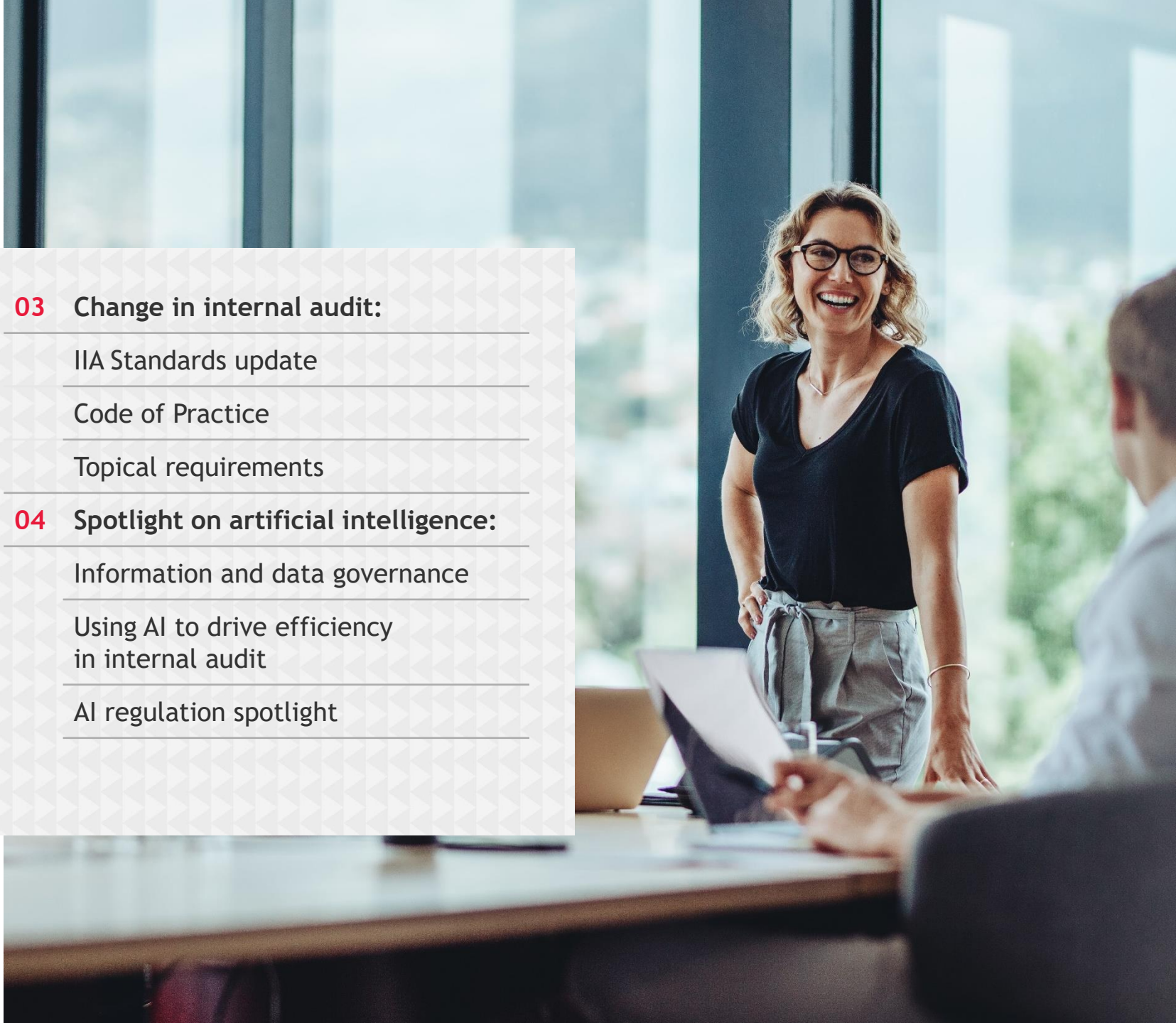
Internal audit and risk agenda

IDEAS | PEOPLE | TRUST

BDO

Contents



01

The internal audit and risk agenda: Welcome

IDEAS | PEOPLE | TRUST

The internal audit agenda

Welcome

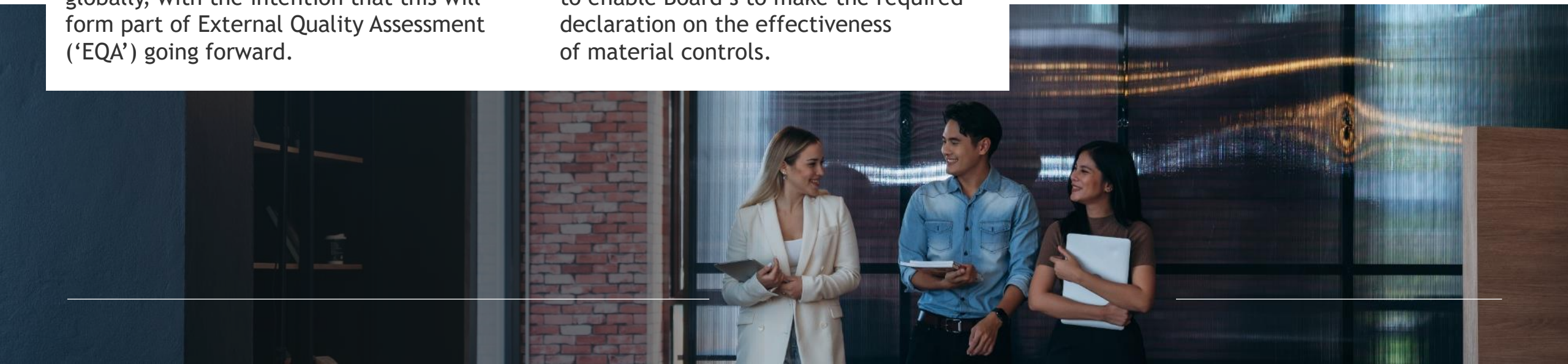
2025 looks to be a landmark year for the Internal Audit profession. New Global Internal Audit Standards come into force in January providing a clearer structure to the professional guidance and raising expectations of Internal Auditors and the Audit Committees that they report to.

Alongside the Global Standards a new Code of Practice has been published – setting a benchmark for good practice globally, with the intention that this will form part of External Quality Assessment ('EQA') going forward.

For UK listed companies, the principles and provisions of the new Corporate Governance Code need to be addressed with implementation of the main provisions for accounting periods starting on or after 1 January 2025.

An additional year has been permitted for the implementation of Provision 29 but work will need to be begin in 2025 to ensure a sound basis is established to enable Board's to make the required declaration on the effectiveness of material controls.

The UK election brought a change of Government but no change in the direction of travel for corporate governance reform. Further legislation is expected over the coming years which is likely to extend the scope of corporate governance requirements to large unlisted companies and to introduce more rigour to the approach adopted to assurance by all large entities.



The internal audit agenda

Welcome

Technological, economic, political and social changes are driving shifts to business models with considerable investment being made to transform delivery and operating models. Cyber, privacy and digital transformation risks are understandably high on the Audit Committee agenda. Artificial Intelligence presents opportunities for significant efficiencies and changes to working practices.

This comes with heightened risks such data loss, fraud and organisations need to ensure that the widespread deployment of AI is mitigated by sound governance and control frameworks.

Internal Audit has a key role to play in supporting organisations as they grapple with these challenges. Professional standards and corporate governance codes increasingly emphasise the importance of assurance and the Internal Audit profession. The challenge for Internal Audit teams is to keep pace with rapidly shifting expectations and to invest in broadening skills in areas such as Information Technology, programme management, ESG and to respond to new standards and regulatory requirements.

This document sets out some of the key challenges on the horizon that Heads of Internal Audit should be considering when thinking about the wider risks relevant to their organisations and the technical skills required to deliver meaningful assurance.

02

Auditing through change

IDEAS | PEOPLE | TRUST

Rising to the change challenge

Businesses and organisations are increasingly recognising that change, as the saying goes, is the one constant we can rely on. With this expectation, the pressure to deliver successful change is ever increasing and keeping up with the quantum, complexity and pace of change is critical. The delivery of change projects is complex and managing the risks and realising the benefits of transformation initiatives such as Finance, Digital, Operations or of a transaction are as difficult as ever - particularly when budgets are tight and skilled and experienced resources are increasingly difficult to secure.

What does this mean for Internal Audit?

The value of auditing through periods of change is pivotal – as this is often when organisations are exposed to some significant risk areas, including:

Commercial risk

The commercial investment in change is significant and organisations want confidence that they are not only doing the right thing commercially but that is delivering the expected benefits within the agreed budget.

Strategic

Transformation initiatives should always be aligned to strategic objectives – the failure of a programme to deliver to time/cost/quality will impact strategic goals.

Compliance

Any time of change can potentially impact the effectiveness of current processes and controls or the resources operating them. The importance of monitoring and maintaining compliance of high-risk processes and controls should be increased.

Rising to the change challenge

Operational

It is important for an organisation to retain the ability to deliver Business-as-Usual operations whilst also undertaking a change programme – particularly the key bottleneck resources who are pivotal to both.

Resources

Securing the right skilled and experienced resources to execute a complex programme is increasingly challenging, but ensuring your people are proactively managed during the change just as important to mitigate the risk of losing good people.

Reputational

The risk of a failed project can impact on any number of internal and/or external stakeholders. The higher the profile of the change being undertaken then the greater the risk of reputational damage.

Understanding which of these risks an organisation is most exposed to during the period of change enables Internal Audit to focus its scarce resources on the critical risk areas.

Rising to the change challenge

How does Internal Audit deliver a value adding 'change' assurance plan?

Once the key areas are identified/agreed IA can develop an assurance plan which will focus on those high priority risks. Key aspects to consider for any review, include:

- The clarity of the objectives, scope and the benefits of each change initiative.
- The alignment of initiatives to strategic goals through the portfolio processes.
- The project governance, approach and processes are balancing pragmatism with control.
- The impacts on people at all levels – is the change management approach working (see page 11 for more detail).
- How process optimisation and the associated controls are being undertaken (see page 12 for more detail).
- Are the impacts on people, process and systems being assessed holistically.

As part of these independent assurance reviews, the IA team has the opportunity to add value to the change initiatives without compromising independence. To achieve this each review needs to:

- Focus on the agreed key risk areas – what are business and programme stakeholders most concerned about?
- Complete reviews quickly – increase the turnover of reviews with a fast turnaround from scope definition, fieldwork and findings supported by pragmatic reporting. A one-week delay can be a long time in a change programme.
- Work with the change projects teams – understand their constraints and perspectives and flex to work with them (without compromising independence).
- Propose (and agree) pragmatic and insightful recommendations.
- 'Hold the line' where needed – if there is a key risk not being mitigated it must be escalated appropriately.

Rising to the change challenge

Assessing risks over how well the people side of change is being managed

Data-led plan

Does the transformation programme have the right mix of quantitative and qualitative data to define change readiness, business impact assessment and benefits realisation?

Delivery

How are people being engaged in co-designing and delivering impactful change solutions that drive adoption?

Track and measure

How appropriate are the chosen change metrics and practices being used to track progress and communicate success to all stakeholders?

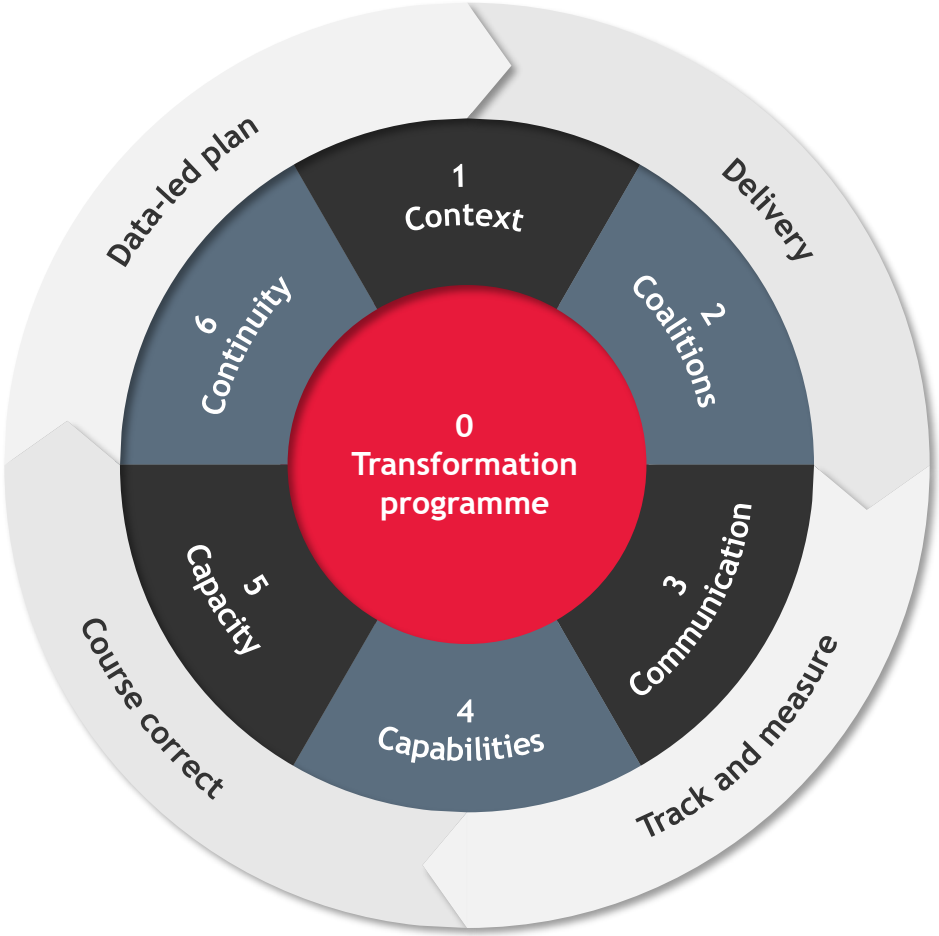
Course correct

How are change risks being mitigated and issues addressed by the project/programme team?

Rising to the change challenge

Assessing risks on how well the people side of change is being managed

0. Transformation programme	
A prerequisite for any successful transformation is flawless programme and project management (PMO) execution.	
1. Context	**2. Coalitions**
What strategic expectations and assumptions are tied to this transformation initiative?	Are the top team united and committed to 'act' as change sponsors?
3. Communication	**4. Capabilities**
How compelling is the change story – can it be easily understood and cascaded?	How will knowledge, skills and behaviours be developed to deliver the required changes?
5. Capacity	**6. Continuity**
Does the organisation have the bandwidth to make the change real and lasting?	What incentives and reinforcement mechanisms will sustain the changes?



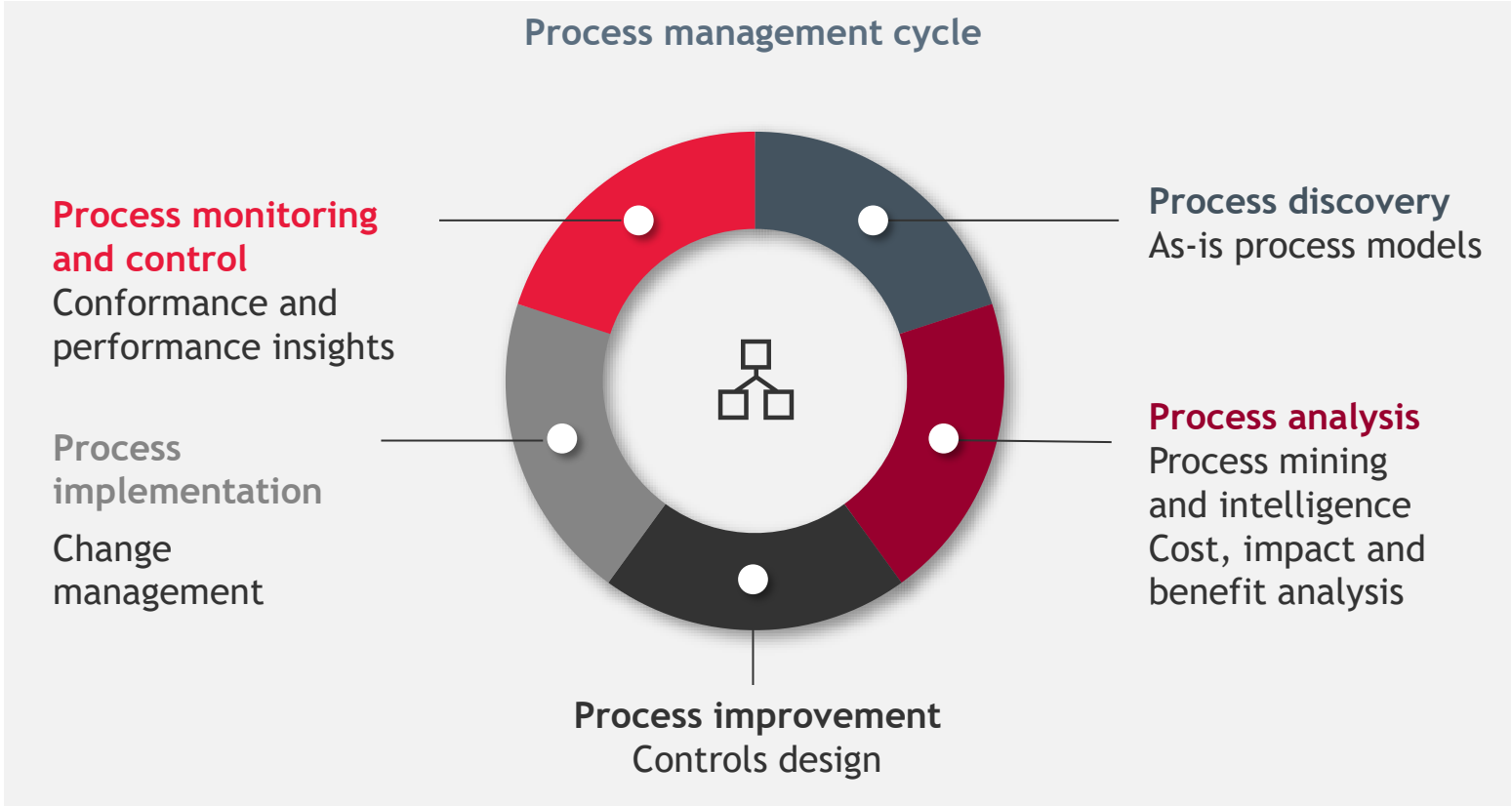
Rising to the change challenge

Understanding the importance of process optimisation/improvement risks during change initiatives

Introduction

When auditing through change, focus should be placed on the importance of process optimisation and improvement risks. Understanding the level of process management maturity within the organisation can help answer:

- Strategy – Are processes goal-oriented and aligned with the organisation's strategic needs?
- Design – Does the process design effectively mitigate and manages risks with robust controls, such as segregation of duties
- Monitoring – Does the organisation has effective measures in place to monitor process adherence and conformance.



Rising to the change challenge

Understanding the importance of process optimisation/improvement risks during change initiatives

Key features

Process ownership model - Establishing clear ownership for each process within the organisation to ensure accountability facilitates effective management. Our model assigns specific individuals as process owners who are responsible for the performance and improvement of their processes. They will have the authority to make changes and drive process efficiency, thereby ensuring that processes are aligned with the organisation goals and stakeholder needs.

Process portfolio management with the underlying governance mechanisms - Implementing a comprehensive management system to manage all processes as a portfolio. This involves categorising processes and assessing their importance and impact on the organisation objectives and allocating resources accordingly at a portfolio level. This ensures that efforts are focused on high value processes that contribute most to the organisation's mission and stakeholder satisfaction.

Rising to the change challenge

Understanding the importance of process optimisation/improvement risks during change initiatives

Stakeholder centric and enterprise level performance measurement and monitoring framework -
Develop and implement a measurement framework that focuses on stakeholder needs and the overall enterprise perspective. This framework should include key performance indicators and metrics that accurately reflect the effectiveness and efficiency of processes in meeting stakeholder requirements.

Repository management -
Create a centralised repository for documenting all business processes, descriptions, related documentation such as process maps and models, and metrics. This repository will serve as a single source of truth for the organisation's process landscape, enhancing visibility, and enabling easy access to process information.

By integrating these features into the organisation's approach to process management it can drive stakeholder centricity and show cross functional accountability and ownership and continuously improve its processes in response to evolving challenges and needs.

UK Corporate Governance Code

The FRC launched the new **Corporate Governance Code** in January 2024, and new Corporate Governance legislation was included in the King's Speech as the draft **audit reform and Corporate Governance Bill** in July 2024.

The new code and the new bill are inextricably linked and the headline changes are:

New Corporate Governance Code

Most significantly the board no longer only has responsibility for monitoring and assessing risk management and internal control system, but in accordance with the new code it now also required to provide a description of ***how*** the board has monitored and reviewed effectiveness of the Controls Framework, and provide a ***declaration of effectiveness*** of the material controls as at the balance sheet date. Together with a description of any material controls which have ***not operated effectively***.

Other changes relate to board culture, diversity and inclusion, and malus and clawback provisions in directors' contracts - These changes should give boards, audit committees and senior management cause to reflect.

Timing - With the exception of Provision 29, which relates to risk management and the internal control framework and becomes effective 1 January 2026, all other changes become effective 1 January 2025.

Principles based - The Code's structure and sections; board leadership and company purpose, division of responsibilities, composition, succession and evaluation, audit, risk and internal control, and remuneration, are unchanged.

Audit Reform and Corporate Governance Bill

Draft Audit Reform and Corporate Governance Bill, announced July 2024 - full details remain in a 'wait and see' status, what we do know is:

The draft bill will act to replace the Financial Reporting Council ('FRC') with a new regulator – the Audit, Reporting and Governance Authority ('ARGA') – with the powers it needs to tackle bad financial reporting and to build that trust.

ARGA will have a wider remit, through extending Public Interest Entity (PIE) status to the largest private companies and thus making sure the audits of those important businesses are high quality and giving early warning of financial problems – and remove unnecessary rules on smaller public interest entities.

Powers to investigate and sanction company directors for serious failures in relation to their financial reporting and audit responsibilities.

A regime to oversee the audit market, protect against conflicts of interest at audit firms, and build resilience so quality audit is available to all companies.

The implications of these changes are particularly relevant for the new Corporate Governance Code.

The requirement to provide a description of how the board has monitored and reviewed effectiveness of the control framework, a declaration of effectiveness of material controls, and description of ineffective material controls – this will be regulated by ARGA, which will have increased powers vs the FRC. This declaration will also fall under the scope of covered by ECCTA (see pages 18-20).

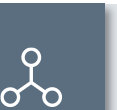
UK Corporate Governance Code

How can IA help?

Questions that remain open

What will changes to the PIE and premium listed definitions mean for the scope of Provision 29?

How will the UK Economic Crime and Corporate Transparency Act capture of the Controls Declaration, drive management's focus on implementation and robustness of reporting?



What does the Code mean by 'material' in the context of all 'material' controls?

How will external audit perform an audit of the controls declaration once it is a live requirement?

With the upgrades to control frameworks, will we expect to see a move from purely substantive audits to more efficient controls-based audits for external auditors?

Our IA teams are helping boards and audit committees prioritise and develop their responses to the Code and Audit Reform Bill changes:

- IA can help boards, audit committees and management with understanding and digesting the new Code and Bill – in particular, navigating the considerations around implementation and ensuring that these elements are appropriately captured within their reporting.
- It is recommended that boards and audit committees should be taking action now, to understand their gaps in relation to the updated Code and identify areas that are likely to be the hardest to remediate – our IA teams can help with performing or steering your organisation with this exercise, and are well placed to support on prioritisation activity:
  - Top of the list are risk management and internal control – whilst none of the updated Principles and Provisions are quickly fixed, effective risk management and internal control require a well coordinated approach, with input from your most senior business leaders, and time to design and embed – hence the longer implementation date
  - A robust risk and internal control framework cannot be fully embedded without the will and understanding of your people and, depending on the maturity of existing arrangements, a significant shift in culture and behaviours may also be required – IA can support with messaging and training.

Economic Crime and Corporate Transparency Act

The cost of fraud to UK companies is significant and BDO's Fraud Track Report 2024 highlights that this is likely to increase with new fraud growth areas such as greenwashing, bluewashing and the increasing use of AI. The UK Fraud Strategy 2023 reported that Fraud represents 41% of all crime committed in the UK and with the Association of Chartered Fraud Examiners Report to the Nations 2022 estimating that the average organisation loses 5% of its annual revenue to fraud each year, fraud is very much on the board agenda.

In October 2023 the UK Economic Crime and Corporate Transparency Act (ECCTA) received royal assent and introduces a third corporate failure to prevent offence – this time in relation to Fraud. Under this offence, an organisation will be liable where a specified fraud offence is committed by an associated person for the organisation's benefit, and the organisation did not have reasonable fraud prevention procedures in place.

The scope of the offence applies to large organisations who meet two of the following three criteria:

01 Average number of employees over 250

02 Turnover in excess of £36m

03 Total balance sheet assets above £18m

Guidance was published in November 2024 and is similar to the published guidance under previous failure to prevent offences for bribery and corruption and tax evasion.

Economic Crime and Corporate Transparency Act

For many organisations this is a fundamental change to the way that they will look at fraud. Traditionally organisations have looked at fraud through the lens of being a victim of fraud, whether that is from an internal or external threat (otherwise known as inward fraud). To mitigate the risk of fraud organisations have therefore focused on financial controls to both prevent and detect fraud.

This new offence focuses on underlying fraud offences from which an organisation or service recipient may benefit, namely outward frauds. This is a new concept for many and will prompt a conversation about a number of issues including how this risk could crystallise, who should be accountable/responsible for fraud and which function should play which roles in response.

Update to the Identification Principle

The previous ‘directing mind and will test’ (which generally means a board member) has been removed and the new Act changes this to a senior manager test:

‘If a senior manager of a body corporate or partnership (‘the organisation’) acting within the actual or apparent scope of their authority commits a relevant offence after this section comes into force, the organisation is also guilty of the offence.’

This should make it much easier for the SFO to bring prosecutions against corporates for offences covered under the new Act.

Economic Crime and Corporate Transparency Act

How internal audit can support

- Fraud is not a new risk consideration for Heads of Internal Audit. They should already have a clear view of their organisation's exposure to fraud and how this is being managed. However previously organisations' focus on fraud has been to ensure that they are not victims of fraud, which means financial controls are imperative, however the new offence relates to the organisation benefiting from fraud and will therefore be more aligned to building framework and compliance controls
- With their experience of helping the organisation establish procedures to address legislation in the past – internal audit teams are well placed to support management in establishing the policy, procedures, fraud risk assessment and monitoring arrangements.

Navigating ESG Changes: The role of Internal Audit

In today's business landscape, Environmental, Social, and Governance (ESG) considerations are no longer optional. Integrating ESG into your strategy is crucial for driving meaningful change and ensuring your organisation remains robust, credible, and viable. ESG should not be a standalone topic on the internal audit plan. It is a fundamental aspect that cuts across all areas of the organisation. Internal audit can help fulfil ESG obligations, engage stakeholders, and navigate the complex regulatory environment, ultimately enhancing your business's long-term success.

Regulatory reporting requirements are increasing, covering more ESG issues. Many companies must comply with the Climate Related Financial Disclosures (CRFD) Regulation and the EU's Corporate Sustainability Reporting Directive (CSRD). The UK is expected to adopt the ISSB standards through the UK Sustainable Disclosure Requirements (SDR) by Q1 2025, supporting Climate Transition Plans (UK TPT) and the Taskforce on Nature-related Financial Disclosures (TNFD). Future regulations like the Corporate Sustainability Due Diligence Directive (CSDDD) and Taskforce on Impact-related Financial Disclosures (TISFD) will follow, initially impacting the largest and listed organisations, first before trickling down to the mid-market.

Robust internal processes and controls are crucial for compliance and obtaining independent assurance over disclosures. Key challenges include assessing the supply chain, engaging stakeholders, and managing climate governance. Companies must navigate these complexities to meet regulatory requirements and demonstrate commitment to sustainability.

Scrutiny over sustainability claims is increasing. Accurate and substantiated claims enhance your brand, while misleading ones can be disastrous. The Competition and Markets Authority (CMA) has investigated various organisation's, advising 17 fashion brands to review their practices. The CMA will soon have the power to fine businesses up to 10% of their worldwide turnover for breaking consumer law. Will it be long before we see fines in the fashion sector or indeed other sectors being fined for misleading statements?

Navigating ESG Changes: The role of Internal Audit

To integrate and embed robust ESG and sustainability practices within a business model, the following factors are critical:

Materiality and focus: Identify key issues for your business and stakeholders. Materiality assessments ensure that organisations focus on the most relevant ESG issues in their reporting and are a requirement for adhering to upcoming regulations.

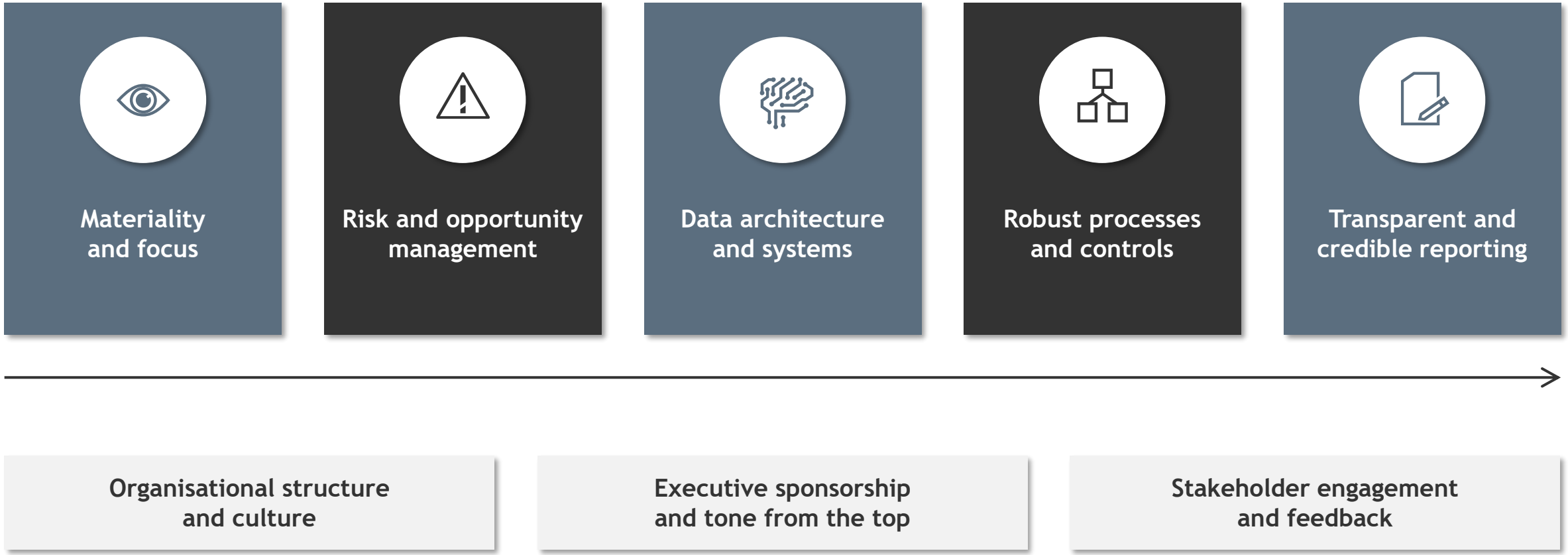
Risk and opportunity management: Integrate ESG into risk management. A holistic approach ensures that ESG is not treated as a standalone risk.

Data architecture and systems: Reliable data is the backbone of any ESG strategy. Implementing robust data architecture and systems ensures accurate tracking, reporting, and decision-making.

Robust processes and controls: Strong controls and processes are essential for maintaining integrity and compliance. They ensure that ESG initiatives are effective and aligned with your overall business strategy.

Transparent and credible reporting: Companies must be prepared to obtain independent assurance over their disclosures, manage climate governance, and engage relevant stakeholders to meet regulatory requirements and demonstrate their commitment to sustainable practices. Companies must also consider the use of social media and risk to reputation of any broad statements made.

Navigating ESG Changes: The role of Internal Audit



Navigating ESG Changes: The role of Internal Audit

How internal audit can support

As internal auditors our remit is to provide assurance, advice, insight, and foresight to our organisations and depending on where you are on the journey this role will evolve over time. Key considerations to build into our internal audit plans are:

- **Evaluating organisational structure and culture:** Identifying areas for improvement to foster a culture that values sustainability and ethical practices and supports the organisational priorities. Are the right governance arrangements in place? Assessing the horizon scanning capability to anticipate changes from regulations and stakeholders, including benchmarking against peers.
- **Robustness of strategy development:** Has the necessary rigour been applied to developing the ESG strategy?
- **Stakeholder engagement:** Are all internal and external stakeholder views being considered? How are we building stakeholder considerations into day to day decision making? Have we missed any key stakeholder groups?
- **Assessing data architecture and systems:** Assessing the capability of systems to capture accurate ESG data collection, reporting, and decision-making, aligned to the overall strategy.
- **Assessing data architecture and systems:** Assessing the capability of systems to capture accurate ESG data collection, reporting, and decision-making, aligned to the overall strategy.
- **Assessing readiness for external verification:** Building disciplines around non-financial reporting and metrics, reducing the risk of greenwashing, and helping build trust between companies and their stakeholders. Assessing appropriateness of ESG metrics and alignment to evolving strategy and regulation, including whether internal methodologies align with the reality of actual processes in place.

Tax governance: A changing landscape

Priority hot topics

Background

Tax governance and risk management are increasingly on the Board and Senior Management agenda, as well as front of mind for a wide range of external stakeholders including shareholders, potential investors, tax authorities and the Regulators.

Senior Accounting Officer ('SAO')

The Finance Act 2009 mandates that large UK businesses (with group annual turnover of £200m+ or balance sheet assets of £2bn+) must certify to HMRC that they have appropriate tax accounting arrangements annually. Non-compliance can lead to financial penalties for both the company and individuals.

Business Risk Review ('BRR')

Large businesses, with a Customer Compliance Manager (CCM) undergo periodic BRRs.

Corporate Criminal Offence ('CCO')

Under the Criminal Finances Act 2017, if an associated person of a business facilitates tax evasion and the business cannot show it had reasonable prevention procedures, the business is guilty of a criminal offence. This applies to all UK businesses and non-UK businesses with some UK nexus.

Drivers - Why should this be considered for audit plan?

- Poor tax governance can expose a business to several potential issues, including:
  - Reputational risk with tax authorities, regulators and other external stakeholders
  - Financial risk either because of non-compliance (with associated penalties, interest and lost management time dealing with enquiries) or a failure to access appropriate tax credits and allowances.
- The Environmental, Social and Governance ('ESG') agenda. Stakeholders in a firm want to know that the firm has a set of strong principles and values that extends to its approach to tax and governance framework
- Specific drivers related to SAO, CCO and BRR compliance.

Tax governance: A changing landscape

Priority hot topics

Indicative scope areas

Tax Governance (including Business Risk Review ('BRR'))

- Review tax governance and strategy, assess tax risk management and evaluate tax performance effectiveness
- Evaluate control documentation (e.g., Tax Strategy, Tax Policy, Tax Process) for suitability based on sector, size, and complexity
- Conduct walkthroughs and interviews with key tax and finance stakeholders and others as needed
- Include a technical review of a specified tax area (e.g., employment duties, VAT, bank levy) to assess control environment effectiveness
- Use the TOMM tool to support analysis and conclusions.

Senior Accounting Officer ('SAO')

- Issue an online questionnaire focused on tax governance and SAO compliance to provide a snapshot of the control environment and potential focus areas
- Conduct a desktop review of control and procedural documentation
- Conduct walkthroughs and interviews with key tax and finance stakeholders and others as needed
- Benchmark the internal SAO process against HMRC Guidance and our knowledge of HMRC's approach
- Identify good practices, control weaknesses, and recommendations for improvement.

Corporate Criminal Offence ('CCO')

- Review key documentation, including CCO risk assessments, policies, and procedures, to understand the control environment, benchmark it against leading practices, and evaluate suitability based on sector, size, and complexity
- Conduct interviews with key staff to establish awareness of the legislation and the controls in place
- Consider the adequacy of mandatory CCO training within the business.

03

Change in internal audit

IDEAS | PEOPLE | TRUST

IIA standards update

Domain III Governing the Internal Audit Function

One of the main changes brought in by the new Global Internal Audit Standards (GIAS) is how internal audit functions are governed. Whilst the Chief Audit Executive (CAE) is responsible for the requirement of Domain III, certain activities that need to be performed by the board and senior management are essential to the internal audit function's ability to fulfil the Purpose of Internal Auditing. These activities are identified as 'essential conditions' and establish the necessary foundation for an effective dialogue between the board, senior management and the chief audit executive, ultimately enabling an effective internal audit function. The following should be discussed:

- The purpose of internal auditing
- The 'essential conditions' to enable an effective IA function
- The potential impact on the effectiveness of the IA function if the board or senior management does not provide the expected levels of support.

Whilst the Board has ultimate responsibility to discuss and approve the IA Charter, setting out the mandate, senior management's perspective helps support the IA function's positioning and promotes the authority granted to the IA function. The nature and frequency of these discussions depends on the circumstances and changes in the organisation.

Set out on pages 29-34 are the nine 'essential' conditions.

IIA standards update

Operational

Requirement:

CAE to provide board and management with the information necessary to establish an IA mandate to determine IA's authority and role and responsibilities. CAE must assess whether changes in circumstance justify a discussion with the board and management about the mandate.

Board:

Discuss with CAE and management the appropriate authority, role and responsibilities for the IA function.

Management:

Participate in discussions with the board and CAE on the IA mandate. Support the mandate throughout the organisation and promote IA's authority.

Internal audit Charter

Requirement:

CAE to develop and maintain an IA charter, outlining the purpose of internal auditing, commitment to the GIA standards, IA mandate, types of service provided and the board's responsibilities and expectations regarding management's support for IA. CAE to review and update the charter periodically in consultation with the board and management.

Board:

Engage in discussions regarding the charter and consider other topics to be included to enable an effective IA function. Approve the charter.

Management:

Communicate with the board and CAE about management's expectations that should be considered for inclusion in the charter.

IIA standards update

Board and senior management support

Requirement:

CAE to provide board and management with the information needed to support and promote recognition of the IA function throughout the organisation.

Board:

Champion the IA function, ensure unrestricted access to information, support the CAE through regular, direct communications, demonstrate support by requiring CAE be suitably positioned to fulfil the IA mandate, approve the plan, budget and resource plan, understand any restrictions placed on scope, meet with CAE without management present.

Management:

Support recognition of the IA function and allow unrestricted access to people and information.

IIA standards update

Independence

Requirement:

CAE confirm to the board the independence of the IA function annually and any incidents where independence may have been breached. CAE must discuss with board and management any potential impairment to independence.

Board:

Establish a direct reporting relationship with CAE, authorise their appointment/removal, provide opportunities for CAE to discuss sensitive matters without management, position CAE at a level they can operate without management interference.

Management:

Position IA at a level in organisation that enables it to perform without interference and recognise CAE's direct reporting line to the board.

CAE qualifications

Requirement:

CAE must help the board understand the qualifications and competencies necessary to manage IA. CAE must maintain and enhance qualifications and competencies necessary to fulfil responsibilities.

Board:

Review the requirements necessary for CAE to manage IA. Approve the CAE role and identify necessary qualifications, experience and competencies required to fulfil responsibilities. Engage with management to appoint CAE with requirement qualifications and competencies.

Management:

Engage with board to determine the CAE's qualifications, experience and competencies.

IIA standards update

Board Interaction

Requirement:

CAE provides board with information needed to conduct oversight of the IA function. CAE escalates significant issues to the board when disagreements with management arise.

Board:

Communicate with the CAE to understand how IA's activities fulfil its mandate, communicate the board's perspective on the organisation's strategies, objectives and risks, establish clear processes for escalating issues and support the CAE to resolve disputes with management.

Management:

Share perspectives on strategies, objectives and risks to assist with determining priorities, establish escalations processes with the board.

IIA standards update

Resources

Requirement:

CAE to evaluate whether resources are sufficient to fulfil IA's mandate and achieve IA plan.

Board:

Collaborate with management to provide IA with sufficient resources, discuss resource with the CAE at least annually, consider the impact of insufficient resources and address any insufficiencies.

Management:

Engage with board to provide sufficient resources to fulfil IA mandate and address any identified resource insufficiencies.

Quality

Requirement:

CAE must develop, implement, and maintain a quality assurance and improvement program (QAIP), conducting internal and external assessments and reporting results annually to the board and management.

Board:

Discuss the QAIP with the CAE, approve the function's performance objectives, assess the function's effectiveness and efficiency of the IA function.

Management:

Provide input on IA's performance objectives and participate in the annual assessment.

IIA standards update

External Quality Assessment (EQA)

Requirement:

CAE must develop a plan for an EQA at least every five years, ensuring that at least one person of the assessment team is suitably qualified.

Board:

Review and approve CAE's EQA plan including scope/frequency of EQA, review results directly from the assessor, and approve action plans for addressing gaps.

Management:

Collaborate with the board and CAE on the EQA and action plans.

Code of Practice

The new Internal Audit Code of Practice recently issued by the Chartered Institute of Internal Auditors (IIA) replaces the existing Internal Audit Financial Services Code of Practice (published in 2013) and the Internal Audit Code of Practice for the private and third sectors (published in 2020).

The IIA's aim for the Code is to enhance 'the overall impact and effectiveness of internal audit within organisations operating in the UK and Ireland.'

The principle-based nature of the Code and focus on outcomes mean that Chief Audit Executives (through agreement with audit committees and senior stakeholders) can take a proportionate and pragmatic approach in its implementation taking into account the nature, scope and complexity of the organisation.
The Code has introduced outcome statements which focus on outcomes rather than a requirement to meet all of the individual associated principles.

Although, whilst the Code is not mandatory and does not form part of the International Professional Practices Framework (IPPF), we're aware that the IIA is expecting the Code to form part of the scope of future external quality assessments.

Code of Practice

Key changes to the Code include:

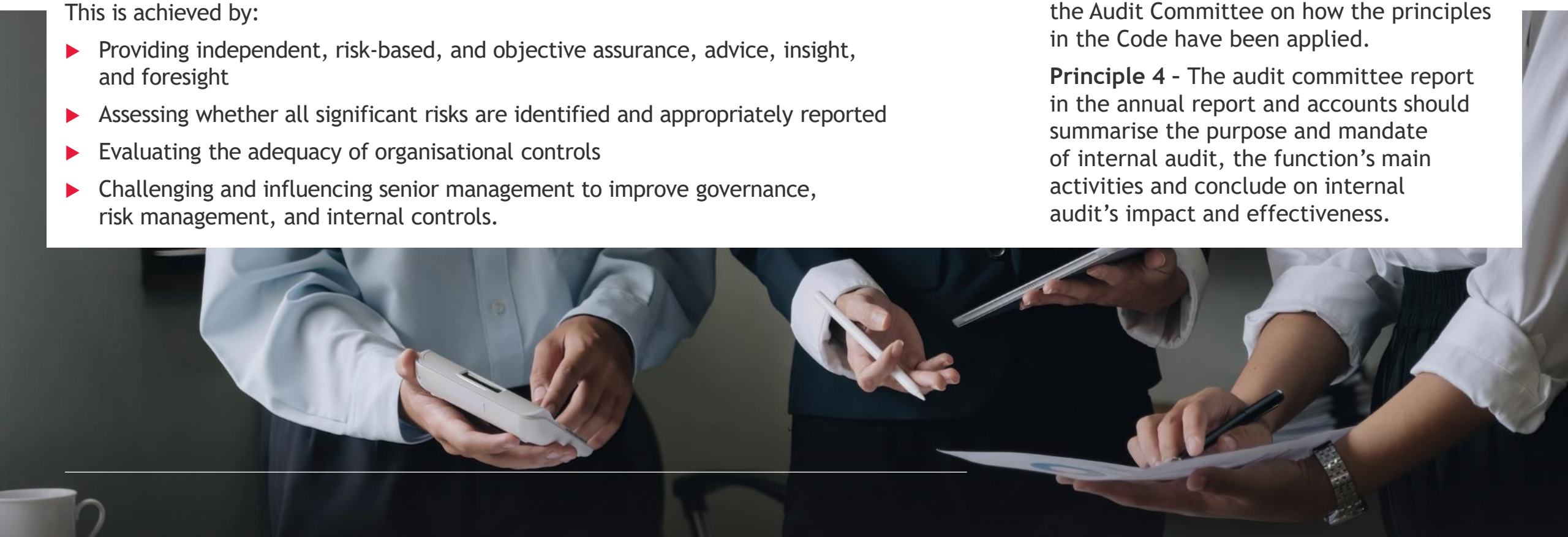
A. Mandate

Principle 1 - The primary role of Internal Audit has been updated to 'help the board and senior management protect the organisation's assets, reputation, and sustainability. This is achieved by:

- Providing independent, risk-based, and objective assurance, advice, insight, and foresight
- Assessing whether all significant risks are identified and appropriately reported
- Evaluating the adequacy of organisational controls
- Challenging and influencing senior management to improve governance, risk management, and internal controls.

Principle 3 - The Chief Audit Executive (or equivalent) must report annually to the Audit Committee on how the principles in the Code have been applied.

Principle 4 - The 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.



Code of Practice

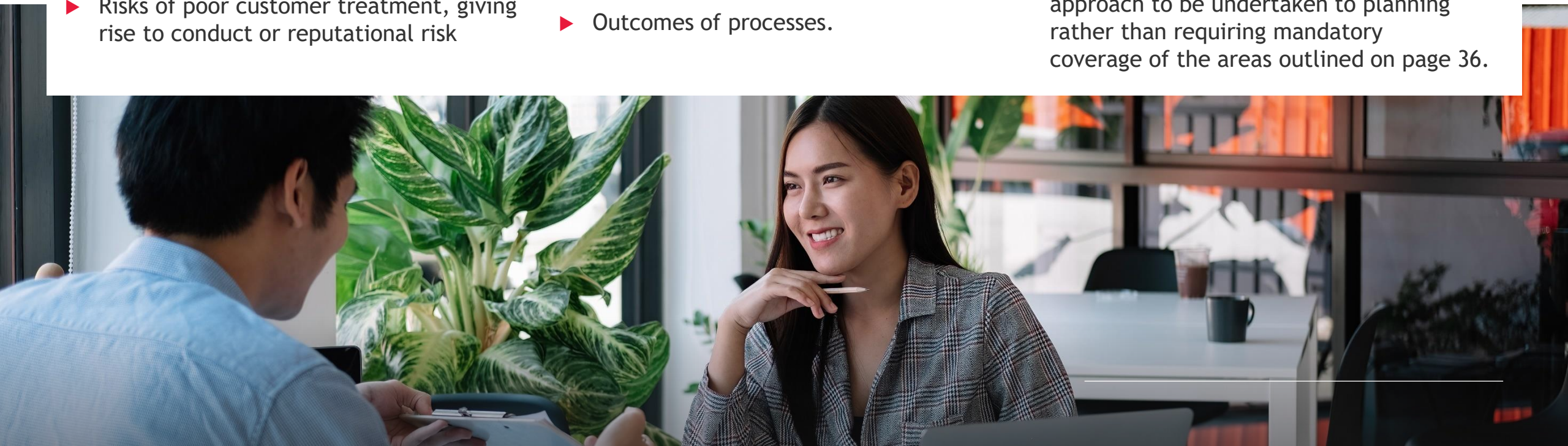
B. Scope and priorities for Internal Audit

Principle 8 - Internal audit should include within its scope the areas outlined below:

- Purpose, strategy, and business model
- Organisational culture
- Capital and liquidity risks
- Risks of poor customer treatment, giving rise to conduct or reputational risk
- Environmental sustainability, climate change risk, and social issues
- Financial crime and fraud, technology and data risks
- Risk management, compliance, finance, and control functions
- Outcomes of processes.

The areas of internal governance, the setting of, and adherence to, the risks the entity is willing to accept (risk appetite) and key corporate events remain from the previous Code.

The Code still expects a risk-based approach to be undertaken to planning rather than requiring mandatory coverage of the areas outlined on page 36.



Code of Practice

C. Reporting

Principle 11- At least annually, internal audit's reporting to the Audit Committee 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.

E. Independence and authority of internal audit

Principle 24 - For financial services organisations, if internal audit has an administrative reporting line, this should be to the chief executive in order to preserve independence from any particular business area or function and to establish the standing of internal audit alongside the executive committee members. For the private and third sectors, the administrative reporting line can be to another member of senior management who promotes, supports and protects internal audit's independent and objective voice.

F. Resources

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 policies and applicable legislation.

Principle 28 - The CAE should ensure that internal audit has the appropriate tools and technology to support the function's impact and effectiveness (e.g. use of data analytics and artificial intelligence), to support its effectiveness and impact.

Topical requirements

What do we know about the Topical requirements?

The Topical Requirements are a mandatory part of the International Professional Practice Framework (IPPF). Since the release of the new Global Internal Audit Standards, these requirements haven't received much publicity. However, they need to be integrated into our methodologies.

In 2024, the IIA released a consultation draft of the Cybersecurity Topical Standards. This draft outlines the expected structure of future Topical Requirements. The Global Guidance Council approved the following topics in March 2024:

- Cybersecurity
- Third-Party Risk Management
- Culture
- Business Resiliency
- Anti-Corruption/Bribery*
- People Management*
- Fraud Risk Management*
- Sustainability: ESG*

* The starred topics are broad and the IIA plan to refine these.

Topical requirements

Key updates

- The IIA held a webinar in June 2024 as part of the Cybersecurity Topical Requirements Consultation. The playback is available on their website
- The final draft of the Cybersecurity Topical Requirements is expected in early 2025
- Development of the Third-Party Risk Management Topical Requirements has started, but no release date for the consultation draft has been given.

Structure of Topical requirements

Each Topical requirement will have three elements:

1.
Requirements: Mandatory and cover essential organisational objectives. They will address Governance, Risk Management, and Control Requirements.

2.
Appendix A: Considerations: Not mandatory but serve as best practices. These should be used as examples to validate the requirements, not as a checklist.

3.
Appendix B: Tool to Document Conformance: This tool helps document conformance with each requirement or provide the rationale for excluding a requirement from the engagement scope.

Topical requirements

What do the new Topical Requirements mean for Internal Audit functions?

The landscape of internal audit is evolving, and the introduction of the new Topical Requirements is a significant development. From January 2025, conformance with these requirements (once released) will be assessed as part of External Quality Assessments. So, what does this mean for your internal audit function? Here are the key elements to consider when implementing new methodologies aligned with the new Standards.

- Annual Planning and Risk Assessment: As part of your annual planning risk assessment, you need to identify whether your risk-based plan includes areas that have an associated Topical Requirement. If these areas are included, you must determine whether your engagement will cover the full scope of the Topical Requirement or focus on specific aspects. If only certain aspects are to be included, document the rationale for excluding other elements in your annual plan
- Engagement Scoping: During the scoping of specific engagements, you may find that not all requirements of the relevant Topical Requirement are necessary. At this stage, it's crucial to document the rationale for excluding certain aspects. This ensures transparency and provides a clear audit trail for future reference and for your next EQA
- Performance of Engagements: Sometimes, during the performance of an engagement that initially appears unrelated to a Topical Requirement, you may discover relevant aspects. For example, while auditing accounts payable, you might identify cybersecurity risks related to the online submission of purchase orders. In such cases, follow the relevant part of the Topical Requirement and document the rationale for not including other requirements in your engagement work papers.

The new Topical Requirements are set to redefine how internal audit functions operate. By integrating these requirements into your methodologies, you ensure compliance and enhance the quality of your audits. Stay proactive, document your rationale for any exclusions, and keep your processes transparent. This approach will not only help you meet the new standards but also elevate the overall effectiveness of your internal audit function.

04

Spotlight on Artificial Intelligence

IDEAS | PEOPLE | TRUST

Information and data governance

Clear policies and procedures

Defined roles and responsibilities

Custom frameworks

Regular monitoring and auditing

Quality assurance

Alignment with strategic objectives

Information and data governance

Information and data governance is a hot topic for internal audit functions due to several key drivers. Regulatory compliance is crucial as stricter data protection laws like GDPR demand adherence, with non-compliance leading to fines and reputational damage. Effective governance also mitigates risks from data breaches and operational inefficiencies. Technological advancements in big data, AI, and cloud computing necessitate robust governance to maintain data integrity and security. Additionally, good governance builds stakeholder trust through transparency and accountability. Overall, information and data governance enhances audit quality, improves risk management, streamlines processes, supports compliance, aids decision-making, and builds trust, making the internal audit function more effective and efficient.

Data integrity:

Reliable and accurate data is essential for auditors to assess risks, evaluate controls, and provide assurance. Good governance ensures data integrity, **making audit findings more credible.**

Compliance:

Organisations must comply with various regulations and standards. Effective data governance helps ensure that data management practices meet these requirements, **reducing the risk of non-compliance.**

Risk management:

Proper governance identifies and mitigates data-related risks, such as data breaches or loss of data quality. This **proactive approach supports** the internal audit function in its **risk assessment processes.**

Efficiency:

Streamlined data governance processes reduce redundancies and improve data accessibility. This efficiency allows auditors to focus on high-value activities, such as developing strategies for effective risk mitigation, rather than data validation.

Decision-making:

High-quality data supports better decision-making. Auditors can **provide more insightful recommendations** when they have access to well-governed data.

Information and data governance

From an internal audit perspective, good information and data governance includes:

- **Clear policies and procedures:** Well-documented guidelines for data management, covering data quality, security, and lifecycle management. These should be easily accessible and regularly updated
- **Defined roles and responsibilities:** Clear assignment of data stewardship and ownership, ensuring accountability and consistent data management across the organisation
- **Regular monitoring and auditing:** Ongoing assessments to ensure compliance with data governance policies. This includes identifying gaps and implementing corrective actions promptly
- **Alignment with strategic objectives:** Data governance should support the organisation's broader goals and be integrated into its risk management and compliance frameworks
- **Quality assurance:** A robust quality assurance process to ensure thorough consideration and due diligence on each engagement and deliverable
- **Custom frameworks:** Utilising frameworks that blend industry standards like DAMA DM-BoK and TOGAF ADM with organisational expertise to assess data governance maturity across design, implementation, and operating effectiveness.

Using AI to drive efficiency in internal audit

One of the main ways AI enables more efficient internal audits is by automating data analysis, enhancing risk assessment, and enabling continuous monitoring, leveraging NLP, and utilising intelligent automation. From an internal audit point of view, when we talk about AI or data in general we must focus on understanding three perspectives:

How

Automated data analysis: Large volumes of data can be quickly processed and analysed, identifying patterns, anomalies, and trends that might be missed by manual reviews. This speeds up the audit process and improves accuracy.

Risk assessment: Algorithms can assess risks more effectively by analysing historical data and predicting potential future risks. This allows auditors to focus on high-risk areas, making the audit process more targeted and efficient.

Continuous monitoring: Real-time monitoring of transactions and processes is ensured, flagging any irregularities immediately. This continuous oversight helps in early detection of issues, reducing the time and effort required for periodic audits.

Natural Language Processing (NLP): NLP can be used to review and interpret unstructured data, such as emails and documents, to identify compliance issues or potential risks. This expands the scope of audits without requiring additional manpower.

Intelligent automation: Intelligent Automation can handle repetitive and time-consuming tasks, such as data entry and reconciliation, freeing up auditors to focus on more complex and value-added activities.

Using AI to drive efficiency in internal audit

Hindsight:

What has happened?

Insight:

Why did it happen?

Foresight:

What is going to happen next and what can we do about it?

Why

Efficiency: AI automates routine tasks such as reviewing the contents of large volumes of documents, allowing auditors to focus on strategic and analytical work such as developing effective risk mitigation strategies. This leads to better quality audits in a manner that is faster and more efficient.

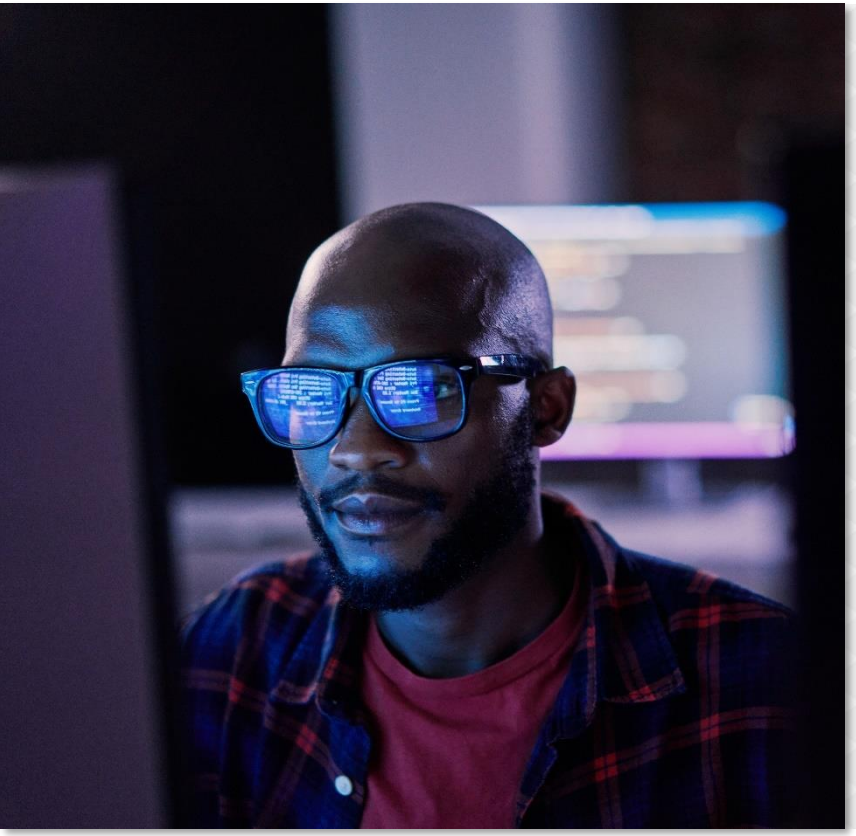
Accuracy: Human error is reduced by consistently applying rules and algorithms, leading to more accurate audit results.

Scalability: Large volumes of data and complex processes are handled by AI, making it easier to scale audit activities as the organisation grows.

Insight: Deeper insights are accessible through advanced data analytics, helping auditors identify underlying issues and trends that might not be apparent through traditional methods.

Proactive risk management: Continuous monitoring and real-time risk assessment are enabled through alerts, allowing organisations to address issues proactively rather than reactively.

Using AI to drive efficiency in internal audit



What good looks like

Integrated systems: AI-enabled tools should be seamlessly integrated with existing audit and enterprise systems to ensure smooth data flow and accessibility.

Customised algorithms: Solutions powered by AI should be tailored to the specific needs and risk profiles of the organisation, ensuring relevant and actionable insights.

User-friendly interfaces: Intuitive interfaces make it easy for auditors to interact with the system and interpret the results.

Continuous improvement: Updated AI systems based on feedback and evolving audit requirements, ensure maintenance of effectiveness and relevance.

Ethical considerations: AI should be used responsibly, with clear guidelines and oversight to ensure ethical use and data privacy.

AI regulation spotlight

Why you should be looking at AI?

AI has become increasingly important in today's world as it is revolutionising many industries. The use of AI to collect, process, and analyse large amounts of data at a faster rate than ever before is improving efficiency, reducing costs, and increasing accuracy in various fields. I am sure many of your IA functions are likely to be utilising AI in your day-to-day IA activities.

These opportunities bring with it risks that requires careful handling. AI risks can have a far-reaching impact on an organisation's reputation, customer confidence, trust as well as legal and regulatory risks.

Having a clearly defined strategy for AI adaptation as well as robust, yet flexible governance to identify and mitigate associated risks can enable your organisation to leverage the opportunities AI brings, with confidence and give assurance to key stakeholders.

There are many countries regulating AI to strengthen their potential to compete globally. This brings added complexities to your approach to compliance and risk management. Internal auditors play a crucial role in ensuring that their organisation is appropriately managing AI-related risks and are developing and deploying AI systems responsibly and ethically in compliance with these new requirements.

AI regulation spotlight

The EU AI Act

Europe's approach is to address the risks generated by specific uses of AI through a set of complementary, proportionate and flexible rules. These rules, encompassed within the EU AI Act, provide a global gold standard in ensuring that AI is human-centric and trustworthy.

The EU AI Act is a product specific regulation that is focused on the risks to users and is a first-of-its-kind regulation aiming to harmonise rules on AI models and systems across the EU. It was adopted in August 2024, with implementation phased across the next three years. It takes a risk based, tiered approach, where high risk systems are subjected to the most burdensome obligations.

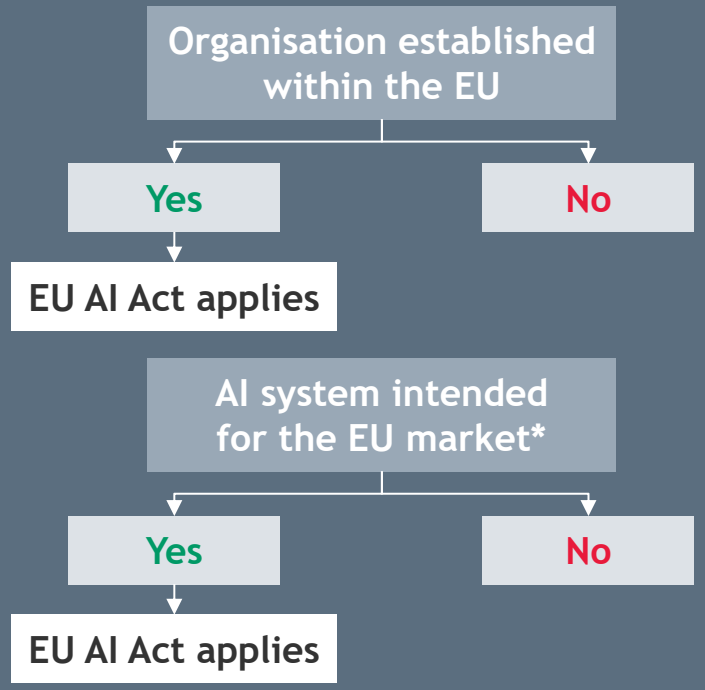
The UK

The UK government has adopted a light-touch and industry-led approach, meaning that there isn't an immediate expectation for a specific legislation like the EU Al Act in the UK.

In the UK GDPR will continue to be the key regulatory instrument in the regulation of emerging technology such as AI. The GDPR will apply to all AI systems processing personal information. The concepts of fairness, necessity and proportionality features of the GDPR are also closely aligned with the principles of data ethics. The UK GDPR incorporates obligations to address the challenges raised by AI, including duties to carry out impact assessments and restrictions on automated decisions.

AI regulation spotlight

Does the EU AI Act apply to your organisation?



When will the AI Act be fully applicable?

The AI Act which came into force August 2024, will apply in two years on 2 August 2026, except for the following specific provisions:

- The prohibitions, definitions and provisions related to AI literacy will apply on 2 February 2025
- The rules on governance and the obligations for general purpose AI become applicable on 2 August 2025
- The obligations for high-risk AI systems that classify as high-risk because they are embedded in regulated products, on 2 August 2027.

* Place on the market or put into service AI in the EU or where the output is used in the EU

AI regulation spotlight

How will the AI Act be enforced?

A robust enforcement and supervision framework is being set up, at the national level and also at the EU level. EU Member States are responsible laying down the rules on penalties and other enforcement measures for infringements of the AI Act, in line with what the AI Act provides as well as guidelines that may be issued by the European Commission. Member States have until 2 August 2025 to designate national competent authorities, who will oversee the application of the rules for AI systems and carry out market surveillance activities.

The AI Act establishes a two-tiered governance system, where national authorities are responsible for overseeing and enforcing rules for AI systems, while the EU level is responsible for governing general-purpose AI models.

To ensure EU-wide coherence and cooperation, the European Artificial Intelligence Board (AI Board) will be established, comprising representatives from Member States, with specialised subgroups for national regulators and other competent authorities.

The AI Office, the Commission's implementing body for the AI Act, will provide strategic guidance to the AI Board.

In addition, the AI Act establishes two advisory bodies to provide expert input: the Scientific Panel and the Advisory Forum. These bodies will offer valuable insights from stakeholders and interdisciplinary scientific communities, informing decision-making and ensuring a balanced approach to AI development.

AI regulation spotlight

What are the penalties for infringement?

Member States will have to lay down effective, proportionate and dissuasive penalties for infringements of the rules for AI systems. The Regulation sets out thresholds that need to be taken into account:

- Up to €35m or 7% of the total worldwide annual turnover of the preceding financial year (whichever is higher) for infringements on prohibited practices or non-compliance related to requirements on data
- Up to €15m or 3% of the total worldwide annual turnover of the preceding financial year for non-compliance with any of the other requirements or obligations of the Regulation
- Up to €7.5m or 1.5% of the total worldwide annual turnover of the preceding financial year for the supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request
- For each category of infringement, the threshold would be the lower of the two amounts for SMEs and the higher for other companies.

The Commission can also enforce the rules on providers of general-purpose AI models by means of fines, taking into account the following threshold:

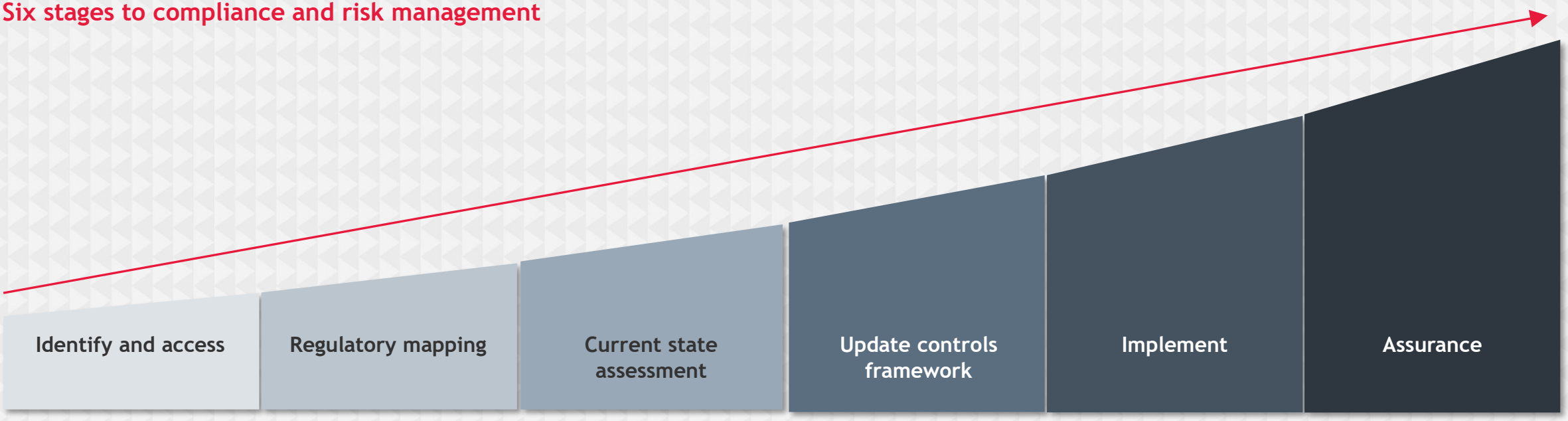
- Up to €15m or 3% of the total worldwide annual turnover of the preceding financial year for non-compliance with any of the obligations or measures requested by the Commission under the Regulation.

AI regulation spotlight

What you can expect from your organisation?

Your organisation could be at any of the below stages, however its worth remembering that many of the controls required under the AI Act may well be already embedded, for example controls around privacy and security. Internal Auditors should be actively looking to audit some of these, existing controls to ensure ongoing assurance, as the organisation moves through the six stages set out below, over the next three years.

Six stages to compliance and risk management



AI regulation spotlight

Six stages to compliance and risk management explained

1. AI system assessment and usage review

Objective: Understand the type of AI systems currently in use and how they are applied within the organisation.

Actions:

- Conduct a comprehensive review of the AI systems
- Perform an initial assessment to identify whether the EU AI Act or other regional regulations apply
- If additional AI-related regulations are discovered, the assessment approach will be revisited and expanded accordingly.

Deliverables:

- Detailed AI system assessment report
- AI Register
- Regulatory applicability summary (EU AI Act and any other relevant regulations).

2. AI regulatory mapping

Objective: Align AI usage with regulatory requirements, focusing on compliance with the EU AI Act and other applicable domestic laws.

Actions:

- Map existing AI systems against the EU AI Act
- Determine the applicability of relevant regulations, including extraterritoriality considerations
- Review and map against other local AI regulations to ensure comprehensive coverage.

Deliverables:

- Regulatory mapping report, outlining all applicable AI regulations and gaps identified.

3. Current state assessment

Objective: Gauge the organisation's current compliance level with AI regulations.

Actions:

- Engage with relevant business units to assess their current AI governance framework, focusing on how well the organisation is equipped to meet AI regulations, including EU AI Act requirements
- Provide a high-level maturity assessment report, categorising risks (RAG rating) based on current readiness.

Deliverables:

- Current state assessment report (including risk rating and areas requiring improvement).

AI regulation spotlight

Six stages to compliance and risk management explained

4. Compliance framework development

Objective: Develop a robust compliance framework for AI systems based on existing controls and industry best practices.

Actions:

- Leverage existing organisational controls and frameworks
- Build a comprehensive AI compliance plan, detailing expected controls and comparing them to the current controls in place
- Develop documentation, or 'bible', containing all necessary recommendations and processes for AI compliance.

Deliverables:

- AI compliance framework- clearly defined controls
- Compliance plan for the organisation, identifying gaps and expected controls
- AI compliance 'bible' with recommendations and procedures.

4. Implementation of control framework

Objective: Support the implementation of the developed control framework.

Actions:

- Assist the organisation in integrating the AI compliance framework into their operations
- Ensure that all control measures are implemented effectively and in alignment with the compliance plan.

Deliverables:

- Implementation support, including the development of relevant polices
- Report on control Framework and implementation progress
- Accountability framework.

5. Assurance and future review

Objective: Provide ongoing assurance and monitoring of the implemented control framework.

Actions:

- Conduct assurance reviews post-implementation to verify that controls are functioning as intended
- Offer an option for future assurance assessments, either conducted internally or by external parties
- Readiness.

Deliverables:

- Assurance report on control framework effectiveness
- Optional assurance services plan for future reviews.

Contact us

Cherry Cromarty
Partner
Risk Advisory Services (RAS)
cherry.cromarty@bdo.co.uk

Jon Dee
Partner
Risk Advisory Services (RAS)
jon.dee@bdo.co.uk

Daniel Dower
Partner
Risk Advisory Services (RAS)
daniel.bower@bdo.co.uk

Jonathan Lanes
Partner
Risk Advisory Services (RAS)
jonathan.lanes@bdo.co.uk

Sarah Hillary
Partner
Risk Advisory Services (RAS)
sarah.hillary@bdo.co.uk

Robert Noye-Allen
Partner
Risk Advisory Services (RAS)
robert.noye-allen@bdo.co.uk

Claire Robertson
Director
Risk Advisory Services (RAS)
claire.robertson@bdo.co.uk

Cherry Cromarty
Partner, Risk Advisory Services (RAS)

+44 (0) 7442 971 309
cherry.cromarty@bdo.co.uk

www.bdo.co.uk

42027472