



The Agenda

An Internal Audit perspective on risks and issues on the boardroom agenda

October 2024



Introduction

In today's rapidly evolving risk landscape, organisations face an array of challenges and uncertainties. Technological advancements, shifting customer expectations, macroeconomic and geopolitical instability, and climate change all demand strategic agility and robust risk management.

Our 27th [Global CEO Survey](#) tells us that, in 2024, CEOs are increasingly concerned about the long-term viability of their organisations, with many taking steps to refine or reinvent their business models.

Internal Audit serves as a vital ally, fortifying organisations against heightened risk and complexity and helping them stay resilient as they seek to deliver their business strategy.

We hope this sector agnostic 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 single point of reference to encourage discussion, stimulate fresh thinking and provide an aide-memoire for planning, re-planning, audit scoping and developing strategy.

The publication for this year is intentionally more detailed than previous editions, with links to further reading added in some sections to reflect the increasing complexity of today's risk landscape.

We have structured the document into 3 sections:

1. Macro-economic trends,
2. Hot topics on the boardroom agenda, and
3. Professional practices update.

Our selected topics and content is not intended to be exhaustive. We have considered those risks that we see as being uppermost on the Board agenda in the coming months.

By focusing on these areas, we aim to provide a strategic overview that will help Internal Auditors to navigate the complexities of the current environment and support Boards and Audit Committees as they seek to enhance their governance effectiveness.



Introduction (continued)

As Boards face an ever wider, more complex and interrelated set of risks, it's no surprise that they are raising the bar on the expectations of Internal Audit teams. These heightened expectations extend beyond the delivery of an audit plan as Internal Auditors are increasingly called on to apply their analytical skills and organisational knowledge to support strategic initiatives, guide key decisions and support improvements in governance, risk and control across all areas of operation.

Alongside this, the new **Global Internal Audit Standards™** (effective on 9 January 2025) also focus on the role, remit and organisational mandate of Internal Audit. The new standards are not just relevant to Internal Auditors – they impact the whole organisation.

This means the Board and each line of defence need to work together to capture the opportunities the new standards bring to enhance value and quality from assurance. **See section 3.**

Below, we illustrate just a few of the key trends underpinning many of the risk areas that we focus on this year.

A rapidly changing and unpredictable environment

Macroeconomics and geopolitics are increasingly driving the shape of the risk environment – creating uncertainty and encouraging a focus on resilience, where foresight becomes vital.

For this reason, **Section 1** of this publication provides our perspectives on these areas.

Strengthening governance

External focus on organisations' performance and conduct continues to dominate.

This drives an expectation for transparency and more timely reporting which expands well beyond traditional areas of financial performance and governance.

Increased regulation

There is a significant body of new and emerging legislation in relation to areas of global significance, such as:

- sustainability and environmental, social, and governance (ESG) matters;
- data use and personal privacy, specifically in relation to AI, and
- tax, tariffs, sanctions, fraud and bribery.

Significant technological advances

The pace at which new technologies are developed and exploited and their impacts has risen considerably in last decade. This has dramatically shifted how individuals and businesses interact – providing opportunities for greater efficiency and improved experiences but also carrying great risks around resilience and privacy.



This year's Agenda



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

01

Macro trends



Geopolitical uncertainty >

UK economic outlook >

02

The Agenda



Technology and security >

Sustainability >

Regulation >

Supply chain management >

People and organisational culture >

03

Professional practices update



The IIA's Global Internal Audit Standards™ >

The Internal Audit Code of Practice consultation >



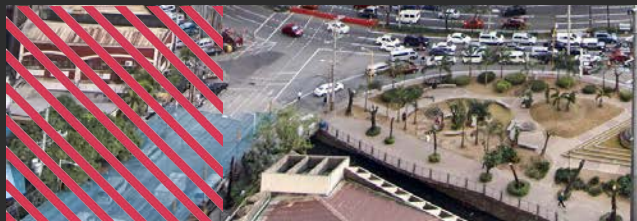
01



Macro trends

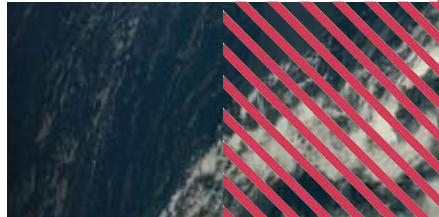
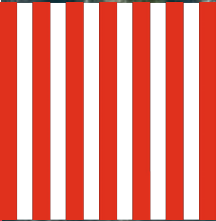
Geopolitical uncertainty

UK economic outlook





Geopolitical uncertainty



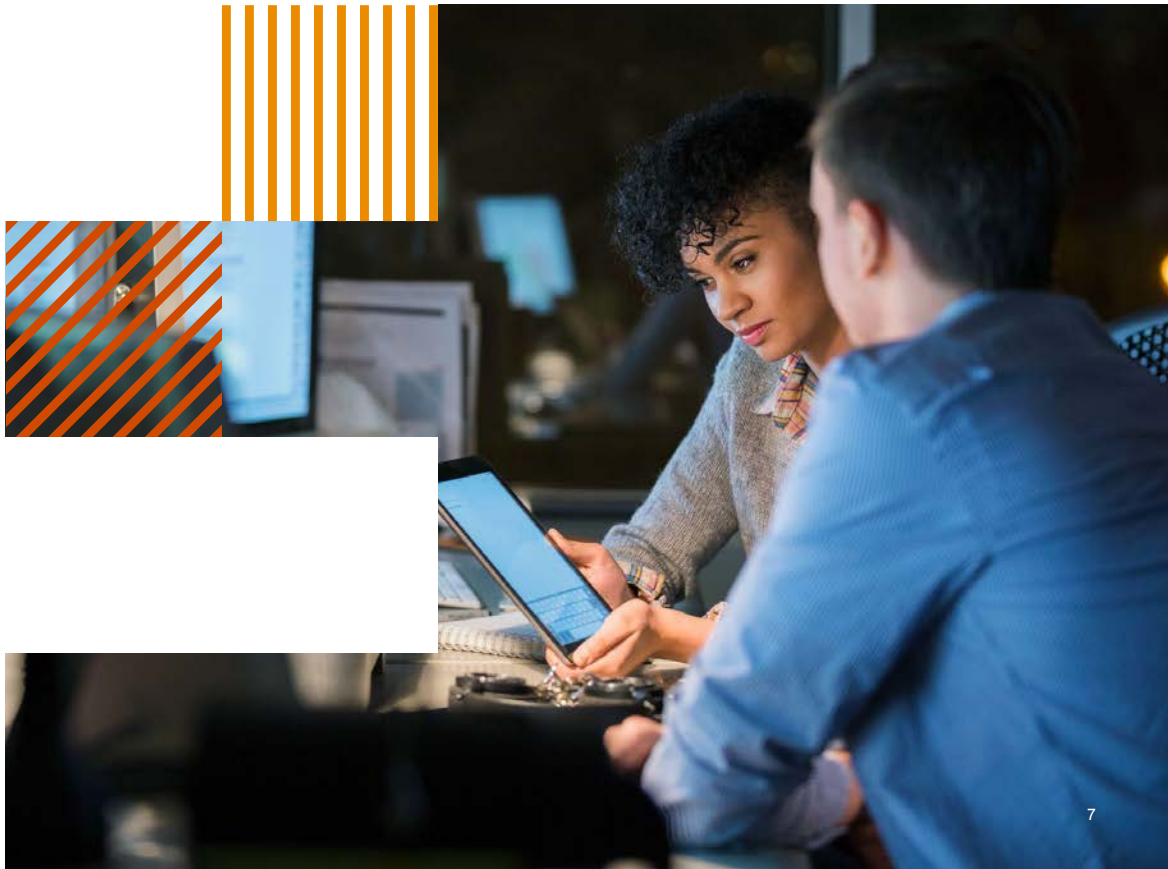
Geopolitical uncertainty



In recent years, global events and geopolitics have shaped the risk environment - creating uncertainty and encouraging a focus on resilience.

The impacts of conflicts, economic challenges and political shifts feature heavily in the list of risks facing organisations in 2024, as the 'year of elections' continues. These sit alongside, and are compounded by, the rapid pace of technological change and its many impacts (on business, consumers, governments and criminals/hacktivists) and continued pressure from regulators, consumers and campaigners for action on climate change and the protection of our natural resources.

These interrelated and fast moving macro risks affect consumer habits and expectations, operations and supply chains. Business leaders face considerable challenges in making sound decisions in the face of such complexity and uncertainty.



Organisational impacts



Risks driven by geopolitics will result in a wide range of impacts to business and organisations. Some of these will manifest in 2024, others will take longer to be felt, but are nevertheless worth considering now. Internal Auditors need to be alert to the changing risk profile and its impacts on the control environment and organisational assurance needs. Based on the current geopolitical risk environment, below are several hypothetical short-term and medium-term scenarios that highlight how geopolitics could plausibly impact business.

Short-term scenarios (2024):

01

Increased supply chain

disruptions: Conflict dynamics and political tensions in the Middle East, Eastern Europe, and Asia expose organisations to supply chain disruption. Advanced technology, data, mineral resources, and semiconductors are especially exposed.

02

A focus on national

resilience: Faced with vulnerability of critical inputs to acute shocks or malicious actions, many governments across the globe have taken short-term measures aimed at incentivising domestic resilience – whether through tariffs and protectionist policies or a focus on food and energy security, for example. For both governments and businesses, resilience is increasingly weighed against economic efficiency in decision-making.

03

A complex and changing environment for global business models:

Driven by protectionism, changes to taxes, duties and tariffs, labour laws and sanctions impact both strategic decision making and day-to-day operations for global operators. Meanwhile, the drive for a focus on sustainable growth and protection of natural resources, has seen the development of a range of new reporting requirements.

Navigating the new landscape poses challenges to cross-border transactions, reputation, ESG management, and talent acquisition.

04

The geopolitical outlook drives heightened cyber risks:

Cyber security has become part of the arsenal in geopolitical conflicts, and attacks can be sophisticated and persistent. Attackers often gain a foothold by stealing user credentials and then move unimpeded between systems. Attacks can spread around the world in hours rather than days thanks to automation. Multinational and global organisations can be affected even if they are not directly targeted.

05

Election results change the investment landscape: By the end of 2024, 75% of democratic countries will have held elections. New governments could invoke shifts in industrial strategy, trading relationships, regulations, and foreign policy, with implications for global competition. We anticipate some market repositioning as investment flows adjust to new conditions.

Organisational impacts (continued)

Medium-term scenarios (2025-27):

01

Impacts of protectionism

filter through: Newly introduced protectionist legislation begins exhibiting impacts more forcefully, generating compliance challenges and risks to business operational models.

02

Global realignment of key powers following elections:

Results of 2024 elections, notably the inauguration of the US presidential election winner, the embedding of the new UK government, and other results in key territories, lead to further trade legislation. Organisations will need to be resilient to withstand change and disruption and to respond with agility to new challenges and opportunities.

03

Geopolitical fault lines shape the competitive landscape:

Scarcity of critical minerals, the desire to accelerate green technology advancements, and state-led protectionism over emerging technologies intensifies the competitive environment. The resources (i.e. raw materials, infrastructure development, and production capacity) of 'non-aligned' countries (those without a clear affiliation to an existing power-block) become increasingly contested. Businesses without plans for managing change become highly exposed.





UK economic outlook



UK economic outlook



Below, we summarise key points from our [analysis](#) of the UK economy, which focuses on UK growth outlook and inflation.

One of the new UK government's top priorities is to kickstart economic growth with the aspirational goal of achieving the 'highest sustained growth in the G7.' Assuming this strictly refers to economic growth rather than a broader measure of prosperity, our analysis indicates that this goal has not been achieved in decades. Additionally, the current government has committed to the previous government's fiscal rules to reduce debt as a share of GDP, and paired with tax cuts from the spring budget, the public purse is tight. The government is expected to rely on three sources of growth: getting people back to work, implementing a robust industrial strategy to attract private investment, and leveraging technology more effectively to boost productivity.

Given that the UK is expected to see very limited growth in its working-age population over the next decade, future growth must focus on increasing the capital stock of the UK economy (being total value of all fixed assets that are in use to produce goods and services) and using existing resources more productively – areas where the UK has historically struggled.

However, there is an opportunity to establish a new model of inclusive growth. The rise of Generative AI and the urgent need to transition to net zero present unique opportunities to drive this change. A key lever to initiate this transformation is committing to an industrial strategy.

PwC UK CEO Survey 2024



UK economic outlook (continued)



01

UK inflation outlook

The worst phase of the cost of living crisis appears to be behind us, and economic activity is gaining momentum, defined by a 0.7% increase in Q1 2024 GDP, 11 consecutive months of real earnings growth, and a rebound in consumer sentiment to levels seen two years ago. Inflation is projected to hover around the 2% target for the rest of 2024. This volatility is due to a reduction in services inflation as the labour market cools. However, rising energy prices, indicated by futures curves, suggest a slight uptick in overall inflation will be seen in October 2024 which may pose a challenge.

The Bank of England has initiated a rate-cutting cycle, though there remains some uncertainty regarding the pace of monetary loosening. Markets are currently [anticipating an additional 35 basis point reduction](#) by the end of the year.

02

Labour market outlook

The Office for National Statistics continues to advise caution when interpreting labour market statistics due to the low response rate to the Labour Force Survey (LFS), which is set to be replaced by the Transformed Labour Force Survey (TLFS) later this year. However, a broad suite of indicators provides strong evidence that the UK labour market is normalising, with unemployment and employment returning to pre-pandemic levels and vacancies down from their peak in June 2024 but still 11.6% higher than pre-pandemic levels. Economic inactivity remains a challenge, with 820,000 more working-age individuals not seeking work or unable to work compared to pre-pandemic levels, driven by long-term sickness and an increase of non-working students.

Although labour demand has softened, vacancy rates in most sectors remain robust compared to pre-pandemic levels.

03

Corporate insolvencies

Corporate insolvencies in the UK reached nearly 27,000 in 2023, the highest level in over three decades and surpassing volumes seen during the global financial crisis. Despite this, the liquidation rate remains relatively low at 54 per 10,000 active firms. Initially, the increase in insolvencies was concentrated among smaller, micro-firms, many of which were newly created during the pandemic by first-time entrepreneurs who typically hired few employees, held minimal debt, and relied heavily on government-backed loans. Econometric modeling predicts that corporate insolvencies will continue to rise, potentially reaching 30,000 by the end of 2024. The profile of insolvent firms is evolving, with larger firms and sectors – such as wholesale and retail, construction, and hotels and catering – increasingly affected by subdued demand, higher borrowing costs and elevated input costs.

UK economic outlook (continued)

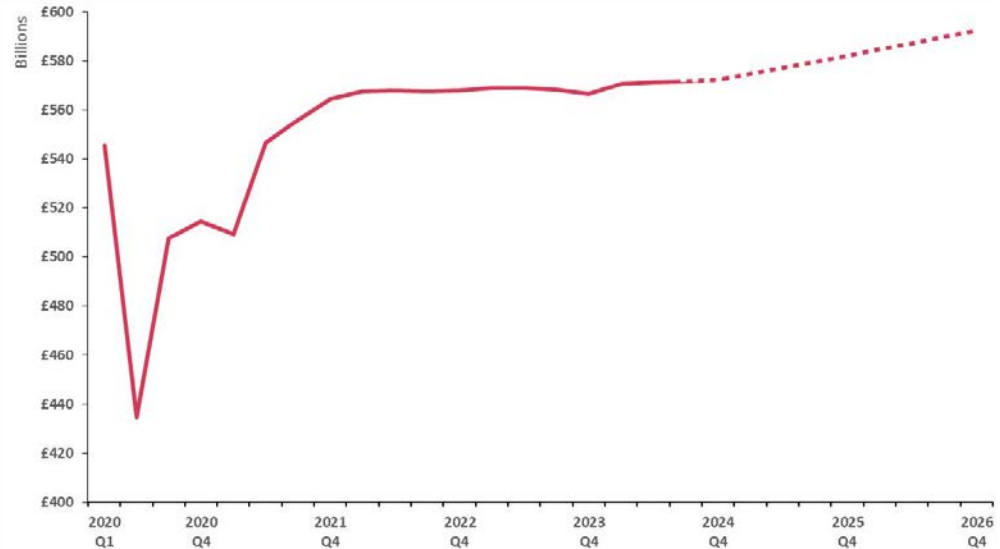


UK growth outlook

This scenario projection suggests annual growth in UK GDP of 1.0% in 2024, up from 0.1% in 2023, and further increasing to 1.7% in 2025 and 1.8% in 2026. However, this somewhat optimistic outlook could be disrupted by factors such as persistent inflation pressures or geopolitical shocks, which could slow down the expected rate-cutting cycle.

While this projection represents our best estimate, it does not account for potential changes in the international trading environment, and the path to economic normality is expected to be bumpy.

Quarterly real UK GDP, actuals and main scenario projections from Q2 2024





02

The Agenda

Technology and security

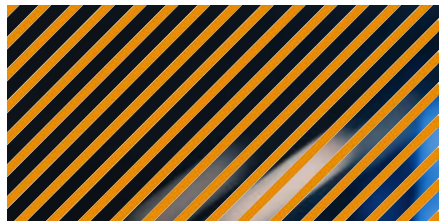
Sustainability

Regulation

Supply chain management

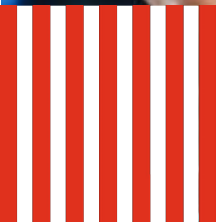
People and organisational culture





Technology and security

- Digital transformation
- Cloud technologies
- Artificial Intelligence
- Cyber security
- Privacy and data risk management
- Operational resilience



Digital transformation



What's on the risk agenda?

Many organisations continue to evolve and progress with their digital transformation programmes with the goal of increasing value through innovation, invention, customer experience or efficiency.

Common challenges

In our experience, the most common root causes of problems with the delivery of such programmes to time, cost and quality requirements include:



Weak governance



Budget and cost overruns



Mismatched people and culture, employee resistance to change



Poor planning



Programme risks not align to entity risk strategy



Lack of stakeholder engagement



Insufficient change control



Poor benefits management



Insufficient resourcing, lack of knowledge and skills

What's changing?

Today's digital transformation programmes take considerable space on the Boardroom agenda as a consequence of their scale, reach and complexity along with their strategic importance and cost.

Regulatory scrutiny has also highlighted that risks associated with material IT changes need to be considered and managed appropriately.

Wider organisational change initiatives depend heavily on IT solutions and resources for their delivery, creating pressure on scarce time and resources.

Common types of significant digital change programmes relate to:

- Cloud technologies
- Artificial intelligence
- Cyber risk management
- Privacy and data risk management

These topics are discussed further in this section, along with resilience.

Digital transformation (continued)



What does this mean for Internal Audit?

When considering digital transformation, Internal Auditors often focus on the following key areas:

Change management and organisational readiness

- Alignment of change initiatives with overall business goals and objectives.
- Readiness and capability of the organisation to adopt and sustain new technologies.

Governance and compliance

- The allocation of roles and responsibilities, and design of governance forums.
- The effectiveness, appropriateness and timeliness of the escalation and approval process by relevant committees and the Board.

Resilience

- Consideration of impact to critical business services.
- 'Failback/what if' scenario assessments in place in the event the programme is delayed or stopped.
- The effectiveness of existing risk management processes to identify, assess, escalate and report key IT change management risks.
- The lessons learned process (including a prioritisation approach over identified actions) to enable continuous improvement.

Technology integration and interoperability

- The integration of new digital tools with existing systems.
- The interoperability and compatibility of different technologies.

Programme management frameworks, such as the one illustrated below, can help Internal Auditors to methodically step through what can go wrong in order to focus attention on key areas of risk.



Cloud technologies



What's on the risk agenda?

All organisations face challenges when seeking to unlock the full potential of cloud technology. For some sectors, such as Financial Services, these challenges are heightened as a result of the intense regulatory scrutiny, requiring firms to demonstrate they are embedding resilience at the heart of their technology architecture.

Learning lessons from the Financial Services sector, offers value for others. Successfully navigating cloud transition challenges requires a holistic approach that addresses the regulatory, security, technical, operational, and organisational aspects of technological change.

What's changing?

Key considerations for organisations using the cloud

Moving to the cloud

Operating in the cloud

Optimising benefits and managing costs

Regulatory compliance – Securing both regulatory and internal policy approval for migrating critical services or workloads to the cloud.

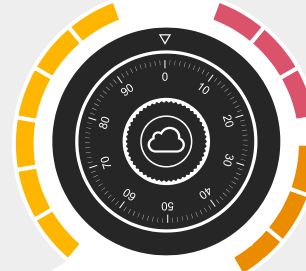
Security and risk management – Managing cloud adoption risks by enhancing risk frameworks and embedding security and operational controls upfront.

Operating model design – Designing and implementing shared responsibility models, and establishing oversight and governance arrangements.

Contracting – Negotiating optimal pricing agreements with Cloud Service Providers (CSPs) to maximise value from contracts and ensure projected spending aligns with commitments.

Data management – Migrating data from legacy systems into the cloud environment and establishing capabilities to govern and protect data post-migration.

AI governance – Managing risks in cloud-enabled GenAI applications, enhancing transparency, trust, and security to accelerate GenAI adoption.



Cyber security – Deploying effective security measures throughout the cloud environment (including access controls, and detection and response mechanisms) to mitigate potential risks.

Third party risk – Assessing and controlling risks for outsourced cloud services, providing assurance through vendor audits and ongoing reviews.

Resilience – Contingency arrangements and user guidance to manage disruption and build resilience, ensuring compliance with operational resilience regulations, where applicable.

Optimisation of cloud expenditure – Assessing expenditure and delivering cost savings through optimisation of infrastructure and services.

Sustainability – Understanding the sustainability implications of cloud usage and assisting with the journey towards net zero.

Process and control optimisation – Reducing the operational complexity associated with hybrid and/or multi-cloud environments.

Cloud technologies (continued)



What does this mean for Internal Audit?

Internal Audit can provide an independent perspective on cloud risks and the associated mitigations. Examples of key elements for Internal Audit to consider include:

Moving to the cloud

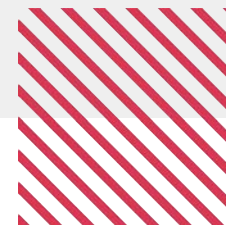
- Having a clearly defined approach to cloud transition, including assessment of the materiality of the workloads to be moved to the cloud.
- For regulated Financial Services firms, following a clear approach to relevant regulatory notifications (such as a material outsourcing notification) to ensure that these are comprehensive and timely.
- Understanding and enforcement of privacy requirements across multiple jurisdictions, including data classification definitions and enforcement of associated controls.
- Developing resilience arrangements for the cloud transition, proportionate to the level of risk associated with the workload to be moved.

Operating in the cloud

- Cyber security risk assessments to identify and prioritise risks, and ensure that strategies to mitigate identified risks are implemented.
- Considering cyber security requirements, compliance and right to audit clauses in contracts with CSPs.
- Developing and refining incident response plans for cloud-related incidents.

Optimising benefits and managing costs

- Attributing costs accurately to specific projects, departments, or business units, enabling better cost accountability and management.
- Tracking key performance indicators (KPIs) to measure the sustainability performance of cloud usage.
- Developing a cross-organisational approach, supported by FinOps or equivalent approaches, tools and frameworks, for controlling ongoing cloud costs.



Artificial intelligence – risks and opportunities



What's on the risk agenda?

Key industry trends we are seeing from our [Global CEO Survey](#) are as follows:

Artificial Intelligence (AI) presents a strategic opportunity, enabling organisations to enhance efficiency, innovation and the customer experience.

However, AI also introduces unique and complex risks requiring proactive assurance and oversight. As AI becomes more sophisticated, assurance functions must adapt their capabilities to provide Boards with reassurance on the effectiveness of controls and guardrails over the development, deployment and performance of AI solutions. Internal Auditors can play a key role in assessing the extent to which AI developments align with strategic objectives, ethical principles, regulatory obligations and stakeholder expectations.



Gen AI

AI is already supporting improvements in productivity and driving efficiency, with Gen AI leading the way. 70% of CEOs said GenAI will significantly change their business in the next 3 years^[1]. CEOs are focusing on scaling GenAI quickly, enabling new business models and investing in the necessary skills and technologies to capitalise on the strategic opportunities.



AI Regulation

With the EU AI Act having come into force on 1 August 2024, its broad scope, statutory requirements and focus on fundamental rights are changing the way organisations classify and govern AI. Many emerging AI use cases may now be subject to additional governance requirements.

The Act also requires organisations to comply with existing financial and data protection regulations for their AI systems, which impose stringent requirements on risk management, performance of systems and monitoring obligations. See Page 22 for more information.



Responsible AI

Use of AI within organisations introduces ethical challenges. Furthermore, AI-related incidents attract negative media coverage which highlights public concern. Ensuring the safe and responsible scaling of AI is essential to unlocking and protecting value from the use of AI.



Accountability

Within the Financial Services sector, the Senior Managers & Certification Regime (SM&CR) stresses Senior Management's accountability, including AI use. The Bank of England is considering 'reasonable steps' for managers to ensure model outputs are explainable and reasonable.

Other organisations should take note and implement policies, processes, and controls, owned by accountable individuals, so that their use of AI stands up to scrutiny.

^[1] PwC Global 27th Annual CEO Survey



Artificial intelligence – risks and opportunities (continued)



What's on the risk agenda? (continued)

Potential threats and risks associated with GenAI

While enabling new opportunities, the ever-growing capabilities and impact of AI introduces and exacerbates a number of risks that need to be managed:



Transparency

A lack of transparency around how and when AI is used can lead to lack of accountability and customer mistrust.



Hallucination

AI models could 'make up' information which is plausible but incorrect.



Copyright and intellectual property

GenAI models which are trained on copyright data may pose liability risks.



Misinformation

Most GenAI solutions are unaware of, and will exclude, events, cases or developments that post-date its training data.



Discrimination

If AI models can 'learn' discrimination and if this is based on protected characteristics, it could pose a significant regulatory and/or reputational risk.



Accountability

Many organisations lack clarity around roles and responsibilities to manage GenAI risks. Further, the ease of access to GenAI solutions, increases the risk of misuse – whether intended or accidental.



Data protection and security

Data leakage risks can be heightened if GenAI tools are granted inappropriate access.



Cyber security

AI could introduce new threat vectors, such as prompt injection attacks.



Misuse

GenAI could be used for malicious purposes, which could result in misalignment against the intended/ approved purposes.

Artificial intelligence - the EU AI Act

What's changing?

The **EU AI Act** is a new legislative framework that sets the precedent for AI regulation. The framework categorises AI into different risk categories and imposes obligations on users, deployers and providers of AI. [Compliance timelines](#) are in place and there is potential for significant fines for non-compliance. Effective audit of EU AI act readiness ensures that organisations are aligned with the regulation in order to gain a first mover advantage and avoid legal risks.

Overview of the EU AI Act

- **Risk-based classification** – AI systems must be classified into different risk categories to support effective governance while promoting innovation.
- **Safety and fundamental human rights** – AI systems must ensure the safety and protection of fundamental human rights, including non-discrimination, privacy, and data protection for all individuals.
- **Unified regulatory framework** – The Act creates consistent standards in order to facilitate lawful, safe, and trustworthy AI in the EU Single Market.
- **Broad, extraterritorial impact** – The AI Act applies to AI systems across all sectors and all systems operating in the EU, or with an impact in the EU, even if the system is abroad. UK based organisations are impacted if they procure, use or deploy systems on the EU market or impact EU customers.
- **Across the AI value chain** – Most obligations fall on providers (creators) and deployers (users), but importers and distributors are also affected.

Company fines for violations of the act range from...

€35m or 7%
of global annual
turnover (if higher)
– for violations of
banned AI

€15m or 3%
of global annual
turnover (if higher)
– for violations of
other obligations

€7.5m or 1%
of global annual
turnover (if higher)
– for supplying
incorrect information

¹EU AI act: Article 99 – penalty.

Artificial intelligence (continued)



What does this mean for Internal Audit?

Examples of key elements for Internal Audit to consider include:

Auditing organisational AI use

EU AI Act readiness

On the next two pages, we set out the key elements to consider in assessing AI readiness for the EU AI Act. Using this as a basis, many IA teams are working now to:

- Assess the existence and suitability of the organisation-wide AI inventory and classification of AI models as per EU AI Act requirements.
- Assess plans and progress with implementation of necessary governance (determined by the risk classifications) covering: transparency, technical documentation, impact assessments and codes of conduct depending on the use case.
- Ensure alignment with other sectoral regulation. The risks posed by AI may fall under the scope of other regulation, such as breaches/disruption of critical AI-enabled services leading to regulatory fines.

AI risk and controls

- Understand the AI universe including use cases and development status.
- Understand your organisation's AI strategy, risk assessment, governance and policy arrangements and how they are being developed and embedded.
- Build and execute a risk-based AI audit programme (referencing materials such as the PwC AI Readiness Framework, overleaf or [Responsible AI Framework](#)).
- Prepare tailored audit programmes for higher risk AI models.

Building AI skills within Internal Audit

AI enabled Internal Audit

- Identify use cases that will drive efficiencies, optimise, automate or enhance Internal Audit processes.
- Collaborate with AI steering committees and/or responsible AI council to ensure that controls and assurance remain high on the agenda.
- Develop or secure access to digital skills to provide confidence in Internal Audit's capacity and capability to use AI effectively and provide assurance over the key and emerging risks associated with AI.

On page 26, we provide more details on internal audit AI use cases.

Artificial intelligence - AI readiness framework

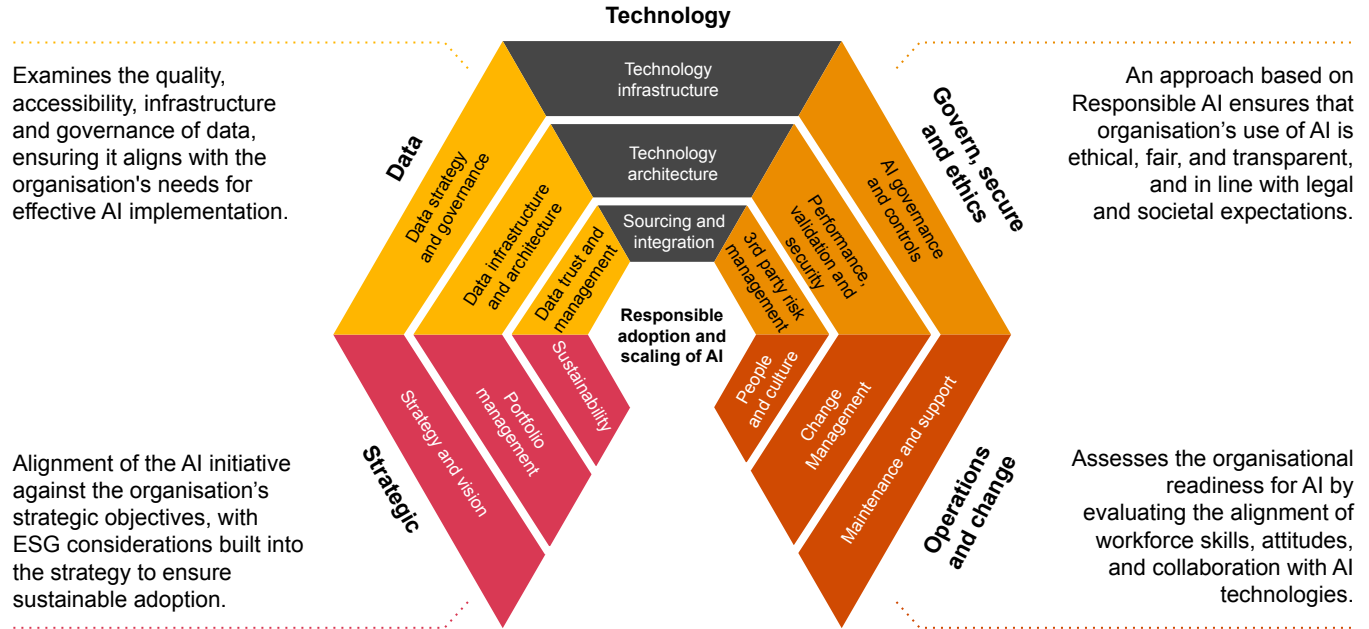


What's does it mean for the Internal Audit? (continued)

PwC's AI readiness framework:

Navigating the evolving landscape of AI involves careful consideration of the different domains that comprise effective and responsible operationalisation of the new technologies at scale. The AI readiness domains, developed by PwC and illustrated here, are aligned with industry standards and regulation such as the National Institute of Standards and Technology ('NIST') AI Risk Management Framework and the EU AI Act.

Evaluates the infrastructure, tools, and technical capabilities to determine the organisation's preparedness for AI adoption.








Artificial intelligence - AI readiness framework (continued)



What does this mean for Internal Audit? (continued)

Examples of key elements to consider in assessing AI readiness are:

Domain	Key Considerations
 Strategic	<ul style="list-style-type: none">• AI strategy to ensure clear ownership, long-term viability, alignment to corporate goals, and effective communication across the organisation.• Robust framework for managing AI opportunities, from identification and communication to monitoring, review, and realisation.• Capability to measure AI initiatives against ESG goals, assess environmental implications, and optimise costs through FinOps principles.
 Data	<ul style="list-style-type: none">• Data governance framework to ensure consideration of regulatory compliance, data reliability, and trust in AI systems.• Data infrastructure to ensure AI integration and effective data management.• High data quality and effective management of personal data.
 Technology	<ul style="list-style-type: none">• Effective processes and mechanisms for sourcing new AI solutions and integrating them into the existing tech landscape.• Standardised AI development lifecycle, maintaining code quality and software integrity in alignment with industry standards.• Robust technology infrastructure, architecture, and cloud resources, adequately set up to support the development and deployment of AI solutions.
 Governance, security and ethics	<ul style="list-style-type: none">• Measures and guardrails in place to manage AI risks, complying with best practices from regulators and standard-setters.• AI assurance solutions including comprehensive testing, explainability, secure design, bias detection, and user experience validation.• Assessment and management of potential risks and vulnerabilities from third parties, ensuring adherence to business policies and contractual requirements.
 Operations and change	<ul style="list-style-type: none">• AI-driven cultural transformation and training efforts to promote organisation-wide change and to leverage AI capabilities.• Comprehensive change management practices addressing cultural, technological, and business implications, ensuring business processes adapt to AI changes and planning for long-term viability.• Appropriate resources and mechanisms are in place to manage, maintain, and support AI solutions post-deployment.

Artificial intelligence - transforming Internal Audit with AI



What does this mean for Internal Audit? (continued)

AI has the potential to revolutionise Internal Audit functions – transforming capabilities, providing opportunities for optimisation of resources and better insight gathering through more detailed analysis. Here are some examples and key benefits of AI use cases that are changing the way organisations conduct Internal Audit.

AI enabled control testing

The capability of AI to process large volumes of unstructured data can be leveraged in controls evaluation and testing to recognise patterns and propose findings. AI is capable of:

- Reviewing documents, emails and summarising evidence submitted,
- Identifying gaps in data,
- Generating test scripts for remediation of identified issues, and
- Evaluating large control databases to identify duplicate controls and incomplete controls description.

Gen AI Internal Audit planning and support

GenAI models can help design Internal Audit plans and provide support on audit engagements, drawing from Internal Audit methodologies, web searches for relevant risk assessments and historic annual reports. Use cases include:

- Automating risk assessments,
- Developing audit plans with tailored domains and risk theming, and
- Drafting audit scope and announcement memorandums (or Terms of Reference).

AI enabled stakeholder engagement

GenAI solutions can enable more effective stakeholder engagement using tools such as Microsoft Copilot, which can improve productivity through:

- Drafting relevant stakeholder questions,
- Transcribing meetings and generating summaries, and
- Identifying next steps based on stakeholder conversations.

Continuous monitoring

AI tools can be used to continuously monitor systems and processes to automatically flag risks and provide an audit trail for review. Examples of continuous monitoring include:

- Identifying of anomalies and potentially fraudulent transactions,
- Automated monitoring to ensure compliance with policies and regulation, and
- Embedding predictive analytics for forecasts and ongoing risk assessments.

Audit practice and quality assurance support

AI can significantly enhance audit quality assurance and enable cost efficiency. Some examples are:

- Using GenAI to review audit reports and completed files to identify quality-related issues, and
- Incorporating interactive chatbots and virtual assistance to provide real time support to auditors on methodologies and audit standards.

Key benefits:

Reduce human error in data analysis and reporting

Improve accuracy of data analysis and verification against regulations

Increase efficiency and cost saving through process automation

Enable ongoing monitoring and real-time risk detection

Enable ongoing quality and continuous improvement

Cyber security



What's on the risk agenda?

Cyber crime continues to be a pervasive threat, affecting all countries and sectors as threat actors deploy a variety of techniques to achieve the common goal of monetising access to organisations and their data. Data-rich organisations delivering services that are critical to the economic fabric of society, such as Financial Services firms, are a high value target for cyber attacks, with their attack surface broadening due to increased innovation, digitisation of operations, and dependence on strategic IT partnerships.

What's changing?

Industry trends and insights

Key findings from PwC's [Global Digital Trust Insights Survey 2024](#):

- **Breach costs** – The proportion of costly cyber breaches (\$1m+) has increased since last year.
- **Digital and cyber risks are intertwined** – This requires Chief Information Security Officers (CISOs) and tech leaders to collaborate in balancing innovation with security risk management.
- **Cloud technologies** – Cloud risks were viewed as the most concerning threat (for 47% of survey respondents) and as a top priority for cyber security investments by 33% of respondents. This reflects the multi-layered security challenges posed by cloud technologies.
- **Modernisation and optimisation** – These areas top the cyber investment priorities for 2024.
- **Simplification** – Movement to integrated tech solutions or suites is increasing as organisations seek to simplify their IT infrastructure.
- **DefenseGPT** – Organisations are starting to deploy generative GenAI tools for cyber defence.
- **Regulation** – Business and tech leaders see various regulations as helpful but anticipate additional compliance costs and, in some cases, this creates a strong case for significant business transformation.
- **Top performing organisations** – Those organisations which display greater maturity in their cyber security initiatives, report a greater number of benefits and a lower incidence of cyber breach events.

PwC Global Digital Trust Insights Survey 2024



This annual survey captures the views of business and tech leaders around the world on the challenges and opportunities to improve and transform cyber security in their organisation in the next 12 to 18 months.

Cyber security (continued)



What's changing? (continued)

Cyber threats - A year in retrospect summary¹

Recurring themes in the threat environment are as follow:



Zero days, critical vulnerabilities, supply chain and cloud compromises have challenged organisations across all sectors, with more vulnerabilities disclosed in 2023 than ever before.



Geopolitical conflicts and tensions around the world have increased. Threat actors – particularly those with espionage, sabotage, and hacktivism motivations – continue to react and respond, shifting direction and broadening their activities.



Threat actors leverage what works, continuing to use known methods in addition to shifting techniques for more effective campaigns, adjusting for emerging technology and increased use of cloud services.



Ransomware and extortion continued to be a significant issue, as the number of leak site victims reached record levels in 2023.

¹ These insights draw upon analysis conducted by the PwC threat intelligence team across 2023, as reported on in the latest Year in Retrospect and reflect trends that we continue to see across the threat landscape in 2024.



Cyber security (continued)



What does this mean for Internal Audit?

We set out below a set of key focus areas and expected controls which Internal Audit teams can consider when evaluating cyber resilience:

Protection of the IT environment

- Multi-factor authentication (MFA) is configured for all email and remote access accounts.
- Web security tooling restricts content and blocks malicious downloads.
- Email tooling restricts attachments and scans for malicious content.
- Hardened endpoints restrict the execution of untrusted scripts and executables.
- Restrictions prevent the execution of untrusted Microsoft Office macros.

Early detection of potential threats

- Endpoint Detection and Response (EDR) tooling is deployed on workstations and servers.
- Continuous monitoring capability rapidly investigates and contains alerts, including out of hours.
- Regular 'red teaming' validates detection and response capabilities.

Prevention of unauthorised access

- Controls restrict and secure the use of accounts with domain administrator privileges.
- Internal vulnerability scanning is coupled with effective remediation processes.
- Proactive hunting and remediation is conducted in relation to Active Directory hygiene issues.
- Host-based firewalls on workstations are configured by default to block inbound traffic.
- Outbound internet access for all servers is restricted to 'allow-list' by firewalls and web filtering tools.

Cyber incident response and recovery

- Cyber incident response and crisis management plans are exercised.
- Playbooks are in place to allow for rapid isolation of parts of network and managing the impact.
- There are validated backups and recovery of infrastructure (e.g., Active Directory) is tested.
- Prioritised recovery plans are in place and regularly updated for key business systems and applications.

Privacy and data risk management



What's on the risk agenda?

In a complex and changing global business environment, organisations need to be focused on their data: to manage and protect it appropriately, recognise the value it presents as an asset, and be able to generate real benefit from it, safely and without breaching the trust of their customers, users and employees.

Managing the risks associated with the volume and range of available data presents technical, legal and regulatory challenges.



Data risk management is increasingly critical, particularly in organisations with high volumes of sensitive personal data, such as Financial Services firms. As organisations tackle legacy and new technologies, they must ensure data privacy and ethical integrity, and navigate the complexities of data sovereignty and international compliance.



Data is at the forefront of the regulatory agenda around the world with a plethora of different rules by territory (country or state) and sector presenting a compliance challenge for businesses operating and/or transferring data internationally.



Data breaches continue to dominate the business headlines – whether as a result of cyber attacks/ ransomware, non-compliant third party data processing or simple human error. The regulatory, financial and reputational costs of data breaches are well documented and so it's no surprise that data privacy and protection feature as a key risk on most organisational risk registers.



Data as an asset – data is a key business enabler and many organisations are looking to make better use of their data as a strategic asset. New technologies and regulations highlight the imperative of balancing data monetisation with ethical considerations.

Privacy and data risk management (continued)



What's changing?



01

Technological advancements

The rise of big data analytics, the Internet of Things (IoT), artificial intelligence (AI), and machine learning is increasing the volume, variety, and speed of data being generated. These technologies also introduce new data privacy concerns, such as the potential for unprecedented surveillance and data breaches.

In response to these challenges, data transformation programmes are now commonplace – typically a multi-year journey, requiring consistent leadership and authority to deliver and cross-organisational support to succeed and be sustained.

02

Regulatory changes

Governments worldwide are introducing or tightening laws and regulations, impacting how organisations manage, use and share personal data.

- UK organisations must comply with the UK General Data Protection Regulation (UK GDPR) and other local regulations such as the Data Protection Act 2018.
- With Brexit, the UK has established its own data protection framework separate from the EU. Organisations need to ensure compliance with the UK's data transfer rules, including implementing Standard Contractual Clauses (SCCs) and ensuring adequate safeguards for data transferred to and from the UK.
- UK Financial Service organisations face a rising bar of supervisory expectations as regulations such as BCBS 239 (Basel principles for risk data aggregation and risk reporting) are now considered an enterprise wide requirement above and beyond their original scope.
- Recent regulatory interventions, such as those by the Federal Reserve Board (FRB), underscore the importance of robust data governance. A number of organisations have faced significant financial penalties and enhanced oversight due to deficiencies in their data management practices, highlighting the necessity for continuous improvement.

Privacy and data risk management (continued)



What's changing? (continued)

03

Talent and training

A range of data-related skills are needed to harness the power of data and protect it: from experts in AI and machine learning to data analysts, compliance and legal specialists, cyber security professionals and technologists. Talent in data is increasingly in demand and the recruitment market is competitive, particularly in relation to emerging technologies.

Organisations should invest not only in these specialist skills, but also in upskilling their wider employee base in privacy literacy in order to protect against inappropriate data sharing or breaches from phishing or social engineering attacks.

04

Consumer awareness

The drive for convenience and flexibility in how individuals interact with businesses and service providers has led to more and different types of data being shared at volume. Yet, against this backdrop, consumers are becoming more aware of their data privacy rights and are increasingly concerned about how their data is being used, leading to higher expectations for transparency and control over personal data. With greater awareness of (a) the potential personal and societal harms of technology and new data use and (b) the important role of data ethics to safeguard equity, there is increased pressure on organisations to have robust and clear data practices.

Sound data management practices are often now seen as fundamental to the long-term value of maintaining customer trust.

Today's organisations need to design data ethics standards that are robust enough to stand up to continual inspection by external stakeholders.

Privacy and data risk management (continued)



What's changing? (continued)

05

The continued growth and evolution of non-financial reporting

With a large number of new and developing disclosure requirements, organisations often struggle to keep pace with what they should disclose, how and to gain the assurance they need that their processes and controls over data collation, analysis and reporting are sufficient robust. For example:

- **Sustainability and carbon reporting** – This is about more than just data – it's about challenging the measures and context organisations use to tell the story of their progress and ensuring compliance with the relevant reporting standards.
- **Diversity and inclusion reporting** – From reporting on gender pay to equal employment opportunities, stakeholders expect organisations to maintain an equitable, inclusive and progressive workplace and must be able to explain their data with confidence.
- **Social impact reporting** – Measuring the impacts that organisational actions are having on society is now commonplace but accusations of widespread 'greenwashing', create caution amongst executives.
- **Supply chain management reporting** – From Health and Safety data to waste and water usage, organisations need a handle not just on their own data but that of its supply chains.



Once seen as a nice to have, non-financial reporting is now driving access to capital and cost of funding, reputation with customers, suppliers and society, attraction and retention of talent and ultimately enterprise value. Reporting must be transparent, stand up to scrutiny from all stakeholders and be trusted.”

Paolo Taurae
Non-financial assurance leader, PwC UK

Privacy and data management (continued)



What does this mean for Internal Audit?

Considerations

In order to identify a focused scope of work for maximum value, Internal Audit should take into account the following:

- Digital and technological maturity.
- The regulatory landscape (international or multinational operations).
- Organisational areas of concern or high risk.
- Industry specific requirements and challenges.
- Internal strategic plans for data management.
- Plans for the introduction of new technologies such as AI and machine learning.
- Technology available to support privacy and data management.
- The importance of ethical data usage for an organisation's customers.

Possible areas for Internal Audit focus

Compliance with regulations – Ensuring compliance with relevant regulations such as the General Data Protection Regulation (GDPR), EU AI Act, California Consumer Privacy Act (CCPA), and other local laws.

Data risk management and governance – Evaluation of the risk management and data governance framework and how policies, procedures and management processes support the maintenance of data quality, integrity, and security. Most large, modern organisations have a clear data strategy, an adequate operating model and a data-driven culture to drive business value with data. The data strategy roadmap should scale and continually recalibrate.

Data management practices – Ensuring accurate, consistent, and reliable data is critical for risk management, compliance, and customer service. Implementing strong data governance frameworks, including data stewardship roles, quality standards, and validation processes, ensures data integrity and supports regulatory compliance and informed decision-making.

Internal Audit can provide much needed assurance over these practices by evaluating processes for third party risk management, incident response and breach management, data security and data privacy to ensure their efficacy for the organisation.

Data ethics and monetisation – Balancing data monetisation with ethical considerations is crucial, especially in heavily regulated and consumer markets such as Financial Services. UK institutions must be transparent about data usage, obtain explicit customer consent, and provide mechanisms for customers to control their data, ensuring ethical and responsible data practices.

Training and awareness – Assessing the levels and impact of organisational training and refresher training and awareness campaigns.

Operational resilience



What's on the risk agenda?

The recent IT outage that sent shockwaves through global enterprises underscores a fundamental truth: the digital age, while transformative, is fraught with risks that can disrupt even the most well-prepared organisations. The incident, which reverberated across various sectors, highlighted the imperative for robust resilience strategies and transparency in communication.

Technical changes are a primary cause of IT incidents, often disabling resilience measures, particularly in complex and integrated technology environments. To avoid disruptions, organisations must implement rigorous change management and prepare for major incidents, drawing lessons from cyber responses to guide secure recovery from accidental disruptions.

Preventative controls are crucial, but organisations must also prepare for inevitable disruptions by planning for severe yet plausible scenarios, requiring an end-to-end understanding of service delivery. Tech-powered dashboards and resilience technology platforms enable real-time tracking and prioritisation, allowing organisations to absorb disruptions effectively and invoke recovery strategies within organisations tolerance levels.

What's changing?

The outage highlighted the need for an enterprise-wide approach to resilience planning, prioritisation and response activities, encompassing the following learnings from recent disruptive events:

- Traditional, siloed approaches lead to fragmented and ineffective crisis responses. Organisations must integrate core resilience competencies and leverage technology to achieve a unified view of events and enable a coordinated, effective response to disruptions focussed on the maintenance or recovery of critical business services.
- Organisations should prepare and test for major incidents - ensuring the people, technology and processes come together as intended to respond with speed and limit operational impacts.
- A successful Cyber ransomware attack presents responders with a more severe challenge than many incidents because it logically destroys an environment leaving the only route back as a complicated and slow recovery from a compromised backup. Lessons from Cyber Recovery have a key role to play in guiding secure recovery from accidental IT disruption.
- There is a need for enhanced collaboration between Third Party Risk Management (TPRM), IT, and service owners to better understand digitisation, product development, and the technology architecture that underpins critical business services.
- Technology solutions can support resilience efforts by streamlining processes, reducing manual errors, enhancing decision-making capabilities, and developing the adaptability needed for effective crisis response.

Operational resilience (continued)

What does this mean for Internal Audit?

Top topics for Internal Audit consideration include an evaluation of:

Technology resilience

- Management's evaluation and quantification of potential risks, considering factors such as threat severity, frequency, and impact on critical operations.
- The thoroughness of understanding and documentation regarding the impact of enabling services (such as IT) on critical services-including downtime duration, third-party provisions, recovery time, and the effectiveness of contingency plans.
- The effectiveness of change management processes and testing regimes.
- The effectiveness of incident management and cyber recovery processes.

Effective crisis response

- The effectiveness of response plans and testing, including crisis exercises to validate and enhance response frameworks.
- Joint exercises, war games and/or scenario tests with critical third parties to embed and rehearse a joined up response capability, and identify vulnerabilities which may impact critical service provision in the event of future outages.
- Management's understanding of the role of insurance to respond to major IT disruptions.

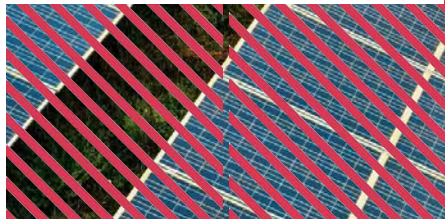
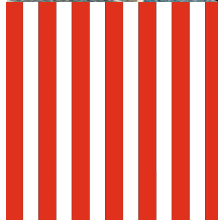
Digital supply chain vulnerabilities

- Supply chain mapping to show service delivery and third-party interactions. Understanding of contractual clauses relating to incidents.
- The effectiveness of risk assessment and due diligence processes over critical suppliers.
- Processes in place to stress-test contingency plans, ensuring robust response capabilities.



Sustainability

- Reporting and regulations
- Energy transition
- Resilience to climate risk



Reporting and regulations



What's on the risk agenda?

We continue to see major sustainability reporting legislative developments from across the globe, that will impact a huge number of businesses. Many regulatory bodies now require that companies disclose, and in some cases, assure, a range of Environmental, Social and Governance ('ESG') information.

The rapid development of potentially overlapping requirements, creates a number of challenges, such as:

1. Identifying and collating the data required;
2. Applying the necessary materiality judgements on what to disclose, and
3. Ensuring the accuracy of information reported.

The work required is far more than a stand-alone compliance exercise given that the failure to get disclosures right creates a risk of:

- a. Having to make costly and potentially reputationally damaging climb downs on publicly made sustainability pledges, and/or
- b. Be labelled as greenwashing
- c. Potential litigation and divestment from institutional investors.

In the UK, important developments coalesce from periods beginning on or after 1 January 2025. More information can be found on the [timeline for key UK and EU sustainability reporting regulations](#) and refer to our [ESG website](#) for further information.

Most of the standards highlighted on the next page were designed for the private sector, with the aim of providing markets with clear, comprehensive, high-quality climate-related information for financial decision-making.

However, the public sector similarly requires sustainability-related information for decision-making and accountability to annual report users. For example, HM Treasury (HMT) sets the requirements for central government annual reports and accounts in consultation with the Financial Reporting Advisory Board (FRAB). HMT have issued [Task Force on Climate-related Financial Disclosure \('TCFD'\) aligned disclosure application guidance](#) relevant to central government - which are being introduced in three phases, with full alignment expected by FY26. Updates to the 'Greening Government Commitments for 2026-2030' are also due soon and will set new targets for sustainability.

Compliance as a strategic differentiator

If the above analysis sounds a little 'doom and gloom' let's remember the many benefits of disclosing progress against a sound sustainability strategy. The reputational and operational benefits to be gained from getting this right include increased transparency with stakeholders, data-informed decision making and better environmental and social performance.

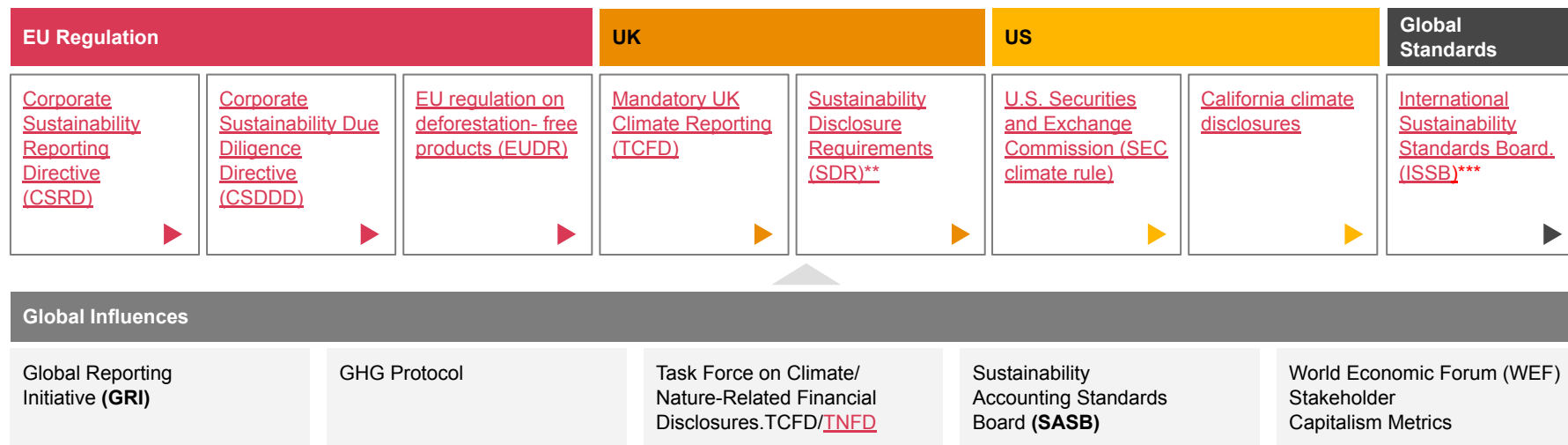


Reporting and regulations (continued)



What's on the risk agenda?

The next 24 months will be a critical transition phase in sustainability reporting. [Sustainability reporting regulations](#) are increasing and in key jurisdictions, mandatory assurance requirements on disclosures have been proposed. We illustrate below, some of the key elements of the evolving regulatory environment, providing links to further information in relation to each of the regulations, along with the voluntary framework, Task Force on Nature-Related Financial Disclosures (TNFD).



*The UK Corporate Governance Reform will require a declaration from the Board to sign off on internal controls for non-financial reporting (as well as financial reporting). More details around these new requirements are provided in the **Regulation section** of this document under [UK Corporate Governance Code](#).

** The Transition Plan Taskforce (TPT) is informing future transition plan requirements in the UK as part of the broader Sustainability Disclosure Requirements (SDR) framework

*** These are being turned into UK standards (UK SRS) which are expected to supersede Mandatory UK Climate Reporting in the same way ISSB has superseded TCFD globally (TCFD has formally been disbanded and its materials are now overseen by ISSB).

Reporting and regulations (continued)



What's changing?

The range and volume of ESG disclosures continues to grow and the public and investor appetite for data and transparency shows no signs of abating. Organisations are therefore getting to grips with which regulations are relevant to which parts of their business and how to develop the data, processes, governance and assurance mechanisms to report with confidence and due context. Key challenges include:



Data availability and use of technology

Organisations need dependable and holistic reporting systems, to manage granular data and deliver reliable reporting at the right level for disclosure or decision making. This might be at an entity, regional, product or portfolio level, within the business and across its value chain, integrating data from different business areas. In many cases, this data does not yet exist or is unreliable, poorly controlled and dependent on judgement. Where data is imperfect or subject to judgement this requires due scrutiny and possible explanation.



Volume, complexity and stages of regulation

The proposed reporting standards are complex with overlapping initiatives and different timelines.

The final versions of the reporting rules may well turn out to be very different to currently published proposals, making it difficult for companies to know how to approach preparations now.

While regulators are collaborating on ESG globally, there are different approaches being taken which brings operational and compliance challenges for organisations with an international footprint.

Organisations must establish processes for examining their activities through multiple reporting lenses to determine which activities they will need to report on at which level and the information they need to obtain to do so. They will also need to be prepared to explain any potential discrepancies or differences between various reports.



Alignment between ESG ambition and reporting strategy

Many organisations have already publicly committed to sustainability and wider ESG targets and ambitions in various ways. Stakeholders want clarity on the strategic plan to achieve these ambitions. Accusations of 'greenwashing' have the power to inflict serious reputational damage. Robust reporting disclosures can help to tell the 'sustainability' story in a credible and reliable way especially where information is assured.

Less than

60%

of organisations have involved their technology function in their sustainability reporting

PwC Global CSRD Survey 2024



and

78%

said many of their biggest challenges in implementing sustainability reporting related to data.

PwC Global 27th Annual CEO Survey



Reporting and regulations (continued)

What does this mean for Internal Audit?

Underlying methodologies or scientific knowledge supporting sustainability disclosures is still developing. To prevent unsupported decision-making, bias, or inaccurate reporting, those charged with governance must ensure that the data on which decisions are taken is full, comprehensive and reliable. To do so, it's critical to understand what sustainability and ESG means in the context of the organisation and its mission. To report accurately, the right processes and procedures must be in place, from the start of the relevant period.

In response, and against a backdrop of growing scepticism about 'greenwashing', Internal Auditors can provide a valuable, independent perspective and real-time challenge to executives around whether disclosures are proportionate, consistent and well articulated for all audiences – customers, employees, suppliers and investors. Internal Audit are well placed to help break down the silos that can exist in relation to sustainability reporting.

Below are just a few examples of how we see Internal Audit functions contributing to assurance over sustainability reporting:

- Readiness or programme governance reviews focussed on the ability of teams to meet reporting timelines and standards.
- Reviewing process for determining which regulations are applicable and need to be incorporated into reporting across complex groups.
- Assessing the alignment of ESG commitments with requirements and organisational strategy and the extent to which governance and operating models support successful delivery.
- Reviewing materiality assessment methodologies and risk assessments that underpin disclosures.
- Reviewing governance, processes and controls in relation to generating disclosures/reporting, including data gathering.
- Assessing data quality - completeness, timeliness, accuracy and key assumptions/ interpretations of rules.

More than

90% of

respondents believe that corporate sustainability reporting contains at least some level of unsupported claims.

PwC UK Investor
Survey 2023





Energy transition



What's on the risk agenda?

The UK has a legal target to achieve net zero by 2050. The target is a pledge to transform the UK economy and prioritise green growth. Billed as the biggest economic transformation since the industrial revolution, it is a challenge that calls for a concerted effort from society, businesses, academia, financial institutions and government.

Beyond these shores, there are wider issues. By 2050, the world's population will grow by two billion, and GDP is forecast to double. Emerging markets and developing economies need abundant and low-cost energy to enable growth and meet development goals.

Climate experts broadly agree that a just and effective energy transition must address reducing the intensity of energy demand, not just transform supply. In order to succeed with minimal disruption, the global transition needs to balance energy security, sustainability and affordability.

71%

of UK businesses expect high energy costs to reduce their ability to compete internationally.

63%

of respondents say that environmental commitments are limiting their ability to manage costs.

81%

of organisations plan to raise prices in the next two years in response to high energy costs.

PwC UK Energy Survey 2024



Energy transition (continued)



What's changing?

The low-carbon energy transition is reshaping the way that organisations power themselves – and the way they generate financial value. In a market where energy supply and demand are uncertain, organisations are struggling to juggle volatile energy costs with progress on decarbonisation. But, as organisations gear up for the next step in their energy transition and to meet their net zero targets, taking control of energy must now become a priority.



Advances in technology mean that companies can drive down their energy intensity by analysing and reducing existing energy use and securing affordable energy from low-carbon sources (i.e. electrifying operations and participating in energy markets). Taking action on energy demand in these ways has potential to unlock savings, boost revenues, and protect against risks and rising costs, while improving sustainability performance.



Increased decarbonisation commitments driven by reporting standards and regulation means UK organisations must solve an energy equation that incorporates not only direct energy costs, but also emissions throughout the value chain, including Scopes 1, 2, and 3.



Price volatility has hit UK organisations hard in the past two years and there may be more economic hardship to come. Many organisations have been protected from price fluctuations by fixed term energy tariffs and government support schemes, both of which will eventually expire. The economic impacts of high and volatile energy costs are significant. According to [PwC's UK Energy Survey 2024](#), technology and telecommunications businesses expect to be most affected, with 44% expecting energy costs to negatively impact profits, compared with 36% in consumer markets and 26% in industrial manufacturing and automotive.



Energy transition (continued)

What does this mean for Internal Audit?

Internal Audit teams are well placed to support their organisations navigate the complexities of the energy transition, achieve sustainability goals, and manage associated risks and opportunities effectively. Below are some possible channels via which Internal Audit can support Boards and add value.

Governance, commitments and strategy

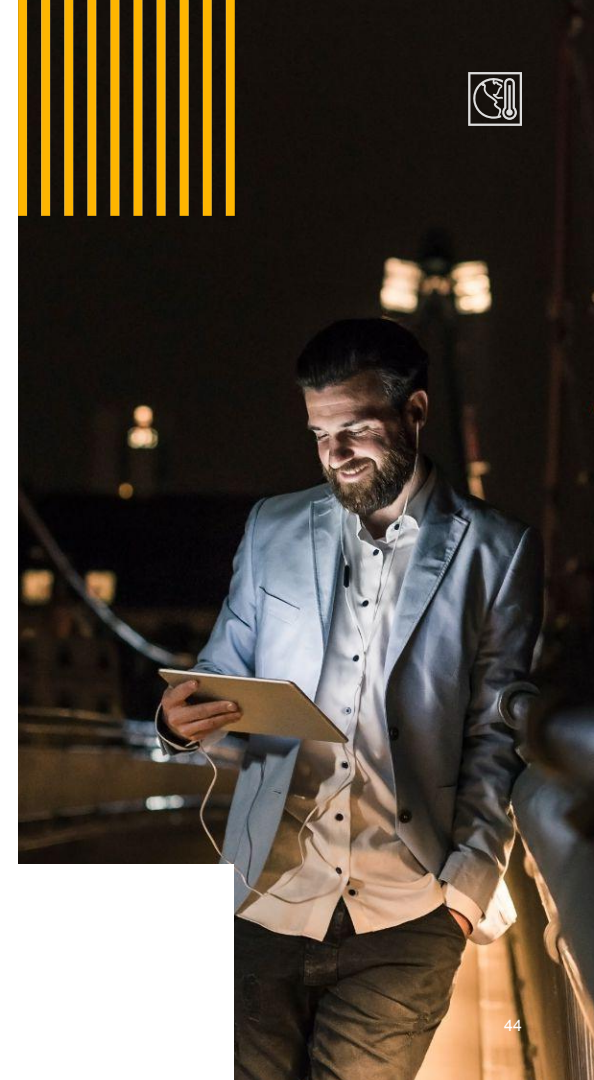
- Critically appraising the enterprise-wide approach to energy management and transition.
- Assessing the extent to which accountable roles and responsibilities for managing the process have been defined and are sufficiently well-resourced.
- Supporting Boards with the identification and assessment of current and emerging risks pertaining to energy management and transition.

Change programmes and business initiatives

- Providing assurance over the programmes and projects relating to energy transition - considering elements such as governance, management of stakeholders, risks and the integrity of benefits management.
- Assessing how energy management goals are embedded into day-to-day decision making.

Metrics, monitoring and reporting

- Supporting the development of energy/ emissions related KPIs
- Supporting with assurance over the processes and controls to ensure data accuracy.
- Assessing alignment with relevant regulations and preparedness for implementing incoming applicable transition plan requirements, for example the Transition Plan Taskforce (TPT) framework and forthcoming guidance. See section on [Reporting and regulations](#).



Resilience to climate risk



What's on the agenda?

The uncertainty around the impact of climate change on our future environment, coupled with new disclosure and policy requirements, means organisations must understand and prepare for the climate physical and transition risks they face.

Physical risks are both acute and chronic and relate to extreme weather events and changes in temperature. These risks can cause severe business disruption and limitations on resource availability.

Transition risks are large-scale and cover more disruptive change such as political, economic or technological transformation. These risks are often associated with changing strategies, policies or investments as society and industry shift to a low carbon economy.

The transition also brings a number of **opportunities**. These include the development of new products and services, as well as new markets for companies to operate in.

More and more businesses are responding to the challenges posed by climate change. In **PwC's 27th Annual Global CEO Survey**, 47% of respondents said their company had taken measures to safeguard its workforce and physical assets against climate risk-up from 17% the year before.

As sustainability and climate consequences emerge, organisations are looking for ways to mitigate climate risk and build more resilient operations. To thrive, they need to deliver in the near-term while building long-term sustainable business practices.



Resilience to climate risk (continued)

What's changing?



Business climate risk

Organisations that fail to properly plan for climate change leave themselves increasingly exposed to risk. Leaders should understand not only the way climate change will impact the environment in which they operate, but should also identify specific vulnerabilities within their sustainability goals.

That means running models and forecasts to determine the likelihood of various climate scenarios and the potential impact on their organisation and strategy.



Regulatory pressure

Investors and consumers alike are calling for companies to take sustained action to reduce emissions, curb climate change and address sustainability targets. This means that sustainability risk doesn't just come in the form of impact from climate change, but also as a reputational risk that, long-term, could close off opportunities, including access to funding.

Sustainability reporting standards and frameworks require in-scope organisations to track and report a clear view of their climate related sustainability practices and take action to work toward net zero.

Other organisations are also taking steps to voluntarily disclose details of climate risks and responses alongside explanations of their sustainability goals and practices. There is an expectation, driven by stakeholder demand, that organisational performance should incorporate much more than the traditional financial measures.

Refer to the sub section on [Reporting and regulations](#) for more specific information pertaining to these pressures.





Resilience to climate risk (continued)



What does this mean for Internal Audit?

To manage the physical and transition risks and impacts of climate change, organisations will need highly reliable data sources, systems, governance and controls. These resources will also help with meeting disclosure requirements and explaining to investors and other stakeholders the strategy and progress in delivering against it.

Here are some key questions for Internal Audit teams as they assess their role in relation to climate resilience.

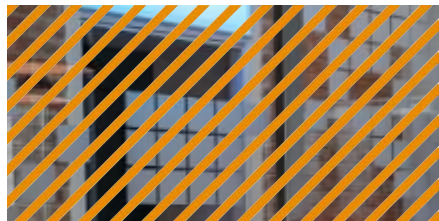
Is it clear how your organisation addresses the risk it poses to the environment and, conversely, how it aims to protect its people and operations from the risks the environment poses? Is this an integral part of strategy and decision making?

Is there a good understanding amongst leadership teams of climate related risks, their impact and likelihood and the mitigations and actions to maintain those risks within appetite?

How is relevant data being gathered in relation to programmes and initiatives aimed at enhancing resilience and delivering desired outcomes in relation to transition risks and opportunities?

How robust are the company's business continuity and disaster recovery plans in the face of climate-related disruptions?

What analytical and modelling capabilities are in place for measuring financial impacts arising from climate change to meet increasing expectations from regulators?



Regulation

- UK Corporate Governance Code
- Fraud and economic crime (ECCTA)
- International tax and transfer pricing



UK Corporate Governance Code



What's on the risk agenda?

In January 2024, revisions to the UK Corporate Governance Code were published. This revised code is effective for periods starting on or after 1 January 2025, with the exception of those revisions in relation to provision 29 (i.e. the declaration over effectiveness of internal controls), which are effective from periods starting on or after 1 January 2026.

The listing rules require all premium listed entities to report against the UK Corporate Governance Code (the Code). Large private companies might also be impacted if, under the Companies (Miscellaneous Reporting) Regulations 2018 they follow the Code.

Further information can be found in our publication below.

PwC UK Restoring trust through risk management and internal control



The Code sets a new bar for corporate governance and we expect its effects will be felt beyond those organisations who must comply as Boards will want greater transparency and assurance over risks and controls.

UK Corporate Governance Code (continued)



What's changing?

The primary focus for affected companies is the new requirement for Boards to make an declaration in the annual report on the effectiveness of all material controls as at the balance sheet date. We set out the key elements of this below:

01

The declaration has a wide-ranging scope covering all material controls, including

- i. financial,
- ii. operational,
- iii. compliance, and
- iv. non-financial reporting controls.

02

Boards must disclose the basis of their declaration - including a description of how the Board has monitored and reviewed the effectiveness of its risk management and internal control framework.

03

Boards will need to disclose 'material' control deficiencies including a description of any material controls that have not operated effectively as at the balance sheet date, the action taken, or proposed, to improve them and any action taken to address previously reported issues.

Many organisations will already have established systems of risk management and internal controls, often aligned to a well-recognised framework such as the Committee of Sponsoring Organisations (COSO). However, in our experience, many organisations have a more advanced internal control framework in relation to financial controls than operational and compliance controls and many are now grappling with how to determine what's material and needs renewed focus. Boards are encouraged not to underestimate the level of effort required to assess current controls and related assurance in order that they can confidently report against the new requirements.

Note: Other changes to the Code are summarised by the FRC in this [Key Changes](#) document.



UK Corporate Governance Code (continued)



What's changing? (continued)

The new Code requires Boards to develop clear processes to oversee, monitor and review the design and operating effectiveness of their systems of risk management and internal control to support the annual controls' declaration. We would expect readiness plans to incorporate the key elements below.

01 A clearly defined vision and strategy for risk, control and assurance will help ensure a common set of goals, prioritisation of resources and clear roadmap to enhance the organisational control environment. This should be reviewed and approved by the Board and aligned to the businesses objectives.

06 Disclosures should include a description of why the Board's processes are considered appropriate and give an explanation for any material failures. Many organisations are opting for a 'dummy run' of the process in advance of the disclosure deadline so they can be sure to be ready.

05 Boards should evaluate the sufficiency of the assurance processes supporting their annual review of the effectiveness of the system of risk management and internal control. Assurance maps are commonly used to support this assessment and we expect compliance and Internal Audit teams will be asked to do more.



02 Boards need to identify material risks pertaining to reporting, compliance and operations. A comprehensive risk management programme will ensure that the Board's process for assessing the effectiveness of these systems of risk management and related controls is focused around key risks and their materiality.

03 To ensure a strong yet proportionate assessment process, organisations need to identify the controls they consider most effective in addressing the risks – 'material controls'. We expect this will be a blend of controls, including entity level controls and IT controls.

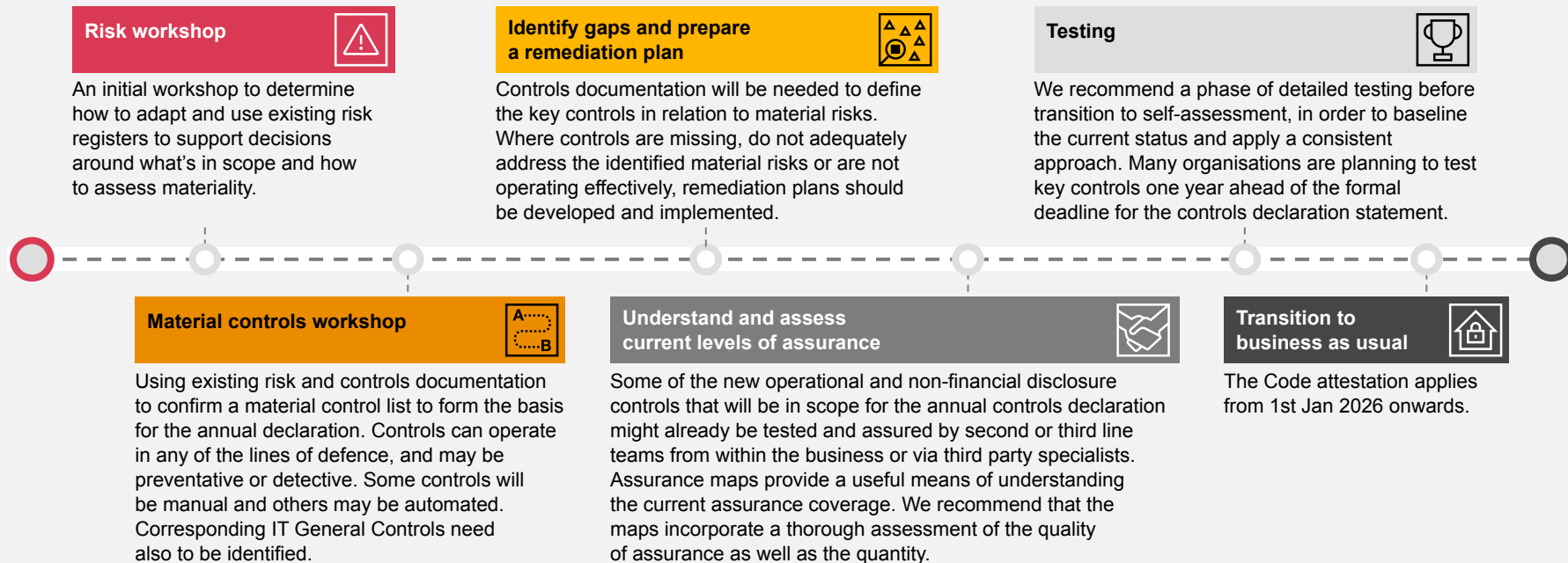
04 The design of material controls, once identified, should be reviewed to consider if they are clearly constructed and articulated in sufficient detail. We anticipate that most companies will implement some form of independent testing as part of considering control operating effectiveness.

UK Corporate Governance Code (continued)



What's changing? (continued)

For organisations who are new to the concept of a formal, broad-based controls and assurance framework, the path to readiness for the new Code will require a programme of work, supported by a cross-functional team and incorporates the following key stages:



UK Corporate Governance Code (continued)



What does this mean for Internal Audit?

Below is a menu of possible areas for Internal Audit to consider in relation to the new Corporate Governance Code, based on where the organisation is on the journey to implementing the code:



Readiness programmes

Many Internal Audit teams are engaged as a 'critical friend' to readiness programme steering committees to support the development and implementation of readiness plans. Areas to consider include:

- Governance: are there clear roles and responsibilities for delivery?
- Goals: is there a clear assessment of the 'as is' and 'to be' state to ensure that plans are based on a sound 'gap analysis'?
- Reporting: does relevant MI exist to track progress against key milestones and to allow for effective interventions as needed?
- Resources: does management understand the skills and levels of resource needed to implement their plans across the organisation?



Risk management

Risk and materiality should be at the heart of all Corporate Governance readiness plans. Internal auditors have the skills and experience to support management in their assessment of which risks, disclosures and financial statement line items should be in scope and to determine the key controls in the related processes. An early critique of the approach, the assumptions made, key judgments and the quality of underlying risk registers can be valuable in focussing efforts and building confidence.



Assurance mapping

Assurance maps are a means of assessing the adequacy and effectiveness of the governance, risk and controls framework in readiness for the controls' declaration.

By identifying and assessing the quality of current levels of assurance against disclosures and risks, management can develop and refine test plans to ensure optimal use of existing resources. Further guidance on assurance maps can be found [here](#).



Internal control evaluation

Internal Audit teams frequently form part of the testing regime to support the annual controls' attestation. Activities include:

- Designing and running controls self-assessment programmes, including 'testing' as may be needed to ensure the integrity of reported outcomes;
- Independent review and evaluation of the design and effectiveness of internal controls over operations, financial reporting, compliance and disclosures.
- Ensuring consistency of the approach to assurance when its delivered across multiple lines of defence.

Fraud and economic crime

What's on the risk agenda?

Slow economic growth across the globe, increased costs and shifts in technology such as AI and deep fakes are resulting in an environment where the risks of fraud are significant and rising. Against this backdrop, many national governments are tightening regulations to ensure that more is done to protect shareholders and consumers.

Data from our [Global Economic Crime Survey 2024](#) highlights that effective fraud prevention and detection programmes must consider the supply chain and customer fraud risk if it is to be effective, because:

55%

of respondents reported that procurement fraud is a widespread concern in their country, yet only a minority are using available tools to identify or combat it. Furthermore, 42% of these organisations either don't have a third-party risk management programme or don't do any form of risk scoring as part of their programme.

33%

of respondents reported that assessing the risk of forced labour in their supply chain is a priority for their company.

59%

of survey respondents agree that export controls have grown more complex and more than half believe controls are being enforced more robustly than two years ago.



81% - 92%

More than eight in ten (81%) executives believe government efforts to enforce anti-corruption laws are becoming more robust or remaining steady in the countries in which they operate – that number reaches 92% for companies headquartered in North America.



Fraud and economic crime (continued)



What's changing?

Greater governmental focus on fraud and bribery around the world

Governments around the world are signalling their rising expectations that corporate compliance programmes become more sophisticated: raising the bar for third-party risk management as well as the use of data analytics in support of compliance and investigation efforts.

New or recently revised protections or incentives for whistleblowers in numerous jurisdictions (i.e. the 2023 EU Whistleblowing Directive) increase the pressure on companies to learn of and react to allegations of misconduct quickly, whether that conduct is within the company or at a third-party. The US Department of Justice has made it clear in their guidelines for prosecutors that the monitoring of high risk transactions should be looked on favourably – this should hearten organisations that investment in prevention, detection and reporting processes and training should provide them with protection in the event of an incident or investigation.

The UK Economic Crime and Corporate Transparency Act (ECCTA)

In the UK, the new ECCTA includes the introduction of a new 'failure to prevent fraud' offence. Under this new offence, an organisation will be liable where a specified fraud offence is committed that either directly or indirectly benefits the organisation, subject to a defence of having reasonable fraud prevention procedures in place.

The new offence encompasses a number of fraud and false accounting offences. The legislation does not include a limitation regarding the materiality (i.e. value or nature) of the fraud and all companies meeting the 'large company' definition set out in the Companies Act, will need to comply.

The offence is designed to enhance corporate accountability and drive a cultural shift towards better fraud prevention. The Act will come into effect once the UK government has issued formal guidance, which has already been drafted.

Fraud and economic crime (continued)



The Government has indicated that the guidance on reasonable procedures will be principles based, similar to previous 'failure to prevent' legislation (i.e. Bribery Act / Corporate Criminal Offence); and consist of the following six guiding principles which help organisations in the design of procedures in readiness for the Act coming into force:

01

Top level commitment

- **Senior Management** demonstrably responsible for fraud (e.g. through documented role descriptions).
- **Governance forum** responsible for fraud oversight (defined in terms of reference).
- **Roles and responsibilities** for fraud defined across 3 line of defence's (LoDs).
- **Management information** reported to Senior Management enables effective oversight.
- **Code of conduct and other policies** in place clearly articulate staff responsibilities.

02

Risk assessment

- **Defined risk assessment methodology** that enables objective and consistent risk evaluation.
- Procedures in place to regularly review and refresh the risk assessment.
- **Risk assessment considers inherent risk and mitigating controls** to enable gaps to be identified.
- Assessment considers fraud broadly, as well as addressing offences specified in the legislation.

03

Proportionate procedures

- **Controls implemented in proportion to risk** identified in the risk assessment.
- **Gaps in control identified** and processes established to address them or consciously to 'risk accept'.
- Procedures in place to **test design and operating effectiveness of controls**.
- **Escalation and fraud response plans in place**, including steps to learn lessons from identified fraud issues.
- Use of technology in transaction monitoring.
- Prescribed response to fraud incidents.

Fraud and economic crime (continued)



04

Communication and training

- **Training** on fraud implemented across the organisation, tailored to individuals' roles and their exposure to fraud risk scenarios.
- Training should cover all individuals that could be deemed as 'associated persons' (i.e. all employees, contractors, agents, etc).
- **Whistleblowing process in place and communicated** effectively to staff. Monitoring in place to understand effectiveness and use of whistleblowing process.

05

Due diligence

- Processes in place to vet prospective employees, suppliers, contractors and other 3rd parties.
- **Monitoring in place** to identify, escalate and take action in relation to suspected wrongdoing in place.
- **Access to investigations capability** to understand and respond effectively to potential wrongdoing.

06

Monitoring and review

- Processes in place to **regularly review the design of the overall fraud risk management** framework and whether it is operating effectively.
- **Review of controls** (e.g. by Internal Audit or external providers) on periodic basis.
- Regular reporting to governance forums on fraud related Key Risk Indicators (KRIs) and on the effectiveness of controls.

Fraud and economic crime (continued)



What does this mean for Internal Audit?

Internal Auditors have the skills, perspective and experience to help their organisations with some key questions as they review the current state of existing fraud risk management programmes:

- Are material fraud risks understood across all key territories?
- What controls/systems are in place to address these risks and are they consistent?
- Are they operating effectively?
- Are there any gaps in the controls?
- What additional preventative/detective measures does the organisation need to put in place?

Senior Management and Board members should also have an active role in addressing the organisational plans for mitigating these risks, particularly in light of internal or external developments.

Internal Audit can help with the following:

- **Evaluating counter-fraud policies and procedures** to confirm these align to the 'reasonable procedures' which underpin the requirements of the Act.
- **Identifying strategies for collaboration** with legal and compliance, including regarding risk assessments, compliance monitoring and onsite audits.
- **Assessing the effectiveness of training** programmes designed to raise staff awareness of fraud risks and their roles.
- **Implementing data analytics and automation** to enhance controls.



International tax and transfer pricing



What's on the risk agenda?

International taxation continues to undergo significant change. As part of the Organisation for Economic Cooperation and Development (OECD's) efforts to counter tax avoidance by the largest multinational groups and fuelled by economic pressure on governments to maintain or increase tax revenues, new public country by country reporting (**CbCR**) and **global minimum effective tax rate (ETR) regimes** are now starting to come into force in many countries, including the UK.

The new regimes aim to increase transparency over taxpayers' affairs for tax administrations and to ensure a fairer allocation of profits and taxes between jurisdictions, including developing economies. These rapid changes are creating complexity and uncertainty for businesses, placing increased pressure on resources, and pose potential reputational risks for effected enterprises.

Transfer pricing continues to be a key tax risk for groups of all sizes, given the focus placed on it by tax authorities and external auditors. Many countries, including the UK, have also introduced new and more onerous transfer pricing compliance requirements in recent years, which has arguably increased the administrative burden and the risk of disputes and adjustments for taxpayers.



Transfer pricing is the term used to describe the complex set of tax rules governing the allocation of profits and losses between jurisdictions, ensuring that each entity in a multinational group earns a result commensurate with its value contribution relative to the other entities in the group. This is achieved by requiring related entities to transact with each other on arm's length terms, i.e. on the same basis that they would transact with unrelated parties.

As transfer pricing can have such a material impact on taxable profits, most countries now formally require businesses to prepare and maintain detailed and extensive annual documentation justifying their transfer pricing positions and evidencing strong controls over transfer pricing. In the event of an adjustment, penalties can be very significant, especially where supporting documentation is deemed inadequate.

International tax and transfer pricing (continued)



What's changing?

Transfer pricing In the UK, the Transfer Pricing Records Regulations 2023 introduced a new requirement for large multinational businesses to prepare and maintain transfer pricing documentation in a set manner - the OECD master and local file format - an approach already enacted by many other countries.

This new UK transfer pricing documentation requirement is effective for accounting periods beginning on or after 1 April 2023 for groups with consolidated global revenues above €750M. Groups below this threshold are strongly encouraged by His Majesty's Revenue and Customs (HMRC) to prepare documentation in the same format in order to demonstrate adherence to the arm's length principle at the time of tax return filing.

Penalties of up to 100% of additional tax assessed may apply where supporting documentation is deemed inadequate.

Country by country reporting ("CbCR"), which was first introduced in 2016, is now becoming public, meaning that annual data on the operations, revenues, profits, taxes and headcount of large multinationals by country will increasingly be accessible to the press and the public.

Under an OECD Inclusive Framework, more than 140 countries have now agreed to enact a two-pillar solution to address the challenges arising from the digitalisation of the economy, although implementation timetables differ between countries, increasing complexity for taxpayers. **Pillar Two** is a once in a generation tax event for organisations, which introduces a global minimum ETR of 15% for the largest multinational groups.

Only groups with qualifying, that is, high quality and accurate CbCR reports prepared on a set basis, will be able to access the Pillar Two transitional safe harbour provisions, which in effect permit the use of that qualifying CbCR data to calculate and report Pillar Two tax liabilities, simplifying the compliance and reporting process significantly.

Groups with non-qualifying CbCR data will have to undertake substantially more work to satisfy the new multi-jurisdictional compliance requirements, which could be both time-consuming and costly.

We expect Pillar Two to be a significant focus area for statutory auditors as well as for tax authorities. See the following page for further details.

International tax and transfer pricing - Pillar Two (continued)



Pillar Two establishes a global minimum tax regime which will apply to both public and privately held multinational groups with consolidated revenue over €750m. Global agreement has been reached to bring these rules into law and the OECD has released model rules, commentary and administrative guidance.

EU member states unanimously adopted a directive which required them to introduce the rules by 31 December 2023. Many other countries are also working on their domestic rules to implement Pillar Two.

UK legislation has been enacted which introduces the OECD's Pillar Two model Income Inclusion Rule into UK law, as well as a domestic top-up tax. These rules first apply to accounting periods commencing on or after 31 December 2023. In addition, the UK is expected to introduce an Undertaxed Profits Rule with effect from 2025.

Whilst the UK has addressed some of the issues and complexities raised in respect of the OECD model rules, a number still remain.

What is Pillar Two?

15%

Global minimum tax in each jurisdiction to curb tax avoidance and create a more equitable playing field.

135+

Countries with different localisation interpretation and implementation of the Pillar Two rules template.

€750m

In consolidated annual group revenue means a multinational is subject to Pillar Two.

Jan'24

Effective date for many aspects of Pillar Two.

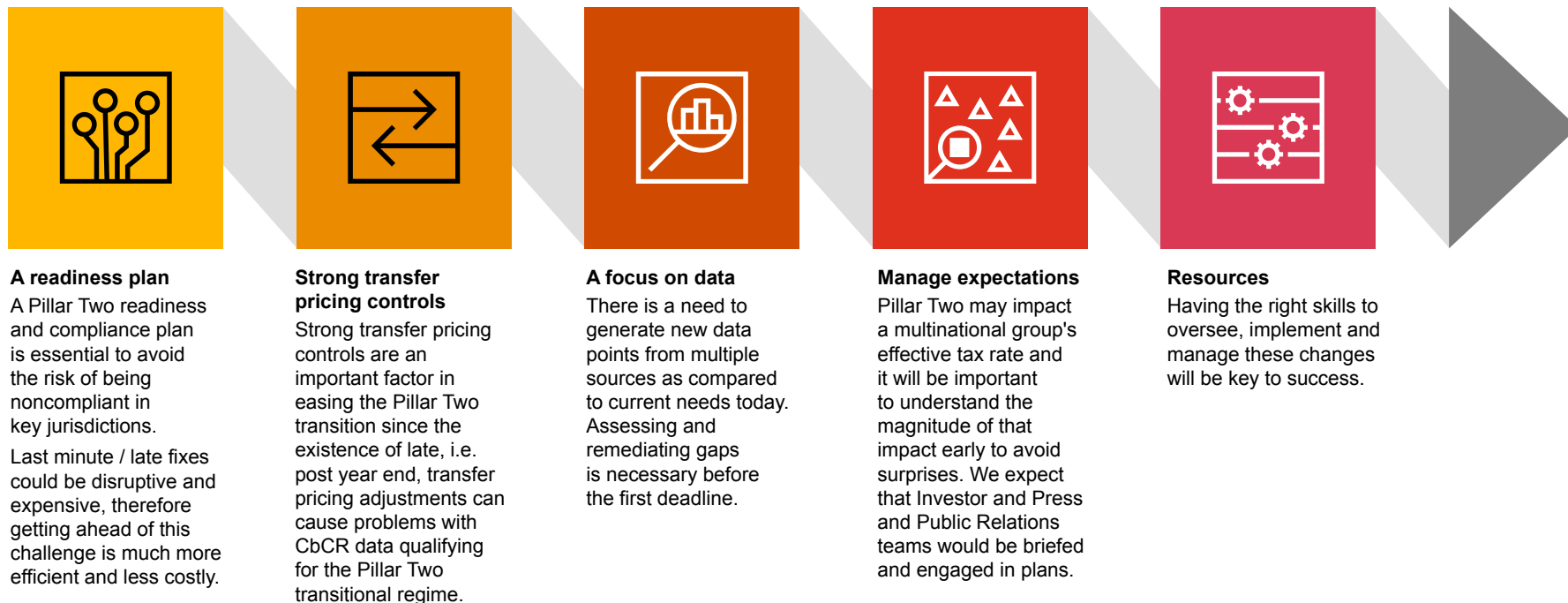
260

Data points needed from multiple tax/non-tax stakeholders, some of which may not already be captured in your systems.

International tax and transfer pricing - Pillar Two (continued)



Sound planning, as detailed below, will be key to ensuring organisational readiness for the changes brought about by Pillar Two



International tax and transfer pricing (continued)



What does this mean for Internal Audit?

Internal Auditors can play a critical role in providing assurance on the tax risks and controls of businesses, especially in light of the fast-changing international tax landscape. The new public CbCR and Pillar Two regimes will have different implementation dates and deadlines in different countries, and the existing transfer pricing rules continue to evolve.



Key questions to ask include:



Capabilities to comply: What are the capabilities and resources of the tax function to maintain data, processes and controls, to keep abreast of developments, track compliance and to communicate effectively with internal stakeholders and tax authorities?



Controls: What controls are currently in place over these processes, and how might they be improved to make the process more efficient and reliable?



Enterprise-wide engagement:

- Are the finance and tax functions communicating effectively to obtain the right data in the right format, on a timely and accurate basis to ensure accurate reporting?
- Is the Board abreast of the developments, the potential consequences and any additional investment required?



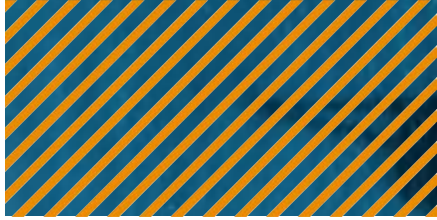
Assurance:

- How is the Board assured of the adequacy or otherwise of the internal controls and procedures required to comply with new tax and transfer pricing rules?
- Are processes in place to ensure that important tax positions such as Pillar Two and transfer pricing are external audit ready, including appropriate technical support for any Uncertain Tax Positions (UTPs)?



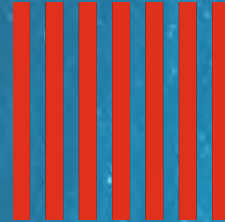
Risk and uncertainty:

- Is there awareness of what potential tax liabilities could arise if the tax risks are not identified and addressed in a timely fashion, such as penalties, interest, double taxation, reputational damage, or litigation?
- Have the implications of a shift to public CbCR reporting been considered from a stakeholder and PR perspective?



Supply chain management

- Third party risk management
- Supply chain and procurement risk



Third party risk management



What's on the risk agenda?

Many service-oriented organisations are increasingly reliant on third party service providers to deliver core IT capability and related services as they embrace digitisation and scale their operations whilst reducing costs. The inherent complexity of the digital supply chain poses significant resilience challenges. In response, many organisations are adopting a 'resilience by design' approach: building a comprehensive understanding of third-party dependencies and managing them proactively.

Key risks relate to:



How third parties handle and protect the personal data of staff and customers.



Understanding and addressing the risks to the continuity of critical operations that depend on third-party services or infrastructure.



For some arrangements, high levels of integration and an absence of substitutes which exacerbates the dependency risks and requires strong contingency and exit planning.



Third party risk management (continued)



What's changing?

Key considerations for organisations include:



Methods for identifying, measuring and managing third party concentration risk – concentration risk takes several forms, varying from organisation's being over-reliant on one third party service provider to being reliant on a number of third parties within one jurisdiction, thus heightening geopolitical or natural disaster risk exposure.

Supply chain visibility and accurate data related to service consumption are key to identifying and managing concentration risk, including generating meaningful metrics that drive risk-based decision making.



The use of AI by third party service providers – as part of upfront risk identification, and on an ongoing basis, organisations should be aware of how their data is being used in AI models and what risks are posed as a result. For example, risks related to the ethical use of AI are prevalent and organisations need to work closely with providers to identify, measure and mitigate bias in AI-based data models.



Use of cloud providers – clear-cut “shared responsibility” models must be fully defined and understood by both the firm and the cloud provider. Importantly, shared responsibility models do not remove Board level responsibilities to oversee third party risk in line with risk appetite.



Consider operational resilience and third party risk management holistically – information gained as part of third party risk assessment and due diligence should be used to feed risk-based development and testing of business continuity plans and disaster recovery measures. Similarly, third party controls should be updated based on test results to increase resilience as part of continuous improvement.



Supply chain visibility – as digital supply chains increase in complexity, organisations are increasingly seeking visibility into 4th, 5th and nth parties and oversight of the data that is being shared with subcontractors. Tracing the full supply chain allows a full understanding of concentration risk and supports continuity planning. Shared data is also crucial for building confidence in ESG disclosures, covering areas such as emissions, resource usage, and corruption and bribery.

Third party risk management (continued)

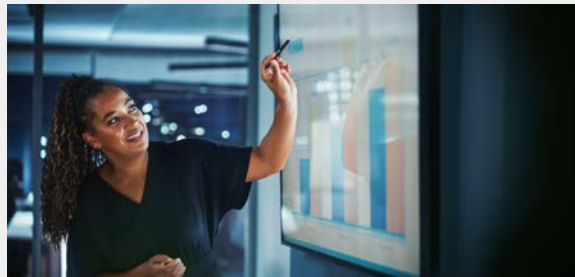


What does this mean for Internal Audit?

Internal Auditors can help their organisations by focusing on the following questions:

Does your organisation have a third party risk management framework that is well designed and operating effectively? This should cover:

- Policies and procedures
- Due diligence processes for onboarding
- Ongoing monitoring, including the maintenance of accurate registers of information and inventories managed by third parties.
- Consideration of intragroup arrangements which also carry risk, especially when they cut across different jurisdictions.



Do your contractual agreements with third parties support your efforts to identify, assess and manage key risks? For example:

- Are contracts subject to robust governance, including due consultation with a range of risk-owners, both prior to being signed and on an ongoing basis to ensure they remain reflective of the arrangements in practice.
- Do contracts contain appropriate contractual clauses that address regulatory requirements, data protection, service level agreements ('SLAs'), and exit strategies?
- Are there provisions for regular audits and assessments of material third party service providers?
- Do your assurance teams have the appropriate skills and technical capability to perform audits and assurance activities on third party service providers, especially those with high degrees of technical complexity performing new and advanced technologies.

Are there specific resilience and incident management measures in place in relation to critical third parties, including intra-group arrangements? These should cover:

- Processes for reporting, investigating, and mitigating incidents involving material third party service providers.
- Mechanisms to learn lessons from third party related incidents and near-misses, which are used to strengthening their approach to risk assessment, due diligence and monitoring.
- Clear integration of organisational recovery plans with those of critical third parties - so that dependencies and key recovery time metrics are consistently understood and tested.
- Exit plans are subject to realistic, scenario-based testing on a regular basis.



Supply chain and procurement risk



What's on the risk agenda?

Numerous disruptive events have impacted supply chains and logistics in recent years, including Covid-19, regional conflicts, fuel and labour shortages, accidents, disasters and climate related incidents.

These events have collectively elevated the importance of supply chain, logistics, and inventory management on the Boardroom agenda, notably in the following areas.

Resilience

In the face of continued uncertainty, organisations are focussed on resilience and continuity of supply to ensure they can continue to meet customer demand. As the need for resilience is balanced against efficiency and cost pressures, different strategies are emerging depending on the specifics of organisational risks and priorities.

Inventory management

Whilst many organisations are now holding stock at levels above pre-pandemic norms and are sourcing it sooner to address concerns around lead times, this trend is possibly easing.

Transport costs and logistics challenges

Hikes in transport costs in recent years, fuelled by conflict, labour shortages and disruptions to key shipping routes have left Boards feeling exposed. And whilst there are some signs that the worst of the challenges may be over, [The Economist Impact report - Trade in Transition 2024](#) found that “*businesses see higher transport costs as the most significant limitation on exports, with 24% of the leaders .. surveyed selecting this as one of their top two concerns.*” Furthermore, “last mile delivery, constituting a substantial portion of shipping and overall supply-chain expenses (53% and 41%, respectively), is becoming even more critical with the uptick in online sales.”

Tariffs

Increased protectionism through tariffs and trade barriers has also influenced trade patterns. According to the Economist Impact report: “Roughly a fifth of businesses are concerned with higher tariffs or uncertainties around tariffs in key markets they export to or import from”.

Regulatory demands for greater traceability and transparency

International trade regulations, Environmental, Social, and Governance (ESG) standards, product safety and quality requirements, data privacy and security regulations and anti-corruption and bribery laws all have significant impacts on today's approaches to supply chain management. Many of the new regulations require better data, greater collaboration between suppliers and customers and a deeper understanding of the full supply chain throughout its many tiers.

Technology

Recent years have seen a considerable increase in the adoption of new technologies designed to improve inventory management, support improved demand forecasting, enhance supply-chain efficiency and visibility and support compliance with regulatory reporting requirements.

Supply chain and procurement risk (continued)



What's changing?

Organisational responses to the complex and inter-related global supply chain risk landscape continue to evolve and develop. We set out some key themes that characterise today's adaptive supply chain strategies:

A customised supply chain strategy is crucial for balancing resilience and cost effectiveness

- Many organisations are responding to geopolitical risks by bringing supply chains closer to home or shifting to more 'politically-aligned' territories ("friendshoring") to reduce their reliance on nations that are perceived to be unstable or might pose a political or military threat.
- Similarly, diversification or establishing dual supply chains has become a common means of addressing vulnerabilities from over-reliance on specific countries or suppliers and provides an effective means for organisations to service different markets with distinct regulatory landscapes. The benefits of this approach need to be set against the costs of juggling multiple supply chains
- On the other hand, in selected markets, many organisations are enhancing supplier relationships with fewer, more strategic suppliers to enhance resilience through risk-sharing and a deeper collaboration (for example, around research and innovation) and many are generating productivity improvements as a result.
- Finally, we continue to see supply chain integration through acquisition as organisations seek to head off potential risks.

Organisations continue to evolve and shift their stock-holding patterns.

- The pre-covid focus on 'just-in-time' deliveries to reduce costs and improve efficiency was rapidly replaced by many organisations with a strategy designed to reduce uncertainty and build resilience by ensuring there were enough materials and products on hand during periods of intense demand.
- According to the '[Economist Impact - Trade in transition 2024](#)' report: "In 2023, companies maintained 9.0 weeks of inventories, compared to 10.1 in 2022 and 8.9 in 2021. This signals a slight recalibration in 2023, likely due to the capital intensity behind higher inventories."

Transport and logistics management remains under the spotlight

Cost management remains a key focus but so too is the need to achieve a faster time to market to meet rising consumer expectations for prompt order fulfilment. Shorter lead-times are compatible with the goal of reducing high inventory levels that tie up working capital, especially in sectors such as retail that often see significant short-term shifts in consumer preferences.

Supply chain and procurement risk (continued)



What's changing? (continued)

Tariffs

- Many organisations have diverted supply chains to lower tariff nations to save costs whilst also addressing concerns around national security and human rights.
- Uncertainty around the costs of potential barriers to trade resulting from tariffs or similar measures create hesitancy amongst organisations considering investing in expansion into new markets
- Technological solutions are increasingly being sought to help organisations navigate the administrative challenges associated with geopolitical tensions which have led to an increasing web of sanctions, tariffs and reporting requirements.

Regulations

- Together, new regulations create a significant administrative burden and increase the reputational risks faced by global businesses through an emphasis on responsible business practices and transparency. Regulatory requirements continue to shape supply chain management practices and, in particular, serve to accelerate the adoption of tech solutions to support compliance and manage the costs of doing so.
- In the UK, **the forthcoming Public Sector Procurement Act 2023** (the implementation of which is now delayed until 24th February 2025) will demand changes to all UK public sector contracting authorities' process, policy, governance, systems, data, and much more. Of note, the Act will provide for greater transparency, including the publication of at least 3 KPIs for contracts over £5m in value. Private sector companies who supply the public sector will also be impacted – with the changes delivering risks (i.e. publication of more information) and opportunities (i.e. receipt of more information to shape BD activity).

Technology

- Digital supply chain management solutions have emerged to provide real-time information and enhanced data.
- GenAI has become a key tool for many in the management of increasingly complex supply-chain operations and is being used to help with demand planning, managing and modelling logistics costs and with inventory management.
- Blockchain technology, which allows secure and access controlled data exchanges, provides many benefits that align with the emerging demands of transparency and accuracy in supply chain management. It is a powerful tool to support product traceability through the end-to-end supply chain to meet regulatory requirements. Uses also include the detection and prevention of fraud and errors, reduced paperwork delays and seamless order fulfilment.
- Finally, 3D printing has emerged as a means for organisations to enhance their design capabilities through virtual modelling: improving production flexibility and responsiveness to market changes.

Supply chain and procurement risk (continued)



What does this mean for Internal Audit?

The key questions for internal auditors detailed on page 67, in relation to third party risk management are also relevant to providing assurance over physical supply chain risks. In addition, the following internal audit topic areas are relevant.

Governance over decision making

- **Supporting and challenging the data and assumptions** that underpin scenario and risk analyses to ensure they form a reliable basis for strategic decision-making. This may take a new dimension where AI or other tools are newly deployed to automate supply chain monitoring activities.
- **Assessing the controls and monitoring tools to support decision-making** - for example, the design and application of delegated authority levels, or the use of KRIs, KPIs and SLAs to understand and monitor supply chain risk.

Contract management

- **Contract life-cycle management:** Assessing the design and operational effectiveness of controls over supplier selection, onboarding, monitoring, relationship management and exit
- **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.

Business controls assurance

Amongst the complexity and change, it's imperative that 'business as usual' supply chain and customer fulfilment controls remain well designed and consistently operated. Internal audits topics might include: demand planning, sales and operational planning, materials and inventory management, transport and logistics management, tariffs, sanctions compliance, ordering process.

New technologies

Please refer to the sections digital transformation, the use of AI and data privacy for further information on the risks and the potential role of Internal Auditors where technologies play a big role in inventory and supply chain management.



People and organisational culture



People and organisational culture

What's on the risk agenda?

Culture is increasingly being recognised by CEOs as a powerful strategic differentiator. Successfully aligning culture and ways of working to strategic goals can bring a competitive edge through increased engagement, productivity and staff retention. Conversely, getting culture 'wrong' can have significant regulatory, financial and reputational impacts.

Regulators remain focused on culture – particularly on leadership messages and behaviours which are critical to underpin compliance and ensure that organisations focus on what's right for customers, workers and wider stakeholders. There is also increased focus on risk culture, accountability and leadership.

Heads of Internal Audit are uniquely positioned to offer an independent and robust assessment of 'people risks'. Successful assurance requires confidence, a focussed approach and a willingness of senior leaders to accept challenge and take action.



A sound workforce strategy is one that connects transformation ambitions with exceptional workforce planning, and provides workers with the reassurance they'll be equipped with the skills and tools they need to thrive."

PwC UK Workforce Hopes and Fears Survey 2024



People and organisational culture (continued)



What's changing?

We know from our latest **UK Workforce Hopes and Fears Survey 2024** that the adoption of new technology, the pace of business transformation, the focus on new skills and the imperative for workplaces to be inclusive: fostering equality and embracing diversity – are all changing the profile of 'people' risks from the perspective of employees as well as CEOs.

PwC UK Workforce Hopes and Fears Survey 2024



Technology (including GenAI) could boost productivity but adoption is sluggish

GenAI has brought unprecedented change to the world of work. To avoid being left behind, organisations should understand the impacts of GenAI on the workforce - assessing risks and opportunities, particularly in relation to future skills needs.

While GenAI remains high on the agenda, workforce adoption of it has been sluggish. The survey shows that only 36% of employees globally report that they regularly use Gen AI tools for work, and 37% report that they have never used it.

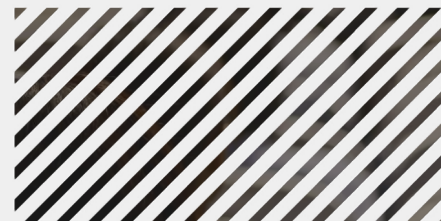
Leading organisations drive adoption and realise the benefits by fostering a culture where employees feel safe to experiment and do things differently. Leadership communication is critical in bringing to life the benefits and transformative potential of technology, whilst acknowledging addressing the fear and uncertainty that's reported.

Upskilling is a top priority for employees

The UK Workforce Hopes and Fears Survey 2024 shows that 8% of business leaders report some extent of skills shortage within their organisation – 68% in relation to technology.

Meanwhile, upskilling has become so valuable to employees that, of the people who say they want to switch employers, 67% indicate this is driven by the opportunity to learn new skills.

These statistics point to a clear strategic advantage for organisations that invest in the employee experience and create opportunities for employees to develop skills.



People and organisational culture (continued)



What's changing? (continued)

Business transformation and change continues but a gap widens on employees understanding the “why”

Organisations face a range of pressures brought on by the need to balance transformation and value creation with compliance and changing regulations, a fast-moving and unpredictable risk landscape, and growing competition. The survey shows that employees are feeling the impact of these changes, with two-thirds reporting that they have experienced more change at work than in the previous 12 months. However, 40% do not understand why change needs to happen. Leading organisations create trust and engagement and protect against change fatigue and burnout through:

- Fostering a culture that is agile and adaptable to change.
- Openly engaging employees in discussions around uncertainty in the political and/or economic environment and its impacts.
- Offering training and support to enhance workforce wellbeing and resilience.

Further focus placed on opportunity, fairness and safety

With geopolitical and economic disruption, the world of work is becoming increasingly polarised. Fostering a culture of inclusion, where diversity is celebrated and strong psychological safety is ensured, has never been more important. Data also indicates that organisations that invest in diversity attract top talent, foster greater innovation, and have improved financial performance.

The [new draft Workforce Information\(Ethnicity\) Bill](#) encourages organisations to expand the legal requirement of equal pay for equal work for men and women to both ethnic minority and disabled people.

Against this backdrop, many organisations are making voluntary disclosures beyond the current legal requirements and increasing transparency around pay and diversity which require sound data and thoughtful narrative.

Work from home or return to the office - the debate continues

As we finalise the drafting of this year's publication, there is an active public debate about which is the most effective means of optimising productivity and enhancing mental health and wellbeing: working from home, returning to offices or hybrid working. Proponents of co-working cite collaboration, learning and development and building of networks as key advantages whilst advocates of work from home practices argue that productivity and engagement are borne from trust and flexibility. Organisations seeking the 'best of both' may experience challenges in creating a sense of 'team' and 'fairness' and find that conflicts can be damaging to culture. Preferred and expected working practices look set to stay as differentiators in recruitment, retention, development and promotion decisions for both individuals and employers.

People and organisational culture (continued)



What this means for Internal Auditors?

In the light of cultural and people changes outlined in the previous pages, the Internal Audit should focus on the following key areas:

01

Cultural alignment and behaviours

Conduct culture audits to validate the extent to which behaviours align with those needed to further strategic objectives. Evaluate ethical frameworks, training programmes, and performance management systems to promote and reward desired behaviours. Regular updates on 'cultural health' and recommendations for improvement can help with alignment.

02

Leadership and communication

Assess leaders' effectiveness in setting the cultural tone and the impact of their communications, both verbally and written. Review leadership development programmes to ensure they reinforce the desired culture and strategic goals. Review the effectiveness of communication channels to ensure clarity, consistency and if employees feel encouraged to speak up and give feedback. Focus on the important and often underrated 'tone from the middle' and not just the 'tone from the top' in order to help shape faster change where it's needed.

03

Risk strategy and governance

Review the organisation's risk strategy, vision, and appetite statements for clarity and communication. Assess governance frameworks and controls to support desired risk behaviours and decision-making processes. Key strategic initiatives to secure benefits and manage risks are more likely to succeed where they are aligned with and supported by cultural expectations.

People and organisational culture (continued)

What this means for Internal Auditors? (continued)

04

Accountability and reinforcement

Evaluate guidelines on salary banding, rewards, and promotions for fairness and alignment with organisational values. Review to ensure that roles and responsibilities are clearly defined and documented, driving accountability at all levels, with linkage back to role profiles, job descriptions and performance objectives. Review informal recognition schemes and consequence management processes to ensure compliance and adherence to the values that your organisation promotes.

05

Diversity, Equity and Inclusion ('DE&I'), and people practices

Assess the organisation's DE&I and workforce strategies for actionable steps and alignment with strategic goals, and evaluate workforce practices such as career development, training, and talent management to create a fair, safe and inclusive environment.





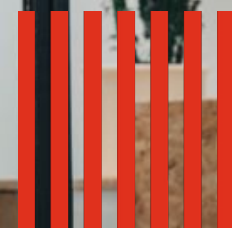
03

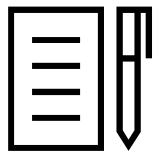


Professional practices update

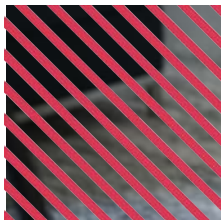
The IIA's Global Internal Audit Standards™

The Internal Audit Code of Practice





The IIA's Global Internal Audit Standards™





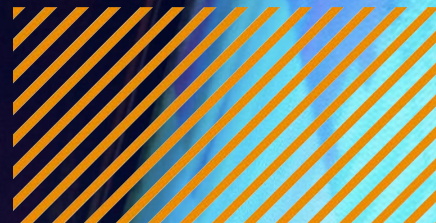
The IIA's Global Internal Audit Standards™



The new Global Internal Audit Standards™ were released by the Institute of Internal Auditors (IIA) in January 2024 and are expected to be implemented by all organisations by 9 January 2025.

They replace the existing International Professional Practice Framework (IPPF), including the standards, last revised in 2017. There is a very different structure to the new Standards, which are centred around **five domains**.

Within the new domains and their 15 principles and 52 standards, there is a large degree of consistency with the previous IPPF and some requirements where the expectations are more defined.



The IIA's Global Internal Audit Standards™ (continued)



Some of the key areas of change for organisations

The new standards will present different challenges for each organisation as it compares its current practices to the new requirements. We highlight below just three of the areas where, in our experience, many teams are seeing the biggest changes in practice.

Board and Senior Management responsibilities

The UK's FS Code has always set a high expectation for the involvement of the Board/Audit Committee in the governance of the Internal Audit function and the management of the Chief Audit Executive. However, the requirements have been less precise for other organisations. Domain III focuses on governance and sets clear expectations for the involvement of the Board and Senior Management in Internal Audit strategy, resourcing, the objectives and assessment of the Chief Audit Executive, and in the scoping and outcome of the external quality assessment.

These stakeholders should be brought up to speed by Internal Audit functions as early as possible, to collectively respond to the requirements of the Standards, and to gain value from this more joined up approach.

Internal Audit strategy

In order to conform with the new standards, Internal Audit must develop and implement a strategy for the function that is aligned to the overall strategy of the organisation, and discuss this with the Board and Senior Management at least annually. For many functions, a strategy will already be in place but we currently see a range of practice in terms of how it is shared across the organisation and the extent to which progress is reported.

This change will encourage those functions without a formal Internal Audit strategy to document their vision and goals. For all organisations, these new requirements should encourage the use of the strategy as a living document that helps drive growth and continuous improvement, and ensure that key stakeholders remain actively engaged.

Internal Audit expected behaviours

For the first time, the standards refer to the need for professional scepticism. Additionally, Domain II places an emphasis on 'professional courage', 'communicating truthfully' and 'taking appropriate action', and for the Chief Audit Executive to maintain a work environment where Internal Auditors feel supported when expressing legitimate, evidence-based engagement results, whether favourable or unfavourable.

These standards reflect good practice, and we recommend that teams actively reinforce these core messages through training and communications. Most importantly, teams should ensure that they have mechanisms in place to monitor and measure whether the training and communications are having the desired outcomes. Teams may be able to leverage their existing quality assurance processes to do so, including regular reporting of the results.

The IIA's Global Internal Audit Standards™ (continued)



The key implications for Internal Audit functions

For those in Financial Services, in particular those subject to sector-specific requirements, such as the UK Financial Services Code, some of the new requirements will not be new at all. Many of them are already commonly adopted practice, such as Standard 14.5, which requires for Internal Audit reports to have an overall rating.

We believe that the new standards will not require a lot of changes to day-to-day working practices for many developed Internal Audit functions. However, work may be required to demonstrate conformance. For example, with the ethics and professionalism requirements of Domain II and the requirements of parties outside of Internal Audit – namely the Board and Senior Management – in Domain III (see overleaf).

Internal Audit functions will need to decide on and document their interpretation of and response to some of the requirements that may be subjective or not currently followed 'to the letter' – for example, those in Domain V regarding the review of 'engagement documentation' by the Chief Audit Executive.

There are some new or evolved areas not just for Internal Auditors, but specifically for the Board and Senior Management, as set out in Domain III – Governing the Internal Audit function. This domain sets out requirements for Board and Senior Management involvement in the strategy, mandate, resources, quality and independence (amongst others) of Internal Audit in a way that is more formalised and explicit than the IPPF.

The new requirements of the Governance domain provide an opportunity for Internal Audit functions and their stakeholders to better align and more clearly articulate their understanding of Internal Audit's mandate, strategy and methods of delivery. The changes have potential to elevate the position of Internal Audit and promote the function's value.



The IIA's Global Internal Audit Standards™ (continued)



On this and the following pages, we set out our perspectives on the requirements of the five domains and their 15 principles and 52 standards.

Domain I: Purpose of Internal Auditing

This replaces the mission and definition within the IPPF. In essence, the purpose of Internal Audit remains largely the same but there are notable changes in the wording, with more focus on 'create, protect and sustain values'.

A key change is the introduction of the need for Internal Audit to provide 'foresight'. This is also reflected in the CIIA's revised Internal Audit Code of Practice published in September 2024.

It is a very short domain, with no principles or standards.

Domain II: Ethics and professionalism

This replaces the code of ethics within the IPPF, but goes much further, setting out the expected behaviours of all individuals responsible for the delivery or governance of Internal Audit activities. This domain will require attention from functions, largely in order to formalise the policies, procedures and controls that are likely already in place, but also to consider how it will demonstrate conformance with the five principles and 13 standards in this domain.

We recommend that functions consider the desired outcomes of this domain and not just the processes, including how they will assess the extent to which these outcomes are being achieved over time. For example, quality assurance practices may be expanded to cover this domain, but whilst it should assess conformance with processes (e.g. delivery of training and issuance of communications), it should focus on whether the desired outcomes of the domain are being met. It is important to assess and measure how well the outcomes are being achieved, and take corrective action if needed.



The IIA's Global Internal Audit Standards™ (continued)



Domain III: Governing the Internal Audit function

This domain will likely necessitate the most change. The three principles and nine standards in Domain III are for the Board and Senior Management, and not for Internal Audit. Many of the expectations are already a requirement of the Financial Services Code and others are common practice. Some requirements, such as the need for Senior Management to discuss with and provide input to the the Board and Chief Audit Executive regarding the expectations for the Internal Audit function when setting its mandate, are not consistently seen across all functions.

Internal Audit teams will need to work with the Board and Senior Management to determine how these standards should be interpreted, enacted and demonstrated. We recommend that Chief Internal Auditors should start talking to their Audit Committee chairs and CEOs now, if they haven't already done so, about the new standards and their

responsibilities, before taking them to the wider Audit Committee/Board and Senior Management. In some organisations, it may take time to get all senior stakeholders comfortable with where Internal Audit is positioned today and its plans for the future, especially if there is work to do.

Despite the challenges, this domain has the potential to yield the biggest benefits. By clarifying and formally agreeing the mission and mandate of Internal Audit and the support and engagement needed from the Board and Senior Management, there is potential for greater alignment. This in turn should foster confidence, allowing teams to deliver their work with purpose and conviction.

Domain IV: Managing the Internal Audit function

This domain includes four principles and 16 standards focussed on the strategy, operations, communication and quality arrangements of the Internal Audit function.

A key change is the requirement to develop and implement an Internal Audit strategy that supports the organisation's strategy, objectives and success, and that aligns with the expectations of the key stakeholders. Many Internal Audit functions do not have a strategy. The requirement is intended to encourage continuous improvement and innovation.

It also includes more emphasis on building trust and relationships with stakeholders in the business, rather than a focus on pure independence, which we see as a positive step.

It includes the development of a risk-based Internal Audit plan, where little has changed except for the need to include considerations of certain risks, such as governance and IT. No changes are seen in the areas of working with/reliance upon other assurance providers.

The IIA's Global Internal Audit Standards™ (continued)



Domain V: Performing Internal Audit services

This domain contains three principles and 1 standard, and focuses on the delivery of individual engagements (audits/reviews/assessments/etc.). The requirements are largely in line with common practice. For example, Standard 14.3 'evaluation of findings' requires Internal Audit to consider the risk and to prioritise (i.e., rate) each finding. The difference between this standard and common practice may be the requirement to 'collaborate with management to identify the root causes'. Root cause analysis is done well by some, but could be improved by many. Internal Audit should consider how this is interpreted, particularly where root causes might be complex and there is disagreement.

Some functions might wish to undertake additional training, update their methodology, and/or allocate additional time to deliver audits and communicate with the business in relation to these subtle but important changes.

Another feature of this domain is that teams will need to make clear decisions on how exactly to interpret and implement requirements. For example, Standard 14.6 'engagement documentation' requires that the Chief Audit Executive reviews and approves engagement documentation. Outside of very small functions, this is often a role that is delegated to audit leaders or managers, and to change this approach may not be seen as practical or the optimal use of team resources. In this and some other areas, we advise that teams document their approach and how it complies with the principles of the standards, if not the exact wording.



The IIA's Global Internal Audit Standards™ (continued)



Key actions for Internal Audit teams to consider now

- 01 Plan and assess**
Perform a readiness assessment and decide on your desired response. Expect that some areas will be easily addressed, but others will take time and require stakeholder engagement, decisions on approach, methodology changes and training.
- 02 Engage key stakeholders early**
Speak to your Audit Committee Chair and Chief Executive as soon as possible. Brief them on the new Standards and their responsibilities under Domain III. Agree on a plan to involve the wider Board and Senior Management. You will need their buy-in to changes and support if you need additional resources to deliver change.
- 03 Look at the wider 3LOD and mandate**
Use this as an opportunity to consider your mandate within the organisation as a whole, collectively working with the other lines of defence to shape the future model and assurance framework.
- 04 Decide on approach to regulated local entity needs**
For those in groups with multiple regulated entities and Boards, consider how your local entity Heads of Internal Audit will respond to the Standards, especially what you expect of smaller teams.
- 05 Make the underlying changes**
Work through your methodology, systems, QA, etc. to update them for the new Standards. This will take time and may flush out areas whether more work is needed to get ready, so start early. Document your interpretation of any areas of subjectivity.
- 06 Pilot and test the changes**
Select a pilot project in your 2024 Audit Plan to trial your proposed updates as a test run before going live in 2025.
- 07 Assess readiness pre-go live**
Consider a pre-go live external assessment to test the robustness of your response, suggest final remediation activities and provide assurance to IA and its stakeholders that you are ready for day 1.



The IIA's Global Internal Audit Standards™ (continued)



What we would expect be reported to the Audit Committee

01 An overview of the new standards, including Board and Senior Management responsibilities – **now**.

02 Gap analysis and remediation plan – **by autumn 2024**.

03 Conformance self assessment – **by January 2025**.

Where to find more information



[Read more](#) on the PwC website.



[Download](#) the new standards on the IIA's global website.



[Download](#) the condensed standards from the IIA's global website.



[Download](#) mapping of the 2017 IPPF to the 2024 standards.

PwC's Global Internal Audit Study: Seeing through walls to find new horizons

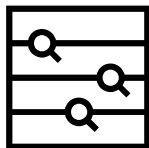


Things to look out for in the coming months

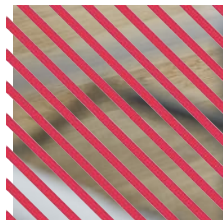
Future editions of [PwC's Reframe IA series on our website](#), helping you to leverage the opportunities presented by the new Standards.

[Future Topical Requirements from the IIA](#). These set out the requirements when providing assurance on a specified risk area. The first one, on the audit of Cyber, has been released.

The Quality Assessment Manual from the IIA, due later in 2024, which we understand is due to set out further expectations on the Standards and assessing conformance with them against a new rating scale.



Internal Audit Code of Practice



Internal Audit Code of Practice



Following an eight-week consultation period, the Chartered Institute of Internal Auditors ('CIIA') released the new [Internal Audit Code of Practice](#) in September 2024. The Code sets out fundamental principles for running a strong and effective internal audit function and replaces both the existing Financial Services Code and IA Code.

Effective from January 2025, the Code will be applicable to all internal audit functions in the financial services, private and third sectors, and is aligned with the new Global Internal Audit Standards and the revised UK Corporate Governance Code.

Per the CIIA, the three key drivers behind the proposed revisions were:

- To ensure the Code align to the new Global Internal Audit Standards.
- To include changes required to support the revised UK Corporate Governance Code.
- To reflect evolving industry practices.

The Code includes a set of 37 principles: six of which are new and four are unchanged. Of the remaining 27, half have only minor wording changes whilst the other half contain changes that are likely to have some impact on Internal Audit functions and their stakeholders.

Building on the new Global Internal Audit Standards and the revised UK Corporate Governance Code, the updated Internal Audit Code of Practice introduces several important enhancements, including:

Enhanced Reporting

Chief Internal Auditors are encouraged to work closely with their Audit Committees to ensure the Annual Report and Accounts include a clear summary of the internal audit function's activities, along with its impact and effectiveness. This is covered under the following principles as per the Code:

- **Principle 3:** The Chief Audit Executive should report annually to the Audit Committee on the application of the Code's principles, focussing on outcomes rather than a self-assessment against the code.
- **Principle 4:** The organisation's Audit Committee report in the Annual Report and Accounts should summarise the purpose and mandate of Internal Audit, the function's main activities and conclude on Internal Audit's impact and effectiveness. There may be a variety of inputs to this assessment, such as internal audit's quality assurance programme and its self-assessments. The assessment provides an opportunity for the CAE and the board audit committee to reflect on an annual basis on the impact the function delivers.
- **Principle 9:** A requirement has been added for Internal Audit to report to the Risk Committee of the Board as appropriate.
- **Principle 10:** The requirement for Internal Audit's consolidated reporting uses the word 'insights' for the first time. It adds additional requirements around ongoing thematic reporting and reporting on areas where Internal Audit has identified efficiencies, including removal of duplicative and/or redundant controls, and a requirement to provide an overall opinion on each of the areas of scope listed in Principle 8.
- **Principle 30:** Key Performance Indicators ('KPIs') must allow the Audit Committee to assess Internal Audit's value, impact, effectiveness and efficiency. We understand that this principle is intended to encourage functions to be more ambitious in defining how they measure their value and impact, beyond completion of annual audit plans. To do so is not straightforward, but can help Internal Audit to strategically focus on activities that add the greatest value to the business and to better articulate the strategic business value they provide.
- **Principle 31:** Internal Audit is required to conduct periodic self-assessments on conformance with this Code and the Global Internal Audit Standards.

Internal Audit Code of Practice (continued)



Wider Scope

All Internal Audit functions should assess risks related to capital, liquidity and poor customer treatment - not just those in the financial services sector, as well as addressing a range of risk areas as set out in Principle 8.

- **Principle 8a, f, h, i, j:** Includes new required areas of scope: purpose, capital and liquidity risks, poor customer treatment, ESG, financial crime, economic crime and fraud, and technology, digital and data risks. In addition, key external events are now required to be considered within scope. The majority of these will already be included in the plans of many functions, but the requirement on auditing against purpose is new. This new requirement is intended to support the role of internal audit as a strategic ally, and should prompt the function to consider whether the organisation has a clear purpose, and whether risk management and related control processes support the organisation in achieving this purpose.
- **Principle 8b:** Internal audit should undertake risk based reviews of organisational culture, incorporating, but not limited to, risk and control culture assessments. This could include the evaluation of relevant processes, tone at the top, behaviours, and ways in which the strategy, values, ethics, and risk policies are aligned and embedded.

Internal Audit remit, independence and a 'ways of working'

Internal Audit functions should have a clear remit and ways of working, while maintaining independence from other control functions, as follows:

- **Principle 6:** The wording removes references to cyclical coverage of the audit universe, instead allowing for purely risk-based plans. The wording explicitly includes regulators as a stakeholder group from whom internal audit should obtain views during the risk assessment process.
- **Principle 7:** 'Internal audit coverage and planning' places a focus on dynamic audit planning.
- **Principle 17:** Includes the requirement for Internal Audit to be given access to Board and Executive Committee papers.



Internal Audit Code of Practice (continued)



Diversity

The Code underscores the importance of Internal Audit teams having diverse backgrounds, skills, and experiences:

Principle 27: The Internal Audit team should comprise internal auditors with a mix of backgrounds, skills and experiences who bring diversity of thought. The Chief Audit Executive should recruit, retain and promote talent in accordance with the organisation's diversity, equity and inclusion ('DE&I') policies and applicable legislation. We fully support this new principle, but recognise that it could be challenging to demonstrate conformance.

Coordination with Assurance Providers

Principle 14: Internal Audit should coordinate with assurance providers to align on the timing of assurance over key risks. This should be included in reports to the Audit Committee.

Technology

The Code encourages Chief Internal Auditors to ensure access to advanced tools and technologies, to enhance audit effectiveness, as follows:

Principle 28: Includes requirements to ensure that the right tools and technologies are in place to support the function's impact and effectiveness e.g. use of data analytics and Artificial Intelligence. To ensure these are implemented and embedded in ways that derive real value might be challenging for some teams.

Alignment with Governance Disclosures

Internal audit's evaluations of risk management and internal controls should now support board disclosures on material controls:

Principle 11: At least annually, Internal Audit's reporting to the board and its Audit or Risk Committees should include an overall opinion on the effectiveness of the governance, and risk and control framework of the organisation, and its overall opinion on whether the organisation's risk appetite is being adhered to. This should support any board disclosure on the organisation's risk management and material controls and should highlight any significant weaknesses identified. This is intended to support the Board in their duties under the UK's new Corporate Governance Code.



The background features a dark scene with vibrant light trails in shades of teal, orange, and red, suggesting motion or data flow. Overlaid on this are several geometric patterns: a yellow and black diagonal striped rectangle in the top left, an orange and black diagonal striped rectangle in the middle right, and a pink and black vertical striped rectangle in the bottom right. A large white rectangular area is positioned above the 'Thank you' text.

Thank you

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2024 PricewaterhouseCoopers LLP. All rights reserved. 'PwC' refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

RITM0081803