RISK IN FOCUS

HOT TOPICS FOR INTERNAL AUDIT 2018

A REPORT FROM EUROPEAN INSTITUTES OF INTERNAL AUDITORS

CONTENTS

Associazione Italiana Internal Auditors
Chartered Institute of Internal Auditors
Switzerland
ifaci institut français de l'audit et du contrôle internes
Instituto de Auditores Internos de España
Instituut van Internal Auditor Nederland

HOT TOPICS FOR INTERNAL AUDIT 2018

In 2016, IFACI , IIA Italy and IIA Spain published 'Hot Topics for Internal Audit 2017'. This year, a wider group of European Institutes of Internal Auditors have taken a more ambitious approach, interviewing Chief Audit Executives (CAEs) from major organisations in six European countries – France, Italy, the Netherlands, Spain, Switzerland and the UK – to home in on key themes requiring the attention of internal audit to mitigate risk and protect and add value in their organisations.

These Hot Topics were identified through in-depth, qualitative interviews with CAEs across a diverse range of critically important sectors – construction/infrastructure, financial services, IT, manufacturing, public sector, retail/consumer, telecoms and utilities/energy – and from organisations that truly lead these industries. To put this into perspective, these organisations have an aggregate market capitalisation in excess of €724bn, revenues of over €441bn, employ more than 1.86 million staff and are present in no less than 173 countries. In the financial services sector alone, the CAEs represent internal audit functions in firms collectively worth €325bn and turning over upwards of €207bn.

We are truly grateful to those who participated in our research. Their knowledge and insights provide an invaluable snapshot of the thinking of leading internal audit professionals across Europe.

The Hot Topics included in this report reflect risk areas that are being prioritised by CAEs as they prepare their audit plans for 2018 and make longer-term risk assessments. For some readers, these themes will already be fully reflected in their audit plans for the coming year. They may want to use our research to highlight to their audit committees that they are indeed on the right track. For others, this report may serve as a timely reminder as they finalise their plans for 2018 and beyond of issues that merit serious reflection. And for all, we hope that our publication will provide a fresh and relevant talking point, both for internal audit professionals and for audit committees and other stakeholders.

Contrasts and changes

Risks are not static and even the most fixed audit plans are subject to change as new risks emerge at the operational, strategic and wider environmental level. What constitutes a potential threat to one organisation may be deemed inconsequential by another. The most commonly identified risk area amongst CAEs of all nationalities and sectors is cybersecurity. This is no surprise given the scale of the threat and the extent to which all organisations have come to depend on technology. This is followed by the EU's General Data Protection Regulation and the broader challenge of managing data, with the pace of innovation businesses face the third most widely cited risk concern.

There are some observable differences in the priorities of CAEs in different sectors and, to a lesser extent, countries. From the sample we selected, it was found that political uncertainty was cited far more frequently by CAEs of organisations based in the UK, prompted by the prospect of Brexit and the potential impacts this may have as negotiations get under way. Spanish CAEs too cited political uncertainty as an area that could expose their organisations to emerging risks but also opportunities. This is the result of multinationals from the country having expanded into Mexico and the implications of the Trump administration's hostile position towards the country.

The financial services cohort were more concerned by regulatory complexity than any other sector. This is due to the passing of recent regulations and the impending introduction of new rules across the European Union. Notably, for CAEs at institutions in France, Italy, the Netherlands and Spain there is an added dimension in the expectations of the European Central Bank under the Single Supervisory Mechanism that came into play three years ago and which continues to develop.

The defining theme of this report, however, is the fundamental impact that technology has in shaping, enabling and disrupting organisations' operations and strategies – a pressure that requires internal auditors to learn new skills and adopt innovative tools to bolster their capabilities in an increasingly digital world.

We hope you enjoy this report and we welcome your feedback and engagement.

GDPR AND THE DATA PROTECTION CHALLENGE

The General Data Protection Regulation (GDPR) could have been filed under the topic of compliance or even the wider cybersecurity umbrella. However, this incoming regulation deserves particular attention for a number of reasons.

First, personal data is so pervasive in today's world that virtually every organisation of scale processes or holds such information in substantial quantities in terms of both customers and employees, making the scope of GDPR unmatched. Secondly, the deadline for compliance is fast approaching (implementation is required by 25 May 2018). Finally, and perhaps most importantly, penalties for failing to comply are potentially huge: for the most damaging breaches, fines of up to 4% of annual turnover, or €20m, whichever is higher may be imposed.

To put this into perspective, it is estimated that under GDPR the £400,000 fine issued by the UK's Information Commissioner's Office to broadband group TalkTalk for its publicised data security failings two years ago would have potentially risen to a massive £59m[1].

Further, a recent poll of 900 business decision makers around the world indicates that only 31% believe their organisations are compliant with GDPR, while analysis showed that only 2% of respondents actually appeared to be fully compliant[2].

The financial stakes for non-compliance are high and with much work still to be done to reach full compliance, boards should have already prioritised GDPR. Whatever progress an organisation has made to date, internal audit has an important role to play in assessing compliance from 25 May 2018 onwards.

Beyond security

The regulation foresees a strengthened role for security measures such as robust firewalls and encryption, and obliges companies (data controllers) to report any personal data breaches within 72 hours, even if it occurs at the third party (data processor) level. This will require enshrining data protection and governance measures into supplier contracts.

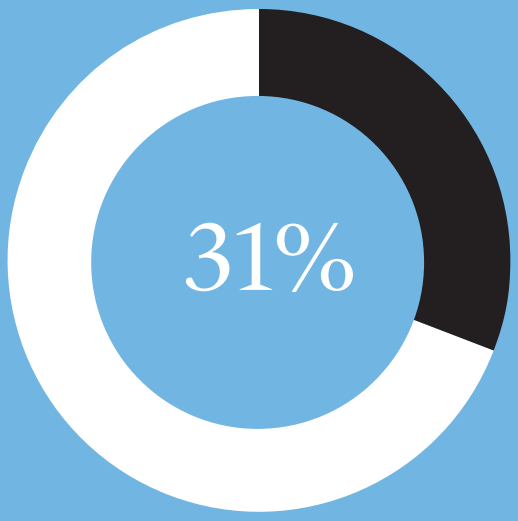
It is worth noting, however, that GDPR is not solely a cybersecurity issue. While it concerns the protection of personal data from hacks and leaks, the regulation is just as concerned with how organisations collect, store, use and disclose this data. (By contrast, the EU's Security of Network and Information Systems (NIS) Directive, which applies only to "operators of essential services", focuses exclusively on network security - see page 12.)

For instance, the new rules set higher standards for the "unambiguous" and "explicit" consent to collect data and in many cases will broaden the definition of personal data, encompassing potential online identifiers such as IP addresses.

Governance is another focus, with firms expected to show that they are implementing data protection by design when developing new products, and maintaining a register of personal data processing activities for companies with 250-plus employees. As well, under the regulation organisations whose core activity is monitoring data subjects and processing large volumes of sensitive data will be expected to appoint a data protection officer (DPO) who reports to the chief executive or other senior management, a responsibility that in practice can be shared amongst key people as long as the role can be identified.

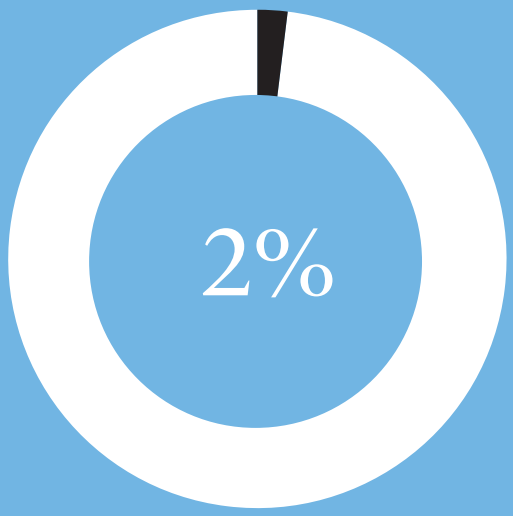
Another major consideration is the geographic reach of GDPR, which not only applies to organisations located within the EU, but also to organisations located outside of the Union that offer goods or services to, or monitor the behaviour of, EU data subjects. Cross-border data transfers are possible if the destination countries' own data protection rules are up to the same standard as GDPR. For example, US-based companies can use the EU-US Privacy Shield, a framework for personal data exchanges that has been assessed as compliant with the EU's incoming regulation.

Is your organisation ready for GDPR?



Only 31% of decision makers believe their organisations are compliant with GDPR

Source: Veritas



Only 2% of organisations actually appear to be fully compliant with GDPR

Source: Veritas

"**Data privacy** is an area we are **focused** on, particularly in view of the GDPR coming into play **next year**. Data and **data management** is becoming more of an emerging theme because data **governance** and **management** of data is not only related to security and privacy - it's also related to the internal processes to really **optimise**, to own data, to be aware of which data are available and the way they are utilised and **managed** for **commercial purposes**."

Chief Audit Executive, multinational UK mobile network provider

"We've done some audit work on **preparedness for GDPR** this year, but as a topic data - **the creation, protection, management of data** - is partially driven by our maturity and our dependence on data as an organisation. For us it is an important area and the new legislation helps to bring focus and momentum. We've looked at it to some degree this year and we will have something on the plan next year, which will likely fall under the **broader data umbrella** given our dependence on data."

Chief Audit Executive, multinational UK engineering and manufacturing company

China's standard

It is not only the EU that is bearing down on data privacy. In June 2017, China introduced its own extensive law that bridges the gap between cybersecurity and data protection, in essence merging the provisions of the EU's NIS Directive and GDPR. In many respects the Cybersecurity Law of the People's Republic of China (CSL) accords with the GDPR, such as requiring consent for data collection and protections against loss through encryption, for example. However, there are other major considerations for multinationals since "critical infrastructure" such as utilities companies and banks must store personal information collected in China inside the country, which may require repatriating data from overseas Cloud services. In addition, companies will have to submit to a review by regulators before transferring large amounts of personal data abroad. Any organisation concerned that they may be exposed to compliance risk in relation to CSL should seek expert legal advice.

An internal audit perspective

Legal and IT teams are already addressing GDPR compliance and internal audit is well placed to provide assurance by conducting a top-down risk assessment of how likely the organisation is to comply, by using gap analysis techniques to review existing controls and identify key areas that require improvement, and by consulting on the practical implementation of new controls and processes.

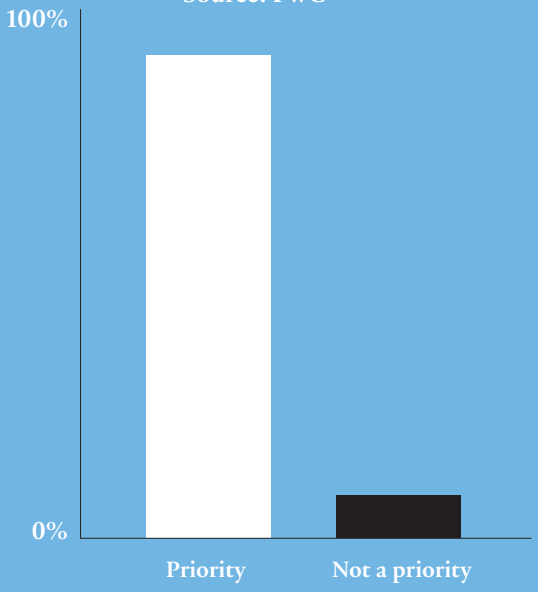
Key questions:

- Has a risk assessment been conducted to understand whether the organisation is compliant and where further work is required?
- Has the organisation mapped out its personal data assets (as distinct from other data assets)?
- Is the organisation's cyber perimeter secure and are personal data assets protected, e.g. encrypted?
- Does the organisation process personal data on a "large scale" and if so has an internal/external DPO been appointed?
- Do assurance providers have access to the DPO role however it is provided?
- Has a reporting procedure to the relevant national authority been established for use in the event of a personal data breach?
- Has the organisation established a programme to raise awareness and train personnel on the mangement, security and disclosure of personal data?
- Have data protection principles been enshrined into contracts with relevant third parties/data processors?
- Are measures in place to ensure the organisation remains compliant after 25 May 2018, including adding a work programme to the audit plan for 2018/19?

US companies are prioritising GDPR

92% of US companies consider compliance with the EU's GDPR a top priority on their data-privacy and security agenda in 2017

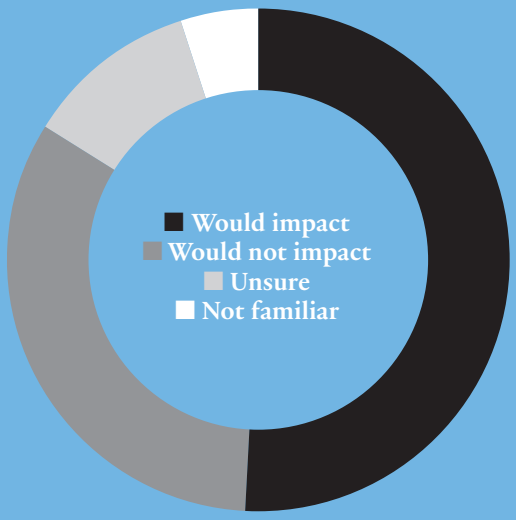
Source: PwC



GDPR awareness

51% of executives and IT security professionals believe GDPR will impact their companies, 33% don't see it impacting them, 11% are unsure and 5% are not familiar with GDPR

Source: Imperva



"GDPR and the **implications** of that are gaining prominence. The company has **set up a multi-disciplinary** team with external support to look at how we get from where we are today to where we need to get to at the point the **legislation** goes **live,** and beyond. From an assurance perspective, the audit committee will want us initially to assess the programme itself but then for us to **develop** our own **programme** on an ongoing basis to make sure the business has the right processes in place in order to continue complying."

Chief Audit Executive, Euro Stoxx 50 multinational banking group

CYBERSECURITY: A PATH TO MATURITY

The global Wannacry attack, which was reported to have infected more than two million computers in over 150 countries, brought cyber resilience and information security into sharp focus in 2017.

Within 24 hours the cryptoworm, a type of self-propagating ransomware, had taken hostage the IT systems of major organisations from the UK's National Health Service to Spain's Telefónica, FedEx and Deutsche Bahn, to name just a few. If boards were already thinking about prioritising cyber assurance then Wannacry, and later Petya, a global attack that followed shortly after, escalated this item to the top of audit committee agendas for 2017 and it will continue to be a high priority through 2018.

Of course, cybersecurity has by now already established itself as a key business risk. Digital information permeates practically all aspects of businesses' operations, regardless of sector, from customer data to intellectual property to HR records. This trend is only set to increase as organisations exploit the Internet of Things, migrate more of their operations to the Cloud and transition to data-dependent, digital-led business models. This means that virtually all organisations are exposed, both to external cyber criminals and hackers, but also malicious employees and careless workers who fail to follow procedures.

Awareness versus preparedness

There is a persistent gap between organisations' cyber risk awareness and their preparedness to withstand potential attacks, which must be closed. Notably, 62% of organisations expect cyber risk to cause disruption in the next three years, and yet 74% have low or no cyber risk maturity[3]. Clearly this is a cause for serious concern.

In recent years governments have responded to the rising threat by launching centre's of expertise, such as the UK's National Cyber Security Centre and Spain's National Cryptologic Centre, to defend public administration systems and warn the private sector of emerging threats. Europe-wide bodies such as the European Cyber Security Organisation have also been established to promote cyber innovation and best practice.

Additionally, government guidance and certification programmes are a good place for organisations to start fortifying themselves against breaches and give internal audit a foundation for providing fundamental assurance to the board. For example, by now every UK organisation should have undergone a Cyber Essentials Plus evaluation, and while this is only open to organisations based in the UK, all businesses should at the very least have adopted the scheme's five key controls (see page 13).

Once the basics are covered, organisations have a choice of guides and frameworks to adopt, such as NIST Framework for Improving Critical Infrastructure Cybersecurity, ISACA COBIT 5 and the Emerging Cyber Nexus, SANS Institute and the Top 20 Critical Security Controls and PCI DSS Control Catalog. As well, internal audit functions should consult the Institute of Internal Auditors' Global Technology Audit Guide 'Assessing Cyber security Risk: Roles of the Three Lines of Defence' for guidance on how it can add assurance value.

Installing basic controls, adopting a framework that suits the organisation and positioning internal audit to assess the effectiveness of these initial measures are essential to reaching at least a modest level of cyber risk maturity.

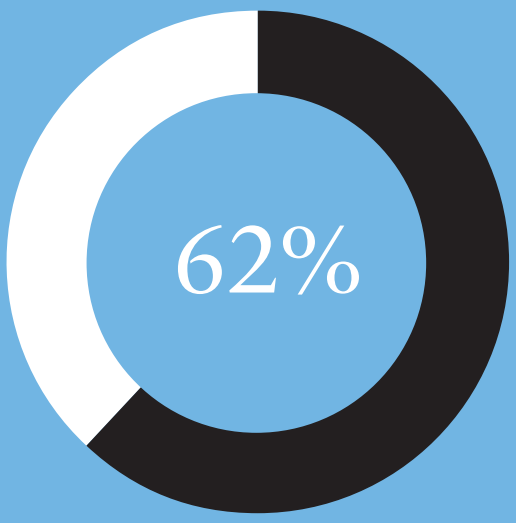
Cyber culture

Understandably, organisations tend to view cyber-security through a technical lens by investing in the latest security tools, then seek assurance that these are working and controls and procedures are of a sufficiently high standard. However, while the behaviour of correctly configured and maintained software and technology is relatively predictable, the same cannot be said for user behaviour. Mission critical data can be compromised or lost through the carelessness of employees. It is therefore critical that - in addition to controls and technical defences such as firewalls - organisations embed a cyber culture that manifests itself in staff behaviour and is developed through company-wide training and awareness programmes.

"We have been doing audits regarding **cyber threats**, data loss, network security, mobile devices and so on for three or four years, and it's an area where we need to increase our focus. Unlike the more traditional, operational risks, technology is **constantly changing**, so just being stable doesn't help you for the future. We have to keep track of what is changing so that our **situation doesn't erode further**."

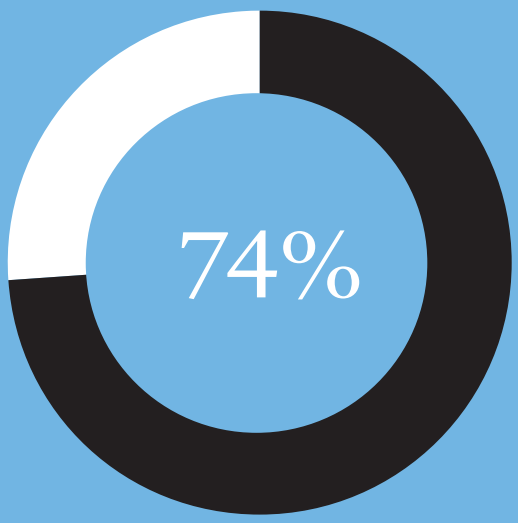
Chief Audit Executive, multinational Spanish construction and infrastructure group

The gap between cyber awareness and cyber preparedness persists



62% of organisations expect cyber risk to cause disruption in the next three years

Source: PwC



Yet 74% of organisations have low or no cyber risk maturity

Source: PwC

"**People talk about digital disruption and innovation** and how that will impact upon them, but are **they still doing what they should about their legacy systems?** What happened earlier in the year with the global **Wannacry attack** shows what can happen when organisations forget about all of the open back doors. We're setting up an **IT audit specialism at the moment**, bringing together our people with **capabilities in that area** and seeing how we can **enhance our offering**."

Director, UK government agency

All employees, including contractors and remote workers, must understand exactly what is expected of them with regards to policies and behaviours. This organisational response is one of the most crucial steps in mitigating cyber/IT vulnerability risk. In this respect, internal audit can play a valuable role by providing assurance that, not only cyber controls are in place and working, but cyber risk awareness is high and best practice is reflected in employee behaviour.

Cyber compliance

In addition to the need to protect valuable information assets and the organisation's reputation, there is a compliance component to consider. We have dedicated a topic to the EU's incoming GDPR (see page 6) because it applies to all businesses and is distinct in that it concerns personal data only.

What gets less attention is the Security of Network and Information Systems (NIS) Directive, which by 9 May 2018 will be implemented into national law. NIS, which applies to "operators of essential services" in both the private and public sectors, is more concerned with network security and the continuity of services. Unlike GDPR, NIS does not impose fines for data breaches, only for not reporting hacks.

The first step for all organisations is to determine whether they fall under the scope of the directive, which covers energy, transport, banking and financial market infrastructures, health, water, elements of public administration, and certain digital service providers. Regulated operators will have to take appropriate security measures to prevent network breaches, ensure the security of network and information systems, and handle incidents including reporting any "serious" breaches to the relevant national authority. Organisations should speak to their national regulator to determine what constitutes a serious breach.

Internal audit has a role to play in providing assurance to the board that the organisation has determined whether it will be subject to NIS and has put measures and processes in place to abide by the new rules, by fortifying networks and installing appropriate reporting procedures.

An internal audit perspective

All boards should, with the help of internal audit, have a broad view of the organisation's response to the rising cyber threat and the quality of its cyber governance and risk management. Moving forward, assurance work may drill down into the specifics, including, but not limited to, the completeness of data asset and network/entry point mapping, the robustness of access rights management, network penetration testing, audits of third party Cloud service providers, ensuring that contingency and response plans are sufficient, and assessing how able the organisation is to respond to this evolving threat.

Key questions:

- Has the organisation recognised the potential threat to business resilience, reputation and even revenues that cyber risk poses?
- Are key controls in place and/or has a recognised framework been installed?
- Does the organisation understand which of its data assets are most valuable and have they been mapped?
- Does the organisation have effective and updated firewalls and malware protections in place?
- Are existing protections being effectively penetration-tested?
- Is the governance around access rights sufficiently robust?
- Is the IT/dedicated cyber function staying abreast of developing threats and emerging cyber attacks?
- Has a healthy cyber culture been established and are policies reflected in employee behaviour?
- Do assurance functions have sufficient technical skills to interpret their findings?
- Is the organisation prepared to respond and recover in the likely event of an attack?

"It's a big concern because it's still an unknown risk. The **maturity level** of the organisation to mitigate and monitor the risk still **requires attention from the board**, the risk committees and senior management. Then there's the maturity from a technical perspective, the teams and the skills. This is the **focus of internal audit**. We are reshaping and changing our skills profile, hiring subject matter experts and establishing a **basic cybersecurity audit programme**. Our understanding is that most organisations in our sector are in the same situation."

Chief Audit Executive, multinational Spanish banking group

5 Cyber Essentials

1 Boundary firewalls and internet gateways

Mapping and protecting your perimeter is the first step. Firewalls and gateways provide a basic level of protection where a user connects to the internet and keeps attackers or external threats from gaining access to the organisation's network by monitoring all traffic and blocking incoming breaches, as well as employees from accessing areas of the network for which they don't have privileges.

2 Secure configuration

Firewalls and gateways are of no use if they are not correctly configured. Rogue agents can use common security scanning tools to easily detect network vulnerabilities, which can then be exploited resulting in a compromised system and data loss.

3 Access control

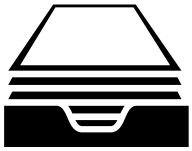
It is important to restrict access to a minimum and avoid so-called "privilege creep". User accounts, particularly those with special access privileges should be assigned only to authorised individuals; they must also be managed effectively, and provide the minimum level of access to applications, computers and networks. This should also include the use of unique usernames and the regular update of passwords. Access rights should be reviewed periodically.

4 Malware protection

It is important to protect the business from malicious software which will seek to access files stored on the network. Once installed, malware can access and steal confidential information, damage files or lock them and hold them at ransom. Malware protection helps to identify and prevent/remove any potential threats from malicious software. Such protective software must be regularly updated and installed on all connected devices.

5 Patch management

Cyber criminals often exploit widely known vulnerabilities in software or operating systems to gain access. Patch management is about keeping software on computers and network devices up to date and capable of withstanding breaches. Updates and security patches should be installed in a timely manner and any unsupported or unlicensed software removed.



REGULATORY COMPLEXITY AND UNCERTAINTY

As organisations look to 2018 and beyond, the compliance burden can appear daunting. Virtually all CAEs cite GDPR as an area that requires attention and for this reason we dedicated an entire topic to this wide-reaching impending regulation. But other regulatory issues are high on organisations' agendas.

Highly regulated sectors such as utilities and telecoms have their own regulatory considerations to contend with in Europe, but it is the financial services sector that will bear the brunt of impending regulation.

MiFID II

Arguably the biggest shake-up of legislation in the European financial sector for over a decade is due on 3 January 2018. The purpose of the second Markets in Financial Instruments Directive, or MiFID II as it's better known, is to strengthen investor protection, prevent market abuse and increase the transparency of trading in investment products such as stocks, bonds and swaps, and touches on all aspects of electronic trading, reporting and storing of information. Efforts to implement the required changes should be equally directed at how the organisation's control environment needs to change to maintain compliance after the legilsation goes live.

Its implementation had to be delayed by a year because firms and regulators did not have their systems in place to comply with it. Even as recently as July 2017 research showed that 90% of institutional investors in Europe risked being non-compliant, and were under-prepared and overstretched in their efforts to comply[4]. This isn't helped by the fact that midway through 2017 approximately a third of the rules were yet to be formalised, either by national regulators or through technical guidance detailing exactly how they should be implemented.

Compliance clash

The picture is complicated further by the apparent incompatibility of MiFID II and the GDPR. Under the former, any telephone calls, emails and other electronic communications that are intended to result in trades and transactions are expected to be recorded. Meanwhile, the GDPR imposes much tougher rules on the protection

New accounting standards impending
2018 will see the introduction of two new IFRS Standards and the early adoption of IFRS 17.

IFRS 9 Financial Instruments requires an entity to recognise a financial asset or liability in its statement of financial position when it becomes party to the contractual provisions of the instrument, measured by its fair value.

IFRS 15 Revenue from Contracts with Customers establishes principles an entity applies when reporting information about the nature, amount, timing and uncertainty of revenue from a contract with a customer.

IFRS 17 Insurance Contracts discloses information that shows the effect that insurance contracts have on the financial position, financial performance and cash flows of an entity.

For more information, visit www.ifrs.org

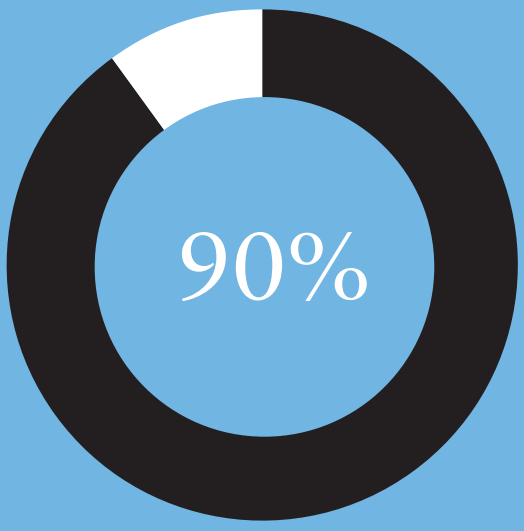
"We find **contradictions** between what **local regulators** say and what the **European Central Bank** requires for the entire group. This affects multinationals and is a huge headache for us. Knowing **how to address many regulators** while being a profitable, well organised company is very difficult. That has **incentivised dialogue** with regulators."

Chief Audit Executive,
multinational Spanish banking group

"The regulatory agenda connected to **Brexit** in terms of where we do certain types of business and **who** that **will be regulated** by is huge. The ongoing pace, scale and **complexity of regulatory change** is something that our emerging risk team is having to air-traffic control and understand what the organisation must focus on - whether it's **changing systems, processes or reporting** required by regulators and our ability to **land that change** at the appropriate times."

Chief Audit Executive, multinational UK banking group

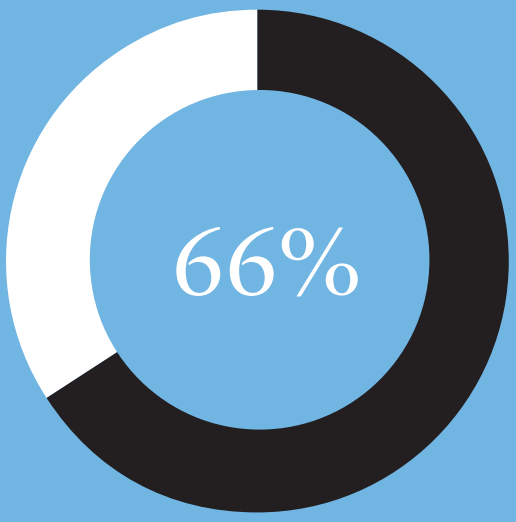
Preparing for MiFID II



90% of institutional investors in Europe risked being non-compliant with MiFID II

Source: PwC

Risk of regulatory scrutiny



Regulatory change and heightened regulatory scrutiny is seen as a "significant impact" risk for 66% of board members

Source: PwC

of sensitive data captured by any means of recording, with potentially huge penalties for any breaches. By strengthening the rights of individuals to choose not to have data captured by call recording and other means, the GDPR appears to conflict with interpretations of MiFID II.

If exceptions to this discretionary data collection can be made under MiFID II, it still leaves financial services firms exposed to potential data breach risk as they will be expected to adequately safeguard a whole new set of personal communications data.

Also going live in January 2018 is the Payment Services Directive II (PSD2), which as well as putting an end to credit card surcharges is designed to increase competition by lowering the barriers to entry for fintech start-ups. It aims to do this by obliging banks, which are seen to have the unfair advantage of having years or decades-long headstarts over fintechs, to provide other organisations with access to their customers' financial information. Once again, this is seen as being at odds with GDPR's data protection measures. PSD2 means that banks are likely to be sharing customer data with dozens of fintech companies. GDPR is concerned with making customer data traceable, secure and easy to erase. Reconciling the two will be a challenge.

Personal accountability

In the UK, financial services firms are under pressure to comply with the Senior Managers and Certification Regime (SM&CR), which was introduced in the banking sector in 2016. In 2017 the Financial Conduct Authority (FCA) extended the rules to the rest of the financial services sector, with the wider scope expected to be implemented in 2018. The set of rules apply to all staff and require that individuals must act with integrity, due care, skill and diligence, be open and co-operative with regulators, pay due regard to customer interests and treat them fairly, and observe proper standards of market conduct. The FCA recently published a consultation document on its website and is seeking feedback on the roll-out of the rules until 3 November 2017.

The most crucial aspect of SM&CR is that it introduced accountability for senior managers, so that should something that falls under their remit go wrong they can be held personally liable. The rules apply to all firms operating in the UK including foreign organisations operating in the country via a single branch.

With so much change taking place, it is little wonder that compliance functions are feeling the pressure to keep up. Data show that the volume and pace of regulatory change is the top concern for not only compliance professionals in the financial services sector but their boards, ahead of cyber and technology resilience. Looking across all industries, regulatory change and heightened regulatory scrutiny is seen as a "significant impact" risk for 66% of board members and executives[5]. This suggests that boards and audit committees are likely to require assurance that compliance is being effectively managed.

An internal audit perspective

Compliance and regulatory risk is a constant concern for organisations. But with so many milestone rule changes either on the horizon or having recently passed, there is more pressure than ever to ensure compliance is being effectively managed. This has not been helped by the Brexit referendum and US Presidential vote, which represent major regulatory unknowns for countless organisations, particularly where future trade rules are concerned. Internal audit has a role to play in assessing whether compliance functions are on top of the latest applicable regulations and that appropriate steps have been taken to ensure that the organisation is compliant, and - where there is uncertainty or conflict with existing or other incoming rules - that dialogue with the relevant regulator/s has been established.

Key questions:

- Is the organisation confident that it has done everything in its powers to comply with all relevant regulations?
- Does the organisation have systems and procedures in place for reporting non-compliance incidents and disciplinary deterrents to prevent them from occurring in the first place?
- Does the organisation review compliance breaches and take steps to ensure they are not repeated?
- Is the compliance function adequately resourced and capable of effectively monitoring, prioritising and implementing forthcoming regulations?
- Are training programmes in place to ensure that employees and other company representatives are aware of their compliance responsibilities?
- If the organisation is a multinational has it identified any regulatory clashes between jurisdictions, and where these can't be reconciled has this been reported to the appropriate regulator?
- Is the business flexible and adaptable enough to remain fully compliant while maintaining growth?

Tax planning

In August 2016 the European Union ordered Apple to pay a record-breaking €13bn in back taxes to Ireland after it was ruled that an arrangement between the world's largest company and the Irish tax authorities amounted to illegal state aid. Apple had been levied as little as 0.5% under the deal instead of the country's 12.5% corporate tax rate.

By booking profits at an Irish head office that existed only on paper, the company avoided paying tax on virtually all of the profits made on the billions of euros of products sold across the EU's single market. Both Apple and Ireland have appealed the decision in court, which will take years to resolve. If the European Commission wins it will establish it as the ultimate arbiter on taxation in Europe, superseding national government policy.

The Apple ruling and fine were well-timed. A month prior the EU had introduced the Anti Tax Avoidance Directive (ATAD), aimed at preventing this exact exploitation of tax mismatches between member states. Less than a year later in May 2017 and ATAD II was introduced, extending the mismatch treatment between member states and non-EU countries. The new rules will come into force on 1 January 2020.

The directive was largely prompted by the Organisation for Economic Co-operation and Development's BEPS (Base Erosion and Profit Shifting) framework, published in December 2015. So far more than 100 countries have issued rules on implementing these reporting requirements, which were written to create a fairer and more effective international tax system, including increasing efforts to close loopholes, improve transparency and ensure that multinational enterprises pay tax where they carry out their activities.

Tax planning is unlikely to fall off the agenda any time soon, with the public and national governments paying close attention to how businesses treat this issue. Ninety-one per cent of multinationals say that tax structures are under greater scrutiny from authorities now than they were a year ago, although encouragingly, 86% of multinationals say that their organisation has assessed the potential impact of changes related to BEPS[6].

However, the political uncertainty seen today, including Brexit, the future stability of the EU and the new US administration, requires organisations to pay close attention to potential tax changes and their associated impact on strategic decisions.

Many boards will want to understand how the BEPS framework impacts upon the business's operations and financial reporting processes, and what must be done to respond to national policy changes in response to the BEPS initiative. In some cases assurance will be required around the alignment of tax planning strategies with the organisation's strategic goals and public image, and around contingency plans in the event that any reputational controversies emerge.

"**Regulatory aspects** change often and are very **complex**, for example the EU's unbundling requirements under the 'Third Package' legislation, which have forced the separation of energy groups' sales and distribution activities. The result is an ad hoc setup for selling and another one for distribution. The **audit plan needs headroom** as laws and regulations change. It also needs to be flexible so that internal audit can respond to requests coming from the regulator."

Chief Audit Executive, Italian multiutility group

PACE OF INNOVATION

Market leaders increasingly have to think like start-ups in order not only to defend their market positions but to spearhead innovation. In the 11 years between 2005 and 2016 global R&D expenditure increased by a compound annual growth rate (CAGR) of 4.94% to $680bn[7], as businesses have sought to increase their revenues through innovation at a time when technological advances continue apace.

The primary emphasis is transforming companies of the old, analogue economy to agile digital players that exploit back office optimisation and automation efficiencies and harness big data for competitive advantage. Banks are investing heavily in fintech to reposition their local bricks-and-mortar business models to become digital operators that can compete at a time when blockchain technology is establishing itself. Retailers are exploring virtual reality applications and the use of drones to improve customer experience. Businesses, particularly in manufacturing, are employing the Internet of Things to smarten up their operations and make efficiency gains. Automakers increasingly identify as software and tech companies in the era of self-driving cars.

"It's very difficult to create innovative businesses that can **compete with fintechs** that have been built in the last 12 to 24 months. We are a multinational bank and were **established more than a century ago**. From a risk perspective, internal audit needs to be **on top of how the organisation innovates**. Everybody wants to create **data lakes and use blockchain**, but few think about what the **correct risk frameworks** for those activities are. The challenge is if you start managing this innovation with old risk management perspectives, because you are going to **limit the innovation as it is conceptualised**. This will be a huge challenge for internal audit from now on."

Chief Audit Executive,
Spanish multinational banking group

This rapid pace of innovation is not natural for well-established, slow-moving organisations. Start-ups thrive because they create environments in which speed, experimentation, failure and learning fast are part of the way their business works. This contrasts with the environments typically found in large organisations, which have carefully constructed risk management frameworks and where change is intentionally incremental.

Such slow-moving environments can stifle innovation and leave market incumbents exposed to digital disruption. One in three directors say that their business model will be disrupted in the next five years[8]. Clearly, becoming obsolete is a significant strategic risk that organisations must mitigate; at the same time, rushing headlong in a new direction and investing heavily comes with its own risk of failure. Organisations must understand where investment would be most effectively directed, fund and resource the most appropriate projects, understand the return on investment (RoI) and know when to pull the plug on lacklustre innovations.

Approaches to innovation are also growing more complex. In the past, internal R&D departments were solely responsible for this activity. Recently, multinationals have sought to sample from Silicon Valley's entrepreneurial spirit by setting up proprietary corporate venture capital arms and start-up accelerators. Even more recently this is giving way to "co-opetition", i.e. open innovation strategies that see organisations, and in some cases competitors, co-operate to their mutual benefit and to progress their industries. In the next decade, internal models will decrease by 23% and collaboration networks will increase by 50%[9]. This raises questions for how to manage the risk of such shared models.

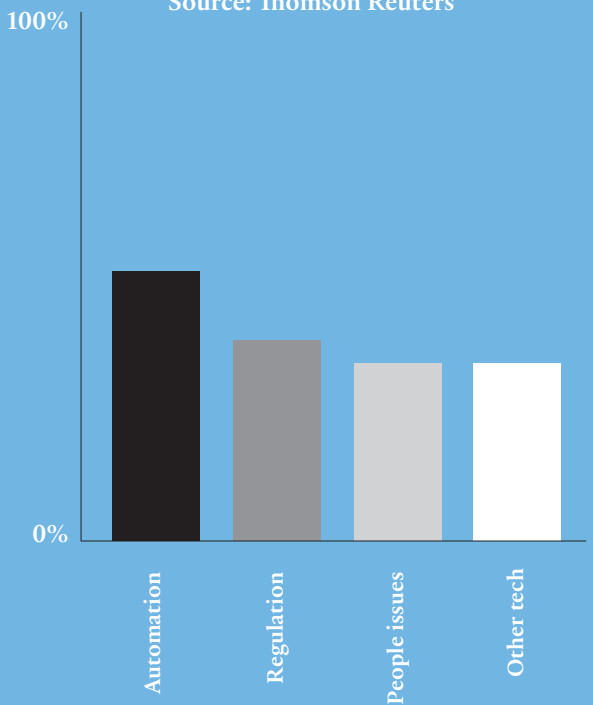
Big data, big risk

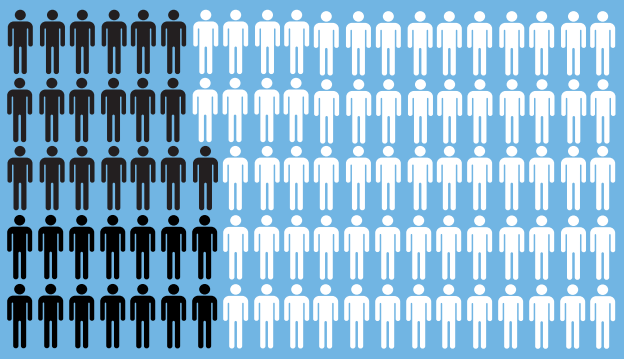
One of the biggest buzz terms in the business world of recent years is big data. As more of us are connected to the internet more of the time, leaving a data trail everywhere we go, organisations have almost limitless opportunities to gain insights. Data has become crucial to understanding

The biggest business disruptors

51% of executives say that automation will be the biggest business disruptor 25 years from now, followed by regulation (43%), people issues (38%) and other technology that is not not yet available (38%)

Source: Thomson Reuters





A third of directors say that their business model will be disrupted in the next five years

Source: McKinsey

"There is a set of new world **risks** related to the **transformation** of the **economy.** The **digital world** is increasingly **replacing** the physical world and the pace of **innovation**, digitalisation and **e-commerce** is rapid and **constantly changing.** That results in a lot of changes to systems, **processes**, **controls** and risks themselves. Many of this links to third parties that are used for **new kinds** of **operations** such as logistics, which for us is a very **important risk.**"

Chief Audit Executive, multinational Dutch clothing company

"The world is continuously changing and the **pace of change is accelerating**, which puts **pressure on organisations to adapt** in order to keep up. Organisations may be trying to make too many simultaneous changes and are not truly able to deal with everything they intend to achieve. This leads to a difficult reconciliation between all of the objectives the organisation has set and all of the **changing priorities** they have. When there is a crisis there is a rush to put out fires, but then you have 20 more fires behind you. That can be seen as **excessive ambition** on the part of organisations, which are **trying to embrace everything at the same time** and in doing so are putting themselves at risk."

Chief Audit Executive, multinational Spanish IT services provider

customer behaviour and companies are looking at ways they can harness data to predict future sales and precisely target marketing to achieve higher conversion rates.

Worldwide revenues for big data and business analytics will grow from $130.1bn in 2016 to more than $203bn in 2020, a CAGR of 11.7%. In addition to being the industry with the largest investment in big data and business analytics solutions (nearly $17bn in 2016), banking will see the fastest spending growth[10].

But one of the criticisms of organisations' rush to crack big data is a failure to ask 'why?' before asking 'how?'. Many have gained insights into their businesses and their customers that alone have no intrinsic value and won't help to grow revenues. This isn't helped by the fact that many big data projects don't have a tangible RoI that can be determined upfront.

The fast-paced development of analysable data lakes and other big data projects is relatively new. However, operational change is not. With change comes uncertainty and risk and the implementation of new procedures, processes, systems and operations to respond to changes in the business environment and grow revenues requires change management - whether that change is digital or not.

An internal audit perspective

Technology is fast-moving and organisations must ride the wave of innovation to keep up. This puts pressure on internal audit to ensure that senior management thinking around investment into new technologies, business models and organisational approaches is robust and results in RoI. Organisations should have horizon scanning procedures in place to identify technological threats and opportunities, and internal audit can play a part in assessing the quality of this intelligence gathering.

R&D and innovation projects should be audited to ensure they are effectively managed to mitigate project risk and, as they near commercial roll-out, delivery risk. All the while internal audit must strike a balance by not slowing or standing in the way of rapid innovation that will be crucial to the organisation's future success, but equally providing an assurance that projects deliver the promised benefits. Digitisation also has an impact on the control environment, which may increase the likelihood of fraud, meaning that basic controls such as the separation of duties may require renewed focus from internal audit.

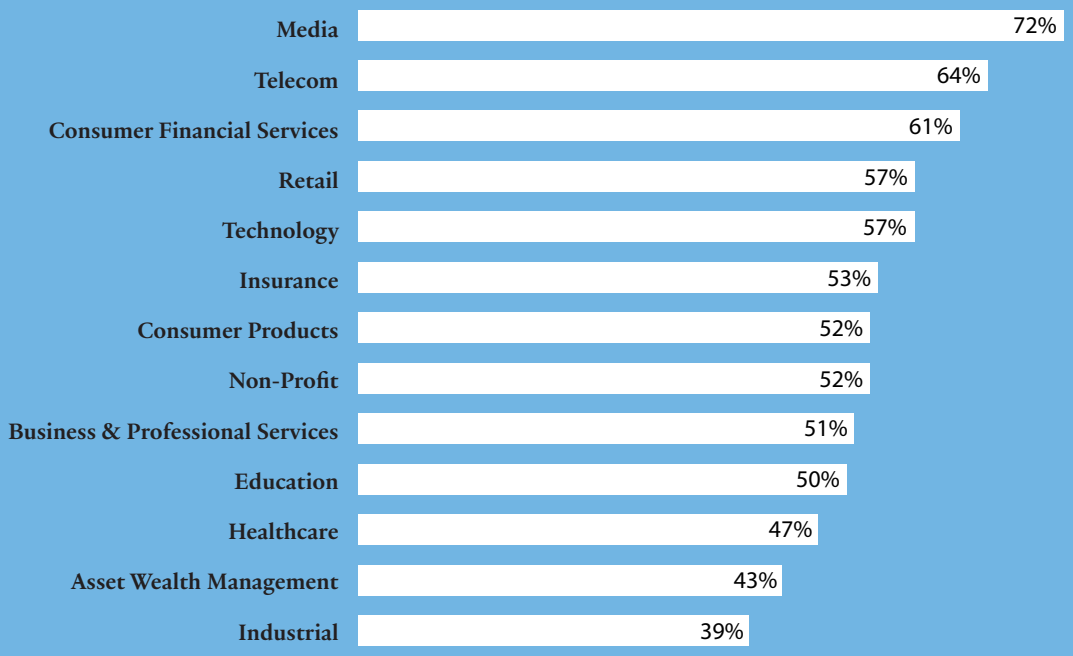
Key questions:

- Are all change projects effectively managed?
- Does the organisation have a process for identifying emerging technology threats and opportunities? Is it robust?
- Are all of the organisation's R&D and innovation projects mapped?
- Is there a risk management process in place for assessing the validity of these projects, which includes internal audit, from the outset and on an ongoing basis?
- Is the organisation thinking about the 'why?' as well as the 'how?' when it comes to innovation?
- Does the firm evaluate innovation in the short, medium and long terms?
- Does the organisation have the necessary skills to make its innovations a success?
- Is the RoI of R&D expenditure effectively measured and does this feed back into where investment is directed?
- Does the organisation have the responsiveness and agility to increase or decrease innovation if necessary?
- Is there an expectation at the board or senior management level that internal audit will provide an assurance in relation to the robustness of project management within the business?

Sectors most disrupted by digital

Senior executives' view on which sectors face moderate to massive digital disruption in the next 12 months

Source: Russell Reynolds Associates



"The **digitisation and innovation** piece is something that's very big for the retail sector, as well as many others. There's the **strategic threat** of disruptive technologies, but also the potential to gain a competitive advantage. That could be the development of **virtual reality** to enhance the customer experience or the use of **drones** to complete the final kilometre of product delivery. That's very fast paced and comes with inherent risks."

Chief Audit Executive, international Dutch food e-commerce and supermarket group

POLITICAL UNCERTAINTY: BREXIT AND OTHER UNKNOWNS

The unexpected Brexit referendum and US Presidential election results of last year have profound implications for the risk landscape. To date, Brexit negotiations have scarcely got underway and the bold, protectionist trade reform policies that drove Trump's campaign have yet to materialise. But both could result in significant change - and with change comes risk.

In themselves, Brexit and the stability of the EU are not strictly risks. But Brexit will have a knock-on effect on key areas such as immigration and trade, both of which could have meaningful impacts on organisations' workforces and supply chains. As has already been seen, foreign exchange rates have experienced volatility, increasing currency risk at organisations that do not benefit from the natural hedge of a broad, diverse geographic presence.

In a post-monetary-easing world in which growth has been relatively weak and propped up by central bank policy, any shock political developments surrounding trade and the free movement of labour could cause confidence to evaporate and economies to turn down.

The operative word here is "could". It is difficult for organisations to prepare for the impact of political and legislative negotiations when their outcome is unknown; for example, only 29% of UK businesses have made plans for exiting the EU, which is likely due to the lack of anything meaningful on which to base a plan. However, more worrying is that more than half (57%) of businesses have not even gone as far as discussing the risks that Brexit poses to them[11].

The future of the EU

At the beginning of 2017 a number of key elections looked to be heading in the favour of hard-right political parties, raising concerns over the future of the European Union. Populist parties have largely gained momentum campaigning on the spike in immigration, and have been exploiting nationalist sentiment concerned with reclaiming sovereignty from the EU, a spillover effect from the Brexit referendum.

"**Brexit** will feature quite strongly in next year's audit plan. It's **difficult to know what the impact will be**. At the moment the work is around resilience - so regardless of what happens how agile are we and how quick are we able to **respond as the situation emerges** and to what the future model might look like? You don't know what's going to happen, but **how resilient the organisation is** to those potential changes is going to be an increasing theme, and I expect that will **change over the course of the year**. So we'll have time set aside for Brexit-related work without necessarily knowing at this stage what we're going to be doing."

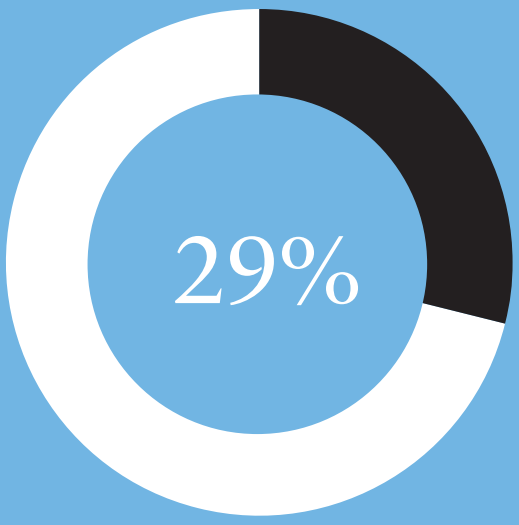
Chief Audit Executive,

FTSE 100 engineering and manufacturing group

"It's about considering what the **impact** of **Brexit** is on us as a business and once we know what some of those effects are then we'll have to put in plans and **react accordingly**. At the moment it's very much about monitoring, trying to sometimes second-guess what might happen, because the business is trying to plan three to five years ahead. We are not doing a formal **Brexit audit**, it's just about asking: 'Is this the right decision to make and will Brexit affect this decision?' So we're taking more of an **advisory role**."

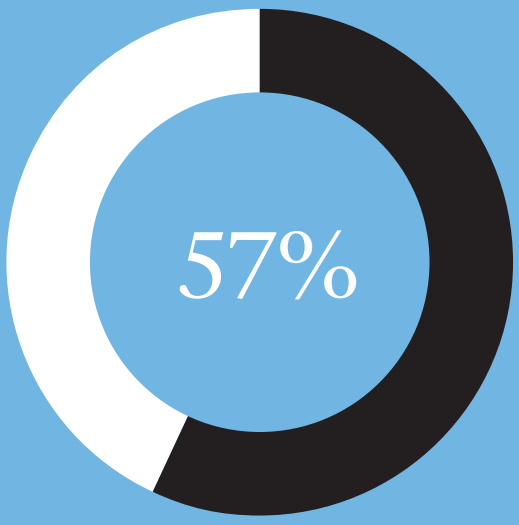
Chief Audit Executive, FTSE 100 UK retail group

Businesses failing to plan for Brexit



Only 29% of UK businesses have made plans for exiting the EU

Source: ICAEW



57% of businesses have not even gone as far as discussing the risks that Brexit poses to them

Source: ICAEW

"**Brexit requires agility**. It's a moving feast, so you end up setting aside time without allocating it to a specific piece of work. In other areas it's much easier to consider what the **possible scenarios** may be and then you can see whether the organisation's approach looks sensible. A lot of our work at the moment is asking: '**Are you as a department thinking about what the impacts may be on you?**'"

Director, UK government agency

Emmanuel Macron beat his far-right opponent Marine Le Pen in the final round of the French Presidential elections in 2017, followed by the defeat of anti-EU populist Geert Wilders by prime minister Mark Rutte in the Dutch elections. Both of these results can be seen as a win for mainstream politics and a tilt away from the populism of the far right.

Germany and Italy, both of which have seen a surge in support for far-right parties, face their own elections, in September 2017 and by the end of May 2018 respectively. There are so far no Eurosceptic parties in Germany, with data showing that only 24% of Germans would vote to leave the EU[12].

The key campaign issue remains immigration which, despite subsiding since the crisis escalated in 2015, is a pressure still being significantly felt in Italy. Political support in the country has been drifting to the right in recent months, which could realistically result in the election of a party that supports the reintroduction of a national currency, if not a full exit from the EU.

Once again, "could" is the operative word and uncertainty is what defines developing political risk. Suffice it to say, the future of the European Project is not guaranteed and organisations across the Union should remain aware of the potential for significant change and determine whether they are prepared to respond to, and withstand, any changes in the broader political landscape.

Until recently most organisations were largely indifferent to which side of the political spectrum, left or right, governed as both sides had become pro-market and pro-business. However, politics have polarised and the rise of nationalist parties with anti-global, anti-immigration and protectionist economic policies threatens to discriminate against foreign trade, workers and goods, creating significant business risk.

An internal audit perspective

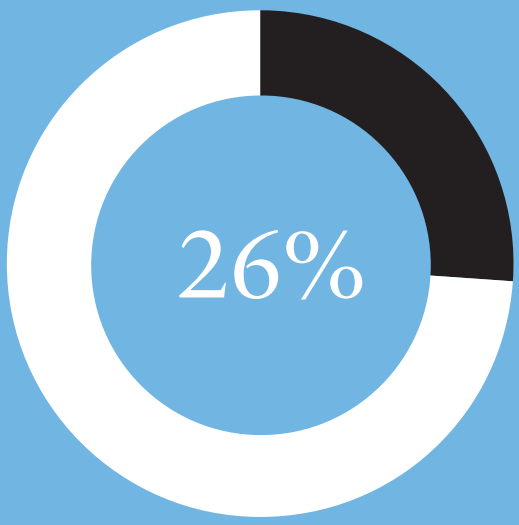
Given the unpredictability of Brexit, the future of the EU, the policy direction of the Trump administration and other political and geopolitical unknowns, it is difficult for internal audit and other assurance providers to give specific and detailed advice to their organisation.

At this stage, the key consideration is business resilience. Internal audit will be expected to provide an assurance that organisations are agile and responsive enough to swiftly adapt their operations to an uncertain, changing political landscape. The internal audit function should also review whether the organisation has a process in place to identify potential political changes, whether management is thinking about these changes and their specific impact on the organisation, and also has a consultative part to play on multi-disciplinary Brexit/political risk working groups in its trusted advisor role. For many, formal audits will not be necessary or required until concrete policies emerge. Once the picture on future immigration, trade and other policies becomes clearer, the internal audit function will be expected to monitor how effectively the organisation is responding, and has responded, to these changes.

Key questions:

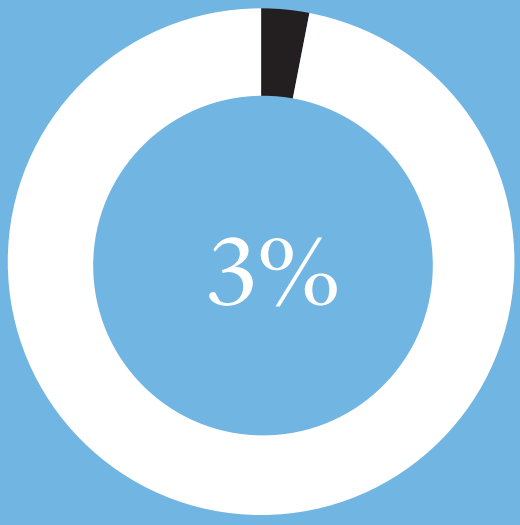
- Does the organisation have a process in place for identifying political risk?
- Has management considered what specific political risks might mean for the organisation and mapped these to different business units?
- Has this mapping process been extended to the organisation's supply chain and other third parties?
- Is the treasury function effectively managing/hedging currency risk?
- Has management considered worst case scenarios concerning immigration barriers, trade tariffs, fiscal and monetary policy changes and how effectively the organisation would respond?
- Is the organisation agile enough to adapt its operations if necessary?

Political risk a priority for insurers



This year political risk was the top macroeconomic risk for 26% of insurers

Source: Goldman Sachs Asset Management



In 2016 only 3% of respondents identified it as the top risk

Source: Goldman Sachs Asset Management

"Things like **Trump** and **Brexit** and **elections** in many countries, these represent a potentially **huge shift** in the way businesses need to be run. **Organisations** need to learn how to be **flexible enough** to adapt. A three-year strategic plan can change in months or even weeks, so you really need a **contingency plan** to be able to rectify **strategic planning** because, more and more, uncertainty is going to be the normal scenario in which **businesses operate.**"

Chief Audit Executive, multinational Spanish banking group

VENDOR RISK AND THIRD PARTY ASSURANCE

Third party risk has returned to the fore. This is in part because organisations continue to seek cost efficiencies from outsourcing and are increasingly migrating their operations to Cloud-hosted services. The so-called "make or buy decision" also continues to shift, meaning traditional manufacturers increasingly source original components for assembly instead of making them in-house. All of this means that processes and assets that were once housed internally are outside of the organisation but, nonetheless, must be effectively managed and secure.

Broadly speaking, the underlying risks relate to business resilience and reputation (see box, right). The organisation must understand how exposed its business is to the potential interruption caused by a third party supplier suffering a cyber attack, losing its licence to operate, becoming insolvent or simply failing to meet increased demand; third parties should be mapped out and a risk assessment conducted to score the likelihood and severity of risk a third party or supplier poses.

There must be a clear view of how the organisation would respond to such a situation and whether contingencies are in place to maintain business continuity. This includes assessing the business resilience of third parties themselves by reviewing and querying their own governance and controls.

This is where sound due diligence processes are crucial. When the organisation takes on a new supplier it should be thinking beyond the products and services that the vendor is supplying and its ability to deliver them, and look at whether the third party itself prioritises business resilience and effectively manages its own risks such as bribery compliance, cybersecurity and data protection.

Human rights agenda

Third party risk is not only about ensuring business resilience and protecting the organisation's reputation. There have also been a number of recent legislative developments concerning human rights that escalated this risk to the top of the agenda. For example, the UK's Modern Slavery Act is prompting organisations to ensure they can live up to mandatory transparency statements highlighting their efforts to stamp out human rights abuses, both internally and in their supply chains. Other countries have introduced their own legislation aimed at putting a stop to slave labour in supply chains. In a globalised world this raises an important question: how deep into supply chains do assurance activities need to reach? The answer will depend on organisations' risk appetite.

Reputational risk by proxy

There can be a tendency to assume that outsourcing means outsourcing risk, but third party crises typically trace back to the client organisations, which tend to be more high-profile and newsworthy. This is especially true where the crisis in question involves loss of customer data, where the third party is indirectly tax-funded or the end product or service is consumer-focused.

For example, the TalkTalk data breach that cost the UK telecommunications company 100,000 customers was the result of a cyber attack that occurred via a third party that had access to the company's network.

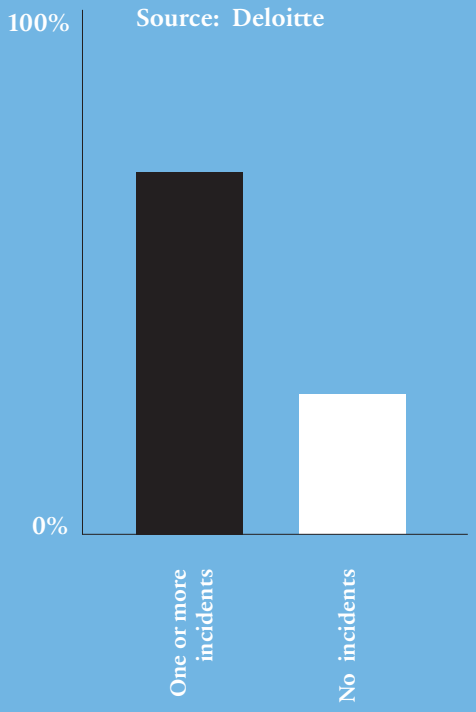
Meanwhile, suicides at China's Foxconn factories resulting from low pay and poor working conditions sparked a mediastorm against Apple largely because the factories were responsible for manufacturing the company's popular iPhone handsets.

Similarly, retailers such as Primark and Matalan found themselves embroiled in the tragic collapse of Rana Plaza, a Bangladeshi factory in the clothing retailers' supply chains in which 1,400 workers lost their lives.

Third party incidents

74.1% of global companies have faced at least one third party related incident in the last three years

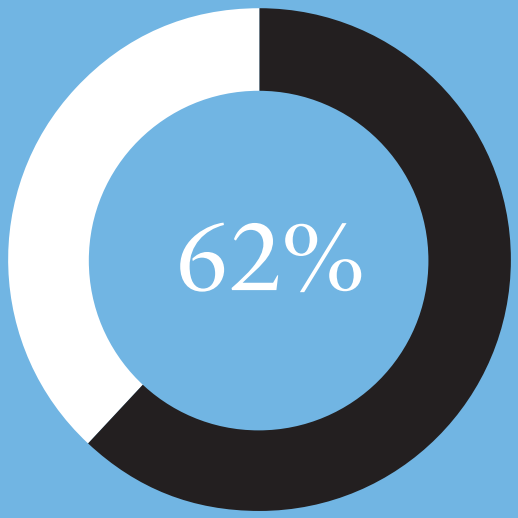
Source: Deloitte



Supplier due diligence

Global companies conduct due diligence on just 62% of their suppliers, distributors and third party relationships

Source: Thomson Reuters



"**Gaining assurance** over third party **control environments** is becoming more pertinent for our company. We're **outsourcing more and more** of our activities, particularly on the IT and Cloud computing side. Everyone **understands** what it's being used for to **enhance** the businesses, but no one's that sure what it means from a **risk perspective** and therefore what assurance they should be getting from their third parties. The **organisation** needs to get much better at understanding those risks and the **assurance coverage**."

Chief Audit Executive, multinational UK recruitment group

In France a new law, "le devoir de vigilance", requires that the client organisation must assess and monitor contractors' commitment to the prevention of environmental, human rights and corruption risks; and in 2017 the Dutch Parliament proposed a bill that, if enacted, will require businesses to investigate the existence of child labour within their operations and supply chains. The bill covers not only businesses registered in the Netherlands, but also companies selling products to Dutch consumers, including online retailers, although small businesses will be exempt.

Similarly, Italy last year committed to its five-year National Action Plan on Business and Human Rights, which places an emphasis on the ethical integrity of supply chains, in line with the UN Guiding Principles on Business and Human Rights.

Policymaking increasingly puts human rights at the heart of business regulation and this is only due to increase as countries adopt best practice. This means that robust due diligence processes are essential and should combine human rights considerations with the review of business resilience and other key third party risks.

"Supply chain **disruption and sustainability** is **important** for us and that includes auditing third party risk and also business continuity within our own estate. That's not just **interruptions to manufacturing activity** but also **quality issues** and delivery cost. Internal audit needs to ask how far the organisation **peels back the onion** into the **depths of the supply chain**. What's necessary? What risks is the organisation prepared to take? Is that being articulated well? Are mitigation measures in place? Does everyone understand the **risks they are taking**?"

Chief Audit Executive,
UK engineering and manufacturing group

An internal audit perspective

Internal audit has a crucial role to play in providing assurance around supply chain risk. At a basic level the organisation must be confident its supplier can deliver the product or service required, including increasing or decreasing production or service on demand. But a growing emphasis on human rights, cybersecurity, strong bribery governance and high environmental standards - and the potential reputational fallout from third party incidents manifesting - means that due diligence of suppliers and contractors has never been more important.

Internal audit can add value by reviewing the governance around procurement and contract management, checking that audit rights are written into supplier contracts, that suppliers have robust whistleblowing procedures in place and by working with the procurement function to ensure that due diligence processes are comprehensive and meet the risk mitigation needs of the organisation. A major challenge is deciding how far down the supply chain audits and assurance should extend. This will depend on how much risk the organisation is willing to expose itself to and how well resourced its assurance activities are. As a rule of thumb, assessing three tiers along any given supply chain should provide appropriate assurance.

Key questions:

- Has an end-to-end third party risk assessment been conducted to map the business's external activities (e.g. procurement, logistics, distribution, manufacturing and Cloud hosting) and the organisation's exposure to risks?
- Is the organisation confident that suppliers are able to cope with any increases in demand?
- Do the organisation's procurement activities have robust due diligence processes to assess the governance and risk profile of outside suppliers?
- What assurances are there that third parties are effectively managing their own risks, including business resilience, cyber security and bribery compliance?
- Are third parties complying with new human rights focused legislation?
- Have suppliers and third parties been risk scored depending on their geography and sector, and therefore susceptibility to human rights, corruption and other risks?
- Is the organisation confident that the level of risk their third parties are exposed to is consistent with its own risk appetite?
- Is the organisation confident that the behaviour of third parties doesn't impact its reputational risk?
- Does the organisation have a contingency plan in place in the event of a loss of third party operations or a reputational incident?

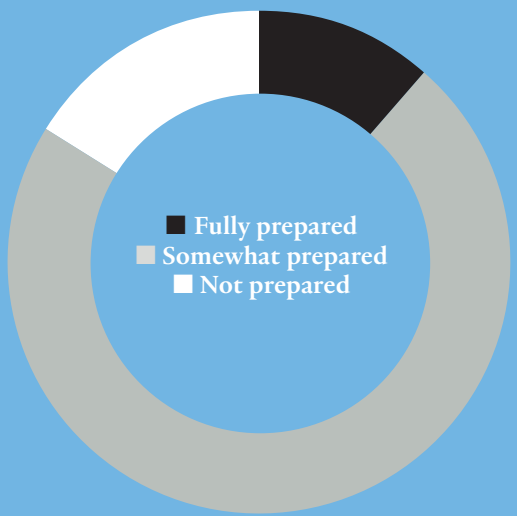
"**Third parties** include everything from **pensions administration** and parts of the financing function to, more recently, the **management** of **customer data**. That comes back to GDPR. Not only do we have to be compliant, our **customers entrust** us with their personal data and we don't want to break that trust. So ensuring that third parties are **managing our data effectively** and securely is important. Management can sometimes see risk as being pushed over the fence when it comes to outsourcing, but that's not the case. We need to **help management understand our third party risk** and whether the company is keeping pace with its changing relationships."

Chief Audit Executive, multinational Dutch retail group

Third party uncertainty

Just 11.6% of companies feel "fully prepared" to deal with the increased uncertainty in the external environment, while 72.3% feel "somewhat prepared" and 16.1% are "not prepared" to deal with this uncertainty

Source: Deloitte



THE CULTURE CONUNDRUM

Corporate culture has by now established itself as a boardroom priority. Many organisations, particularly in the financial services and the energy sectors, have lost the public's trust and must work hard to repair their reputations. And the issues and incidents that jeopardised those reputations have largely been the direct or indirect result of poor corporate culture.

Building a strong culture and tone at the top is crucial for minimising reputational and compliance risk, and also creating long-term value. But how do organisations ensure that the tone at the top reflects an organisation's values? How can boards be sure that the tone effectively cascades down through to middle management and the shop floor? How is culture assessed and if it is found to be poor, how is it changed? Organisations continue to grapple with these questions.

First, it's important to define what is meant by culture. In a corporate context it refers to the shared values, attitudes, standards and beliefs that characterise members of an organisation and define its nature. Therefore, one of the most important steps in being able to assess corporate culture is understanding whether staff feel able to report poor behaviour or management malfeasance without fear of reprisals. If people within the organisation are scared to speak up it can be difficult to detect bad practice.

Top down

Strong culture ultimately starts with strong leadership and a well communicated vision for the organisation's purpose and strategy. Employees need to feel valued and that they and their conduct and behaviour are integral to the organisation achieving its goals, therefore aligning individuals' values with those of the organisation.

A common mistake is to assume that setting the correct tone at the top will trickle down. Realistically this will not always happen, especially in multinationals where local business units have their own indigenous cultures and ways of working. Instead, senior management should put pressure on lower rungs of management to encourage correct behaviour and foster the desired tone at the middle.

In many cases, the risk culture of an organisation is not consistent with its stated values and what it claims to be. In the banking sector some firms have presented themselves as responsible lenders while at the same time employing aggressive sales incentives and targets that have resulted in the misselling of products. One key step, therefore, is to ensure that sales models do not inadvertently incentivise undesirable behaviour and even compliance breaches (see box, above).

Assessing and reshaping culture is not only about rooting out undesirable behaviour, such as incentivisation practices that put profits before principles. As mentioned already in this report, organisations are undergoing huge change, particularly on the digital front. Without a cultural

Culture Coalition

In 2016 the Financial Reporting Council, the UK and Ireland's independent regulator responsible for promoting high quality corporate governance and reporting, issued a report on corporate culture that drew on the research and work of a number of partners, including the Chartered Institute of Internal Auditors. The 'culture coalition' identified three important issues to look at when taking action in this area.

Connect purpose and strategy to culture. Establishing a company's overall purpose is crucial in supporting its values and driving the correct behaviours. The strategy to achieve a company's purpose should reflect the values and culture of the company and should not be developed in isolation. Boards should oversee both.

Align values and incentives. Recruitment, performance management and reward should support and encourage behaviours consistent with the company's purpose, values, strategy and business model. Financial and non-financial incentives should be appropriately balanced and linked to positive behavioural objectives.

Assess and measure. Boards should give careful thought to how culture is assessed and reported on. A wide range of potential indicators are available. Companies can choose and monitor those that are appropriate to the business and the outcomes they seek. Objectively assessing culture involves interpreting information sensitively to gain practical insight.

For more, visit: www.frc.org.uk

Culture audit options

According to the Chartered Institute of Internal Auditors, there are at least four potential audit options for assessing corporate culture. Every organisation will have their own approach, whether dedicating a work programme specifically to the topic or taking a broad view by incorporating cultural measurements into existing audits. What matters is finding an approach that works for your internal audit function.

1 'Meta-audit' of consolidated findings - using cultural insights from individual audits over a given period of time.

2 Comprehensive general assurance on culture - compliance/effectiveness assurance against expectations, preferably defined by the board.

3 Standard assurance audit of a specific aspect - e.g. assurance that the defined governance structure is operating as intended, meetings held, right people attending, decisions made in meetings not corridors, risks considered, options debated, group think avoided, e.g. assurance that there is compliance with a diversity policy.

4 Consultancy review providing insight into a specific aspect - e.g. advising on project/ change ways of working, e.g. collaborating with HR on identifying risks and next steps after an employee "health check" survey.

For more, visit: www.iia.org.uk/culture

"**Culture** is definitely high on the management **agenda**. If you look at the **population** of our organisation, **38%** have been with the company for less than a year. In the **tech space** that figure is closer to **50%**. I don't know how many **nationalities** work here nowadays, we **stopped counting**. So how do you keep the culture **alive**? How do you create an **inclusive environment** in which people feel safe to **speak up**?"

Chief Audit Executive,
multinational Dutch IT services provider

"Banks need to take proactive steps to **avoid any type of inappropriate sales practices**. That is something that is definitely aligned with cultural risk. The organisation must make sure **employees are aware of behaviour** that is prohibited in all circumstances, and ensure economic incentives aren't driving bad behaviour. **Cultural change needs to come from the very top** of the organisation. Management must lead by example and send clear instructions and, like any change, that is going to **take time**. In the meantime, internal audit needs to monitor controls to avoid what has happened at other banks."

Chief Audit Executive, multinational Spanish banking group

shift, the organisation will cling on to old behaviours and ways of doing business.

Transforming an existing culture into one that better aligns with the future strategy of the organisation requires creating an environment of wanting to change behaviours. Corporate culture will have been embedded over years, even decades, intentionally or not, and changing it will take time.

But before any of this, the organisation must be clear on its future strategy, in the short, medium and long terms. It must understand what it wants to be, why and how to get there. The rapid pace of innovation means that many companies are having to reshape existing business models and think hard about their goals and what will underpin their success. Only once this has been clearly articulated can the organisation strive for a culture that supports those new goals.

Uber and the cost of poor culture

Even forward-thinking, disruptive companies can fall victim to poor culture. Uber, one of the most successful tech firms of the last decade, saw its CEO and founder Travis Kalanick outsted in 2017 for his mismanagement of the company.

Following his departure the start-up released the recommendations from a months-long investigation into its corporate culture. It stressed that Kalanick's 14 "core values", which started with and became embedded in the company, needed addressing as they had "been used to justify poor behaviour".

These values included "toe-stepping", the notion that success should be based on merit even if people have to be stepped on along the path to success; "always be hustlin'"; and "principled confrontation" with the incumbent taxi driving industry and even regulators. Ultimately these values and the behaviour they engendered cost Kalanick his job. Now Uber must embark on the huge task of transforming its culture.

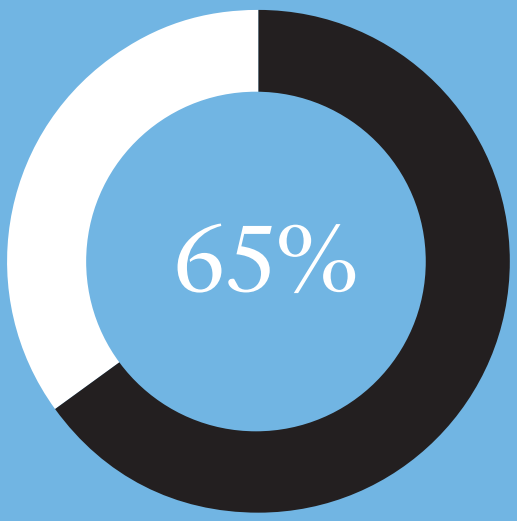
An internal audit perspective

The issue of corporate culture and how exactly it should be audited remains at the forefront of CAEs' minds. Some have conducted initial standalone culture audits, some have built cultural measurements into each audit they do, while others have yet to act. But the fact remains that boards wish to understand their organisational culture and internal audit is still exploring how best to do this. Internal audit has a critical role to play in assessing whether the existing culture and staff behaviour reflects the company's stated ethos and values, whether it stands in the way of the organisation achieving the transformation it seeks and how effective measures to reshape the culture are.

Key questions:

- Are the organisation's strategy, goals and values aligned with its culture?
- Does the organisation's culture deliver those goals throughout the organisation?
- Is what the organisation claims to be reflected in the behaviour of management and staff?
- Is the tone at the top "healthy" and does it effectively cascade through the organisation?
- Does middle management place an emphasis on good behaviour that reflects well on the organisation?
- Does HR have effective onboarding policies so that new staff adopt the desired culture?
- Do recruitment processes seek to ensure that the organisation's shared values are embraced by candidates before they are appointed?
- Does the internal audit function have the necessary skills and experience to assess culture and behavioural metrics?
- Do staff feel confident to speak up and report any misbehaviour or poor practices?
- Does the organisation directly or indirectly incentivise unethical behaviour towards customers or its own staff?

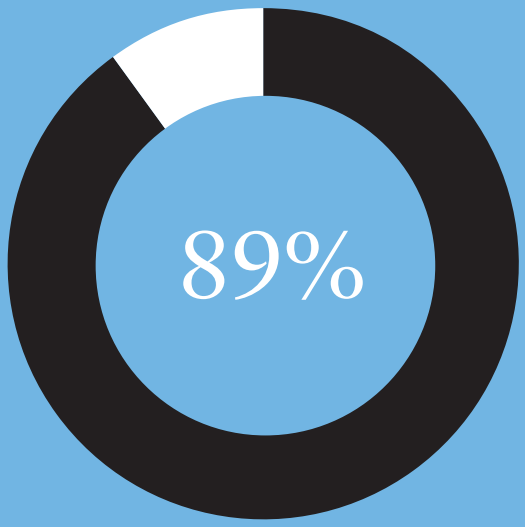
Employee trust



Only 65% of employees say they trust the company they work for

Source: Grant Thornton

Value in trust



89% of employees believe trust is important for job satisfaction

Source: Grant Thornton

"At the **beginning** of each **audit** assignment we come to a **conclusion** on the **culture**. I have two **senior people** that do nothing else, day in and day out, **helping** to **reach** those conclusions. I have someone in my team with a PhD in **organisational behaviour** who worked for many years with the Dutch regulators. She helps me on the design aspect. We then **extrapolate** from conclusions in specific parts of the **organisation**, in different countries, to give a **systemic comment** to the board. Some organisations do **standalone** culture audits, but this is the option I feel more comfortable with and I know that our peers take the same **approach**."

Chief Audit Executive, multinational Dutch banking and financial services group

WORKFORCES: PLANNING FOR THE FUTURE

Organisations are having to think more strategically about their workforce planning than ever before for a number of reasons, one of which is demographic. Many major economies are witnessing their labour workforces shrink as the baby boom generation continues to transition into retirement.

At an organisational level, this means companies are having to think long term about addressing any shortfalls of staff for key roles, and more broadly how to attract and retain younger talent with the necessary skills and create new roles to ensure the future success of the business as the world becomes increasingly digital.

Today millennials, the youngest generation in the workforce, represent the majority in the workplace. However, it is not simply a case of replacing older workers. These employees have different attitudes towards work and what they expect from their careers and day-to-day working lives.

Automated workers

Rapid advances in artificial intelligence (AI) and robotics mean that many jobs that were once exclusively carried out by humans are, or soon will be, automated for the first time. Machines and software are no longer limited to manufacturing tasks, but have found applications in everything from self-driving cars to news reporting.

For example, Thomson Reuters has delegated the writing of corporate results to algorithms, freeing up the time of its human journalists to focus on more involved stories. This allows the firm to cover the results of the entire stock market rather than selecting earnings reports for the most high-profile companies.

Of the disrupting forces that will have the greatest impact on businesses 25 years from now, automation is cited most frequently, with 51% of companies naming it, followed by regulation (43%), people issues (38%) and other technology that is not not yet available (38%)[16].

The headline is that many of today's workers will be replaced. However, there will inevitably be an interface between humans and workforce technology and automation may lead to the creation of millions of unforeseen new jobs. Ultimately firms must consider how automation will impact their future workforces, as well as their business models.

For example, millennials value "flextime", that is the freedom to work flexible hours and remotely. Given their comfort and familiarity with digital technology this generation is well adapted to working from home. For the majority (75%) of this age group work-life balance drives their career choices[13], and so organisations must think carefully about offering flexible work schedules, work-from-home policies, job appraisals based on outcomes and deliverables, and the freedom to take unpaid leave.

But it is about more than offering flexibility. Research shows that more than half (51%) of millennials look externally for career opportunities compared with 37% of Gen Xers (the preceding generation) and 18% of baby boomers (the next preceding generation)[14]. This means organisations must work harder than ever to retain talent by offering diverse opportunities, creating both vertical and horizontal career paths.

The case for strategic workforce planning is also supported by the changing nature of work. Executives estimate that in three years 44% of the labour force will comprise contractors and temporary internal positions. And 79% of this so-called "liquid workforce" will be assigned to dynamic projects rather than traditional, static job functions[15].

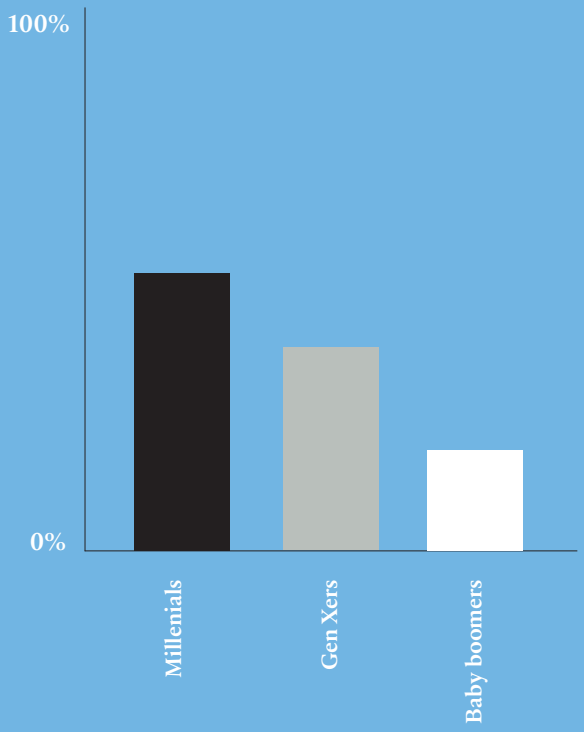
Companies are under constant and continual pressure to change products, services and even business models as each new technology or innovation emerges. This requires them to be agile in terms of their skills and projects. Those companies that access the necessary skills faster and more successfully match those skills to their needs will be more effective in adapting and growing.

This means that senior management and the HR function should be thinking about how much and what segments of the workforce needs to be permanently employed in future and how this aligns with the needs of the company in the short, medium and long terms.

Climbing the career ladder

51% of millennials look externally for career opportunities compared with 37% of Gen Xers and 18% of baby boomers

Source: PwC



Reshaping the workforce

Only 13% of UK companies say they are ready to respond to disruption to the workforce and create "the organisation of the future"

Source: Deloitte

This is despite 88% believing that creating the organisation of the future has become a priority

Source: Deloitte

"HR is a **huge topic** for us because of our size as an employer and the pressure that the civil service has been under for a number of years regarding the size of central government. There's an expectation that we do more with less, and that's not just money but also people. So there's an awful lot of internal audit work around workforce planning. We're looking at the **organisation's age profile**. What do you do if you've got an older workforce? That will **stay on the agenda** for the next few years."

Director, UK government agency

"A challenge the business identified some time ago and **we're supporting from an audit perspective** is around people and retention and how the organisation approaches diversity, **work-life balance** and so on. The audit committee will want assurance that the business is doing what it says it's doing. **The younger generation** expects to be able to work differently, it expects more **flexibility.** All of that has a knock-on effect on cybersecurity - if you've got more home-working staff then you have more mobile devices connected to your network; people want to be able **to connect with their own devices** as well and that's being trialled in certain countries now. It's not necessarily a problem to do these things, but they need to be done in a **controlled way** and the associated **risks** must be **understood.**"

Chief Audit Executive, multinational UK recruitment group

Skills gap widens

As companies transition from the old, analogue economy to digital businesses that can exploit the advantages that new and emerging technologies offer, their demand for IT, data and other tech-related skills is increasing. This requires filling skills gaps and reshaping the workforce to be able to effectively drive the organisation in a new strategic direction.

In Europe, the skills gap has widened by 14% over the last five years and one of the areas for concern is is the digital sphere[17]. This prompted the European Commission in December 2016 to publish its e-Skills Manifesto and launch the Digital Skills and Jobs Coalition, which brings together EU member states, companies, social partners, non-profit organisations and education providers to take action to tackle the lack of digital skills in Europe.

With this in mind, organisations must pay close attention to their future skills needs and, where necessary, put in place programmes to attract talent equipped with desired skill sets, train up existing employees and outsource on an ad hoc basis.

An internal audit perspective

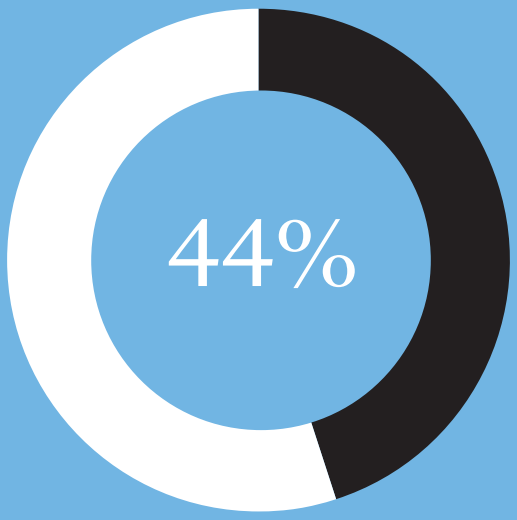
The success of any organisation is dependent on its people, so the inability to hire and retain the right talent is a significant operational risk. As such, internal audit must be able to assess whether HR risk is being effectively managed and provide assurance that the organisation's workforce planning strategy is in line with its strategic vision. Where does the organisation want to be five years from now and how do its recruitment and retention policies support that?

IT, technology and digital skills are going to be in high demand for the foreseeable future, so internal audit should assess whether the organisation is making efforts to reduce any IT skills gap that exists today and could widen in the coming years. Boards will also want assurance that the transition to the millennial majority workforce is being effectively managed to ensure that new talent is attracted to the organisation while previous generations' needs are being met.

Key questions:

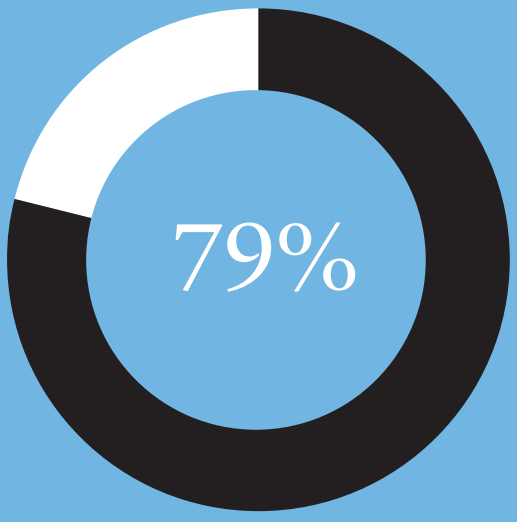
- To what extent has the organisation assessed its current and future skills gaps?
- Is the organisation equipped with adequate IT and digital skills?
- Is the HR strategy aligned with the organisation's overall strategy? Do recruitment and retainment policies support its future goals?
- Has the organisation thought about the demographic makeup of its workforce and how the ongoing baby boom retirement will impact its operations?
- Is enough being done to ensure that the organisation is attracting younger talent with flexible arrangements and diverse career opportunities?
- Is the organisation in a sector that is likely to be overhauled by automation and how will this impact upon the workforce?
- Has the organisation considered what an increasingly "liquid workforce" means for it and can the HR function cope with sourcing ad hoc talent to meet changing organisational demands?

The liquid workforce



Executives estimate that in three years 44% of the labour force will comprise contractors and temporary internal positions - the "liquid workforce"

Source: Accenture



79% of this so-called "liquid workforce" will be assigned to dynamic projects rather than traditional, static job functions

Source: Accenture

"**People management** is a big issue in the context of greater **collaborative work,** project management, **networking** and **managerial autonomy versus** close hierarchical monitoring. Roles and responsibilities have to evolve, especially those of HR and management, but the outcomes of these **changes must be challenged**. Internal audit has to take into account transgenerational issues, stress on the workforce, and global and professional mobility which may need to be more transitory to cope with the need for skills required by the pace of **change in the business**."

Chief Audit Executive, French manufacturing group

EVOLVING THE INTERNAL AUDIT FUNCTION

Expectations of internal audit have never been greater and as the risk profiles of organisations develop over time, so too do their assurance needs. Of course, much of the work of internal audit continues to centre on assessing operational risks and the internal controls in place to mitigate these risks.

However, organisations are increasingly looking outwards to external threats such as cyber attacks, the impact of Brexit and other political events, and the strategic risk posed by rapidly evolving technologies and disruptive business models. This means that internal audit must also be outward-looking.

Some organisations will benefit from increased internal audit budgets, but for many greater expectations mean doing more with the same resources. This requires effectively prioritising audit work, developing risk-based audit plans that truly meet the needs of the organisation, pursuing efficient approaches to work, hiring/co-sourcing subject matter experts and adopting data analytics and other technology expertise to improve the delivery of audits and potentially increase the level of assurance provided.

CAEs must take a view on how well their functions are responding to the risk mitigation needs of the organisation, and take necessary steps to address skills gaps through recruitment, co-sourcing or outsourcing, as well as change existing audit methods and models to optimise time and resources.

Depending on the organisation, the following areas may require attention to ensure that the internal audit function is reaching its full potential:

Agile auditing

Agile with a capital 'A' is by now a well-established approach to project management and software development - and is now beginning to find application in internal audit. Agile focuses on continuous improvement, scope flexibility, team input and delivering essential products, whether applied to software development or audits. This involves close collaboration across audits and function members, auditee collaboration (whilst maintaining independence), and responding to changing requirements during audits and the delivery of audit plans. Audits are delivered in pre-allocated bursts of work known as "sprints" and brief team "scrums" are held to share progress and knowledge on a daily basis.

Value-add

Internal audit is not only about assessing checks and balances, but adding value where it can. Given their expertise in governance, risk management and controls, heads of internal audit are sometimes asked to take on additional tasks, which can include helping management make decisions based on the CAE's insight into the organisation's management of risk and where assurance

The benefits of internal audit analytics

The potential of data analytics is only limited by the datasets available for analysis and how creative auditors are in identifying how it can be applied. A report recently published by the Chartered Institute of Internal Auditors identified the following benefits:

- Increase efficiency. For example, scripts can be reused for periodic audits, resulting in efficiency benefits through using analytics vs performing the analysis manually
- Increase effectiveness by performing whole-population testing instead of random or judgmental sampling
- Improve assurance
- Enable a greater focus on strategic risks by moving away from the more routine tasks which can be automated to a greater degree
- Provide greater audit coverage
- Realise significant savings, in terms of time and money, over the longer term.

You can find the full report at: www.iia.org.uk/dataanalytics

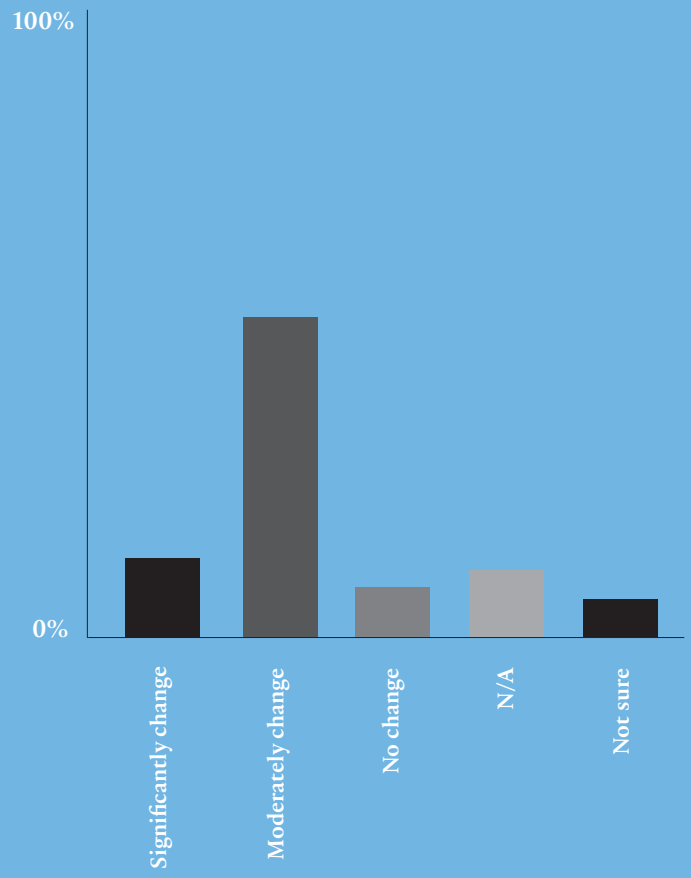
"**Traditionally** auditors had **accounting backgrounds**. Today I have far too many people that **understand accounting** well and not enough that understand, for example, **technology**. Lots of what we do as a bank is also more and more linked to modelling. Not only the **regulatory capital** models but also **quantitative tools** and models to help retail customers decide on the most suitable products for **investing their savings**. The skill set of understanding the math behind those tools and how they work is quite **different from traditional accounting skills**. Also, our bank is using more and more data analytics in its operations and in internal audit **we are using more and more data analytics** to assess what the bank does."

Chef Audit Executive,
multinational Dutch bank and insurer

Audit committees require change

12% of UK CAEs say their audit committee requires internal audit to "significantly change", while 52% say "moderate change" is expected

Source: Deloitte



"How much **value do you deliver** by giving a view of the **organisation** at a point in time when three months on it's already a very different beast? Increasingly it's not about **auditing** the now but **the now and the future.** With every audit we're constantly looking at whether the work we're doing is going to be **valuable to management** a year down the track, or **are we ticking a box** and moving on? Are we really looking at what matters and then looking at it in a way that maintains audit's relevance? Because you can look at the right topic area but if you're looking at it in a **static way** when it's a moving feast then **people are going to start ignoring you**."

Chief Audit Executive, multinational UK engineering and manufacturing group

is adequate or lacking. In this respect, internal audit should be seen by management as a trusted adviser.

Given their unique perspective as an inside-outsider, CAEs may also be consulted on the organisation's ability to adapt its business model, transform and innovate in the face of strategic threats. Additionally, multi-disciplinary committees are likely to seek input from internal audit.

To add value, audits should move away from offering a review of a risk area at a snapshot in time. The business environment is increasingly fast-paced and static audits that fail to consider the future as well as the present quickly date, and therefore offer less value. Audits are also more effective when they consider the source of problems, whether those shortcomings are linked to controls or behavioural issues related to culture, which may require skilling up in Root Cause Analysis.

Cyber/IT

The overarching shift of recent years has been technological, and this has meant auditors are expected to have higher digital competencies than ever before in order to better understand how risks may be managed and to more effectively interpret their audit findings for boards and audit committees who may lack cyber literacy.

Cybersecurity has fast become one of the most severe risks faced by organisations and this means that functions should be equipped with IT audit specialists or co-source resources to understand how well the organisation is prepared for outside attacks, potential malicious employees and other IT vulnerabilities, as well as take a broad view on its cyber governance.

Data and data analytics

Organisations are producing growing stores of data from their operations. This presents two key challenges for internal audit. The first is to help the board and management understand how that data is being collected, managed, protected and harnessed for commercial gain. The second is how to exploit this growing data from an internal audit perspective by applying analytics tools to audit processes, therefore automating routine audits and freeing up the function's time to focus its efforts on emerging risk areas and ad hoc projects (see box, page 38).

Culture

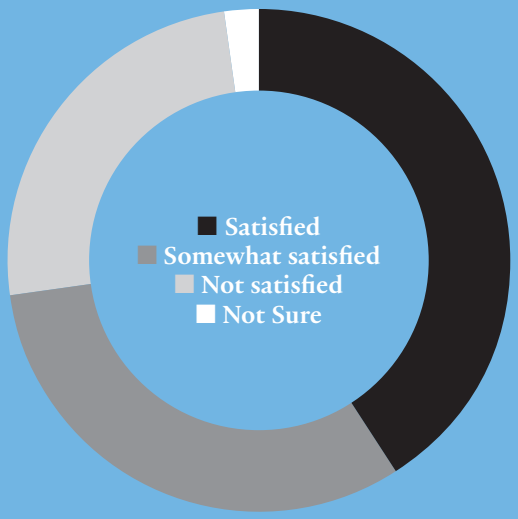
Organisational culture has made its way to the top of many boardroom agendas (see page 30) as the result of serious corporate failings. Boards want assurance that the organisation's stated values are reflected in the behaviour of staff and that their everyday conduct doesn't increase the risk of reputational damage. As such, behavioural competencies will become increasingly valued in internal audit. This will require understanding how to measure individual and group behaviour using sociological metrics and being able to draw meaningful conclusions from softer audits that help boards and audit committees understand the organisation's culture and how it relates to risk.

Key questions:

- Has internal audit performed a gap analysis to assess where it may be lacking skills?
- Does the CAE understand what the organisation's assurance requirements are today and are likely to be in the future, and is this consistent with the internal audit function's collective skill set?
- Has the internal audit function considered the net benefit of adopting data analytics tools?
- If the function is co-sourcing/ outsourcing to address any gaps do these ad hoc resources deliver the right level of insight, expertise and assurance?
- Has the function considered new and efficient approaches to working such as the Agile method?
- Has the audit committee defined what it believes good internal audit looks like and does the internal audit function match up to that?
- Has the internal audit function benchmarked its effectiveness with External Quality Assessments and does it live up to the IIA Core Principles?
- Does the function have an adequate Quality Assurance and Improvement Program in place to ensure it is advancing and evolving?

CAEs' satisfaction with the internal audit function's capabilities

Source: Deloitte



CAEs' top 5 gaps in capabilities

Source: Deloitte

"We're using what we call an '**Agile audit**' approach to see how we can get more efficient in delivering quality more quickly, increase the effectiveness of **stakeholder engagement** and how we relate with our auditees. We're a year or so into this and we're seeing a lot of gains already in terms of the **quality and speed** of delivery. That involves **two-week sprints**, 'scrum masters', collaborative workspaces, **daily stand-ups** for the teams to discuss and understand what the critical areas of focus for that day are and **share knowledge** to improve the quality of the audits."

Chief Audit Executive, multinational UK banking group

SOURCES

1. www.nccgroup.trust/uk/about-us/newsroom-and-events/press-releases/2017/april/last-years-ico-fines-would-soar-to-69-million-post-gdpr/

2. www.veritas.com news-releases/2017-07-25-veritas-study-organizations-worldwide-mistakenly-believe-they-are-gdpr-compliant

3. www.pwc.com/us/en/risk-assurance/risk-in-review-study.html

4. jwg-it.eu/90-of-buy-side-firms-are-at-risk-of-non-compliance-by-mifid-ii-deadline-jwg-survey-finds/

5. risk.thomsonreuters.com/content/dam/openweb/documents/pdf/risk/report/cost-of-compliance-2017.pdf

6. www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-beps-full-survey-results-may-2017.pdf

7. www.strategyand.pwc.com/media/file/2016-Global-Innovation-1000-Fact-Pack.pdf

8. www.mckinsey.com/business-functions/digital-mckinsey/our-insights/adapting-your-board-to-the-digital-age

9. www.paconsulting.com/insights/survey-on-innovation-for-peak-performance/

10. www.idc.com/getdoc.jsp?containerId=prUS41826116

11. economia.icaew.com/en/news/july-2017/two-thirds-of-uk-businesses-have-no-brexit-plans

12. project28.eu/opinions-2017/

13. www.uschamberfoundation.org/reports/millennial-generation-research-review

14. www.cebglobal.com/human-resources/millenial-talent.html

15. www.accenture.com/gb-en/insight-strategic-workforce-planning

16. www.thomsonreuters.com/en/press-releases/2017/march/thomson-reuters-survey-automation-will-change-businesses-for-better.html

17. www.hays-index.com/wp-content/uploads/2016/09/Hays-GSI-Report-2016.pdf