algorithms that compute that data and whether the resulting outputs are consistent and repeatable. Internal audit should therefore first determine whether it possesses the expertise to audit the technology itself.

Key questions

- What different technologies are being adopted? Is there a clear, documented rationale for doing so that is consistent with the organisation's broader operational and strategic objectives?
- Who is accountable for these projects and are they taking into account the potential risks that come with digitalisation?
- To what extent will new technologies require updates and modifications to the control environment? Is the first line making these control changes?
- Is there enough buy-in and sponsorship from middle management to give technology adoption the required momentum to be successful?
- Is there resistance to digitalisation in the workforce and is it negatively impacting culture? If so, what steps can be taken to measure and remediate this?
- Are automated processes being risk assessed for data quality, the accuracy of algorithms and outputs and is internal audit equipped to confirm that technologies are working as intended? If not, who is providing this independent assurance?

"This is a **huge challenge** for internal audit because even though we've seen a **shift towards technology** in the past 10 years, we still haven't seen that same shift within internal audit. Internal audit tends to like things it can put its **hands on** and the transition is moving **faster and faster**. You don't need **core skills** in automation and AI, but you need to understand and audit classic business plan and **project management**. Do projects have enough resources to meet expectations? Is there risk analysis from senior management in order to fulfil the plans? You can **audit** it in a **traditional** way even though we're talking about **high technology** evolution."

Chief Audit Executive,
Swedish professional services firm

15%

Only 15% of enterprises are using AI as of today...

31%

...however 31% are expected to employ it over the coming 12 months

Source: Adobe

87%

87% of industrial companies plan to implement AI in production within the next three years....

...but only **28%** have established a comprehensive implementation roadmap

Source: Boston Consulting Group

"We have fewer projects in volume, but the ones we do have are being **driven by digitalisation**. We require a shift in technology and that means fewer projects with **bigger budgets**, including upgrading IT infrastructure and digitalisation of the back office. In terms of **safeguarding assets**, the battle is auditing these ongoing projects. Once you have finalised a project it will take more effort to audit afterwards and then change anything. That's a **waste of time** and money. Internal audit needs to be there during the project to give assurance to the board of directors and CEO that the method for **running projects** is being followed."

Chief Audit Executive,
Swedish insurance group

SUSTAINABILITY: THE ENVIRONMENT & SOCIAL ETHICS

Companies are increasingly expected to behave in an environmentally and socially responsible manner, both by regulators and the public. This is creating sustainability reporting challenges and is influencing the strategic decisions companies must take to achieve future growth.

Some 27% of our interviewee cohort cited environmental and social ethics as an area of focus, and this is the first time that this topic has made it into Risk in Focus; there was a notable bias towards the Netherlands, with half of CAEs in the country highlighting this as an area in need of attention. Further, in our quantitative survey nearly one in ten (8%) respondents cited environment and climate change as a top five risk faced by their organisations.

The EU's Non-Financial Reporting Directive, applicable since 2017, requires that listed companies and banks with more than 500 employees publish reports on various policy implementation, relevant risks and performance results. These policies concern:

- Environmental protection
- Social responsibility and treatment of employees
- Respect for human rights
- Anti-corruption and bribery
- Diversity on company boards

Sustainability reporting requirements are clearly a welcome development — they help to improve corporate transparency and highlight the efforts companies are making to meet environmental and social targets. However, a major challenge is in providing accurate information. The maturity of sustainability reporting is far behind financial reporting and not all organisations are well equipped to measure and report on KPIs. This increases reputational risk as there is potential for a company's behaviour to be found to contradict or fall short of its claims. Even if sustainability reporting is deemed to be sufficiently accurate, any KPIs that show the organisation has low standards relative to its peers will be looked upon unfavourably by investors, who increasingly benchmark companies' environmental and social governance (ESG) performance.

There is also a strategy risk dimension to heightened environmental regulation. Lawmaking in the EU is extensive, covering everything from the energy efficiency of appliances to water quality. The most pervasive policies to date, however, stem from the Paris Agreement on climate change, which aims to keep global temperatures below 2.0C above pre-industrial levels, by curbing carbon and other greenhouse gas emissions.

The EU has set emissions targets for 2030 in a bid to fulfil the Agreement in what is known as the "effort sharing" legislation. Member states have their own individual targets and are responsible for national policies and measures to limit emissions. The general trend is to follow more climate-friendly farming practices, improve the energy performance of buildings, increase the use of renewable energy sources and reduce vehicle emissions.

Further, the G20's Task Force on Climate-Related Financial Disclosures is urging companies to disclose how they manage the financial risks to their business from climate change and greenhouse gas emission cuts. While such disclosure is not mandatory, it gives investors the information they need to assess the impact of climate risk on their portfolios.

Certain sectors, such as the automotive and oil and gas industries, are therefore under immense pressure to understand what tightening carbon emissions regulations and targets mean for them, their product development and corporate strategies. This also extends to industrial companies that are suppliers in these sectors. For example, a chemicals company that derives a significant portion of its revenue from materials used for plating diesel car engines will face significant strategic risk from not diversifying into new growth areas, such as rechargeable battery manufacturing for electric cars.

Social impact

The increased impetus on organisations to be socially responsible and protect human rights represents another challenge. Compulsory non-financial reports must be published annually, and should include what steps are taken to identify risks to human rights in the company's operations and how these are managed.

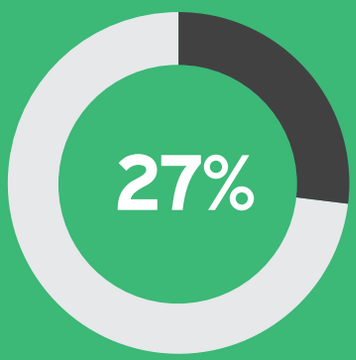
This will be familiar territory for UK businesses, who have had to comply with the Modern Slavery Act for two years already. Similarly, last year Spain committed to its National Action Plan (NAP) on

Nearly one in ten CAEs cited environment and climate change as one of the top five risks their organisation faces

Source: Proprietary Quantitative Data

"There is an **important discussion** to be had around the **emerging role** of the internal audit function for sustainability. Now that **non-financial reporting** has become **mandatory** for public companies, what is our new role? Do we all become experts on carbon emissions **Scope 1, 2 and 3** and all of this? That is an enormous debate for the audit profession."

Chief Audit Executive,
Italian retail group



27% of CAEs said that issues related to sustainability are expected to be an area of focus going forward

Source: Proprietary Qualitative Data

40%

Under the EU's 2030 climate and energy framework greenhouse gas emissions are to be cut to at least 40% of 1990 levels. A number of European countries including Germany, the Netherlands and the UK have committed to banning the sale of new gasoline and diesel cars between 2030 and 2040.

Source: European Commission

"We produce products for diesel vehicle markets, so all of the **clean air** and sustainability issues we see as **massively impacting** our business, albeit over a period of time. So, the organisation has been moving into the development of **new materials**. You have the **legislative side** and the ethics and compliance, but there is also an external market outlook. What is going on in the world that will impact our **strategy** and drive strategic change? So, in internal audit we are looking at the **strategic planning** process and how relevant and **dynamic** it is, because there is a lot of change in the external environment."

Chief Audit Executive,
UK multinational chemicals group

$2 trillion

The effect of rising temperatures on workers' productivity could cost the global economy more than $2 trillion by 2030

Source: Academic Study

human rights, following in the footsteps of Italy which committed to its own human rights NAP a year prior. These measures emphasise the need for ethical integrity in operations and supply chains by applying the United Nations Guiding Principles on Business and Human Rights.

It is worth noting, however, that while these instruments help to improve transparency, there is no legal requirement to improve due diligence or eradicate human rights abuses, only to report on what, if any, steps have been taken to mitigate these risks.

France's recently introduced Loi sur le devoir de vigilance, or corporate duty of vigilance law, goes one step further. As of 2018, large French companies (5,000-plus employees, or 10,000 if not headquartered in the country) must draw up and publish a vigilance plan to prevent environmental, human rights and corruption risks in their own activities as well as those of their subsidiaries, subcontractors and suppliers. Crucially, if these plans are not properly implemented, companies face potential civil claims.

If the law proves successful, there is a chance that other countries, particularly in Europe, will begin to introduce similarly punitive legislation. Even if they don't, however, and social ethics continues to be largely a reporting requirement only, the fact remains that the public is holding businesses to account for any negative social and environmental consequences of their operations. This represents a reputational risk, and any transgressions may result in lasting damage to brands and stock prices.

An internal audit perspective

Organisations must now report on what they are doing to identify and mitigate sustainability risks and should look to the Global Reporting Initiative's Sustainability Reporting Standards (GRI Standards) for guidelines on how to achieve this. You can also find the UK's Chartered Institute of Internal Auditors' work on non-financial reporting here: bit.ly/IIAnon-fin

Internal audit can assist by simply ensuring that this reporting requirement is being fulfilled, although it can go deeper by seeking evidence that what the company claims in its non-financial reports is accurate, complete, up to date and being put into practice. There is also value in seeking evidence of how processes are being developed to improve the maturity of such reporting, such as the number of KPIs measured and the accuracy of data collection. The deepest audits may assess sustainability reports within the relevant industry to benchmark both the organisation's reporting and its performance relative to its peers.

Corporate human rights obligations are relatively immature and general, and are typically centred around reporting on efforts that are being made to minimise harm. Environmental laws, however, are already well developed in Europe and, if required, compliance audit programmes may include assurance that industry-specific environmental legislation is being adhered to. Regulatory and legal compliance notwithstanding, many organisations face an existential threat from carbon emissions targets and internal audit may be required to provide assurance that senior management is factoring this into strategic decision-making.

It is important not to overlook the damage that environmental and human rights incidents can inflict upon organisations. Meeting legal requirements and standards is not a substitute for continuous improvement as regards ESG standards, and internal audit can, on a rolling basis, offer an independent perspective on ongoing progress made to improve operations and limit environmental and social harm over the medium to long term.

Key questions

- Is the organisation publishing non-financial reports as required by the EU?
- Is there scope for internal audit to assess the maturity of sustainability reporting and review the extent to which the company's environmental and social ethics statements reflect reality?
- Does the organisation benchmark sustainability performance against sector-specific KPIs? Is there a gap between both the organisation's sustainability reporting and performance compared with that of its industry peers?
- Is the organisation complying with all relevant environmental laws in all territories?
- To what extent is tightening environmental regulation likely to impact the company's strategy, e.g. targets to reduce carbon emissions? Is senior management aware of this likely impact?
- Does senior management understand the importance of continuously improving operations in order to minimise environmental and social harm?
- Is there value in internal audit assessing progress and providing evidence of relevant sustainability improvements?

Around half of EU member states missed the December 2016 deadline for transposing the Non-Financial Reporting Directive into national law. By December 2017 all member states had updated their laws to reflect the Directive's requirements. This means a clear picture on compliance and the quality of sustainability reporting will only begin to emerge from 2019.

22% of businesses globally are addressing child labour concerns in the supply chain...

...**23%** are actively tackling climate change...

... and just **32%** ensure they aren't sourcing from areas affected by conflict and violence

Source: Economist Intelligence Unit

"We are being assessed for the Dow Jones Sustainability Index so this is being driven by the **capital markets** because certain investment funds only **invest** within a certain sustainability programme. There are **environmental laws** which we also respect. If you do business in the food trading industry you have to acknowledge that resources are finite and need to show certain **responsible behaviours** related to the ethical treatment of the planet and animals. It is important for our customers that products are **sustainably sourced**, so we need to check that is the case. "

Chief Audit Executive, German retail group

"This is unusual but my internal audit function is also in charge of **corporate social responsibility**, so I coordinate the sustainability process and the reporting exercise, which is **mandatory** by law for public companies from this year. I'm also in charge of supporting the business in **monitoring** its **progress** against its sustainability targets and framework. So sustainability risks are quite important for me and have been strongly considered in the audit plan for **next year**. I am starting with a different team to provide assurance in this area, not only looking at **KPIs** internally but through the supply chain regarding environmental and **human rights** issues, diversity and inclusivity."

Chief Audit Executive,
Italian retail group

ANTI-BRIBERY & ANTI-CORRUPTION COMPLIANCE

Anti-bribery and corruption (ABC) risk is longstanding; however, national legislative reforms, coordinated global enforcement by regulators and record-breaking fines are raising the stakes and pushing this issue to the top of the corporate agenda.

We found that one in five interviewees in our qualititative research raised the issue of ABC compliance risk and the need to dedicate an audit programme to this area in 2019. Half of these CAEs were based in Spain, while at least one CAE in every sector apart from retail and information, technology and communication is prioritising this issue. This is consistent with our quantitative survey, in which 58% of respondents said that compliance is a top five risk, second only to cybersecurity (66%) and on par with data security.

This finding coincides with a number of jurisdictions having recently reformed, or beginning the process of modernising, their ABC laws. Generally speaking these have been brought in line with the UK Bribery Act, which prohibits both private-to-public and private-to-private bribery, and the involvement of agents and other third parties.

- China updated its Anti-Unfair Competition Law at the beginning of 2018, expanding the scope for liability in respect of bribes paid through third parties.

- Ireland passed updates to its ABC law in 2018 that introduced a number of new offences and expanded the scope beyond targeting bribery of public officials to businesses operating across the private sector.

- Australia's government has tabled a series of new laws covering foreign bribery, including the new offence of "failure to prevent bribery of foreign officials" in line with the UK Bribery Act.

- France has introduced a comprehensive new transparency and anti-corruption law, Sapin II, that can hold companies liable for failure to implement an effective anti-corruption programme, even when no corrupt activity has taken place. The law established an anti-corruption agency, AFA, which published guidance in December 2017 and which it began to enforce in the first half of 2018.

Coordinated enforcement

In addition to the tightening of laws, a trend that looks set to continue, there is strong evidence that enforcement agencies are coordinating their efforts and sharing intelligence to bring penalties against offenders and impose sanctions in multiple jurisdictions. In 2016, 42% of resolutions in US foreign bribery cases involved co-operation with foreign law enforcement agencies, a significant increase from ten years prior [6]. This collaboration has increased ABC risk by increasing the probability that a company will be found in breach.

Such cooperation was evidenced in the largest ever bribery case. In December 2016, Brazilian engineering and construction company Odebrecht agreed to pay a record $3.5bn in fines after being accused of having given billions in bribes to officials running Brazilian oil company Petrobras. Notably, penalties were paid to authorities in Brazil, Switzerland and the US.

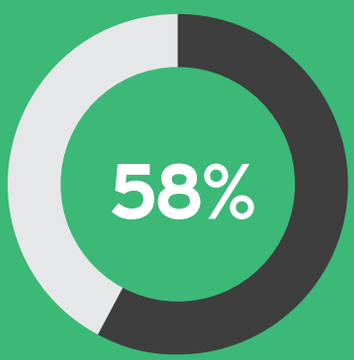
Ultimately the company's penalty was reduced to $2.6bn after it lost major contracts for construction projects with the governments of Peru, Colombia, and Panama, a clear sign that the financial impacts of ABC breaches extend further than enforcement penalties - they can cause significant commercial damage.

Anti-bribery and corruption programme

To protect themselves against the risk of high penalties, organisations should develop and implement an anti-bribery and corruption programme to demonstrate its ethical values and commitment to combating bribery. The organisation should make it explicitly clear that bribery in any form, direct or indirect, is prohibited ('zero tolerance'). Implementing such a programme also demonstrates that an organisation is making reasonable efforts to prevent the organisation from paying or receiving bribes. It should take into account all relevant laws and regulations and additional guidance applicable in the countries in which the organisation operates. The programme should be proportionate, taking into account the specific bribery risks that

One in five CAEs
said that anti-bribery and corruption compliance is a priority for 2019

Source: Proprietary Qualititative Research



58% of CAEs say compliance is a top five risk, second only to cybersecurity; 13% said it is the single biggest risk their organisation faces

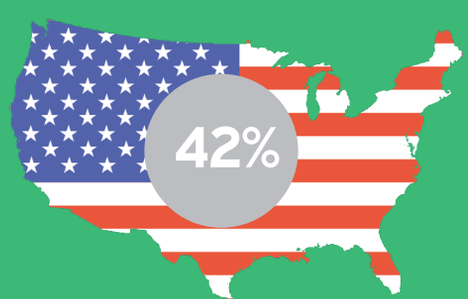
Source: Proprietary Quantitative Research

"We are trying to implement the same standards, risk policies and corporate governance throughout the group. Corruption and the relationships we have with **third parties** we **pay for licences** is always a focus for us in countries in which we are **growing and building**. There is an important investment effort in **Latin America** and in these countries corruption with third parties is a big issue in terms of penalties and reputation."

Chief Audit Executive,
Spanish multinational utilities group

"With **bribery** and **anti-corruption**, it would be **idiotic** to make large profits and then lose them after paying fines just because you are **not compliant enough** for the French anti-corruption agency or, even worse, found in breach of the **Foreign Corrupt Practices Act** by the US authorities. We would have to **pay a huge fine** and be supervised by the Department of Justice for three years. That's why these **compliance audits are so important**."

Chief Audit Executive,
French multinational engineering company



42% of resolutions in US foreign bribery cases in 2016 involved cooperation with foreign law enforcement agencies

Source: US Department of Justice

$1.5 trillion

Businesses and individuals pay an estimated $1.5 trillion in bribes each year. This is around 2% of global GDP

Source: World Bank

relate to the industry, the size of the organisation and complexity of its operations, as well as the various geographies in which the organisation operates. Doing this will significantly reduce the risk of paying high financial penalties in instances of non-compliance.

"France has now transposed the EU regulation into the national Sapin II law, and there is a new dedicated anti-corruption agency which deals not just with public entities such as ours but with private companies as well. This has been enforced since the end of 2017, so in 2019 and the following years this will be a major compliance issue. It's exactly the same for data protection implementation and follow-up with regards to the GDPR. These are undoubtedly the two main compliance issues we are facing today and will require internal audit's attention."

Chief Audit Executive, French public sector

An effective anti-bribery and corruption programme demonstrates that the organisation is taking reasonable efforts to minimise non-compliance. The authorities will take this into account when investigating corruption. It is in the best interests of the organisation to report bribery and corruption issues themselves timely to the authorities and to fully cooperate with their investigation. This is likely to reduce penalties, if any are issued at all.

A global standard

The introduction of ISO 37001, the first international anti-bribery management system standard, in 2016, set out a number of measures that companies can take to prevent and detect bribery. Microsoft was the first multinational to pursue ISO 37001 certification and has said that the patchwork of often inconsistent guidance from different government agencies and the numerous changing laws complicates anti-bribery efforts and therefore increases risk. The new ISO standard addresses this by creating a common language and clear specifications for organisations to establish, implement, maintain and continually improve their anti-bribery management systems. Therefore, ISO 37001 certification should be considered by those organisations for which bribery and corruption risk is a priority — at the very least the standard can be used as a benchmark.

An internal audit perspective

Internal audit has a crucial role to play in assessing the validity of the organisation's bribery risk mitigation efforts. The first step will be understanding senior management and the board's tolerance for this risk, which should be closely correlated with the likelihood of bribery occurring. Any sector in which high-value government contracts are awarded (e.g. construction and infrastructure, oil and gas, mining and other extractive industries) are seen as particularly high-risk, as are territories with a high frequency of bribery and corruption.

Internal audit should evaluate the design of the organisation's anti-bribery and corruption programme for completeness. It should include the organisational values, a zero tolerance statement, codes of conduct for employees and suppliers, a bribery and corruption risk assessment and policies and procedures, including whistleblowing. The risk assessment should include country, sectoral, transaction and partnerships risks. Any identified gaps in the design of the anti-bribery and corruption programme should be reported to the board. The next step is to assess the effectiveness of each of the programme's elements.

Internal audit should also highlight to senior management the importance of self-reporting incidents and cooperating with authorities in order to avoid criminal proceedings and reduce, or entirely mitigate, financial penalties. The Institute of Internal Auditors Netherlands has published a comprehensive report on this topic, which can be found here: bit.ly/IIA_ABC

Key questions

- Does the organisation have an all-inclusive and effective anti-bribery and corruption programme?
- Is there a zero-tolerance statement from management?
- Are there staff awareness and training programmes and an established whistleblowing procedure?
- Does an anti-bribery culture permeate the organisation?
- Has a risk assessment been conducted on the organisation's exposure to bribery and corruption?
- Is second line activity sufficiently risk-based and directed at territories and business units most exposed to bribery risk?
- Has senior management considered whether to become ISO 37001 certified? If not, against which guidance/framework does the organisation benchmark itself?
- Is there a segregation of duties regarding facilitation payments to agents and advisers, and are due diligence policies for bringing on board third parties followed in practice?

The top four sectors in which bribery is most prevalent account for 59% of such activity

- Extractive/mining
- Construction
- Transportation & storage
- Information & communication
- Other

Source: OECD

"Our impression is that corruption is decreasing. At the same time, taxpayers and the press have less and **less acceptance** for what they feel is **inappropriate behaviour**, so more cases are coming to the surface. That creates a greater challenge for us because the media asks '**where was internal audit**?' when incidents emerge. Now, with social media, a small indication of **corruption** is blown up and it spreads everywhere."

Chief Audit Executive, Swedish public sector

"We are viewed to a large extent as assessing the **potential** for **corruption** of our civil servant employees. It's my opinion that in our agency the level of fraud is very **low** if you compare it against the rest of the country. Even if the level is low, the problem is that any single case of corruption in our agency is a **serious problem**."

Chief Audit Executive,
Spanish public sector

Corruption adds up to **10%** to the cost of doing business globally and up to **25%** to the cost of procurement contracts in developing countries

Source: UNPRI

57% of bribes are paid to obtain public procurement contracts...

...followed by **12%** paid for clearance of customs procedures

Source: OECD

COMMUNICATIONS RISK: PROTECTING BRAND & REPUTATION

The risks associated with brand and reputational harm have become more prominent as high-profile mistakes continue to be made in the public forum. Companies must think carefully about how they present themselves.

We found that just under one in five CAEs in our qualitative research has communications risk on their radar screens for 2019 and further into the future. Not all of this minority said they would definitely include this in their audit plans for the next 12 months, but it is a topic to watch as brand and reputational issues become more prevalent and there is an impetus for companies to think carefully about how they present themselves to the outside world.

Communications risk should be understood as the potential for an organisation to inadvertently harm its own brand value and reputation as the result of what it says in public. The importance of growing and protecting an organisation's brand and reputation is widely accepted. Reputation can have an immediate and long-term impact on an organisation's success by increasing consumer sales, as well as attracting investment and talent. Meanwhile, any number of incidents or events can damage reputation, from the uncovering of bribery, data leakages, or outstandingly poor customer service. The way in which an organisation responds to such events in the public domain can substantially mediate or exacerbate reputational harm. What's more, a poor communications strategy or ill-conceived marketing campaign can itself negatively impact upon reputation.

Therefore, organisations must take great care in the way that they present their image and values in the public domain. This is especially true in today's immediate and transparent social media age in which a single tweet can swiftly have unintended consequences. For example, in 2017 McDonald's tweeted an anti-Trump/pro-Obama message that, despite quickly being taken down, was retweeted and liked more than 1,000 times. Perhaps naively, the company did not foresee an inevitable backlash from Trump supporters and the subsequent #BoycottMcDonalds hashtag. It issued an apology and explained that its account had been hacked.

Social media platforms have helped businesses to open direct, spontaneous dialogue with their customers while giving companies a personality and a voice. It is a low-cost, responsive marketing tool that reaches millions of eyes. At the same time, social media increases reputational risk. At a time of political polarisation, social sensitivities are heightened and "saying the wrong thing" can seriously harm a company's reputation and brand value. Organisations must therefore be mindful of inappropriate messaging on social media and in their broader marketing and communications strategies.

Strategy, policies, roles

Undoubtedly, a key element of marketing is the efficacy of such efforts. Internal audit has a role to play in seeking evidence for the effectiveness of marketing budgets and expenditure, especially where this is quantifiable, such as pay-per-click spend on internet advertising. This, however, is an operational efficiency issue, not a reputational one. Similarly, there are compliance considerations regarding the way in which an organisation markets its products, services and itself, such as avoiding misleading statements and representations or targeting children. Again, internal audit can add value in assuring that controls are in place to mitigate the risk of breaches of relevant marketing regulations, such as those imposed by Ofcom in the UK, which could constitute a threat to an organisation's reputation.

However, even if a social media or other marketing campaign is fully compliant with local laws and regulations, it may not be appropriate or may be likely to offend, even if unintentionally. In 2018, clothing retailer H&M was publicly censured for promoting an item of clothing with the message 'Coolest monkey in the jungle' printed on it and worn by a young black model. The company rightly apologised for any offence caused and removed the image from its website, but the incident nonetheless sparked protests in the company's South African stores.

75% of board directors identify reputational risk as a top concern...

...yet only **6%** say they are well-versed in social media issues

Source: EisnerAmper

"We've seen a number of organisations **manifestly fail** in dealing with comms issues. **Oxfam** is a good example of how not to deal with a crisis, the CEO's response was dreadful. And yet others like **TSB** have been exemplary, by taking out adverts **apologising** for their mistakes. Comms departments need to understand who gives them **permission to operate**, whether they're regulators, the government, major suppliers or funders, or customers, and they need a really good understanding of those markets and how they deal with them. That relates to **social media** and how the organisation communicates on those platforms. There needs to be a **strategic understanding** of who the real audience is."

Chief Audit Executive,
UK public sector

7 DIMENSIONS OF REPUTATION

According to the Reputation Institute, there are seven dimensions of reputation that impact the way people perceive companies. These are:

Leadership
How is your company leading the way? Companies with CEOs and senior executives who take a stand on critical, often controversial, issues tend to outperform those companies that remain silent.

Performance
Numbers matter. Performance and profitability are key indicators of reputation success.

Products
Consistent delivery of quality products and services determine a company's value.

Innovation
Is your company static or dynamic? Innovative companies that creatively push the status quo are more highly regarded.

Workplace
Corporate culture directly impacts recruitment, retainment, and the quality, ability and willingness of companies' greatest asset — human resources — to deliver on strategy.

Governance
Only with stakeholder support from those providing your company a licence to operate and benefit of the doubt will result in continued growth.

Citizenship
How does your company add value above and beyond delivering products and services? Corporate social responsibility, charitable giving, volunteer efforts, and philanthropic campaigns help to make the world a little better.

When it comes to being "on message" there needs to be a strategy in place for how the organisation presents itself in the public domain. This should be closely aligned with the brand values and personality of the organisation and be consistent across all channels. All marketing and communications staff should be aware of, and have access to, written brand guidelines as well as policies that determine what can and can't be said. This is particularly salient for social media, which can often be treated as an add-on to existing strategies. Social media should not be an end unto itself but connected to broader business goals.

Appropriate sign-off processes should also be in place to mitigate reputational risks. This will depend on the medium for communication. For instance, scheduled press releases are likely to be approved by the Head of Public Relations/Communications whereas a Head of Marketing may sign off tweets and other social media posts. The objective is strong governance, effective line management and accountability, all of which should be documented and communicated to relevant staff.

Damage limitation

A crisis management plan should also be in place to follow in the event of the organisation acting improperly or inappropriately, whether as a consequence of its day-to-day operations, the comments of its CEO or other high-profile staff, or a misjudged marketing campaign. It is also advisable that senior mangement undertake media training so they understand how to deal with the press. The public will expect a swift and appropriate response and the organisation should understand how to apologise and "own" its errors of judgement in the public forum. Here, tone is important. All messaging should be earnest and empathetic and not seek to absolve the organisation (see Oxfam comment on opposite page). Canned statements are unlikely to be looked upon favourably, and a solution should be offered, such as the matter being reviewed so that it is not repeated or offending statements retracted. In many cases, a prompt, appropriate, measured and authentic response will be enough to mitigate what would otherwise be a catastrophic situation that could cause lasting reputational damage.

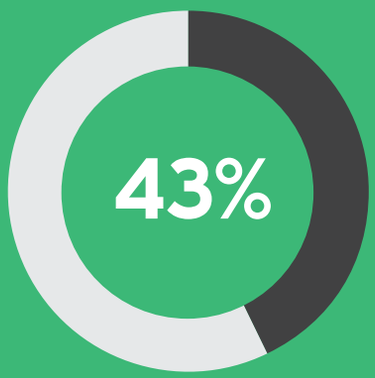
An internal audit perspective

Senior management and the board should be aware of the importance of brand value and the principle that a reputation takes years to build and only minutes to tarnish. If the organisation requires assurance around communications risk, internal audit should look for clear roles, responsibilities, ownership and accountability. Sign-off processes ensure that communications have been vetted and any potentially offensive or ambiguous messaging is prevented from publication. Documented communications guidelines and policies for what can be said and what should be avoided help to mitigate risk. Other internal controls and processes include access rights management to ensure that only those with authority can publish on social media accounts and corporate blogs, as well as crisis response plans to address company wrongdoings that have been publicised or communications that have been poorly received, such as ill-judged marketing campaigns or social media posts.

> "I have an audit for 2019 on social media. I want to make sure that the strategy is low risk and that we implement sound controls around the way the company manages the social media accounts. It's a key source of communications and marketing and it is managed at the corporate level, and we also have channels for our CEO, who is very high profile, and channels for each of the brands that we own. So this is definitely a hot topic for us."
>
> Chief Audit Executive, Italian retail group

Key questions

- Is the board and management aware of the potential reputational harm caused by poor communications?
- Who is responsible for the organisation's various communications channels and do they acknowledge their accountability?
- Are marketing staff aware of brand guidelines, the organisation's "voice" and what can and can't be said, e.g. policies around engaging in political debates?
- Are policies around what can and can't be said and the segregation of roles and responsibilities documented?
- Are access rights appropriately managed, e.g. changing social media account and corporate blog passwords when people leave the company?
- Is there a crisis response plan in place that involves both the CEO and the communications function?
- Does the organisation engage in communications scenario practices and are lessons learned from competitors' mistakes?
- Does the organisation have media training in place for those employees required to deal with the media e.g. CEO, Chairman?



43% of business leaders globally believe that their organisation is highly susceptible to reputational risk

Source: British Standards Institution

"There's **genuine risk** that an organisation's reputation is damaged if it does not approach ethics as an organisation in the right way and does not handle the media well. **Media management** is important. We are communicating a lot, increasingly via **social media**, and we need to be aware of how the organisation is **perceived**."

Chief Audit Executive,
Swedish telecoms company

"A **new risk** that is emerging is the relationship a company like ours has with social media and customer relations. It's becoming **more important** because we have new ways of **communicating** that are easier and more **direct with customers** and the public in general. With social media the gap between the public and the company has closed compared with an era in which mass media was the main channel for communication. So we have to **pay attention** to that."

Chief Audit Executive,
Spanish clothing company

"The **appropriateness** of the cultural messages that we **communicate** and send out into the world is an important issue. There have been instances where companies have run **marketing campaigns** that have been seen as offensive. It's very easy to **cause** cultural or religious **offence** and poorly judged messages can easily **damage** a company's **reputation**."

Chief Audit Executive,
Spanish consumer business

"The intensity and the ferocity of the attack makes you wonder, what did we do? We murdered babies in their cots? Certainly, the scale and the intensity of the attacks feels out of proportion to the level of culpability. I struggle to understand it."

In early 2018, then Oxfam CEO Mark Goldring responded to a staff misconduct scandal in Haiti. His comments in an interview with The Guardian newspaper elicited a backlash and Goldring was forced to apologise.

WORKPLACE CULTURE: DISCRIMINATION & STAFF INEQUALITY

Widespread allegations of the mistreatment of female actors in Hollywood emerged in 2017, giving rise to the #MeToo movement. While harassment in the workplace and society at large is not new, the pressure for this to change has never been greater, owing to the use of social media to spread global awareness of this issue.

Last year's report saw the inclusion of corporate culture as a hot topic and this remains a key risk area. Virtually all internal risk is predicated on the behaviour of staff, from senior management all the way down to workers on the shop floor. In our quantitative survey we found that 25% of respondents cited culture as one of the top five risks to their organisation, with 6% saying it is the single biggest risk. The fair treatment of staff and equality in the workplace is a subset of culture and we found that nearly 10% of interviewees in our qualitative research said they anticipate internal audit focussing more attention on this area going forward.

High-profile companies have been swift to respond to the #MeToo movement in recent months. Perhaps unsurprisingly, given the prevalence of claims emanating from the US entertainment industry, video streaming service Netflix, which produces its own television and film content, has issued an anti-harassment policy and training that prohibits staring, flirting and hugging in the workplace. Ride-hailing service Uber has dropped a controversial requirement that harassment allegations made against its drivers must go through a confidential arbitration process, allowing lawsuits to now be filed in open court. Meanwhile, a number of senior Nike executives departed in 2018 after a group of women at the sportswear company circulated a survey revealing numerous incidences of inappropriate behaviour, and a corporate culture that marginalised female staff and failed to take workplace complaints seriously.

While notable examples of anti-harassment awareness spreading into the business world since the #MeToo movement exploded have so far been concentrated in the US, corporate values in Europe and the rest of the world will increasingly be held to those expected in society. There is a need, therefore, for organisations to determine whether they are exposed to toxic male-oriented culture and inappropriate behaviours that put their workers and reputations at risk. This will mean ensuring that robust whistleblowing procedures are in place to uncover specific abuses and that HR functions take complaints seriously, follow up on reports of misconduct and embed robust policies around harassment, as well as diversity and inclusivity.

Supporting the staff diversity and corporate culture agendas is the revised UK Corporate Governance Code, which applies from 2019 onwards. The updated Code includes new principles and provisions on diversity and inclusion, as well as the alignment of company purpose, strategy, values and corporate culture, and the board's role in monitoring and assessing culture. Further, in a recent report the Women and Equalities Committee recommended that the UK government take action on sexual harrasment in the workplace by focussing on a number of priorities including the introduction of a new duty on employers to prevent harassment; improving enforcement processes, supported by a statutory code of practice; and greater controls around the use of non-disclosure agreements to silence victims.

Pay gap reporting

Viewed through a business lens, this issue falls under the umbrella of ESG (see page 16 on the topic of Sustainability: the environment and social ethics), a broader theme that is gaining regulatory traction and public attention. Authorities require that corporations are more transparent by reporting how they manage social issues, which ultimately exposes them to reputational risk once that information is published. As previously mentioned (see page 16), the EU's Non-Financial Reporting Directive requires that large companies publish reports on the policies they implement in relation to the treatment of employees and diversity on boards, among other indicators.

Supporting this reporting requirement is a broader commitment

25% of CAEs say that culture is one of the top five risks their organisation faces...

...**10%** say they anticipate that internal audit will focus more attention on discrimination and the fair treatment of staff going forward

Source: Proprietary Quantitative Research / Proprietary Qualitative Research

18%
of men in the UK workplace have experienced unwanted sexual behaviour

40%
of women in the UK workplace have experienced unwanted sexual behaviour

Source: BBC Survey

"If you look at key issues for 2019, a discussion around the #**MeToo movement** has to come up. It's an ethics issue but also concerns how people in the organisation behave with each other. Currently we are doing a lot of **investigations** into organisations where they have these exact issues that are being raised by #MeToo but are **not publicised** to the outside world. Internal auditors might have to look into that. In the past they may have focused on financial audits but now they have to look at all of the risks facing the organisation and **reputation** is a huge issue."

Chief Audit Executive,
Dutch professional services firm

"So far we have not looked at how employees treat each other or **gender discrimination**. There has not yet been a request to do that from the board or the labour council and we have not had a lot of **whistleblower cases** in this respect. But I think as an answer to society and what **society deems correct** and decent, it's likely to be something that **comes into play**."

Chief Audit Executive,
Dutch banking group

28%
of women have been subject to comments of a sexual nature about their body or clothes

Source: Trades Union Congress / Everyday Sexism Project:

35%
of women have heard comments of a sexual nature being made about other women in the workplace

from the European Commission with its 'Strategic engagement for gender equality 2016-2019'. This initiative seeks to:

- Increase female labour-market participation and the equal economic independence of women and men;
- Reduce the gender pay, earnings and pension gaps and thus fight poverty among women;
- Promote equality between women and men in decision-making;
- Combat gender-based violence and protect and support victims; and
- Promote gender equality and women's rights across the world.

At the national level, Germany and the UK have already introduced laws obliging listed companies to disclose their gender pay gaps in company reports. In the UK, official figures show that 78% of firms pay men more than women, with the median pay gap standing at 9.7%. As many as 1,500 British businesses failed to meet the 4 April reporting deadline, putting them in breach of the law. In addition to this compliance risk, such disclosure opens individual businesses up to public scrutiny and criticism. For example, it was shown that retailer The Body Shop had a pay gap of 38.9% despite employing more women throughout its business.

In France, President Emmanuel Macron awarded the Fédération Nationale Solidarité Femmes, a network of 65 feminist organisations, as the "grande cause nationale" for 2018 and has pledged to tackle the 25% pay gap. Proposed legislation would force companies to close any gaps within three years or face fines. If parliament passes the law, it is expected to be introduced by 2020.

Under a law introduced in 2018, German employers are required to disclose details of what they pay their staff and why any differences in remuneration exist. The law almost directly matches the UK's legislation, however, notably, companies in Germany are encouraged to carry out internal audits of pay structures to ensure compliance. Legislators fell short of making such audits mandatory, but this emphasis clearly demonstrates the value that internal audit can offer in supporting efforts to close the pay gap.

An internal audit perspective

Regulatory requirements are increasing with regards to the fair treatment of staff. In Europe this has centred around disclosures in company reports, so at a fundamental level internal audit can assist in ensuring that organisations are compliant, i.e. that, at the very least, the gender pay gap has been reported and published ahead of the deadline.

More than this, senior management and the board should be taking discrimination and inequality in the workplace seriously in all its forms (misogyny, homophobia, transphobia, racism etc). This should include having clear conduct, pay and promotion policies in place that are agreed with and enforced by the human resources function. HR should also document and follow up on accusations of mistreatment.

The issue of corporate culture has become and will continue to be a major consideration for organisations and internal audit has begun to address this by looking at soft factors, such as how senior management assure that the corporate values are reflected in everyday behaviour and whether excessive risk-taking is incentivised. Harassment and the unfair treatment of staff is undoubtedly a cultural issue, therefore internal audit should incorporate this into its existing work by seeking assurance that toxic culture is not harming certain demographics in the workplace.

Key questions

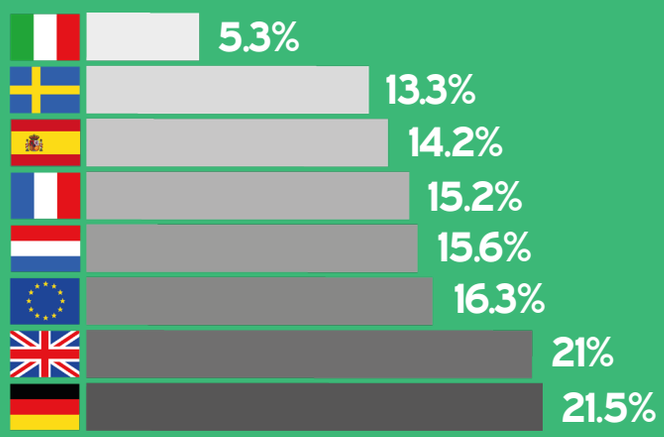
- Are senior management and the board paying sufficient attention to the shift in society regarding the fair treatment of women and other marginalised demographics?
- Have management set an appropriate 'tone at the top' with respect to harassment?
- Does the organisation have a clear and adequate anti-harassment policy in place?
- Is the organisation obliged to report on its gender pay gap? If so, is it compliant? And is the data accurate?
- Does HR communicate this policy, raise awareness among staff and effectively record and follow up on accusations of mistreatment?
- Does internal audit undertake audits that take into account culture? If so, is there scope to include surveys and other assessments that can shed light on how staff are treated within the organisation?

"Something we should have more of a view on is **diversity**, which is a hugely topical issue at the moment, and the impact diversity has on the quality of businesses. Whatever you think of the **gender pay gap**, it is here and businesses are having to respond to it. For companies like ours, the composition of boards absolutely **needs to be justified**. Greater diversity can only be a positive thing for organisations. So what can internal audit do about that? Well, what is the policy? How is that being deployed across the organisation? What are the barriers and are organisations genuinely **being honest** about their diversity and agendas?"

Chief Audit Executive,
UK financial services company

Gender pay gaps in key European markets

Source: Eurostat



-0.6%

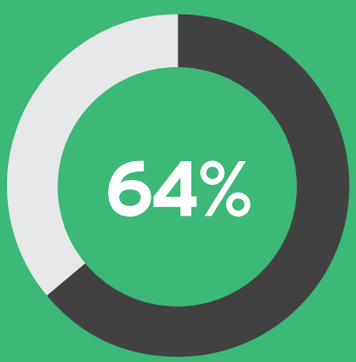
Across the EU, the pay gap has decreased by just 0.6 percentage points since 2011

Source: Eurostat

28%

The gender pay gap in the financial services sector across the EU is 28%, higher than in any other industry

Source: Eurostat



64% of Europeans are in favour of the publication of average wages by job type and gender at their company

Source: European Commission

"Internal audit should be thinking about how the first, second and third lines of defence operate together, and what sort of **investigative capacity** they have, who should do it and how that would fit together. That can be built into **culture audits** — what's the culture of power and how is it exercised? That could be broadened into a **gender** audit or **equal pay audit**. Thematically, that's very interesting and heads of audit can get on the **front foot** if they do something about that."

Chief Audit Executive, UK public sector

A NEW ERA OF TRADE: PROTECTIONISM & SANCTIONS

The recent rise of protectionist trade policies poses a significant risk to businesses. The US has engaged in a tit-for-tat with China over the competitiveness of imports which has spilled over to Europe and has the potential to depress sales into the US, the world's largest economy. Added to this burden is an increase in trade sanctions that carry heavy penalties.

We found that one in five interviewees in our qualitative research raised the potential impact of trade protectionism and the need to comply with export controls as important risk areas. There is no discernible country trend, although as might be expected the majority (66%) of those who cited these issues were in the construction and manufacturing, retail, or information, technology and communications sectors, i.e. multinationals that sell products and services globally.

Adhering to new trade sanctions and avoiding associated penalties can be defined as a regulatory and/or compliance risk; our quantitative survey found that 58% and 37% of CAEs see compliance and regulatory change as top five risks to their organisations respectively. Cumulatively, this puts these areas in the top five alongside cybersecurity, data security and digitalisation.

Trade protectionism, i.e. the introduction of import tariffs, is however better understood as a political risk that can result in reduced competitiveness and a loss of business; 23% of CAEs in our quantitative survey cited political uncertainty as a top five risk.

Last year, political risk made it to the hot topics shortlist in the form of uncertainties related to Brexit, national elections in Europe and Trump's plans to erect trade barriers. The prospect of Britain's departure from the EU remains a real and present risk, however is likely to weigh most heavily on the minds of export-oriented UK businesses and we anticipate internal audit will keep a watching brief as political negotiations develop and the deadline nears. At the time of writing, the UK and EU have still yet to agree on the terms of departure.

The trade threats made by the Trump administration a year ago, a key pillar of the President's election campaign, meanwhile, are now coming to bear. China has been the prime target so far. On 15 June 2018 the US published a list of Chinese products worth approximately $50bn that it plans to tariff at 25%. China retaliated with proportionate measures and the US subsequently drew up a second inventory of products valued at $200bn it will tariff at 10%, as well as a further list should China choose to respond again. The so-called trade war is now in effect.

But it's not just China that is bearing the brunt of these policies: 25% and 10% levies introduced on all steel and aluminium imports in the US are being felt in Europe, which along with Canada is the biggest exporter of these metals to America. In what is seen as a political statement, the EU has imposed its own 25% tariffs on iconic US goods including bourbon whiskey and Harley-Davidson motorcycles. If additional products and materials are burdened with duties and taxes, companies in Europe could see their revenues stall or fall if products become uncompetitive in the US market. At the same time, input costs for materials acquired in the US could rise, putting pressure on margins.

Following the introduction of these tariffs, Trump and European Commission President Jean-Claude Juncker entered into preliminary negotiations to avoid a full-scale trade war between the US and the European Union. Juncker said the goal is "zero tariffs, zero barriers, and zero subsidies on non-auto industrial goods", suggesting that Trump will follow through with proposals to tax European car imports. The US President added that he hoped to resolve the steel and aluminium tariffs issue and Europe's retaliatory tariffs.

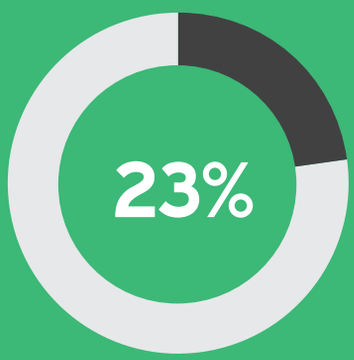
One of the defining hallmarks of Trump's presidency to date has been the unpredictability of his administration's policymaking. If negotiations are successful, the impact on European exporters will be limited, but political risk regarding trade remains and multinationals with subsidiaries in the US and China may bear a financial cost related to these developments.

One in five CAEs
say the potential impact of trade protectionism and the need to comply with export controls is likely to be an area of focus in 2019 and beyond

Source: Proprietary Qualititative Research

7,000 protectionist trade measures worth $400bn were introduced in the eight years following the financial crisis. This does not account for the recent raft of measures imposed by Trump, which includes 25% tariffs on $50bn worth of Chinese goods.

Source: Gowling WLG



23% of CAEs say political uncertainty is a top five risk their organisation faces

Source: Proprietary Quantitative Research

"Regulations are a concern, including the US's proposed **import taxes** on European products. I'm referring to cars but generally speaking this is a problem. I believe Trump's proposed tariffs are more significant for the mass market, so would not necessarily affect us. But the **US** is the most **important market** for us in terms of sales. This may impact us, depending on the meaning and **details** of the **tariffs**. It's too early to say but for sure this is an issue we need to **keep a watch** on."

Chief Audit Executive, Italian car manufacturer

"Political risk is a major consideration. The **potential** for **trade wars** that we see will impact us one way or another. Our **supply chain** is long and stretches across Europe and Asia. So those trade risks linked to developments in the US and how we secure the **flow of** our **goods** all the way from China to the Netherlands at the same cheap prices is definitely a concern, and is something that could develop into a **risk area** that requires internal audit's attention."

Chief Audit Executive, Dutch retailer

Germany is the European country most likely to be affected by any tarriffs as it has a high trade-to-GDP ratio of 86% due to its high proportion of companies that export goods

Source: World Bank

Sanctions compliance

Added to these protectionist challenges are complications surrounding trade and economic sanctions, again emanating from the US. These are largely focused on Iran and Russia; America pulled out of the historic nuclear deal brokered in 2015 which has wide-reaching consequences for trade with Iran. The US also introduced a round of sanctions on key Russian oligarchs, oligarch-owned companies, Russian government officials, and state-owned companies.

These developments can have significant unintended consequences that go beyond paying heavy penalties for non-compliance. For instance, a crackdown on Russian aluminium producer Rusal in April 2018 was meant to punish the company's owner, oligarch Oleg Deripaska. The move disrupted the market, sending aluminium prices higher and hurting carmakers and other manufacturers. The sanction was later softened, giving companies a grace period for cutting off ties with Rusal.

If the first 18 months of Trump's presidency are any indication of what is to follow, companies face an ongoing regulatory challenge. Last year the Office of Foreign Assets Control (OFAC) added 1,000 entities to its blacklist, almost 30% more than in Barack Obama's final year, making export controls a moving target that must be constantly watched. This creates a compliance burden for businesses with exposure to affected markets.

The effects of tariffs and sanctions are not always immediately obvious or direct. Businesses must be mindful of the disruption they can cause and decide whether they are significant enough to require supply chains to be restructured. Sudden shifts that affect supply chains can impact quality and availability, since companies may encounter issues when scrambling to reduce production in some places and ramp it up in others. Having visibility over suppliers and supply routes will be essential to minimise disruption and maintain profits.

An internal audit perspective

It is debatable whether trade protectionism and export sanctions, and geopolitics more generally, are auditable risks. The reactivity of governments is high and it is difficult to predict what goods will be affected and to what extent before formal guidelines are published. However, the ability of the organisation to respond to the policy changes and put into effect contingency and mitigation strategies is something internal audit can provide assurance on.

There is increased need for risk assessments through the supply chain, across geographies, to determine the potential for disruption, increased costs and depressed sales. Internal audit can assist by emphasising the importance of this assessment activity and providing evidence to management and the board that sufficient time and resources are being directed at these efforts, and that they account for the most recently available policy information. It is not for internal audit to say whether supply chains should or should not be restructured, but it can provide insight on the process of evaluating strategic decisions and reacting to political risks and assurance that the operational impacts on the supply chain are being considered.

Similarly, there is value to be added in assuring that the organisation's compliance and procurement functions are on top of export controls and sanctions. This should be directed at ensuring the organisation avoids penalties, but, more than that, sanctions can impact market pricing and competitiveness. The board may require assurance, therefore, that compliance efforts are linked to strategy-making processes, for example does the prohibition of trade in a sanctioned market increase the impetus for entering untapped geographic markets?

Key questions

- To what extent is the organisation likely to be affected by trade tariffs and in what way, e.g. direct impact on revenues and/or input costs, disruption to the supply chain? Is senior management aware of this?
- Is the organisation flexible enough to adapt to these changes, e.g. by reducing prices to remain competitive, or are revenues sufficiently hedged across markets such that the impact of US tariffs will be minimal?
- Does the supply chain need to be restructured or can the organisation withstand potentially higher costs and keep things as they are?
- Is the organisation responding to trade policy changes by conducting regular risk assessments?
- Are the compliance and procurement functions updating the trade sanctions register and ensuring that it is being complied with across the organisation?

Nearly 1,000 entities and individuals were added to the US sanctions blacklist in Trump's first year. This represents a nearly 30% increase over the number added during Obama's last year in office, and a nearly three-fold increase over the number added during Obama's first year.

Source: World Bank

"There's a lot of **unpredictability** regarding the markets we are present in and how they might be impacted by sanctions from the US. We operate in **Russia** and **export controls** is something that is always developing in one direction or another. If we want to **expand** into new countries, we have to be very conscious of what the situation might be in **five years'** time - can we be really sure that the **political system** is stable, there are no political conflicts and this country is not likely to be **sanctioned**?"

Chief Audit Executive, German retail group

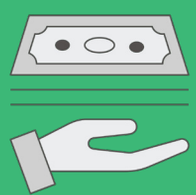
"Export controls and sanctions have always cropped up, but now that we have an **extended** sanctions **regime**, especially from the US, towards countries like **Iran** and **Russia**, that's now a real focus point. The Office of Foreign Assets Control of the US Department of the Treasury, which is responsible for **prosecuting** these kinds of violations, are tough on **penalties**. Sanctions are being imposed on Iran and if you ask all of the big players they are all looking into the **Middle East** to sell their products."

Chief Audit Executive, German software company

$10+

Trump's decision to re-impose sanctions on Iran seems to have played a major role in the roughly $10/barrel rise in the oil price since mid-March. This will put inflationary pressure on companies' production costs

Source: HSBC



$2,087,207,524

Over the past five years, the US Department of the Treasury's Office of Foreign Assets Control has assessed 90 penalties worth more than $2bn for apparent violations of economic and trade sanctions.

Source: Holland & Hart

RISK GOVERNANCE & CONTROLS: ADAPTING TO CHANGE

The pace of change to businesses' operations and the risks they are exposed to has never been faster. As organisations adapt to achieve growth, risk governance standards and control environments that were designed to mitigate yesterday's risks can quickly become outdated.

We found that one in ten interviewees in our qualitative research emphasised the need to assess or reassess their organisation's approaches to risk governance and controls structuring. This may seem self-evident. The purpose of internal audit is to provide assurance to board and audit committee in relation to governance, risk and internal controls across all areas of the organisation. They do this by testing and evaluating key controls and processes across individual business units, or apply audit programmes across the organisation as a whole. These efforts should provide a comprehensive, holistic view of the organisation's ability to adapt and update its control environment.

Modifying controls and deploying effective risk management in order to mitigate today's and tomorrow's risks and create maximum value has never been more urgent. International and national regulatory requirements are growing more complex, market disruptors are forcing established companies to quickly adapt their business models and strategies, control environments are combined in mergers and acquisitions, business functions are increasingly outsourced and processes are being streamlined and accelerated through digitalisation. This requires the introduction of new controls and refining existing ones to ensure that associated risks continue to be appropriately managed. In this sense, risk mitigation is in constant flux.

Some internal control and process changes are mandatory, such as those required by laws and regulations. The recent introduction of the GDPR is a clear instance of a regulatory development that is forcing wide-scale change to organisations' internal controls. However, in many cases the design and implementation of rigorous controls may fall behind the pace of change within the organisation.

To take an example, companies continue to migrate to the cloud critical software and data that were previously stored on internal servers. A previous business continuity plan (BCP) may have involved switching to an on-premise back-up server in the event of a network outage, but this may no longer be possible and if the continuity policy has not been updated the company's operations may come to a halt if their cloud provider's services go offline. This would require an update to the BCP.

Of course, it is not the responsibility of internal audit to design or implement the control environment, doing so would be a serious conflict of interest and undermine the third line's independence and objectivity. But that does not mean internal audit cannot give a holistic, top-down view of how effective and responsive the first line is in designing and implementing new controls across the organisation and not just the efficacy of specific controls in mitigating specific risks. That is, is the control design process itself sufficiently nimble and responsive, or is the control environment generally weak and rapidly outdated?

Agile innovation

This issue is particularly relevant for highly innovative companies investing in the development of new software applications and other technologies that the organisation can adopt once they are business-ready, either to sell to customers or to utilise in the company's own operations.

Businesses are using agile development in order to improve their rates of innovation and increase speed to market. It is a lean system under which technologies and other products are developed through collaboration between self-organising cross-functional teams and, in some cases, end users. This method produces rapid, incremental development cycles and it is estimated that companies deploying agile strategies at scale have accelerated their innovation by up to 80% [7].

According to the Agile Manifesto, this development method prioritises:

- Individuals and interactions over processes and tools
- Working software over comprehensive documentation
- Customer collaboration over contract negotiation
- Responding to change over following a plan

This may seem to be at odds with process-driven, controls-focused internal audit. It might be difficult to see what value internal audit can add in an environment that benefits from a high degree of autonomy, light risk management or soft controls. However, there is a hands-off, consultative role for internal audit to play in advising development teams on "risk by design". Rather than retrofitting controls to a new app or technology, internal audit can be involved in the development process from the start and offer its unique perspective and experience so that potential pitfalls are avoided, and the resulting product or service can be seamlessly integrated into the organisation's control environment once it is ready.

Providing assurance on the organisation's ability to innovate will also be of increasing value. Senior management may want a sense of the overall performance of innovation processes and whether deficiencies exist. At the heart of innovation audits lie the need to understand whether innovation strategies are aligned with the overarching corporate strategy, whether this is understood through the organisation, whether projects are effectively tracked, reviewed and scored, whether appropriate staff and departments communicate and coordinate effectively, and how successfully completed developments (e.g. products or apps) are integrated into the business.

A key challenge for organisations and internal audit is understanding how to measure the effectiveness of agile and other development approaches in delivering value and, taking a step back, the impact that constantly changing organisational structures has on risk governance and the overall control environment.

Key questions

- What is the overall quality of risk governance and management, e.g. is the second line generally effective, what does it do on a day-to-day basis and is it responsive to change?
- Has the organisation undergone, or does it intend to undergo, significant change in the last/next three years? What is the change (joint venture, digitalisation, app development etc) and does the internal control framework need to be adapted accordingly?
- Is control design and implementation responsive to changes and growth in the organisation?
- How is the adoption of technology impacting upon the control environment?
- Are ineffective and redundant controls that provide little value in mitigating risk dropped or replaced?
- Is internal audit able to stay on top of organisational change and the resulting impact on the control environment?
- Does the organisation engage in agile development methods and are they delivering results whilst mitigating future risks? Is this agile activity effectively coordinated or is it siloed and scattered?
- Can internal audit add value by advising on risk considerations early in development processes?

"We are striving for a real **simplification** of the control environment. Currently the control system is **too complicated** and with too much emphasis on legality and conformity. With our new integrated IT system and new organisational procedures, it's the right time for all stakeholders to put everything on the table to try and find smarter, more **fluent controls** for the operational engine."

Chief Audit Executive,
French public sector

"Internal audit is often focused on old organisational structures and the **risk governance** linked to that. Now we are moving more towards networked organisations and **agile development**. Are we equipped to assess that and can we think in the same way as we have in the past when it comes to controls, steering documents and the whole **assessment** of that? Does internal audit need to **adapt its approach** when it comes to agile development?"

Chief Audit Executive,
Swedish telecoms group

AUDITING THE RIGHT RISKS: TAKING A GENUINELY RISK-BASED APPROACH

There is a notable inconsistency between organisations' priority risk areas and where internal audit focuses its time. CAEs should therefore re-evaluate with their audit committees and stakeholders whether internal audit is being used effectively to deliver sound risk-based assurance.

One of the most striking observations from our quantitative survey is the mismatch between organisations' biggest risks and where internal audit spends its time. For instance, 15% of respondents said cybersecurity is the single biggest risk to their organisation and 66% said it is a top five risk, but only 5% said they spend the majority of their time auditing this risk. Conversely, 13% said compliance is the top risk and 58% said it is a top five risk, but a full 33% said this is where most time is allocated.

In other words, cybersecurity is more commonly seen as a priority risk than compliance, and yet more time is spent auditing the latter. This raises the question of whether internal audit is taking a truly risk-based approach in its work.

It is important to note that there are a number of possible explanations for this discrepancy, and these should be taken into account before drawing firm conclusions. These include the possibility that:

- CAEs and audit committees are not effectively assigning internal audit's time and resources to organisations' biggest risks, i.e. internal audit is not sufficiently risk based;

- Internal audit is required to carry out mandatory work, e.g. compliance audits, which may be seen as a priority by regulators but not by the organisation or internal audit itself;

- There is a difference between boards'/audit committees' and CAEs' perception of the greatest risks to the organisation (this should be discussed on at least an annual basis with senior management and the board when the risk-based audit plan is challenged and approved);

- Audit assignments are overrunning their allocated time, meaning that other areas of the business are overlooked;

- Assurance for higher priority risks is not, or is not solely, being provided by internal audit, e.g. they have been moved to the second line or outsourced providers are addressing these areas;

- Certain high-risk areas may not be auditable in practice and only require internal audit to provide less time-consumptive advisory support, e.g. consulting on risks related to political uncertainty.

Whatever the reason behind this finding, it is crucial that CAEs are confident that their audit functions are delivering the most assurance value by addressing their organisations' biggest potential risks.

Businesses are under constant pressure to innovate, grow into adjacent markets and new geographies, adapt business models and continuously change in order to compete. This makes the challenge of matching the third line of defence's assurance efforts with organisations' greatest risks more demanding as risk universes expand and expectations of internal audit rise. There is a danger that internal audit is not being utilised effectively to address the risks of today and tomorrow, and is instead backward-looking. If this is the case then the CAE should address this assurance gap with the audit committee. Indeed, one of the Core Principles of the International Professional Practice Framework states that internal audit's strategic plan should align with the strategies, objectives, and risks of the organisation itself, whether that includes adopting AI, moving into new geographies, or some other strategic goal.

The innovation advantage

True risk-based auditing is not only about correctly identifying an organisations' biggest risks, but balancing time and resources effectively. This is a persistent challenge for internal audit that can be overcome by upskilling and adopting data analytics techniques to achieve continuous auditing. Analytics not only

From our quantitative survey results we can see a notable mismatch between what CAEs perceive to be the biggest risks to their organisations and where internal audit spends its time.

"**Balancing** where we spend our time with where the risks lie is a challenge. The firm buys and sells assets, so clearly the **biggest risk** is that we do that well, the cycle keeps churning and our net asset value increases over time. We **don't spend** a great deal of **time** looking at the detailed investment proposals and whether we're selling to the right buyers at the right price. That process is **mature** and so it's questionable how much value we could lend to it, but there's a **conversation** to be had there. We tend, instead, to look at other things which are **indirectly linked** to valuation such as how well the portfolio is managed."

Chief Audit Executive, UK alternative investments manager

"The company is trying to strike the right balance with regulation. We are a listed company and there are regulations coming from both the equity and the bond markets. Regulators are applying pressure with regards to rules and I don't disagree with that, but we want to get it right in terms of getting value out of the process. This demands that we complete more formal, document-oriented audits that are not necessarily risk-oriented – they don't match what senior management or the audit committee wants from us. What they want is to understand how the business is doing. In internal audit we don't see much value in compliance audits other than ensuring the business is compliant. Whereas other audits of processes and business plans are where the real value lies. It's a challenging balance."
Chief Audit Executive, Spanish multinational construction company

holds the potential to free up internal audit's time, a further benefit is the ability to conduct whole population tests and therefore provide greater levels of assurance over areas such as accounts payable and payroll audits.

It is estimated that 76% of European internal audit functions currently employ analytics as part of the audit process, but of the quarter that don't, more than one-third (34%) have no plans to implement such tools [8], a situation that will become increasingly untenable as organisations continue to digitalise both their back offices and client-facing operations.

Analytics is no panacea, of course. The availability of good-quality data is essential to making continuous auditing effective. However, with the right skills and data it is possible to assess risks and evaluate controls more efficiently and provide broader and deeper coverage, with less time spent, i.e. internal audit achieving more with less. Analytics-powered continuous audits applied to areas such as compliance and financial controls can therefore free up internal audit's time to focus on high-risk areas that are seeing less attention, such as cybersecurity or strategic risks.

Blurred lines

Another solution is closer partnership and more effective information sharing between the second and third lines. Using the second line's risk assessments to inform the audit plan can help to ensure that the third line is homing in on the areas of highest priority. It may even be possible to transfer certain assurance work out of the third line (to the second line or with co-sourced arrangements) so that internal audit can turn its attention to areas where it is most needed. In any case, CAEs should coordinate and document activities with other internal and external assurance providers, through the use of an assurance map, to ensure proper coverage and minimise any duplication of efforts, as outlined by Standard 2050 of the International Professional Practices Framework.

However, a word of caution regarding transferring assurance duties between lines. Our quantitative research shows that 29% of internal audit functions perform some risk management duties. This alone is not a cause for concern, but 38% of this cohort are undertaking second line roles they should not be involved in.

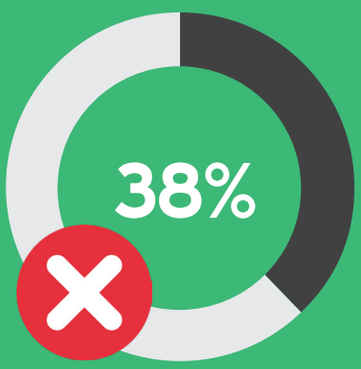
These duties include taking accountability for risk management, setting the risk appetite and imposing risk management processes, among others. Assuming such responsibilities seriously erodes internal audit's objectivity and should be avoided at all costs. Risk appetite must always be set by the board and, as per the revised Standard 1112, where the CAE assumes roles that fall outside of internal auditing, safeguards must be in place to limit impairments to independence and objectivity. As a CAE, if you believe that any responsibility you hold for risk management is impairing your audit objectivity, this should be addressed with the board immediately and any conflicting duties moved into the second or third line of defence, as appropriate.

Key questions

- As the CAE, are you confident that internal audit's time is being effectively matched to the organisation's biggest risks?
- If there is an observable discrepancy, what is the explanation for this? For example, is assurance coverage provided by another function?
- Is there a difference between boards'/audit committees' and CAEs' perception of the greatest risks to the organisation? If so, why and is this addressed and challenged on a regular basis?
- As the CAE, do you have a risk based strategic internal audit plan that is reviewed at least annually and shared and discussed with the audit committee?
- Is there potential to increase data analytics capabilities to achieve continuous auditing for more mature risk areas, e.g. financial controls?
- Are internal audit activities coordinated with other internal and external assurance providers to ensure proper and appropriate coverage?
- Is there an assurance map that clearly documents accountability for assurance across the organisation's key risks?
- Is the internal audit function undertaking second line duties and responsibilities that undermine its objectivity and pull its focus away from key risks that lack assurance coverage?

29% of internal audit functions undertake some risk management duties

Source: Proprietary Quantitative Research



38% of internal audit functions undertake roles that internal audit should not be involved in (see below)

Source: Proprietary Quantitative Research

Core internal audit roles in regard to ERM	Legitimate internal audit roles with safeguards	Roles internal audit should not undertake

Source: Chartered Institute of Internal Auditors

SOURCES

1. Cybersecurity Ventures — 2017 Cybercrime Report:

bit.ly/CyberVentures2017

2. Symantec — Internet Security Threat Report:

www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

3. Bild am Sonntag report:

www.bild.de/wa/ll/bild-de/unangemeldet-42925516.bild.html

4. Reuters/Ipsos — Americans less likely to trust Facebook than rivals on personal data:

bit.ly/FacebookTrust

5. Cisco — The Zettabyte Era:

www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

6. OECD — 2016 Data on Enforcement of the Anti-Bribery Convention:

www.oecd.org/daf/anti-bribery/Anti-Bribery-Convention-Enforcement-Data-2016.pdf

7. McKinsey — An operating model for company-wide agile development

www.mckinsey.com/business-functions/digital-mckinsey/our-insights/an-operating-model-for-company-wide-agile-development

8. Protiviti — Analytics in auditing is a game changer

www.protiviti.com/sites/default/files/2018-internal-audit-capabilities-and-needs-survey-protiviti.pdf