Internal Audit Hot Topics

The Internal Audit & Risk Agenda 2024

IDEAS | PEOPLE | TRUST

BDO

Contents

01

The internal audit & risk agenda: Welcome

The internal audit & risk agenda

Welcome

2024 looks to be another year of permacrisis with significant geopolitical disruption continuing. Most of the world's major economies are undergoing elections in the coming year and the conflicts in the Ukraine and the Middle East continue to impact the global economy. Organisations that are only just beginning to recover from the disruption of three years of pandemic face further uncertainty in respect of inflation, interest rates, energy supply costs and talent shortages.

Dependency on technology has increased even though cyber threats are higher than ever. Despite this, digitalisation is driving business transformation and recent developments in Artificial Intelligence and Blockchain present new opportunities for innovation but these carry a heightened level of risk. Cyber, privacy and digital transformation risks are understandably high on the Audit Committee agenda.

Corporate governance reform was paused by the UK Government in late 2023 but pressure for change is likely to return in late 2024 and most large organisations are continuing to invest in the development of their financial control frameworks. Non-financial data is taking on a much higher profile with reporting obligations and stakeholder requirements being extended to compel disclosure of ESG performance and responses to climate change risks.

This has required organisations to introduce new systems and controls to ensure that this data will stand up to stakeholder scrutiny. Regulators have sought to keep pace with these changes - introducing new legislation and disclosure requirements that need to be complied with.

Expectations of Internal Audit remain high with demand for assurance expanding to cover a wider range of areas than ever before. Alongside the traditional controls knowledge and softer skills essential to the role internal auditors now need to enhance their understanding of governance and regulatory requirements and to develop their technical knowledge of information technology, data analytics, programme and project management, business resilience and ESG.

The new global internal audit standards reflect this and look to raise the bar by making actions that were previously good practice into mandatory requirements for high performing internal audit functions. In addition to this the new standards now include the Audit Committee's responsibilities for the first time. Heads of Internal Audit need to work with their Committee Chairs to make sure these are understood and addressed.

Internal Audit therefore has a key role to play in supporting organisations to navigate a path through this uncertain and changing risk landscape. This document sets out some of the key challenges on the horizon that Heads of Internal Audit should be considering when thinking about the wider risks relevant to their organisations and the technical skills required to deliver meaningful assurance.

As we enter into another challenging year, the Internal Audit profession can continue to show its value by demonstrating its depth of understanding and breadth of business knowledge by getting to grips with the many new and challenging areas for assurance.

Gavin Hayes | Head of Policy and Public Affairs | Chartered Institute of Internal Auditors

02

Hot topics

Artificial intelligence

Providing assurance over AI

Using the term ‘artificial intelligence’ to describe certain types of automation has become increasingly popular. However, when an organisation is genuinely using AI, how do we, as internal auditors, properly assess the risk and deliver a valuable internal audit report?

Organisations that are leveraging AI are looking to govern it as comprehensively and responsibly as possible, and where practicable, in line with their jurisdiction’s AI governance framework. For example, the U.K. does not have a comprehensive AI regulation; however, the government has proposed a context-based, proportionate approach to regulation and will rely on existing sectoral laws to impose guardrails on AI systems. When a framework for the use of AI is created at an organisation, it should define the policies, processes, and controls necessary for responsible AI deployment, whilst being future-proofed to take into account future regulatory movements as well as the ethical use of AI.

A potential risk in the usage of AI is the lack of clarity and transparency within AI models that facilitate their decision-making processes. A focus on the risks associated with these topics, and the ongoing monitoring/tweaking of the AI model could feature in most audits of an organisation’s AI technology. A related risk will be legal compliance and copyright infringement risks, based on what inputs are used within AI models.

Linking to another one of our hot topics in Internal Audit in 2024 is the concept of cyber security controls associated with AI technology. Consideration should be given as to the nature of sensitive data being inputted into AI tools (e.g. sensitive personal data, or confidential corporate data/earnings, etc.; and where the data goes after it is submitted to an AI tool), as well as how well protected the AI environments are from external cyber threats, and ongoing patching and vulnerability management.

Internal Audits over AI, as well as technology concepts within the wider realm of AI (e.g., machine learning), will vary from organisation to organisation, as the levels of maturity are certain to vary greatly based on industry, country, and the technology being used. Internal Audits need to be tailored given the number of variables at play to avoid a mismatch in applicable AI risks and coverage by the Internal Audit plan.

Despite this, as a starting point, the recently released ISO/IEC 42001:2023(E) provides a base level of expected controls and risks to be managed when using AI. Additionally, the provisional version of the EU AI Act, which was set to be finalised at the end of 2023, will also be useful as initial guidance for expected legislative requirements that organisations need to comply with.

Artificial intelligence cont.

Using AI to provide assurance

Internal Audit functions themselves are similarly identifying methods to leverage AI in a beneficial way – in some cases increasing efficiencies and to be able to arrive at insightful recommendations and insights that would not have otherwise been feasible with a standard/ manual approach.

One such method is in the way of predictive analytics and machine learning. By partnering with other lines of defence, Internal Audit can identify methods to implement real-time predictive analytics to identify – for example – software changes that are more likely to introduce a problem or incident in the live environment. This identification can be based on a range of factors such as the size of the change, the time of day it is deployed, the software package, the IT or end users involved, and a history of previously deployed changes, to name a few.

Just as transparency is a key concept to be cognisant of in leveraging and interpreting information that is subject to an internal audit, it is equally important to perform checks to confirm the validity of data generated by an AI tool being used to partner with the auditors to complete an engagement.

Continuous monitoring and machine learning can be useful audit tools to analyse historical data, which may lead to the ability to detect trends that human analysis might overlook.

AI can be a hugely beneficial tool to work alongside human internal auditors, provided the appropriate guardrails and other ethical considerations are taken into account. The integration of AI tools within an Internal Audit department can provide more in-depth insights to stakeholders as well as improve the efficiency and accuracy of audit procedures. By embracing AI, Internal Audit can align with the dynamic requirements of modern business.

Corporate governance reform

UK Corporate Governance Code

2023 began as a year of promise followed by disappointment and frustration when it came to meaningful change to corporate governance in the UK. The withdrawal of the draft legislation relating to key matters, including requirements for an Audit and Assurance Policy, Resilience Statement and Material Fraud Statement that were incorporated into the FRC's proposed Governance Code reforms, means that a less impactful change to UK corporate governance requirements is now expected.

The FRC has stated that it will not take forward over half of its original proposals and that the revised Code, due to be published in January 2024, will take into account the stakeholder feedback received during the FRC's far reaching consultation.

In spite of the profile that governance reform received, 2023 saw its fair share of corporate governance failures each serving as a reminder of the importance of the oversight role of boards and their stewardship of a business on its path to sustainable success. Whether guiding strategy, anticipating and mitigating risk, or demonstrating integrity and good behaviours, boards' responsibilties and accountabilties remain in the public eye.

Boards' effectiveness

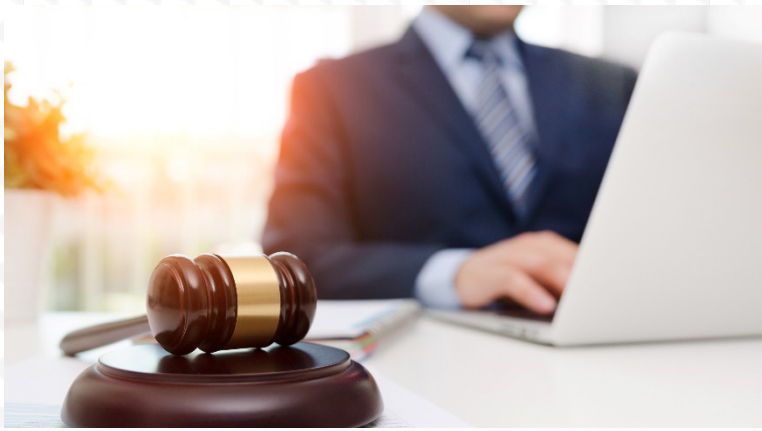
The best performing boards embrace good governance and 'do the right thing' by dedicating time to a continuous process of self-improvement. A board's effectiveness should be self-assessed annually, and externally evaluated every three years and include taking time to reflect on softer aspects like board relationships, culture and behaviours in addition to compliance with the provisions of the relevant Governance Code.

New Regulator

Despite the withdrawal of key governance legislation the UK Government has stated it "remains committed to wider audit and corporate governance reform, including establishing a new Audit, Reporting and Governance Authority (ARGA) to replace the existing Financial Reporting Council". It is anticipated that the new regulator will have greater powers and that the focus on Director accountability is likely to remain, especially in regard to risk, internal control and fraud.

New Offence of Failure to Prevent Fraud - Economic Crime and Corporate Transparency Act 2023 (ECCTA)

The new failure to prevent fraud offence has a familiar feel to the other corporate offences of failure to prevent bribery under s7 Bribery Act 2010 and failure to prevent facilitation of tax evasion under Part 3 of the Criminal Finance Act 2017. Under the proposed new offence, an organisation will be liable where a specified fraud offence is committed by an employee or agent, for the organisation's benefit, and the organisation did not have reasonable fraud prevention procedures in place.



Corporate governance reform cont.

How internal audit can support

UK Corporate Governance Code – Internal controls

The FRC has emphasised that the UK approach to internal controls differentiates from the 'much more intrusive approach adopted in the US' and has confirmed that internal controls will remain a key feature of the revised UK Corporate Governance Code. Whilst the publication of the Code Provision is awaited, Internal Audit should be thinking about 'no regret' activities, the significant risk areas relating to financial and operational controls and to controls over financial and non-financial reporting.

Economic Crime and Corporate Transparency Act (ECCTA)

Companies should have in place a focused fraud risk assessment and have designed and implemented procedures to prevent and detect fraud. This should include Speak Up policies and mechanisms for fraud and suspected fraud to be reported through to the Audit Committee. A review of existing arrangements against the ECCTA requirements should be a priority for 2024.

Board Performance

Even the best performing boards should reflect on their own processes, behaviours and relationships and learn from the failings of others. Regular self-assessment, including board members' appraisal, should be encouraged in-between independent reviews.

Data privacy

All organisations process personal data as part of routine operations, while for some it may form part of their core business activities. When the EU General Data Protection Regulation (GDPR) was enshrined into UK law (UK Data Protection Act 2018) in May 2018 (now known as the UK GDPR, after Brexit), it fundamentally overhauled how organisations manage and safeguard personal data. However, there are proposals to update the existing data protection framework in the UK.

Personal data is considered to now be a valuable asset and in the last five years, an increasing number of jurisdictions across the globe have enacted legislation resembling aspects of the GDPR, which have quickly become the expected global standard. As individuals are increasingly aware of their rights in relation to their personal data, this can influence the companies they engage with.

From a risk perspective, the financial penalties for organisations in the event of non-compliance with data protection legislation can be significant. Organisations should also be aware of the associated reputational damage arising from non-compliance and the associated negative public perception.

In July 2022, the UK's Data Protection and Digital Information Bill (No. 2) was laid before UK Parliament, marking a significant step in the post-Brexit reform of the UK's data protection regime. As the UK government has put it, the bill—which is currently at the committee stage at the House of Lords—seeks to 'reduce costs and burdens for British businesses and charities' by removing some of the existing requirements while trimming down the others (including, those related to a record of processing activities). Regardless of whether the changes materialise, UK organisations will continue to be required to demonstrate accountability. In so doing, it may be more advisable for organisations to keep maintaining the existing controls as currently required by the UK GDPR rather than water them down or altogether set them aside if and when the proposed bill becomes law. In any case, companies exposed to the EU GDPR will still have to ensure that these controls are maintained to comply with the regulation.

Finally, there have been significant developments in the international data transfer landscape in 2023 with the introduction of the UK-US Data Bridge (an extension to the EU-US Transatlantic Data Privacy Framework). This enables UK organisations to transfer personal data freely to participating US organisations; for transfers to non-participating entities, the requirement remains to put in place an appropriate safeguard and to carry out an accompanying transfer risk assessment. As a result, the fundamental requirement remains that organisations need to have a firm understanding of their third-party data transfer exposure and the corresponding impact on contracting requirements to ensure that the applicable data protection regulation is continuously being complied with.

Data privacy cont.

How internal audit can support

- Internal audit is an invaluable tool to provide audit and risk committees with current levels of compliance while outlining recommendations to support the organisation with remedying any gaps in their data protection framework. It is an opportunity to benefit from the knowledge and experience of specialist data protection subject matter experts
- Data protection audits look at whether an organisation has the necessary controls in place to ensure data protection compliance and, if so, whether they operate effectively. This may include, amongst others, checking whether the organisation has mapped their personal data flows as well as whether the relevant policies and procedures have been developed and are fit for purpose
- Internal audit is also a useful tool to determine whether resourcing arrangements are appropriate, to meet on-going compliance requirements.

Digital transformation

Digital transformation goes beyond simple digitisation and represents a fundamental change to the 'how' an organisation's functions through IT-enabled means. Changes of this nature typically present a significant financial investment along with a multitude of business risks, therefore appropriate for inclusion within an internal audit plan.

Within Digital Transformations, technology is the enabler for new ways of working that can open up new markets, enable the deployment of new products more quickly/efficiently, improve back-office efficiency, create data driven organisations, to mention a few. Internal Audit plays a critical role in these transformations by providing assurance at a point in time or throughout the lifecycle of such projects as to help identify/mitigate potential risk/failures of the transformation.

Examples of key focus areas that are relevant to most Digital Transformations include the following:

- Alignment of new technology with operating model changes and strategic objectives
- Programme governance, delivery frameworks and planning
- Requirements and scope definition
- Change management and communication
- Data Strategy, migration, and re-platforming
- Testing and validation
- Benefits definition, tracking and realisation
- Deployment and service transition.

A spotlight on the software development lifecycle (SDLC)

SDLC plays a significant role in ensuring effectiveness, efficiency, and reliability of a business' software development processes and is a key area of risk to consider for many digital transformations, as well.

The way in which organisations execute SDLC to deliver value has been a rapidly evolving landscape that has had numerous changes over the last few years. Initially, organisations transitioned from the traditional waterfall approach (performing software development in a manner whereby each stage is dependent upon finalised deliverables from the previous stage) to a more agile software development approach (development of software using cross-functional teams to perform smaller 'sprints' of activity in order to analyse prototypes of code more rapidly and subsequently learn and adapt). This happened at a similar timeframe to when organisations also tended to remove legacy siloed approaches and instead began to combine software development and operations into 'DevOps' and 'DevSecOps.' Organisations have migrated their ERPs and related systems to the cloud, which has accelerated the adoption of an agile and/or DevOps software development approach.

There has also been a shift towards automation through the principle of Continuous Integration - using pipelines and automated testing to streamline the delivery of updated platforms. This has changed the frequency of delivering software changes in many organisations from the traditional expectation of a few major releases each year to instead entail consistent and frequent smaller releases being migrated to the live environment on a daily or weekly basis.

Digital transformation cont.

How internal audit can support

Internal Audit can be a 'critical friend' throughout the Digital Transformation's lifecycle or pinpoint risks and perform audits over these areas when and where necessary. Each transformation will present a different array of risks that will need to be analysed to determine the most appropriate means of providing assurance to the Audit Committee. Some examples of internal audits that can be especially relevant for Digital Transformations and/or a review of SDLC to include the following:

- Digital/IT/data strategy
- IT operating model
- Cloud infrastructure readiness
- Research and development tax credits review
- Transformation readiness
- Cloud migration and data readiness
- Project or programme assurance (periodic or continuous)
- Compliance with organisational SDLC policies/standards.

Supply chain & commercial risk

Managing your third party risk and driving better outcomes from supplier contracts across the lifecycle

With ever more reliance on third parties to deliver business-critical outcomes, alongside the macro-economic, geopolitical and environmental landscape, businesses are having to navigate an increasingly complex world when it comes to managing risk and driving better outcomes from their third-party relationships across the contracting lifecycle.

The last four years have seen a seemingly relentless set of challenges which have fundamentally shaken global supply chains. Major disruptions including the global pandemic, war in Ukraine, inflation and more recently instability in the Red Sea, have all highlighted fragilities across global supply chains and driven businesses to re-evaluate strategic supply chain models and governance to build greater resilience across the value chain.

Gaining greater transparency and building resilience and better performance across supply chains is therefore integral to helping organisations succeed. Prevalent supply chain and commercial risk themes include:

Supply chain resilience

Resilient supply chains are able to absorb shocks and quickly respond to new situations whilst simultaneously delivering against operational objectives. Creating robust strategic supply chain plans alongside a robust, ongoing risk management environment including key supplier monitoring/due diligence and sourcing contingency plans will significantly reduce the impact of disruptions and help sustain business operations in the face of global change.

Building an understanding of how financially-resilient and stable key suppliers are is a core pillar of providing greater visibility of risk across the supply chain. In addition, understanding the supplier's own risk exposures (geographical, sector, ownership) puts supply chain management teams at an advantage by enabling greater foresight and proactive issue management.

Contract compliance and performance

Most organisations struggle to realise the value and performance expected from their third party relationships. As such, value leakage and non-compliance is commonplace. Indeed, World Commerce & Contracting research has identified that contract non-compliance and wider value leakage cost companies the equivalent of 8.6% of annual revenue.

Reliance on suppliers to manage your reputation and delivery commitments places a high importance on ensuring effective and value-focused third party management. In the current macroeconomic environment, businesses which excel in this area will generate a tangible competitive advantage.

Supply chain & commercial risk cont.

Managing your third party risk and driving better outcomes from supplier contracts across the lifecycle

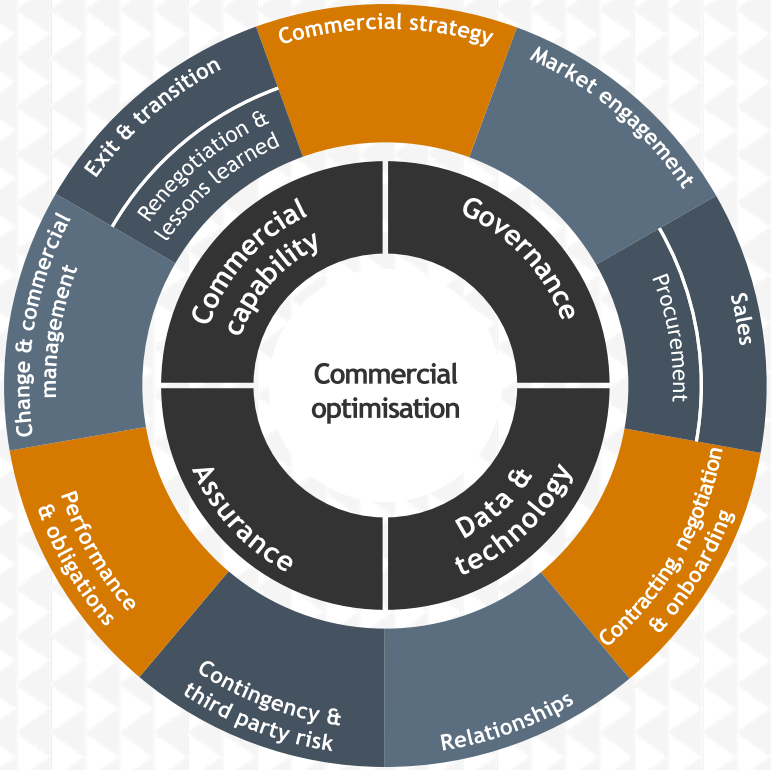
ESG across the supply chain

Managing an organisation's ESG impact extends well beyond its own operations. Reliance on third parties also brings supply chain ESG performance into focus, meaning that in order to fully monitor and manage ESG risks, businesses need to incorporate ESG criteria into procurement and sourcing decisions and ongoing supplier monitoring.

Increasing pressure and regulation from governments is on the way, not least through the EU's Corporate Sustainability Due Diligence Directive.

This in addition to broader societal shifts and consumer expectations means that embedding ESG principles across the supply chain, businesses are not only better able to deliver on sustainability goals, but also enhance their own reputation, viability and resilience.

Internal Audit plays a key role in enabling organisations to enhance and optimise overall supply chain and commercial management outcomes. Overleaf we highlight where IA is well-placed to support the business by identifying and delivering tangible value back into the organisation.



How internal audit can support

Internal Audit plays a crucial role in supporting the wider business in its supply chain and commercial management functions. Ensuring a robust and effectively-operating supply chain and commercial framework has a fundamental impact on the business' performance. IA is well-placed to drive value across the lifecycle including:

- Procurement function maturity assessments
- Strategic sourcing and responsible procurement (ESG)
- Contract and third party management effectiveness reviews
- Supplier resilience programmes
- Contract compliance and cost recovery audits
- Contract exit/transition plan assurance
- Final account settlement support
- Supply chain mapping and risk analysis
- Inventory management assessment and stock counts
- Supply Chain due diligence programmes
- Strategic third party spend reviews.

Economic crime

For the last 13 years organisations have prioritised building out their anti-bribery and corruption frameworks to satisfy the adequate procedures defence to the offence of failing to prevent bribery under s7 Bribery Act 2010. These frameworks have been informed by the six principles set out within guidance published by the Ministry of Justice. Developing and embedding these frameworks year on year provides Boards with the comfort that if bribery were to take place within any part of their business or associated persons then they would be protected.

In 2017 with the implementation of the Criminal Finances Act 2017, a second failure to prevent offence was introduced, namely the failure to prevent the facilitation of tax evasion. Ownership of this risk within organisations is often a joint approach between Tax/Finance teams, who understand that nature of the tax offences committed, and the Compliance teams who have experience in building out the framework to satisfy the defence. HMRC provided the guidance for this offence (Tackling tax evasion: Government guidance for the corporate offences of failure to prevent the criminal facilitation of tax evasion) setting out the defence of reasonable procedures bearing substantial similarity to the previously produced MoJ Guidance a few years earlier.

In October 2023 the Economic Crime and Corporate Transparency Act (ECCTA) received royal assent and introduces a third corporate failure to prevent offence – this time in relation to Fraud. Under this proposed offence, an organisation will be liable where a specified fraud offence is committed by an associated person for the organisation's benefit, and the organisation did not have reasonable fraud prevention procedures in place. The scope of the offence will only apply to large organisations who meet two of the following three criteria:

i. Average number of employees over 250;

ii. Turnover in excess of £36m and;

iii. Total balance sheet assets above £18m.

Guidance published by the Serious Fraud Office is expected in H1 2024. We can expect this to be similar to the published guidance under both previous failure to prevent offences.

Bribery Act 2010 - MoJ Guidance
Failure to prevent bribery

Adequate procedures

- Principle 1 – Proportionate Procedures
- Principle 2 – Top-level Commitment
- Principle 3 – Risk Assessment
- Principle 4 – Due Diligence
- Principle 5 – Communication (including Training)
- Principle 6 – Monitoring and Review.

Criminal Finances Act 2017 - HMRC Guidance
Failure to prevent the criminal facilitation of tax evasion

Reasonable procedures

- Principle 1 – Proportionality of risk-based prevention procedures
- Principle 2 – Top Level Commitment
- Principle 3 – Risk Assessment
- Principle 4 – Due Diligence
- Principle 5 – Communication (including training)
- Principle 6 – Monitoring and Review.

Economic Crime and Corporate Transparency Act ('ECCTA') 2023 – SFO Guidance – to be published 2024.

Failure to prevent Fraud - Reasonable procedures.

Economic crime cont.

How internal audit can support

- Heads of Internal Audit will already be familiar with the two earlier failure to prevent offences under both the Bribery Act and Criminal Finances Act and audits in relation to the design and effective implementation of adequate procedures and reasonable procedures defences should have been taking place for some time
- However, with the new failure to prevent fraud offence Heads of Internal Audit for large organisations within the scope of the act should be ensuring this is high on the agenda of the audit committee and management
- Fraud is not a new risk consideration for Heads of Internal Audit. IIA Standard 2120 requires that “internal audit activity must evaluate the potential for the occurrence of fraud and how the organisation manages fraud risk.” They should already have a clear view of their organisation’s exposure to fraud and how this is being managed. However previously organisations’ focus on fraud has been to ensure that they are not victims of fraud, which means financial controls are imperative, however the new offence relates to the organisation benefiting from fraud and will therefore be more aligned to building framework and compliance controls
- With their experience of helping the organisation establish procedures to address legislation such as the Bribery Act in the past – internal audit teams are well placed to support management in establishing the policy, procedures, fraud risk assessment and monitoring arrangements necessary to meet the requirements of the new Act.

Data visualisation

In today's rapidly evolving technological and data driven landscape, internal audits are no longer confined to historical number crunching exercises. In 2023, we saw some significant advancements on how more sophisticated and interactive visualisations are being used to present data, moving from simple charts and graphs. As we navigate through 2024, the symbiotic relationship between internal audit and data visualisation becomes increasingly important.

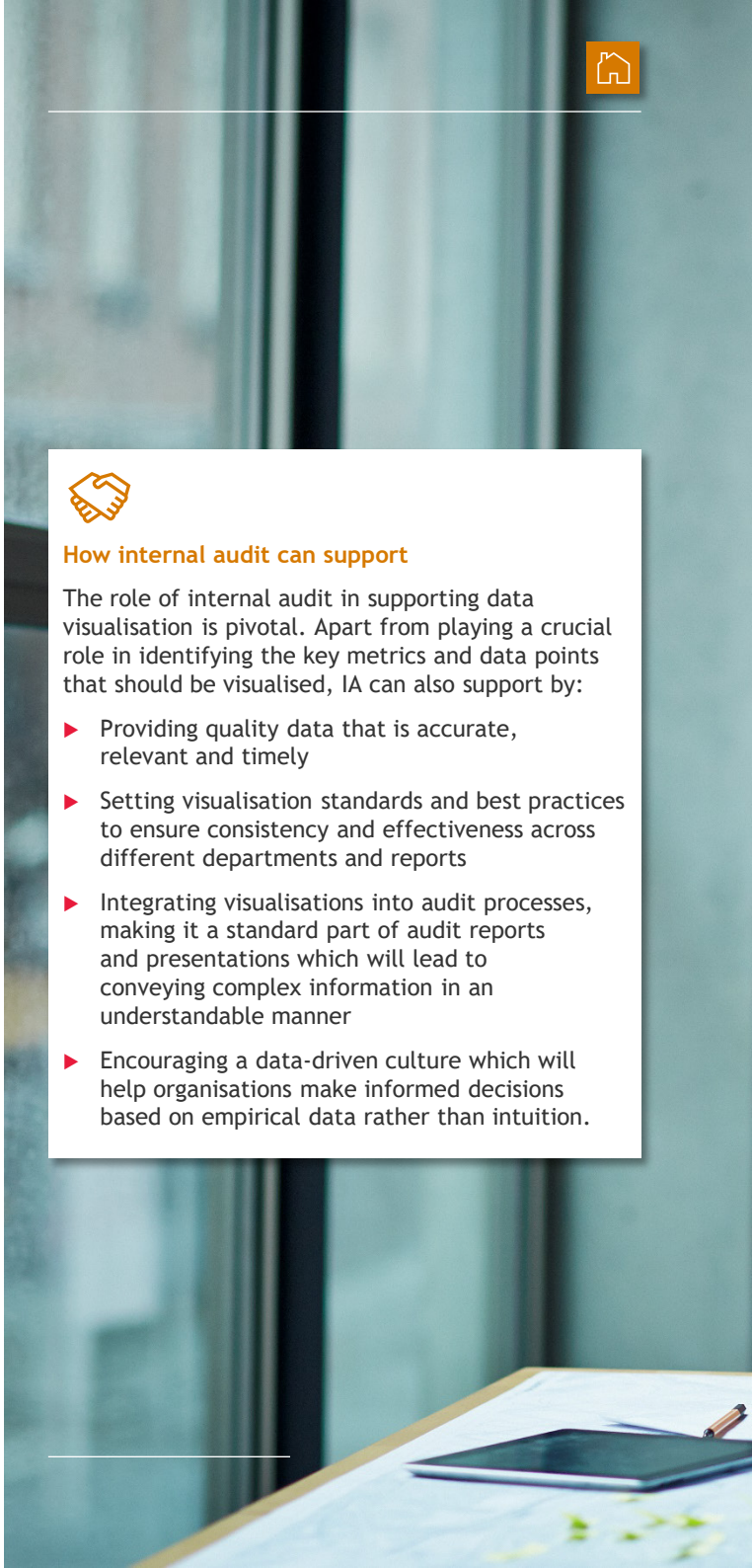
We have seen a substantial leap in how visualisation tools now incorporate advanced analytics, AI, machine learning algorithms and real-time data processing which can be leveraged to allow for a more dynamic, insightful and user-friendly visual representation of internal audit reports and presentations.

As we move forward, we must see data visualisation beyond mere aesthetics. A powerful dashboard, backed by robust data not only provides insights on static data, but also enables continuous monitoring/real time analysis of key risks and controls which from an internal audit perspective allows us to proactively identify potential problems before they escalate. This ongoing oversight, significantly enhances the audit function.

Moreover, the ongoing-oversight that data visualisation has to offer are also being seen as a tool to aid communication with non-auditors. Findings and insights gained from internal audits can be presented more effectively through visual means, making them more comprehensible to a wider group of stakeholders. This is particularly vital in translating complex findings to executive management or the board.

An increased use of data analytics and visualisations is also significantly reducing, and in some cases, eliminating the traditional reliance on sample sizes. This paradigm is being re-shaped in several ways since with the advancements of data analytics/visualisation tools and techniques entire datasets can be analysed quickly and efficiently, removing the inherent risk of sampling errors.

The advancements in the field of data visualisation as well as AI have also opened new horizons for internal audit in terms of accuracy, efficiency and impact. As these trends continue to evolve, they will undoubtedly shape the future landscape of internal auditing.



How internal audit can support

The role of internal audit in supporting data visualisation is pivotal. Apart from playing a crucial role in identifying the key metrics and data points that should be visualised, IA can also support by:

- Providing quality data that is accurate, relevant and timely
- Setting visualisation standards and best practices to ensure consistency and effectiveness across different departments and reports
- Integrating visualisations into audit processes, making it a standard part of audit reports and presentations which will lead to conveying complex information in an understandable manner
- Encouraging a data-driven culture which will help organisations make informed decisions based on empirical data rather than intuition.

Modern slavery

Modern Slavery has been on Internal Audit's agenda since the introduction of the Modern Slavery Act (MSA) in 2015, however the global occurrence of modern slavery is increasing and remains one of the most serious crimes that has devastating effects upon communities and destroys peoples' lives.

In the last couple of years geopolitical issues such as the invasion of Ukraine, the conflict in Gaza and other regional conflicts have all led to devastating effects upon humanity and the global economy and has changed lives across the world. The cost-of-living crisis, reduced accessibility to competitive mortgages and increased rents, as well as new challenges post COVID all have a disproportionate effect on those most vulnerable in our society and as a result the statistics on modern slavery are on the rise.

However, the role of business has not changed, and it is fundamental that organisations, whether within the scope of the MSA or not, do all they can to prevent and mitigate all aspects of modern slavery including slavery, servitude, forced or compulsory labour and human trafficking both within their own organisation and their supply chains. There is a clear expectation set out in the UK Governments' statutory guidance that business will aim to improve year on year and that this is reflected within their published Modern Slavery Statements.

Statistics on Modern Slavery

Unseen, a UK charity who provide support for the survivors of trafficking and modern slavery and run the UK Modern Slavery & Exploitation Helpline estimate that:

- 50 million people worldwide are in modern slavery
- 28 million are in forced labour
- 22 million people are in forced marriages
- Around 10,000 people in the UK are in modern slavery, according to the UK Government
- More than 100,000 people in the UK are in modern slavery, according to slavery experts (i.e. much more than official figures).

How internal audit can support

Internal Audit can provide assurance for organisations and their boards that the processes and controls are in place to prevent and detect modern slavery within the organisation and its supply chains.

In addition, Internal Audit can assess that those controls are adequately designed and implemented to meet the expectations of both the Modern Slavery Act itself as well as the good practice set out in the Home Office statutory guidance – Transparency in Supply Chains and that they are operating effectively.

Change of IIA standards

The greatly anticipated new Global IIA Standards have been released, alongside a report outlining the process followed for developing them, consulting, and responding to the consultation comments.

The release of the new Standards is the biggest change for the profession in over 20 years and over 1,612 consultation surveys were submitted. This number seems relatively low given global membership of over 235,000, although we understand that over a quarter (418) of the surveys were submitted on behalf of organisations and the IIA estimates this represents over 110,00 individuals.

So how does the final version differ to the draft Standards offered for consultation? Firstly, we should reflect there is no substantially new content added to the Standards. The Standards have not become more restrictive, and the changes made are based on the feedback and comments collected as part of the consultation process.

In response to feedback that the new Standards were overly prescriptive the IIA has reviewed the 'Requirements' sections and moved some of the detailed descriptions of how to implement the requirements to the 'Considerations for implementation' which provides guidance on common methods, but which is not mandatory to adopt. We also note that the use of 'must' has been toned down throughout the final version.

In relation to the performance of External Quality Assessments, we are pleased to see some of the requirements for external assessors, such as requiring them to obtain the IIA assessor qualification, have moved to the considerations for implementation. We note the requirement that "at least one person (on the assessment team) holds an active Certified Internal Auditor designation", which is welcomed.

The IIA has recognised the challenges faced by smaller Internal Audit functions and those operating in the Public Sector and reflected on these in the newly titled 'Fundamentals of the Global Internal Audit Standards' section, alongside incorporating a new section 'Applying the Global Internal Audit Standards in the Public Sector'.

The IIA responded to multiple concerns raised over the Standards' requirement for non-certified internal auditors to obtain at least 20 hours of CPE annually, and this has been removed, now reflecting that "practicing Internal auditors who have attained professional internal audit certifications must follow the continuing professional education policies and fulfil the requirements applicable to their certifications".

The key changes introduced by the new Standards are not new concepts for high-performing Internal Audit functions and include:

- The introduction of the Purpose statement for Internal Audit to assist auditors and stakeholders to understand and articulate the value of Internal Audit
- Development of an Internal Audit strategy (including a vision) that supports the strategic objectives and success of the organisation
- Formal Internal Audit performance objectives and measures to evaluate functional performance, which need to be approved and monitored by the Board
- Internal Audit methodology requirements related to identifying root causes, prioritising findings, developing engagement conclusions and communicating themes.

Probably the largest change between the consultation draft and the new Global Standards is to Domain III: Governing the Internal Audit Function where a new section has been added requiring the Chief Audit Executive to meet with senior management and the Board to discuss the Standards and clarify roles. The requirements for the Board have also been changed to 'Essential Conditions' with supporting information on how to address disagreements and non-conformance.

Change of IIA standards cont.

What does this mean for internal audit and what should you do?

- Plan your response, the Standards become effective 9 January 2025 so use this time to plan how you are going to comply accordingly
- Utilise the free resources available to you, the IIA is hosting a series of webinars:
  - 24 January - Get to Know the New Global Internal Audit Standards
  - 13 February - What the New Standards Mean to Quality Assessments.
- If you are having an External Quality Assessment in 2024, take the opportunity to incorporate a gap analysis against the new Standards to support your team's transition
- Watch out for the mapping of the 2017 Standards to the 2024 Standards, coming soon from the IIA
- Have you documented your Internal Audit strategy and methodology? These are both required under the new Standards
- When reviewing your procedures, processes and methodologies against the new Standards, take the opportunity to reflect on how you operate in practice and think about whether different approaches may be better or more effective
- Chief Audit Executives should engage with (and educate) the Board and Chair on the content of the new Standards and enhanced responsibilities of the Board. This is a requirement of the new Standards.

Cyber risk

Cyber security has and will consistently feature as one of the most dynamic and evolving risks that is assessed in many organisations' annual Internal Audit planning exercises (it has been voted the number one risk for the last five years in the CIIA annual Risk in Focus survey).

Organisations are using additional technology and means of automation than previously, such as Robotic Process Automation (RPA) and artificial intelligence (AI), potentially creating new cyber risks in the process. New mandatory requirements are being set in EU legislation such as the Digital Operational Resilience Act (DORA), the NIS2 Directive, Data Act, and Cyber Resilience Act.

Critical information assets ('crown jewels') need to be well protected with defensive, monitoring and recovery controls strengthened as far as possible. Internal Audit should assess their audit plans to determine whether the audit plan will be sufficient to meet the needs of the Audit Committee and the organisation during this period of heightened risk, rapidly emerging technologies, and new regulations.

The skill sets and sub-specialisms that are required by Internal Auditors and any SMEs that they bring to partner with them on cyber security internal audits are constantly evolving as well, in line with the changing nature of threats by cyber threat actors and changes to technology.

An alignment between Internal Audit teams and in-house IT security teams is becoming more commonplace in some organisations to leverage their respective expertise. This collaboration can help Internal Audit functions to become closer to the range of cyber security risks and the current state of any remediation and to help ensure that audit activities align with the rapidly evolving technology landscape. The closer collaboration can also help Internal Audit teams to become closer to the detailed cyber risks, and help them with risk quantification of such risks, which may help to avoid a scenario whereby every cyber Internal Audit report receives a 'high' rating, which may lead to fatigue from the audited parties.

Given the heavy reliance on third parties, including cloud providers and software-as-a-service providers, cyber security across the entire supply chain is also a focus area that we have observed at our clients. Internal Audit's role is expanding in these interconnected environments to consider cyber security risks and controls both within the primary organisation as well as the cyber security posture of any supplier that it relies upon.

As organisations continue to navigate changes to cyber security risks, the more recent trends indicate a shift toward proactive, collaborative, and technologically advanced approaches.

How internal audit can support

Internal Audit can provide assurance and Advisory services to the first line of defence in a variety of ways in order to help enhance the cyber security controls environment, including:

- Penetration testing
- Information security
- Cyber maturity assessments and threat modelling
- Cyber resilience, recovery, and wider business continuity
- Cyber regulation and compliance (including DORA, ISO, PCI, Cyber Essentials, etc.)
- Frequent/continuous vulnerability assessments
- Supply chain security
- Cloud security
- Incident and crisis response simulations
- Privileged access management, identity governance and cloud access governance
- IT Security awareness education.

ESG (Environment, Social and Governance)

ESG is a mechanism to quantify and report on an organisations sustainability efforts and goals and is increasingly important to internal and external stakeholders. This is because embedding sustainable business practices and ESG within the organisational strategy creates value, protects value and manages risk. To achieve this, it is critical to understand what sustainability and ESG means in the context of the organisation and its mission.

2023 saw an increase in regulatory reporting requirements across the globe and the launch of the International Sustainability Standards Board's (ISSB) global sustainability standards, following the aim to increase the consistency and quality of ESG reporting, to focus on material sustainability risks and opportunities and address greenwashing concerns.

The trend of increasing regulatory and reporting requirements is expected to continue for the foreseeable future alongside an increasing demand for assurance over non-financial disclosures to add credibility to disclosures.

For organisations to create and protect value and to be able to communicate effectively, ESG should not be considered as a year-end reporting requirement but be embedded within business as usual activities and decision making.

Key considerations to achieve this include:

- Which ESG topics represent the greatest potential risk or opportunity to the organisation and its long-term success?
- Have clear ESG and sustainability objectives and targets been set and communicated across the organisation?
- Are climate and sustainability risks integrated into wider risk management activities? Have key risk indicators been identified?
- Are there robust processes, controls and systems in place across each of the ESG priority areas?
- Is quality data readily available to enable performance to be monitored?
- Is ESG reporting transparent, balanced, credible and fair? Does it focus on the material ESG risks to the organisations enterprise value?

ESG cont.

How internal audit can support

Internal audit has a key role to play in understanding and robustly assessing how ESG topics impact the organisations risk landscape over the short, medium and longer term. ESG considerations and priorities should be built into assurance maps, considering the internal audit effort alongside the organisations wider assurance landscape. Specifically, internal audit can:

- Review and challenge the approach taken to identify the ESG topics which present the greatest risk to the organisation, considering the extent of stakeholder engagement (internal and external)
- Throughout all internal audit work, consider how sustainability and ESG objectives are integrated across the organisation, considered in decision making and risk management, and supported by an appropriate tone from the top
- Undertake internal audit reviews focused on ESG priority areas to provide assurance over the processes and controls in place to manage the risks and exploit the opportunities. Internal audit reviews can also support organisations in preparing for independent third party assurance over non-financial metrics
- Provide assurance over sustainability reporting, considering alignment with regulatory requirements and whether claims made are transparent and appropriately supported. There continues to be a focus on greenwashing which presents a reputational risk. Whilst there remains the ability for organisations to 'pick and choose' what they report, internal audit has a role to play in challenging whether the content of reporting is aligned with the greatest risks to the organisation and whether there are robust controls in place to prevent 'greenwashing' or misleading and inaccurate statements. Internal audit should consider:
  - Are topics excluded which are material by omission?
  - Are topics and metrics included as 'good news stories' which have limited impact on the organisations strategy or success?

Geo-political risk

With geopolitical risk and uncertainty escalating in recent years, risk management and internal audit functions must recognise the increasing need to more closely monitor the potential impact of political, economic, and social factors on an organisation's operations and investments.

Geopolitical risk can arise from a variety of sources, including changes in government policies, civil unrest, terrorism, natural disasters, and international conflicts. To respond to such swiftly changing conditions effectively, organisations need to take both a proactive and reactive approach to mitigating this risk.

With many geopolitical experts predicting 2024 to be the most dangerous and uncertain year from a global political perspective, we consider the dominant themes to keep abreast of below:

- **Continued economic uncertainty:** Operating in a subdued growth environment, affected by high interest rates and geopolitical events impacting on consumption, investment and trade trends. Coupled with a shifting labour market, this will continue to bear higher costs for businesses
- **Military conflict:** The ongoing conflicts in Ukraine and Gaza, tension in the South China Sea and Taiwan put key regions under further strain and potential for spillover into broader regional escalation
- **Climate change:** The El Nino climate pattern will highlight the increasing vulnerabilities connected to climate change, and it and other natural disaster events will increase water stress, disrupt logistics and lead to reactive policies directly impacting businesses
- **Political regime change:** Key elections in the United States, the UK, across Europe, India, Indonesia and others will bring risks and opportunities as key policies shift and businesses face into changing industrial policies and trade
- **AI Governance:** Breakthroughs in artificial intelligence outpace governmental efforts to regulate it. This bears risk of how AI augmentation affects labour forces, as well as its role in intensifying the likelihood and impact of cyber attacks.

Internal audit and risk management functions play a key role in building awareness around geopolitical risk and how it is mitigated, and clear guidance from Boards will shape and enable assurance efforts.

Key considerations for promoting an effective approach to managing and auditing geopolitical risk include:

- Who bears the responsibility for identifying and mitigating geopolitical risk within the organisation?
- How is geopolitical expertise prioritised and deployed across the organisation's assurance coverage?
- What role does risk management have driving geopolitical risk recognition via risk registers or risk assessments?
- If the organisation operates across different jurisdictions, what is the strength of relationships with local stakeholders (governments, communities, suppliers)?
- Is the business (first line) aware of available geopolitical specialist expertise to draw on for strategic decision-making?
- What MI and external data is readily available to guide swift decision-making in relation to geopolitical risk?
- How will geopolitical risk be considered across all lines of defence to emphasise a holistic impact for the business and link back to strategic decision-making?
- What contingency plans are or can be put into place to respond effectively to crystalised geopolitical risk?

Geo-political risk cont.

How internal audit can support

Given the global escalation in geopolitical instability and the complexity of consequences, direct and indirect, internal audit can play an important role in helping organisations understand where to focus assurance.

A key starting point is to assess the organisation's exposure to geopolitical risks and evaluate the effectiveness of the risk management strategies in place (reviewing key risk management policies and procedures, assessing the effectiveness of risk assessments, and evaluating the adequacy of the overall risk management approach and strategies).

Internal audit can review business continuity plans to ensure that they address potential geopolitical risks and that they are regularly tested and updated. Another key area for internal audit to review is the organisation's compliance with relevant laws and regulations related to geopolitical risks, such as sanctions and export controls.

More broadly, to effectively audit geopolitical risk, internal audit needs to have a good understanding of the organisation's operations and how exposure to geopolitical risks may impact them. This may involve research on political and economic developments in the regions where the organisation operates, as well as consulting with subject matter experts both within and outside the organisation.

People

A new horizon for workforce risk audit approach

IA and HR professionals must look beyond traditional scope and metrics, such as staff retention and turnover, and take a broader view, focusing on mitigating the impact of intersecting human capital risks rather than trying to minimise the scope.

From a risk perspective, our quantitative and qualitative research has found that **retention** (47%), **contingent worker arrangements** (43%) and **recruitment challenges** (41%) are the leading human capital risks in a year. For HR professionals to deal with these risks proactively, the intersecting risks that magnify these main challenges must be examined.

To move towards a risk-welcoming, risk multiplier approach and succeed in this new operating environment, HR professionals must take **a more holistic approach** and collaborate with people across the business to understand how multiple risks affect hiring and retention. Few organisations bring together expertise from across the organisation to help understand and manage risk multipliers.

Five main hot topics are vital to operating in a risk-welcoming landscape, all of which can be applied by IA professionals to manage human capital risks proactively with their HR counterparts.

Number one is the **agility of mindset** across leadership and the organisation—if you do things the same way, why would you expect a different outcome?

The second one concerns connectivity and a clear understanding of organisational risks. Not everybody needs to be an expert on internal audit methodologies, but everybody needs better people **risk awareness**.

Culture is vital, so the tone from the top, psychological safety around reporting (concerns), the ability to have forums where you have discussions, and then technology as something that can drive the pace of response (to risks).

Technology is an enabler, rather than the cart that goes before the horse. The focus on data and measurement that is enabled by HR technologies – aligns well with the overall risk concepts of data-driven objectivity and transparency and opens new risks but also new opportunities.

Managing proactively **reputational risks** means HR professionals must consider how their organisations remain attractive to potential employees. The reputational risks intersect with other risks that can hinder recruitment, such as the effects on the talent pool of changing demographics and evolving attitudes to issues including climate, human rights, and social responsibilities. The great resignation wave created a new risk: the overheated recruitment market. The perfect storm of insufficiently trained people and the urgent need to recruit made a ‘lopsided’ situation of multiple risks where people demanded higher pay; some accepted more junior roles, while others took jobs beyond their experience.

In a market where employees, suppliers and contractors are more discerning about where they choose to work, a company’s **social capital and reputation** for ethical behaviour become fundamental factors in its ability to meet its hiring needs.

Improving working capital

Following 14 consecutive increases to interest rates, Bank Rate is at its highest level for 15 years. This increases the cost of funding for businesses and elevates the need to focus on effective management of cash and working capital.

From historic lows, there has been a significant risk in interest rates since 2021 to respond to high rates of inflation. This has impacted on consumers, for example as energy bills, the cost of food and mortgage interest rates all increased.

The future path of interest rates is uncertain. At the time of this update, there are concerns about the Suez canal and a spike in shipping costs resulting from the war in the Middle East but there is also a prospect of further falls in inflation driven by reductions in food and energy prices.

Not only do these factors impact on funding costs but disruption to global shopping routes also creates wider problems for working capital, for example if goods spend longer in transit and do not arrive on time.

With this context in mind more attention to cash and working capital management is increasingly a key area of focus which has the potential to materially impact upon financial performance.

Key considerations include:

- Has the funding and hedging strategy been reviewed taking into account the interest rate environment
- Has your treasury function considered how to achieve a suitable return on day to day management of cash and investment of surplus funds
- Have the options to improve cash positions been fully explored, for example by securing improvements to creditor days
- Do you have robust credit policies and processes to monitor customer payments and to drive improvements in cash collection practices
- Are your inventory management policies and processes operating effectively to ensure that inventory levels are optimised, there are key performance measures for days inventory outstanding and that inventory turnover rates are measured and understood.

FOR MORE INFORMATION:

Tim Foster

+44 (0)7583 114 121
tim.foster@bdo.co.uk

Cherry Cromarty

+44 (0)2045 495 056
cherry.cromarty@bdo.co.uk

www.bdo.co.uk

42023839