The Agenda

An internal audit perspective on risks and issues on the boardroom agenda

May 2023

pwc

Introduction

Our 26th global CEO survey tells us that, in 2023, CEOs are facing both long-term threats to financial and environmental sustainability; and immediate pressures associated with inflation, economic volatility and geopolitical risk.

These threats and associated opportunities are more complex than ever before. It is therefore no wonder that CEOs are increasingly focussed on resilience: investing in people, processes, data and technology to allow their organisations to survive and thrive.

Internal Audit has a critical role to play as a performance partner, helping to strengthen their organisations in the face of increased risk and complexity, and supporting resilient growth. We hope this sector agnostic hot topics guide will be a valuable source of insight to help Internal Audit in fulfilling that role.

It has been designed as an accessible, easy reference resource to encourage discussion, stimulate fresh thinking and provide an aide-memoire for planning, re-planning, audit scoping and developing strategy.

This summary of topics is not intended to be exhaustive. We have taken a pragmatic approach to focus on a selection of those topics that we see as being uppermost on the Board agenda and therefore, believe will need to be front and centre on Internal Audit plans in the coming months.

For each agenda topic we set out:

a. what's on the risk agenda;
b. what's changed; and
c. what does this mean for Internal Auditors.

We have provided observations not only on what Internal Audit teams should focus on but also how. This reflects our observation that the complex, interconnected and changing risk environment sets the scene for a new focus on how Internal Auditors provide value.

We observe that leading functions are:

Delivering agile assurance and insight	**Operating as a critical friend**	**Working in collaboration with the second line**	**Keeping abreast of emerging trends in technology and automation**	**Helping business leaders to navigate the opportunities and challenges presented by the increased demand for, and scrutiny of, published information**
Working in a range of different ways to deliver quicker, deeper or more focussed outcomes in areas of interest.	Challenging the Board and executive management to build resilience in the areas that matter most.	To build a transparent picture of risks and assurance, and to ensure that themes around root causes, insights, and culture are shared to better inform their respective programmes of work.	In readiness to advise and assure the guardrails needed as organisations seek to capitalise on tech opportunities whilst managing the wide-ranging risks.	Covering wide ranging topics such as environmental, social and governance goals; risks and risk management and tax matters.

Please click the links opposite to move directly to the topics that are at the forefront of your mind:

Sustainability strategy and reporting

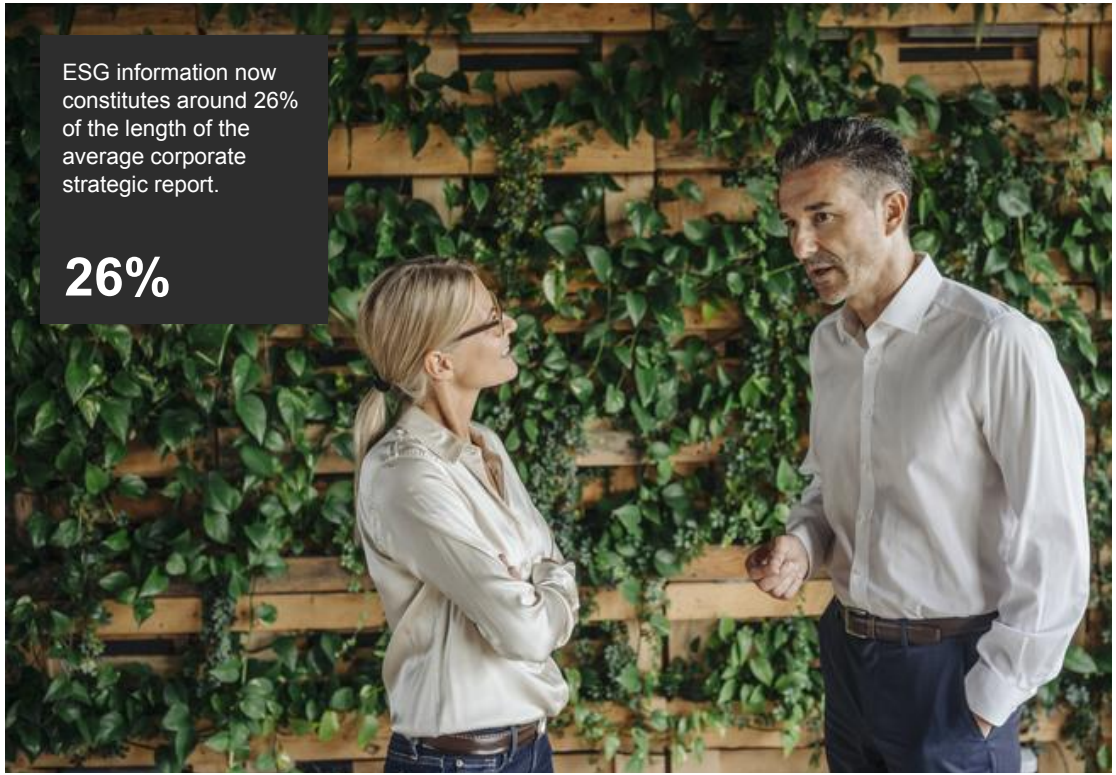
Sustainability strategy and reporting

What's on the risk agenda?

Recent years have seen increased levels of corporate disclosures covering climate related risks, opportunities and progress against environmental commitments. The demand for increased reporting is driven by rising investor expectations, growing scrutiny and activism and supported by increased regulation. ESG information – including climate change disclosures – constituted around 26% of the length of the average FTSE 350 corporate strategic report in 2021/2 according to PwC analysis (up from 21% in the previous year).

In the public sector too, the latest Greening Government Commitments ('GGCs') require entities to present an assessment of their progress in meeting the headline commitments and targets, as well as on other sustainable policies.

Furthermore, a growing number of leading companies, governments and investors have committed to net zero, and are embracing this as an opportunity to drive innovation, increase competitiveness, and stimulate resilient growth.



Sustainability strategy and reporting

What's changing?

The pathway to net zero

In order to be confident of delivering against ambitious sustainability goals, organisations are integrating carbon reduction plans into all aspects of their strategy. The impacts are widespread: real estate and energy strategies are evolving and there is more scrutiny of supply chains and sourcing. We increasingly expect to see some conflicts between 'cost out' and 'carbon out' strategies which will require inventive solutions.

Growing scrutiny and activism

A focus on climate issues by NGOs means that organisations need to be robust in their climate-related reporting and associated actions. For organisations that don't get this right, there's a risk of damage to brand value and reputation.

Investor expectations

Investors are influential in calling for consistency and high quality in climate disclosures for them to use as a basis for investment decisions.

Reporting regulation

The UK is the first major economy to mandate the use of the Task Force on Climate-related Financial Disclosures framework ('TCFD'). The Government's TCFD roadmap sets out when businesses will be required to disclose with the aim of having most UK companies within the scope of mandatory TCFD reporting by 2025.

The IFRS Foundation's announcement at COP26 to align global sustainability reporting standards will build upon momentum from the EU's proposed Corporate Sustainability Reporting Directive ('CSRD'). The CSRD is expected to impact more than 49,000 companies; UK businesses with European parent companies might be asked to report more non-financial data upwards within their group structure.

The International Sustainability Standards Board ('ISSB') has also published a consultation on two exposure drafts of proposed standards, focusing on general sustainability-related and climate-related disclosure requirements.

> Customers, investors, employees and society as a whole expect more from organisations today. They expect businesses to do 'good business'. This is not a box ticking exercise, but a whole new mindset which needs to be woven into an organisation's DNA.

Lynne Baber,
PwC UK Partner, Sustainability Leader

Sustainability strategy and reporting

What does this mean for Internal Auditors?

Organisations are sourcing new data and developing new processes to support their reporting against developing climate related disclosures, including, but not limited to TCFD requirements. In response, with growing scepticism about ‘greenwashing’, Internal Auditors can provide a valuable, independent perspective on the alignment of external communications with internal strategy and the delivery of climate related initiatives. They can provide real-time challenge to executives around whether disclosures are proportionate, consistent and well articulated for all audiences – customers, employees, suppliers and investors.

Leading internal audit teams are delivering assurance over net zero programmes, covering:

- Target setting, progress reporting and measuring of impacts;
- The governance, culture and incentives designed to align projects around a common purpose and cut across silos;
- Assessing ESG risk appetite, and;
- Providing benchmarking against peer organisations.

Many Internal Audit teams are investing in upskilling team members and developing partnerships with third party specialists in order to deliver assurance across this wide ranging topic.

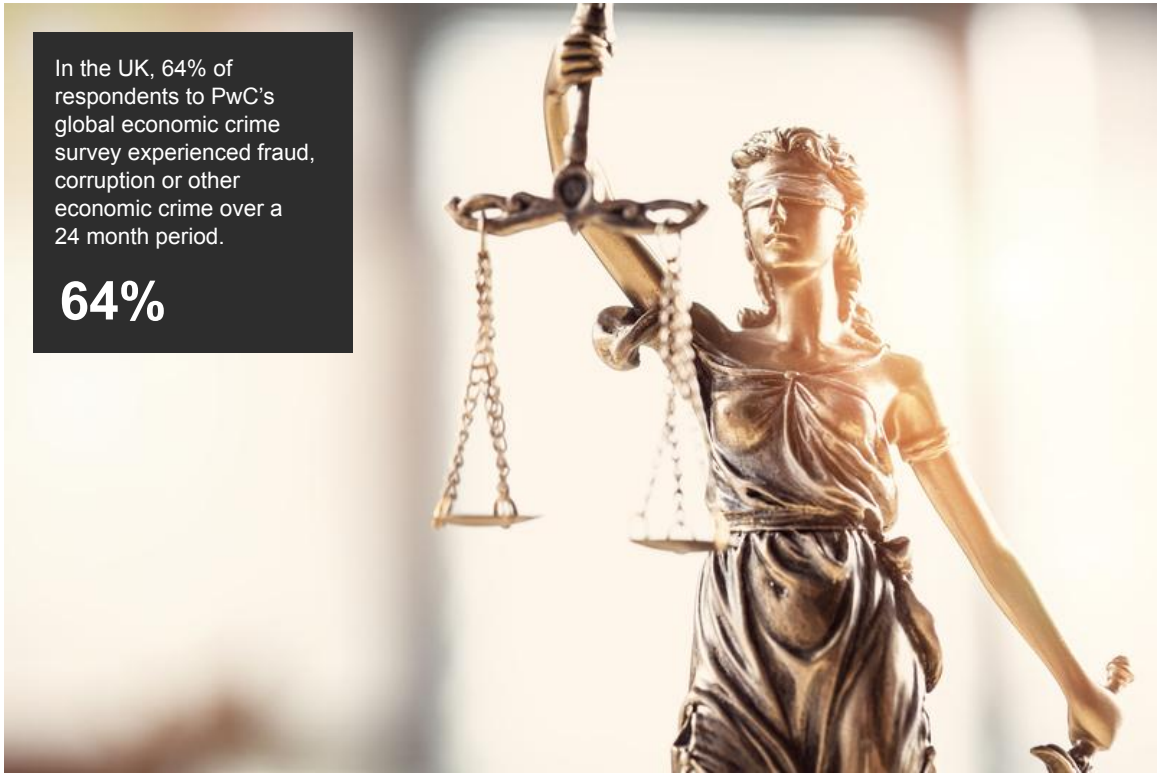
A focus on fraud risks

A focus on fraud risks

What's on the risk agenda?

As evidenced in our 2022 Global Economic Crime Survey, the past few years have seen a significant degree of disruption and change to the way business is being done and to the way people work. Fraud is now a greater and more costly threat to business than ever before, and the risk landscape continues to change.

In the UK, 64% of respondents to the above survey experienced fraud, corruption or other economic crime over a 24 month period; a steady and substantial rise from 56% in 2020 and 50% in 2018. Organisations in the UK are dealing with a higher number of fraud attacks than many other territories (the global average is 46%).



A focus on fraud risks

What's changing?

Macroeconomics

Experience shows that fraudsters flourish in times of disruption and uncertainty such as those currently experienced in global markets. History also teaches us that fraud trends don't emerge immediately; typically it takes 18 to 24 months after the initial turmoil for frauds to be exposed. As a result, there's every reason to increase scrutiny on fraud risks in 2023.

The current inflationary pressures put stress on many individuals and organisations; for some, the very real threat of running out of cash (or other liquid assets) becomes a rationale to commit fraud. We are observing an increase in the level of lower value, but highly disruptive, expense claim fraud, procurement card abuse and other similar types of employee fraud. At an organisational level, financial pressures can result in individuals manipulating financial data to prevent the breach of a banking covenant or to reach performance targets.

Technology

Of those organisations experiencing fraud in the last two years, four in ten experienced some form of fraud connected to the digital platforms they rely on. Whilst technology changes can lead to an increase in fraud risk, technology can also be a powerful and effective tool to prevent and detect potential fraud.

Widening of the net

Many organisations are widening their definition of fraud risk to reflect the growing range of non-financial metrics included in performance reporting, and the increased level of interest shareholders and other stakeholders are placing on these measures. More than two thirds (69%) of our UK fraud survey respondents were concerned about manipulation of ESG reporting by their employees, and 66% were concerned about deception within ESG reporting by third parties that they rely on.

A focus on fraud risks

Regulation

Over the last two years, the UK Government has taken a number of steps, through proposed and actual regulatory or legislative changes, to ensure that Directors of UK businesses are more accountable for the consequences of fraud. These have included:

Corporate Governance Reforms

In May 2022, the Government proposed a number of reforms to strengthen the audit, corporate reporting and corporate governance systems. These proposals include the requirement for directors of qualifying companies to disclose the *"steps taken to prevent and detect material fraud"* within their Annual Reports.[1] Whilst exact requirements are not clarified, the impact assessment that accompanied the consultation states that such actions may include undertaking an appropriate fraud risk assessment; responding appropriately to identified risks; promoting an appropriate corporate culture and values and ensuring that appropriate controls are in place and operating effectively. We expect to see a move towards more explicit internal definition of key elements of the fraud risk management framework within formal policies and standards, in readiness for the new external reporting requirements.

'Failure to prevent' legislation

In June 2022, the UK Law Commission published 'Corporate Criminal Liability: an options paper', on *"how it can improve the law to ensure that corporations are effectively held to account for committing serious crimes"*, including a number of 'failure to prevent' offences. In November 2022, an amendment to the Economic Crime and Corporate Transparency Bill was proposed which set out an offence of failure to prevent fraud, false accounting or money laundering and a new basis of criminal liability for senior management. This amendment is still to be debated and thus has not yet been incorporated into the Bill.

Corporate Governance Changes to auditing standards

Recent revisions to the auditing standard ISA (UK) 240 on the auditor's responsibilities in relation to fraud in the audit of financial statements, have increased the focus that external auditors place on the robustness of a company's fraud risk management framework. Auditors are required to assess the consistency of the new directors' disclosures with their knowledge from the audit.

1. For UK plc's that meet the criteria (i.e. at least £750m revenue and 750 employees), it is expected that disclosure could be required for financial periods beginning 1 January 2024. Non-listed organisations could have to comply from 1 January 2025.

A focus on fraud risks

What does this mean for Internal Auditors?

Internal Auditors are uniquely positioned and experienced to:

- Provide support and challenge to organisations as they look to redefine fraud and assess their risks across geographies and divisions.
- Coordinate engagement between different parts of the organisation (customer facing teams, cyber security, compliance and IT, for example) to ensure a holistic view is taken to risk assessment, prevention and detection measures.
- Consider how the macroeconomic climate may place pressure on particular areas of the organisation and work with management to design and test appropriate controls.
- Map the various sources of assurance over fraud prevention and detection controls against fraud risks to support the director's disclosures.
- Champion the use of technology as a tool to combat fraud – through the likes of risk-based analytics and exception reporting.
- Support the organisational approach to investigations, providing assurance over the processes, skills and support available for a suitable and effective response to reported incidents.

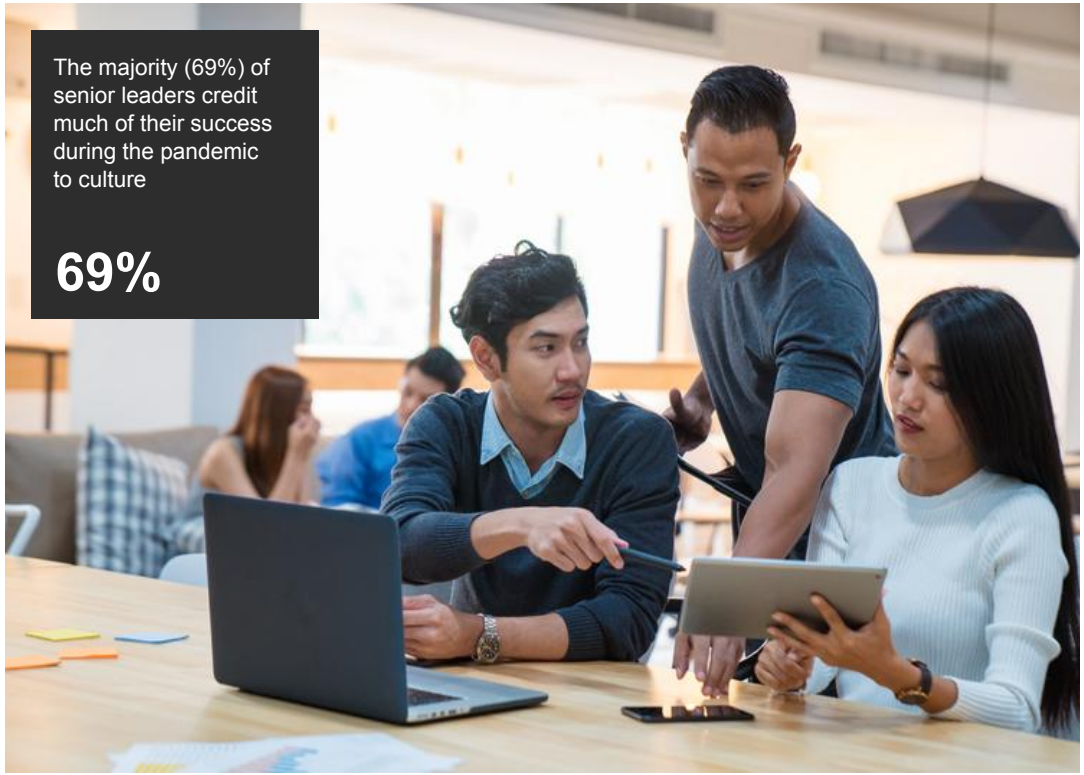
People and organisational culture

People and organisational culture

What's on the risk agenda?

Organisational culture can be either a key enabler or blocker to the achievement of strategic goals. Experience tells us that an organisation's culture is deeply rooted and slow to evolve, and yet the pandemic also taught us that organisations can achieve rapid changes with a targeted focus on a few critical behaviours.

According to our 2021 global survey of 3,200 workers in more than 40 countries, the importance of culture was confirmed with respondents agreeing that strong cultures drive better business outcomes. In fact, the majority (69%) of senior leaders credit much of their success during the pandemic to culture. The majority of survey respondents agreed that top cultural priorities should include recruitment and retention, digitisation, health and safety and collaboration.



People and organisational culture

What's changing?

The post-pandemic transition to hybrid working

The pandemic accelerated organisational use of technology as an enabler of more flexible working and this created new expectations from workers around work-life balance. Despite the strong demand among employees for flexible work, momentum is growing for a 'return to the office' environment with 64% of respondents to our global survey either agreeing or strongly agreeing that their company needs as many people as possible back on-site to achieve their strategic goals. In this world of hybrid work, many executives continue to struggle to create a culture that promotes an inclusive workplace for all employees.

The war on talent

In August 2022, the Federation of Small Businesses found that 80% of small firms faced difficulties recruiting applicants with suitable skills in the previous 12 months. To succeed in this challenging environment, organisations need to develop their attraction and retention policies, invest in training and development and focus on diversity, equality and inclusion. Underlying these investments is culture – a fundamental component of an employee's sense of belonging and loyalty.

Workforce diversity

Today's workforce comprises people from diverse backgrounds and spans the generations – from the Baby Boomers to Gen X, Millennials and Gen Z. For many organisations, that's four generations coexisting in one workforce with different needs and expectations of the corporate culture and associated behaviours.

Economic uncertainty

In January 2023, the World Bank described the global economy as "perilously close to falling into recession". Higher inflation and higher borrowing costs place pressures on margins and stifle business investments. Against this backdrop, staff concerns about pay, reward and job security are growing. Pay demands present financial challenges to boards, can unsettle established cultures and hence drive unwanted behaviours and increased risks. Recent strikes are evidence of the disruptive challenges this can pose.

> A healthy culture both protects and generates value. It is therefore important to have a continuous focus on culture, rather than wait for a crisis.
>
> **Sir Winfried Bischoff, FRC former Chair**

People and organisational culture

What does this mean for Internal Auditors?

Areas of current focus for Internal Auditors include:

Culture: Boards, guided by their regulators, are encouraged to consider how they define, assess and monitor their organisational culture, and what enablers and barriers their people encounter. Many board members look to Internal Auditors to provide an independent perspective on how things get done and whether staff feel they can speak up. Such work is often focussed on risk areas such as H&S, security or compliance or key 'moments that matter' to employees.

Talent management: reviewing strategic workforce planning and the related processes to ensure continuity of key skills: building the employee value proposition, recruitment, retention, talent development, succession planning, and performance management.

Diversity, inclusion and equality: Metrics around staff equality, diversity and inclusion are often published along with extensive narratives to explain the data within the organisational context. Internal Auditors can play a vital role in assessing the quality, integrity and consistency of disclosures, which are often developed without the same quality or process controls as the more traditional financial measures.

A number of leading Internal Audit functions have invested in training and development to build team skills, confidence and competencies in providing reviews around people and organisational culture effectively and with credibility.

MENU

Cloud technologies

Cloud technologies

What's on the risk agenda?

Cloud computing provides many benefits including universal network access, on-demand service and flexible supply. Rapid deployment capabilities can also create cost savings when compared to the implementation of traditional 'on-premise' solutions. Finally, standardised and tested security capabilities can provide enhanced system availability and resilience compared with legacy technology.

However, no solution is risk-free. A recent 'State of the Cloud' report by Flexera concludes that "Today's top challenges for organisations of all sizes are security, managing cloud spend and a lack of resources or expertise".

Furthermore, organisations need a clear strategy and the right expertise to manage the initial transition – keeping migrations on schedule whilst managing costs and securing benefits. Business-as-usual data and access controls, regulatory compliance requirements and service monitoring also present novel challenges for new Cloud users.

What's changing?

The pandemic accelerated the trend towards adoption of Cloud solutions and spending continues to rise. Many organisations have found themselves ill-equipped to stay on top of escalating consumption-based ('pay-as-you-go') charges, and the ever-larger contracts which underpin them. Flexera reports that 82% of companies have a major concern with the management of cloud computing spend. Today's challenging business environment places pressure on CIOs to get a grip on costs and drive benefits through supplier management and increased automation.

82% of companies have a major concern with the management of cloud computing spend.

82%

Experience indicates that a number of key factors separate those organisations who have successfully secured the many benefits from the cloud from those who have not. These include:

- Initial clarity about the business drivers for change
- Strong risk management frameworks which capture and track the wide range of organisational risks associated with cloud technology
- Development of a holistic change strategy with investment in people and operating model changes supported
- Robust data management frameworks

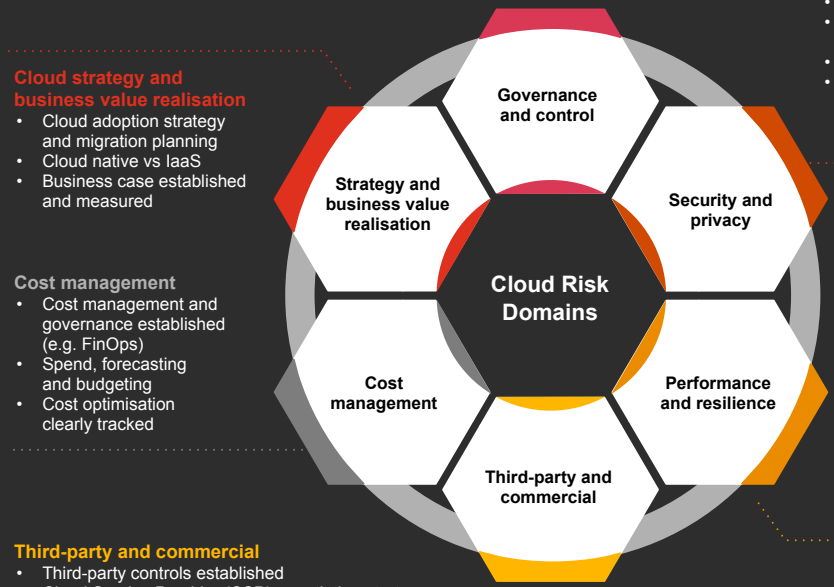
Cloud technologies

What does this mean for Internal Auditors?

Increasingly, organisations are looking to Internal Audit to provide an independent perspective on Cloud risks (illustrated right) and the associated mitigations.

Typical audit remits include:

- Independent challenge of Cloud strategies, governance and programme delivery;
- Scrutiny of vendor risks and contract management, FinOps cost management and delivery against agreed service levels;
- Assurance over data privacy, access management and cyber security; and
- Views on how to capitalise on Cloud technologies to automate and standardise controls, taking out time and cost whilst improving customer experiences.



MENU

Tax

Tax

What's on the risk agenda?

The complexity of laws and regulations in relation to UK taxation present continued challenges for tax and finance professionals as they strive to deliver accurate reporting, credible forecasting and wider support to the development and delivery of organisational strategy.

There is growing public and regulatory pressure to increase transparency in tax affairs and an appetite to see 'fair play' at a time of pressure on public sector services and infrastructure.

Tax teams have recently been tested by an unprecedented demand for advice and reporting on tax costs, risks and compliance amidst rapid changes to employee working patterns, international trade and inflationary pressures arising from the pandemic, supply chain challenges and geopolitical risks and events – all of which have significant tax implications.

Finally, tax compliance and reporting are key to the Government's focus on building public trust in how organisations are governed, ensuring the UK's frameworks remain at the forefront of international best practice.

What's changing?

New and forthcoming requirements and regimes are being introduced (e.g. HMRC's enhanced Business Risk Review and Making Tax Digital for Corporation Tax) yet many tax functions are continuing to operate with the same amount of resources and infrastructure. This places pressure on resources and will ultimately lead to innovation through changes in tax operating models, use of technology and outsourcing.

More tax authorities globally are embedding the concept of tax control frameworks in their regulations and using them in their auditing. Tax authorities are becoming increasingly digitally savvy, enabling them to find anomalies and errors across large data sets.

The role of the tax system in setting incentives for the economy is increasingly seen as a powerful lever in answering the longer-term challenge of ensuring we have a fair, sustainable and growing economy. Hence we might expect to see continued development of tax rates and allowances to reflect wider national and international priorities such as environmentally sustainable growth, and inter-generational and inter-regional inequalities. Similarly, budgetary gaps may lead to new 'technology' taxes to reflect the trend towards automation and away from labour.

There is growing public and regulatory pressure to increase transparency in tax affairs via EU public country-by-country reporting, OECD tax reform and growing expectations around sustainability reporting (via CSRD), to name a few. To create the required and voluntary disclosures requires a joined up approach to collation and verification of data, and the development of processes and controls to manage disclosure risks around both numbers and associated narratives.

Tax

What does this mean for Internal Auditors?

The role of Internal Audit in relation to tax risk may traditionally have been focussed on reviews of controls in relation to specific taxes and types of transaction. This remains a key component of the role of many Internal Audit functions, focussed on areas of tax that present most risk. However, Internal Audit, in partnership with risk management functions, can play a key role in supporting Boards in tracking tax risks at all levels: strategic, compliance and reporting.

Internal Audit's unique perspective on end to end processes means they are well placed to identify possible 'unseen' tax implications in relation to changes in revenue and cost streams, processes and controls.

As many organisations outsource elements of their tax frameworks, Internal Audit can provide confidence around how these contracts are managed and monitored to ensure that tax risks are appropriately understood and reported to the Board.

In relation to disclosures, Internal Auditors can provide useful assurance over controls to ensure data quality; checks on consistency between various tax disclosures (e.g. CbCR, CSRD, Pillar 2), between disclosures made by Tax, Finance and Sustainability teams and between the front-end and back-end of company reports. Finally, the narrative to explain the data should be subject to the same level of scrutiny and assurance as the data and tables themselves.

MENU

Supply chain disruption

Supply chain disruption

What's on the risk agenda?

Across all industries and sectors, complex global supply chains have come under increased scrutiny as a result of the rapid changes to demand and supply caused by Covid-19. The many shortages of critical goods are well documented and supply chain uncertainty has proven to be a sticky issue – compounded by the war in Ukraine and wider geopolitical forces, labour shortages, price inflation and delays with shipping and logistics.

Overall, recent events have served to shift the focus of supply chain management from cost to continuity, from just in time to just in case and from efficient to flexible. We can expect to see a continued focus on, and investment in, ensuring that supply chains are resilient, sustainable and connected.

Supply chain disruption

What's changing?

A focus on resilience

New strategies have emerged to ensure continuity of supply, including vertical integration through M&A (e.g. buying key suppliers), providing financial and wider support to strategically important suppliers and / or re-engineering products and services at pace to reduce the reliance on scarce components and raw materials. More conventional strategies have also been widely deployed – such as increasing inventory levels and dual sourcing.

The transparency imperative

A range of factors have converged to generate demand for more transparency at all levels of the supply chain. These include:

- Rising customer expectations – consumers and businesses expect to know when their goods will be delivered and to receive updates along the way. Data and communications are needed throughout the supply and logistics chain to enable this.
- Organisations recognise the need for greater understanding of vulnerabilities in Tier 2 and Tier 3 suppliers to support timely risk mitigation. As a result, end to end supply chain collaboration and data sharing is becoming more commonplace, supported by technologies such as blockchain (allowing secure and access controlled data exchange).

ESG

The move to net zero requires organisations to better manage and control emissions throughout the supply chain. Furthermore, the legal and reputational risks associated with Modern Slavery, Conflict Minerals and bribery and corruption require increasing levels of data, controls and governance.

The emergence of national industrial strategies

There is a resurgence of nation-state initiatives aimed at self-reliance or promotion and protection of national interests in strategic sectors such as technology and communications. These strategies are supported by a range of business incentives for in-nation investments alongside protective tariffs and sanctions. These strategies may have a significant influence on strategic sourcing decisions in some sectors.

Digitisation

As more companies innovate to drive improvements in customer experience, and seek greater efficiencies from automation, they increasingly need the support of third parties. Traditional cost and supplier management processes are not always fit to manage the scale and complexity of these new service arrangements.

Supply chain disruption

What does this mean for Internal Auditors?

The rapidly changing business environment presents challenges to many procurement and commercial functions whose people, processes, tools and technologies are increasingly stretched. Internal Audit review hot topics currently include:

Assessments of commercial controls: related to procurement and/or ongoing supplier risk monitoring and management. Reviews can be wide ranging or focussed on particular supplier groups (i.e. single source providers or technology service providers) or particular risk issues (i.e. financial, environmental, quality, regulatory or performance).

Risk reassessment: For many organisations, some contracting decisions were made rapidly and under duress during and immediately after the pandemic, so these may warrant some focus to assess any risks that may have been overlooked.

Contract level cost verification and assurance: to assess whether high-risk suppliers are delivering against quality and service level agreements and that payments, penalties and discounts are being applied in accordance with contract terms.

Contract risk assessment procedures: many Internal Audit functions are using AI technology to highlight unfavourable contract terms or ‘hidden risks’ across the supply chain.

Reviews of supplier risk mitigation strategies: For example (a) looking at governance over key initiatives such as supplier diversification plans or contingency plans in the event of suppliers failing to deliver; or (b) assessing the efficacy and integrity of data and assumptions supporting demand forecasting and inventory planning as a basis for decision making.

MENU

Pressures on finance teams

Pressures on finance teams

What's on the risk agenda?

Finance teams are under pressure. A myriad of post-pandemic factors have come together to create a growing disconnect between the business need for quicker, deeper and more efficient processing, reporting and insight and the finance people, processes and technology in place to deliver.

Finance teams play multiple roles as processors, controllers, technical advisors, insight generators and business partners – and each is being asked to deliver more whilst competing for talent in a challenging marketplace. In particular, as more key business decisions are based on rapidly collated forecasts and scenario planning, organisations are exposed to the risks of poor judgements due to errors in data and assumptions. Furthermore, demands for greater transparency across a range of financial and non-financial metrics increases the reporting burden and the level of reputational risk associated with inaccurate, inconsistent or potentially misleading information.

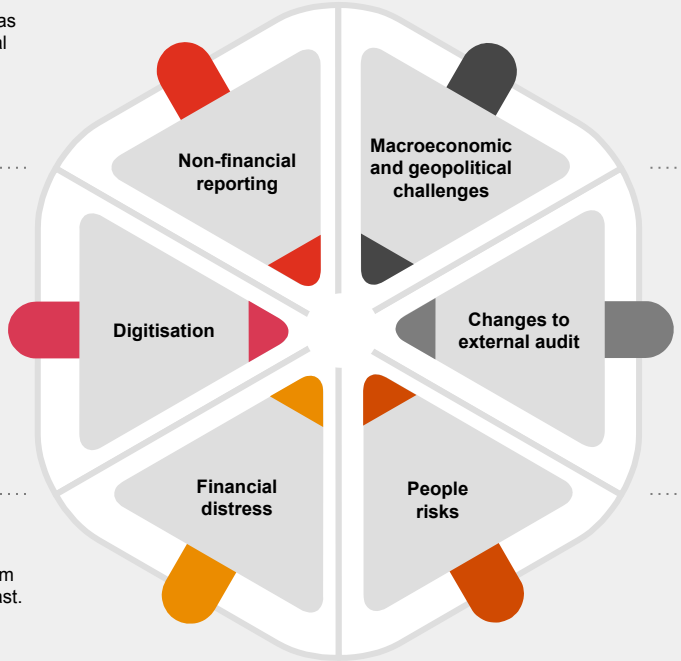
Pressures on finance teams

What's changing?

The increasing demand for transparency has seen a rise in the scale and complexity of non-financial reporting requirements. The processes and controls over these areas of reporting are typically less mature than for core financial reporting and finance teams are frequently called upon to lend their skills to data capture, analysis and reporting.

Many finance teams have yet to fully harness the many benefits of improved technology platforms to realise the benefits of greater efficiency, automation and data insights. In many cases, investment in technology skills is needed and yet can be hard to secure against a backdrop of cost control and uncertain returns on investment. A further and more unexpected impact of digitisation has been the increased complexity of revenue and cost accounting in relation to consumption based contracts for IT and tech-enabled services, both with suppliers and customers.

Current economic challenges and future uncertainty have created a focus on liquidity and working capital, capital efficiency and deleveraging – all of which require input from skilled finance professionals to monitor, control and forecast.



Business practices have changed with unprecedented pace as a result of changes in demand brought about by the pandemic and the energy crisis, supply chain disruption, financing challenges, geopolitical shocks and continued uncertainty. Furthermore, inflation and rising interest rates have placed pressure on margins. This has generated a significant workload for financial planners and has increased reliance on finance teams to monitor heightened fraud risks.

The ongoing reform of the corporate governance, reporting and audit system, FRC scrutiny and new auditing standards such as ISA 315 are leading to more challenge from external auditors in relation to controls. Many businesses are now focussing investment in policies, processes and systems to improve the control environment in response to the growing expectations. Furthermore, external auditors are exhibiting greater levels of scepticism which, in turn, has resulted in higher expectations around the quality of analysis and evidence prepared by finance teams in support of key judgements.

The demand for qualified and experienced finance professionals, especially those with digital skills, has risen as a result of the above factors at the same time as supply has diminished. Since the pandemic, many workers are less willing to undertake office-based, stressful work for long hours and the 'Great Resignation' has been impactful.

Pressures on finance teams

What does this mean for Internal Auditors?

Common areas of focus for Internal Auditors include:

- **Identifying pressure points:** through engagement with finance teams and the external auditors, Internal Audit can explore the areas where people, processes and technology are most stretched, creating scope for controls to break down.
- **Review of policies and processes:** to what extent have they kept pace with the above changes in governance, data processes, systems and controls? Do internal standards provide the clear guidance needed by teams experiencing staff turnover during turbulent times?
- **Compliance testing:** by using process mapping tools and analytics Internal Audit can work effectively to identify opportunities for process efficiency gains, saving time and costs.
- **Shining a light in the corners:** as travel to less visited locations is now possible again after the covid restrictions, Internal Audit has a key role to play in instilling a controls culture and acting as a deterrent against internal fraud.
- **Taking the long view:** by assessing processes, data flows and controls over non-financial disclosures with reference to risks of ‘greenwashing’ or user misinterpretation of data that might expose the organisation to reputational risk.

Technology transformed

Technology transformed

What's on the risk agenda?

The pace of technological change and its impacts continue to increase. From the invention of the microchip in the late-1950s, the development of the world wide web through the 1990s through to the 21st century when smart devices have become commonplace – all have transformed how customers and businesses communicate and trade.

Examples of developing technologies which are transforming industry include:

Augmented and Virtual Reality

Wearable technology will couples an immersive experience with practical applications, changing both the way customers interact with businesses as well as how staff work.

Artificial Intelligence and Software Robotics

Automation of business operations and repetitive processes through the use of robotic software provides a scalable and cost-effective approach to realising operational benefits.

Internet of Things ('IoT')

As more technology is networked we are creating an internet of everything, from watches to dishwashers. The impact of this digital integration will be incredibly far-reaching, changing everything from the way we work to how we shop.

Blockchain

Blockchain is a technology that enables the secure on-line sharing of immutable information. Blockchain technologies can enable secure and cost effective transactions (such as payments and letters of credit), reduce compliance risks and costs (through automated Know-Your-Customer, identity or provenance checks), and enable seamless and automated contract fulfilment thus reducing time, costs and errors.

3D Printing

3D Printing techniques use special liquid polymers that then harden. Being able to download and print out real three-dimensional products is proving to be a disruptive digital technology.

Health Technology

Whether for personal health or to manage disease epidemics, technology and health go hand in hand.

Drones

Drones are a powerful technology that can deliver significant safety, environmental and cost benefits. The majority of drone use in the UK is for inspection and survey but other applications, such as drone delivery, are likely to increase over time.

Technology transformed

What's changing?

Organisations who seek to benefit from innovations in technology are learning that they must also invest in building the right organisational structures and process ownership to manage risks. The following are just some of the control areas that can protect against the risks associated with today's tech transformation initiatives:

Appropriate, corporate-wide governance: Innovation is increasingly embedded across businesses so everyone can promote efficiency gains and offer new ideas that contribute to success. To manage the many and varied risks this could present, appropriate guide rails are needed, through standards and rule sets. These include clear process and technology ownership, risk management and controls – supported by expertise from across a range of disciplines.

Contract management: Acquisitions, alliances and collaborative partnerships are being developed as organisations recognise the need for 'outside in' expertise and perspectives to quickly mobilise the right technologies at the right price to gain competitive advantage. Furthermore, those organisations with legacy technology to manage at the same time as they develop new solutions, are increasingly turning to managed service providers to focus on old technologies, enabling leadership to focus on their digital future.

Data governance and culture: Uncontrolled, citizen developed robotics and AI can run counter to organisational initiatives designed to produce a single version of the truth through use of standardised databases and data analytics tools.

Process controls: As a wide range of teams increasingly place reliance on robotics, AI, automated controls and even end-user computing output, there is a risk that existing processes fail to evolve and control gaps emerge.

Reputational risks: It is impossible to have missed the ongoing debate about the ethical and other risks surrounding the expanded use of AI. Board members should anticipate external challenge of their AI technology use and governance.

Operational risks: Drones, 3D printing and augmented reality tools have potential to introduce new risks to health and safety.

Prioritising people: Digital transformation depends on having the right people with the right skills which is increasingly challenging in today's fiercely competitive job market. The challenge is in no way limited to skills on the shop floor – many organisations lack 'tech-savvy' individuals in their Top Management Team – who can provide the critical technology foresight, commercial experience and ability to identify ways that technology can improve business performance. Successful organisations recognise the imperative to upskill existing staff and recruit talent to realise the many benefits of a tech enabled future.

Technology transformed

What does this mean for Internal Auditors?

Typical Internal Audit reviews over technology cover:

- **Technology governance:** covering the whole end to end product lifecycle from setting requirements and business cases, implementation project management and ongoing process and change controls.
- **Process and controls assurance:** Process owners and assurance providers have a role to play in questioning whether tools deliver as expected and to provide assurance over controls adequacy in areas such as system access and change, with clear audit trails in place.
- **Assessment of contract management controls:** Strong contract management controls are needed to manage tech provider support costs, track delivery against SLAs and ensure third party conformance with wider controls requirements in relation to security, access management, change management and data privacy.
- **Wider technology related risks and their management:** including cyber security, data management, health and safety, operational controls and employee training and development.

MENU

Data management and governance

Data management and governance

What's on the risk agenda?

Data presents exciting opportunities for leaders to better understand their organisations, the external environment and its customers or service users. A strong control environment is needed to keep this information protected, of high quality and compliant with regulations.

Getting this right is both an operational and cultural challenge, and requires an understanding of data and how it flows through processes within and outside of the organisation. Key elements of effective data management and governance are as follows:

Data vision

Aligned goals and business value aspiration from data.

Data protection and privacy

Data must be handled and used in a legal, ethical and appropriate way to maintain trust and avoid regulatory fines and interventions. Remote working can increase data privacy risks, especially if staff are overseas.

Data quality

The way in which an organisation addresses data quality can have an impact on its overall effectiveness, service delivery standards, margins, legal and regulatory compliance, and reputation.

Insight and analytics

Clear reporting and data visualisation are key to unlocking the value of data. It helps leaders to make informed decisions, manage risk exposures and monitor operations in real time.

Data governance

The effectiveness of data governance policies, standards and processes is dependent upon organisations having a clear operating model and ownership structures. Key elements of effective governance are quality, access, security and use.

Data strategy

Organisations should have a clear strategy in place to ensure that data is managed well and leveraged responsibly. A good data strategy will look to enable and accelerate the overall organisational strategy. A strategy must be uniquely bound to an organisation's technology and regulatory landscape and develop in lock-step.

Data architecture

Describes the models, policies and standards governing which data is collected and how it is managed from collection to storage, transformation/ integration, distribution and consumption. Simplicity, integration and access are key features of a sound architecture to provide a single version of the truth.

Data culture and ethics

As more data is available from a wider range of sources and organisations increasingly base decisions on that data, often using AI; data ethics is receiving increased attention from boards, regulators and civil groups. One organisational response is to educate data users about the principles of good data management to instil the right culture of controls.

Data management and governance

What's changing?

The basic principles of good data management and governance are well understood but the systems, processes, skills to adhere to them are often lacking. And the task is getting harder as increased automation, the move to the Cloud and new disruptive technologies (wearable technology, AI, machine learning) all change the data landscape and the associated risks.

Boards are increasingly focussed on assessing ethical and legal risks around data usage and seeking assurance of mitigations. Strong leadership and stewardship is needed to maintain trust through using data responsibly.

Technology is increasingly deployed to reduce risks of human-centred data breaches in relation to routine, remote customer transactions through machine learning and NLP.

What does this mean for Internal Auditors?

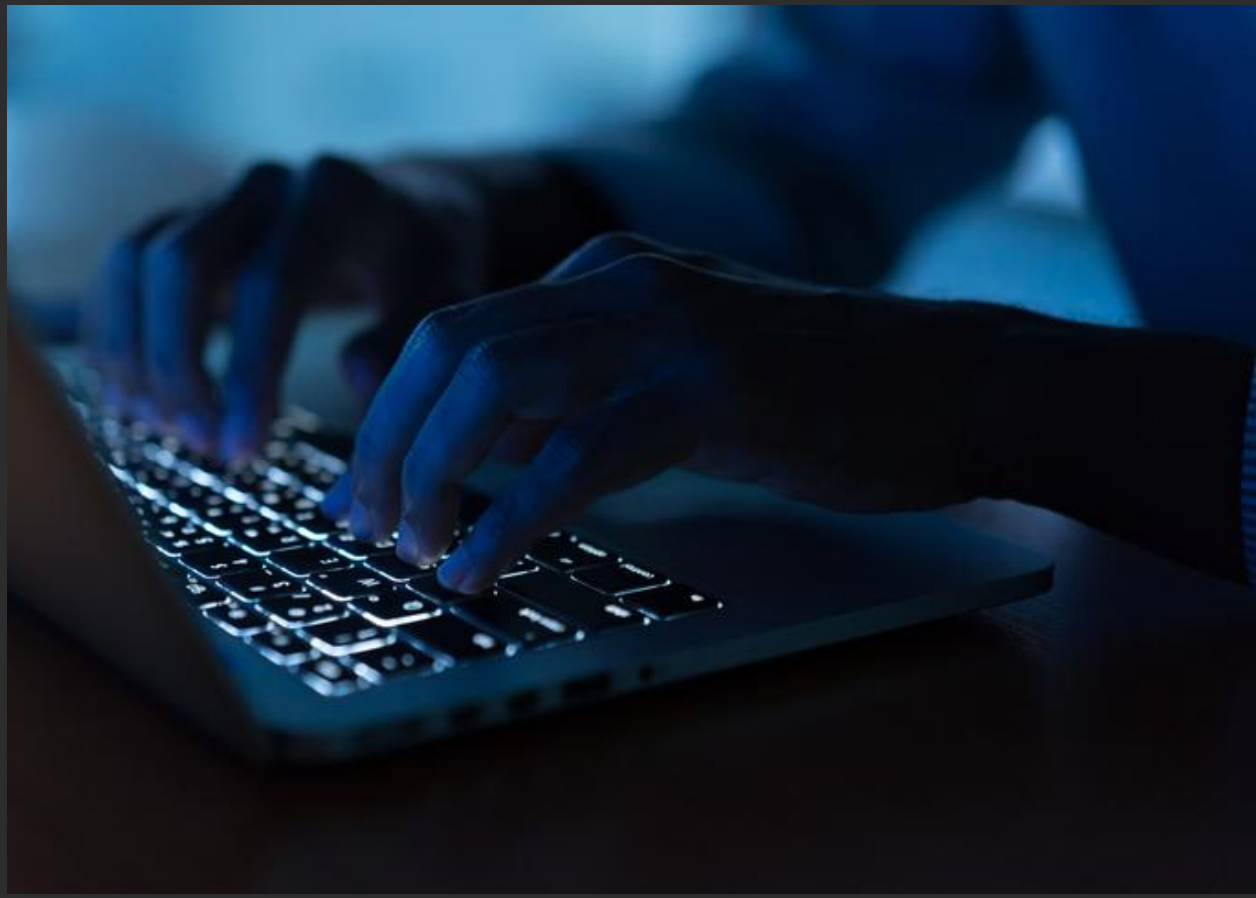
Internal Audit teams need to be well versed in these new technologies to provide effective assurance over the risks that they bring.

Furthermore, Internal Audit can harness the wealth of available data and related tools: data driven auditing can lead to better risk coverage, greater insights, speedier delivery and efficiencies in audit processes.

There are opportunities for Internal Audit teams to partner with the business to manage data risks and data transformation e.g. data savvy auditors can support businesses through programme assurance to ensure data quality controls are designed effectively.

MENU

Cyber security



Cyber security

What's on the risk agenda?

Cyber security remains a top concern for organisations of all sizes and in all sectors. The cyber threat landscape is constantly changing as new threats emerge and existing threats evolve. Recently reported cyber security attacks, including ransomware events, have shown how the failure to effectively manage cyber security risks can significantly impact organisations' reputation and bottom line. Organisations that operate in a regulated environment face increased scrutiny of their cyber security measures.

Executives and board members increasingly recognise that cyber security is a business issue rather than an IT issue. Board awareness of the impact of cyber threats leads to an understanding of the cyber security risk exposure and promotes informed decision making. Board oversight also encourages a risk-based and organisation-wide approach for managing cyber security risks.

Cyber security

What's changing?

Organisational strategies are increasingly enabled and underpinned by advances in technology and this increases the attack surface, and hence the risks of cyber attack. For example:

As supply chain networks extend and grow to involve more complex collaborations and joint ventures, there is an increase in the connections that can be exploited to steal data or disrupt services.

As remote working has become the norm, more users than ever are remotely connected to corporate networks from anywhere in the world and using any device. This increases the risk of unauthorised access and exfiltration of sensitive data due to poorly managed credentials and weak authentication mechanisms.

Organisations are modernising the way they work by adopting internet-enabled operational technology to monitor and control physical assets such as plant and equipment. Use of connected devices increases both the proliferation of unmanaged sensitive data and vulnerability to cyber attacks.

As more business transactions are undertaken through a range of new digital channels, these online touch points can be targeted by hackers looking to steal or manipulate rich and valuable data assets.

As organisations accelerate their adoption of public cloud hosted services to improve agility and innovation, the cyber risk environment changes. Organisations must be vigilant in identifying any weaknesses in security configuration which could be compromised to steal data or disrupt critical services.

According to PwC's 2023 Digital Trust Insights survey, an overwhelming majority – 90% – of UK senior executives ranked the increased exposure to cyber risk due to accelerating digital transformation as the biggest cyber security challenge their organisation has experienced since 2020.

The increased range of threats and number of attack surfaces require a sophisticated response. Organisations need to be clear about their risks in order to safely navigate the challenges. Indeed, 59% of UK survey respondents said they expected their cyber security budgets to increase in the course of 2023.

Rather than focussing on individual risk scenarios, resilient organisations are planning for continuity of operations in the face of simultaneous risks, taking preventative and anticipatory actions and embedding resilience capabilities to all aspects of operations.

Cyber security

What does this mean for Internal Auditors?

In today's complex environment, it is not surprising to see a range of sources of assurance over cyber security risks across all lines of defence, often complemented with third party technical expertise. Potential areas for Internal Audit functions to review include:

Cyber security capability, awareness and culture: An independent assessment of 'security culture' is often revealing, especially one that looks at the issue from a variety of angles: top down (starting with the board), bottom up (looking at staff training and awareness campaigns, testing outcomes etc) and role specific – (covering a range of people with responsibilities at every stage in the security lifecycle).

Exercising: Simulations, wargaming, traditional ITDR testing and exercising are all important elements of cyber security: allowing board members and staff from across an organisation to practise, learn and improve defences and response capabilities.

Security strategy: A strategy audit should consider whether cyber security plans are aligned to wider changes in the business – its people, processes and technology and changes in the external environment.

Third party management: An assessment of cyber protection throughout the supply chain (in contracts and how the relationships are managed) throughout the supplier life-cycle from procurement, take-on, management, reporting and exit.

Ransomware: Evaluating organisational capability to prevent, detect, mitigate, and respond to ransomware incidents, which differ in nature from more traditional forms of attack.

MENU

Enterprise resilience

Enterprise resilience

What's on the risk agenda?

Operational resilience is defined as the ability of an organisation to prevent, adapt, respond to, recover, and learn from operational disruptions. While recent regulatory interventions by the Financial Conduct Authority underpin operational resilience requirements in financial services, other industries and organisations have leveraged the same practices to enhance their ability to absorb and adapt to disruption.

This includes:

- Identifying business critical products and services;
- Agreeing the impact tolerance for these products and services;
- Mapping the end-to-end processes which underpin the delivery of business critical products and services;
- Developing a stress testing framework to resume operations within agreed impact tolerances.

According to our annual Digital Trust Insights Survey, 43% of UK senior executives still focus on isolated risk scenarios and how to address recovery for that specific disruption, instead of an approach that builds a 360-degree view of the risk the organisation faces and how to continue operations across simultaneous, connected risks.

At a more strategic 'enterprise' level, the ability to adapt and respond to disruption is vital to maintaining the trust built with stakeholders at a time when the expectations of the resilience of businesses and government have never been higher.

PwC's latest thought leadership provides a range of perspectives on how organisations can 'rethink resilience' in order to survive and thrive in an era where disruption in the norm.

Enterprise resilience

What's changing?

Organisations increasingly recognise the need for a more strategic, integrated and aligned approach to resilience disciplines, including enterprise risk management, technology resilience, supply chain management, cyber security and crisis management. A coordinated approach helps concentrate efforts on preparing for and responding to high impact risks.

> The most resilient organisations are able to adapt quickly, unlock new opportunities and emerge stronger, whatever the nature of the disruption.
>
> **Lord Gavin Barwell, Strategic Advisor, PwC UK**

At a strategic level, the key organisational activities and attributes to drive resilience are:

01

A strong 'risk radar': mining intelligence to understand and assess cross-organisational threats and their potential impacts.

02

Prioritising investments where 'strength' is most needed: looking not at systems but at services and service outcomes to focus resilience where it matters most.

03

Boosting the corporate 'immune system' through investing in the crisis response skills and personal resilience of leaders and teams, enabled by supporting technologies.

04

'Detoxifying failure': creating a culture of openness to improve the organisational understanding of risks and engender an approach that preempts possible causes of failure.

At an operational level, sound plans are founded on:

- Clear ownership for resilience by an individual or team with due skills and authority to coordinate specialist functions to ensure alignment and integration.
- A clear and agreed organisational view of which products and services matter most. This can be achieved through mapping external-facing Critical Business Services ('CBS') and internal-facing critical activities through a Strategic Business Impact Analysis ('SBIA').
- Alignment of operational resilience with both Enterprise Risk Management (to determine what scenarios resilience planning and testing should focus on), and enterprise controls (to identify and monitor key resilience indicators across the business).

Enterprise resilience

What does this mean for Internal Auditors?

The role of Internal Audit has traditionally focussed on conducting distinct specialist reviews of crisis and incident management, business continuity, cyber security and other risk disciplines. This approach remains valid and valuable. However, Internal Audit's unique ability to cut across key resilience functions means they are well placed to provide a more holistic view – providing confidence in an organisation's ability to protect the services which matter the most in the event of disruption. Critical elements of an overarching resilience review, and hence potential review topics for internal audit, comprise:

- Governance: including the roles and responsibilities of an executive sponsored steering committee and management information and reporting;
- Processes to identify and reconfirm Critical Business Services, defining tolerances and mapping all dependencies;
- Alignment of business continuity, ITDR, supply chain, cyber, technology resilience and physical security around the outcomes which are of most importance to the business;
- Exercising of resilience capabilities using plausible and realistic scenarios to validate plans and identify vulnerabilities;
- Crisis management ('CM') capability which can step in if resilience plans are overwhelmed;
- The use of technology-enabled resilience capability commensurate to the organisation's size and position in the market.

Geopolitical uncertainty

Geopolitical uncertainty

What's on the risk agenda?

In recent years, we have experienced heightened levels of geopolitical instability and uncertainty and this looks set to continue through the rest of 2023 and beyond.

All organisations will need to analyse global trends, anticipate their impacts and plan for multiple scenarios in order to manage risks such as those related to inflationary cost pressures and supply chain resilience. There will also be opportunities generated by the changing policies of many governments to focus on self-sufficiency: in relation to key technologies, to address insecurity of food supplies and build greater environmental sustainability.

Geopolitical uncertainty

What's changing?

The emergence of multipolar global politics

The Cold War era was characterised by a clear bi-polar East-West divide, but the new world order is more complex. US-China relations remain tense on a number of fronts and both nations are also preoccupied with domestic challenges. Many 'middle powers' and growing economies in Africa, Asia and South America will seek to remain impartial in matters of global politics to secure maximum economic advantage. There are also tensions between governments in the West as each tries to navigate international politics against a backdrop of domestic political and economic pressures.

Inflation, interest rates and energy costs

As 2023 unfolds, inflation and high energy prices continue to place pressure on European households and businesses alike. There remains uncertainty around the scale, speed and longevity of China's bounceback from zero-covid restrictions which could have a significant impact on the global outlook. Recent upset in financial markets, precipitated by some high profile banking collapses and buy-outs, has compounded investor caution. Finally, emerging market sovereign debts remain a cause for concern for some investors and commentators.

Developing global tensions around trade and natural resources

Most commentators agree that we can expect to see continued efforts by governments to reduce the reliance of their national economies on trade with 'unfriendly' states. Through use of sanctions, export controls, tariffs and national tax incentives, we can expect nation states to continue to promote greater self-sufficiency and invest in trade agreements with allies, particularly in relation to technology which is seen as a key area of competitive advantage.

Matters of energy and food security will remain high on the agenda of many governments and this may further fuel international tensions. More widely, the prevalence of water shortages mean that governments are increasingly focussed on ensuring domestic supply which can create considerable tensions and conflicts with impacts on migration and trade.

Geopolitical uncertainty

What does this mean for Internal Auditors?

It is common for Internal Audit teams to focus their attention on the more ‘controllable’ risks on an organisation’s risk register. However, the current turbulent geopolitical environment has wide-ranging impacts and is hard to ignore. Auditors may not be able to predict future crises, but they can provide insights around the organisational capacity and capability to anticipate, prepare, respond and recover from market shocks. The following questions will help determine whether your Internal Audit team is equipped for insight.

- **Culture:** do your Internal Auditors have the confidence to speak up when things don’t feel right? Is your voice heard when you hold up the mirror to highlight symptoms of weakened organisational resilience?
- **Resilience:** does your work cut across traditional silos? Do you understand and report on the ability of your organisation to identify threats, build strength in the critical business services that need it, to recover quickly and plan for the next event and challenge?
- **Agility:** are your plans sufficiently flexible? Is there capacity and capability to support investigations, undertake lessons learnt exercises, provide real-time project assurance and support the business in identifying and responding to near and long-term uncertainties?
- **Looking to the horizon:** do your senior IA leaders have the space to look broadly across the risk landscape to ‘join the dots’ and anticipate the impacts and knock-on impacts of disruptive events and to share ‘lessons learnt’ in a proactive and practical manner?
- Finally, do you have a seat at the board table to provide real-time insights and guidance as your organisation responds to and plans for ongoing uncertainty?

MENU

Thank you

pwc.co.uk

RITM11864990