# Deloitte.

## Global internal audit hot topics 2025

Risks and opportunities

# Executive summary

Against a volatile geopolitical backdrop, organizations are navigating risks posed by regulations, evolving technologies such as generative artificial intelligence (GenAI), and a change in workforces' needs and aspirations. In today's business environment, and with the launch of the new Global Internal Audit Standards, effective from January 2025, internal audit functions must work hard to keep pace with the fast-changing risk landscape.

We are pleased to present our perspective on the most significant risks facing organizations today and what internal audit functions should consider including in their audit plans. As boards and management continue to grapple with these topics, the need for internal audit to provide assurance and timely insights is more pressing than ever before. **Global internal audit hot topics 2025: Risks and opportunities** looks at internal audit's role in 16 topical and relevant areas including the use of GenAI in internal audit, fraud risk management, motivating the workforce, and cybersecurity. It presents our view, warning signs, fundamentals, and next steps for each topic.

We hope you find this insightful and thought provoking.

Our teams welcome the opportunity to assist internal audit functions in exploring any of these topics to embrace new risks, uncover new opportunities, and emerge stronger by tackling these unprecedented challenges. Please get in touch to discuss further.

# Content
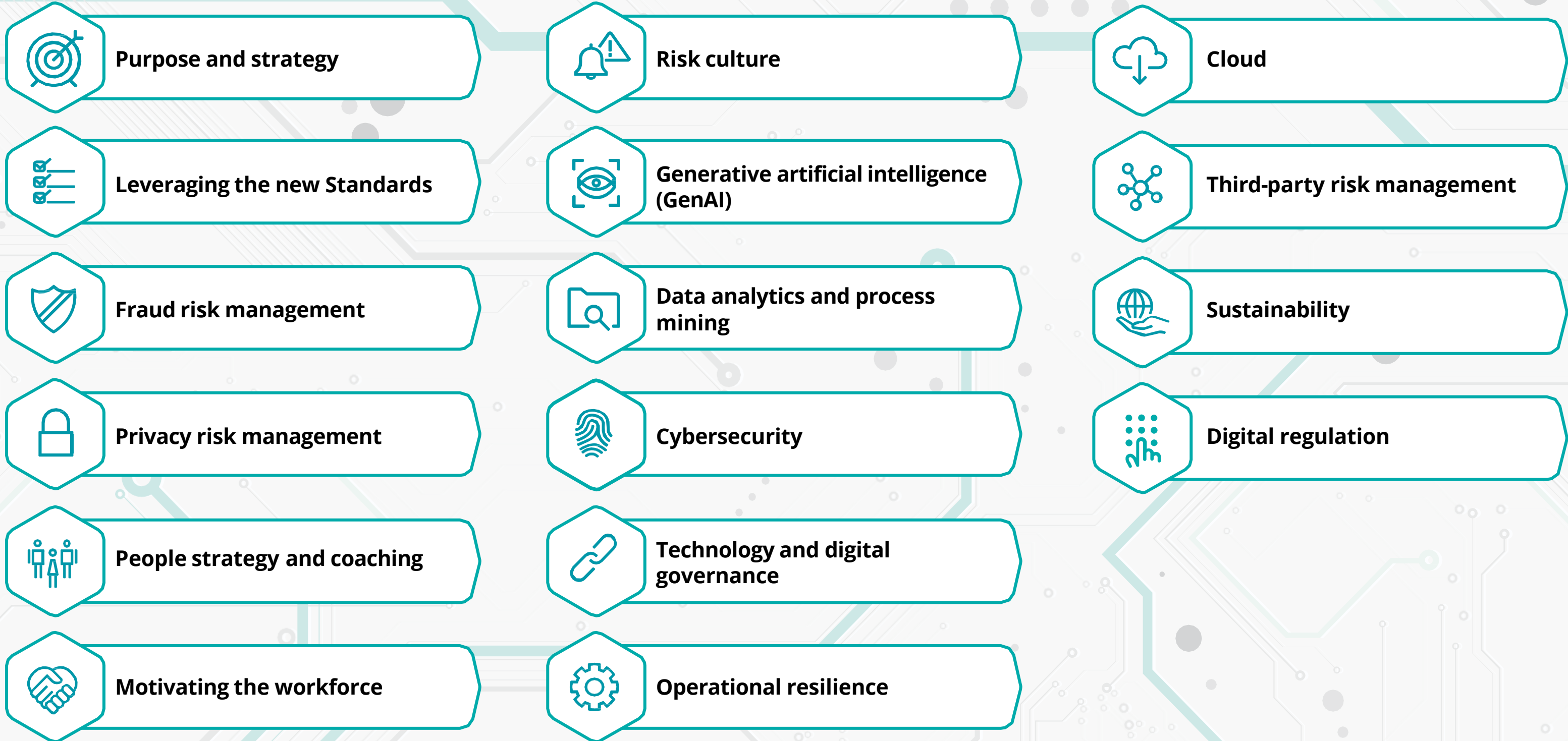
# Purpose and strategy

## Introduction

The new Global Internal Audit Standards emphasize the importance of purpose and strategy—key components of Deloitte's Internal Audit 4.0 framework, which calls for internal audit functions to align their roles and remits with their organization's purpose to maximize impact and value.

While our 2024 Global Chief Audit Executive (CAE) survey found that 82% of internal audit functions have increased their impact in the last three years, only 14% feel they have reached their full potential. CAEs must become better at articulating internal audit's value and translate it into the function's purpose. This requires CAEs to be more ambitious and willing to explore, disrupt, and reimagine their functions.

## What's new?

In our experience, internal audit functions with a high degree of alignment between their purpose, strategic objectives, continuous improvement efforts, and operational key performance indicators (KPIs) are most effective in driving high performance and impact. This clarity starts with a strategy, a key document that many functions have yet to create.

» Strategic mandate: CAEs must develop and implement a strategy aligned with organizational objectives and stakeholder expectations. This should include a vision, objectives, and enabling initiatives, and be periodically reviewed with the board and senior management.

» Purpose-driven: Strategy starts with defining the value and impact that internal audit wants to create and aligning this with the broader organizational purpose. Purpose-driven functions are more impactful by design, embedding value creation in their roles and remits, operating models, and ways of working.

» Technology-enabled: Standard 10.3 (Technological Resources) of the Global Internal Audit Standards requires CAEs to ensure that internal audit is equipped with technology that supports its ways of working and to evaluate opportunities to enhance effectiveness and efficiency.

» Collaborative development: Creating a robust and compelling strategy—and ensuring that the function has the financial, human, and technological resources to successfully achieve it—requires strategic thinking, effective stakeholder engagement, and often, dedicated sessions for brainstorming and alignment.

» A clear brand identity: Standard 6.3 (Board and Senior Management Support) underscores the importance of board and senior management support in promoting internal audit's recognition and value on a continuing basis. A clear brand identity, and providing relevant information to leadership, is crucial for securing this support.

# Purpose and strategy

## What internal audit should do

**1** Revisit and challenge your existing purpose, vision, and strategy: Conduct stakeholder feedback sessions and team workshops to envision the future needs of the organization and internal audit's role. Consider using an independent facilitator to bring fresh perspectives and constructive challenge. Think beyond current boundaries and activities to consider what is needed and what will be most impactful.

**2** Clarity and conciseness are key: Develop a concise strategy document that clearly describes the function's role and remit. This should articulate the value it seeks to provide, the objectives and key results it will target in the pursuit of this, how it will evolve its ways of working to achieve these objectives and results, and the performance measurement criteria and indicators it will use to assess progress.

**3** Measure what matters: Shift focus from process-oriented key performance indicators (KPIs) to outcome-based measures that demonstrate impact. Align performance objectives with the function's purpose and desired impact stories.

**4** Elevate the function's brand: Champion your purpose, vision, and strategy, using this as an opportunity to demonstrate internal audit's relevance to the organization's purpose and strategy. Actively engage the board and management in this process.

**5** Embrace continuous improvement: Prioritize incremental improvements over drastic changes. Foster a culture of experimentation, measurement, learning, and adaptation.

- Internal Audit 4.0
- Global Chief Audit Executive survey

## Leveraging the new Standards

## Introduction

The countdown to the Institute of Internal Auditors (IIA) new Global Internal Audit Standards (Standards), effective as of January 9, 2025, has begun.

The new Standards are intended to raise the bar for internal audit globally. Functions are noting that the ability to demonstrate conformance is leading to most having to update key artifacts including their charter, methodology, board and senior management communications, and team training plans. Others are looking to take advantage of the opportunity presented by the Standards to define or reset the function's purpose and longer-term vision, tailored to that of the broader organization that they serve.

It is crucial that internal audit functions are well-prepared. The time to accelerate and finalize readiness activities is now.

## What's new?

» Timely compliance: Key stakeholders including the Audit Committee will expect functions to conform with the Standards or have clear plans to bridge any gaps. Some functions have been delayed from starting their readiness activities, either by not sufficiently considering their conformance gaps, or through a need to prioritize plan delivery.

» Self-assessment at the individual requirement level: The Standards require functions to perform periodic self-assessments of conformance. Detailed self-assessments at the individual requirement level are critical to avoid future conformance issues. We are seeing significant variation in the level of detail that functions have worked to when documenting their self-assessments.

» Engagement with the board and senior management: This will be required to fully realize the benefits intended by the newer elements of the Standards and will be key to help develop a forward-looking internal audit strategy, with a clear vision, aligned to the broader organizational objectives.

» Training: Many functions have already identified gaps around training their people, with plans focused on enhancing the design of ethics-based training and being confident that their team members are maintaining their continuing professional development (CPD). Few functions have plans to provide teams with training on the new Standards more broadly, despite readiness activities typically being performed by a relatively small number of individuals charged with quality or methodology oversight.

» Future developments: For UK-based organizations the bar is likely to raise further still. For example, the IIA has been consulting on a revised, combined internal audit Code of Practice, which will cover internal audit functions in all industries and sectors, and which was launched in the United Kingdom in September 2024. Other global developments are likely to follow.

# Leveraging the new Standards

## What internal audit should do

**1** Accelerate readiness activities: Functions should be looking to accelerate completion of readiness activities to meet stakeholder expectations in line with the compliance deadline.

**2** Challenge the completeness of readiness self-assessments and action plans: Investing time now to clearly document your self-assessment, in line with individual requirements and in sufficient detail, will ensure that action plans are comprehensive. It will also bring added benefits when performing future periodic self-assessments in terms of repeatability and efficiency.

**3** Use this as an opportunity to enhance your function's brand within the organization: Forward-thinking functions are using the release of the new Standards to act as a springboard, not only to align on roles and responsibilities, but to enhance internal audit's position, by demonstrating clear relevance to the broader purpose and vision of the organization.

**4** The below are hot spots that should be factored into internal audit training programs, if not included already:

- Ethics and professionalism

- Broader education on the requirements of the new Standards

- Required updates/changes to audit methodology resulting from the requirements of the new Standards

**5** Prepare for the UK IIA Code of Practice (and for those outside of the United Kingdom, watch for similar developments locally): Once released, all functions should read and understand the new requirements placed on them by the new internal audit Code of Practice. Appropriate actions, coordinated with Standards readiness plans, will then need to be taken to ensure conformance with the new requirements of the Code.

- Internal Audit 4.0
- Global Chief Audit Executive survey

# Fraud risk management

## Introduction

Fraud is now the most common criminal offense in most jurisdictions globally, and organizations across all industries and sectors continue to suffer sustained financial and reputational losses. As a result, there are increasing expectations and requirements on organizations to prevent, detect, and deter fraud.

In an environment where fraud is an ever-increasing threat and where fraudsters continue to evolve and advance their techniques, internal audit must rise to this challenge, evolving from watchdog to vigilant guardian of organizational integrity.

## What's new?

» Delivering organizational value:  Leading internal audit functions are evolving beyond traditional assurance to actively contribute to tangible savings by bolstering fraud prevention and detection efforts, directly impacting their organization's bottom line.

» The expanding battlefield—non-financial fraud risk: Internal audit's focus must evolve beyond traditional financial statement fraud to encompass the rising tide of non-financial fraud risks. This includes areas such as misrepresentation of environmental, social, and governance (ESG) data, fraudulent customer interactions, and manipulation of safety or quality control data.

» Evolving regulations: Organizations need to meet increasing regulatory requirements aimed at strengthening fraud prevention and detection frameworks. For example, the United Kingdom's Failure to Prevent Fraud Offence has global extraterrestrial powers and places a greater onus on organizations to proactively prevent fraud, while other jurisdictions are considering similar legislation. Internal audit functions must be aware of and adapt to these evolving regulations, to ensure that their organizations remain compliant.

» Embracing the power of technology: With fraudsters leveraging technology in increasingly sophisticated ways, internal audit functions need to be knowledgeable about emerging technologies and how they can be used to enhance fraud detection efforts. Data analytics and artificial intelligence, for example, can be used to identify patterns and anomalies that may indicate fraud.

» Unmasking the human factor: While technology plays a crucial role, it's essential to remember that fraud often involves human actors exploiting weaknesses in systems or processes. Internal audit should also delve into understanding the human factors that contribute to fraud (i.e., the Fraud Triangle) and support strategies that mitigate these risks.

# Fraud risk management

## What internal audit should do

**1** Prioritize fraud risk in audit plans: Internal audit functions should routinely review and incorporate the organization's fraud risk assessment findings into their periodic internal audit planning activities. This linkage is critical so that audit plans focus on the organization's most significant fraud risks.

**2** Demonstrate targeted fraud assurance: Within internal audit plans and scoping documents, clearly articulate the specific fraud risks derived from the organization's fraud risk assessment and how they are being addressed. This transparency demonstrates how internal audit is focused on providing assurance against the organization's most pressing vulnerabilities.

**3** Assess fraud risk management maturity: Conduct a comprehensive, enterprise-wide fraud risk management maturity assessment to evaluate the organization's ability to prevent and detect fraud. This provides valuable insights for improvement and strengthens the organization's overall fraud resilience. Areas to assess should include fraud risk assessment; anti-fraud controls; policies and procedures; training and awareness; monitoring and review; and governance and culture.

**4** Cultivating specialist expertise: Internal audit functions should proactively develop and cultivate specialist skills in fraud detection, investigation, and data analytics to effectively address evolving fraud risks. Consider specialized training (e.g., interview techniques, data analysis techniques) and certifications (e.g., CFE) for internal auditors.

**5** Leverage data analytics and artificial intelligence (AI) for impact: Internal audit should harness the power of data analytics and AI to enhance the effectiveness and efficiency of fraud-related audits. This includes using data analysis techniques for targeted sample selection, identifying anomalous transactions or patterns indicative of fraud, and visualizing complex data sets to gain deeper insights into key fraud risks.

- Fraud - National Crime Agency
- Economic Crime and Corporate Transparency Act: failure to prevent fraud offence - GOV.UK
- Fraud 101: What is Fraud?

# Privacy risk management

## Introduction

The General Data Protection Regulation (GDPR) was introduced in 2018 (other regulations may apply in other countries, but the GDPR principles discussed here equally apply more broadly) to protect individuals' fundamental rights and freedoms and for organizations to maintain trust with their customers. This is becoming increasingly important given the high volumes of digital data now being processed, a greater focus on embedding AI into collecting and processing data, and the increasing frequency and impact of cyber incidents.

We have seen organizations continue to struggle to demonstrate their compliance with the core GDPR principles, often because updates required by other regulatory changes have been prioritized. In addition, the increasing complexity and amount of data being processed has made it difficult to effectively identify the personal data being both processed and held, resulting in organizations being unable to implement the right safeguards to manage this risk.

Regulators are holding organizations accountable, with GDPR fines being issued across multiple areas of the requirements, including insufficient legal basis for processing, inappropriate website cookies and marketing practices, and failing to respond to information access requests in a timely manner.

Effective privacy risk management helps organizations:

- Build and maintain trust: Demonstrating a commitment to privacy builds transparency and trust with customers, employees, and partners.

- Enhance business operations: Implementing a strong privacy framework can streamline data processing activities, improve data quality, and reduce the risk of data breaches.

- Protect individual rights: Embedding processes to facilitate individuals' rights creates efficiency and puts safeguards in place to respect individual choice.

- Mitigate regulatory penalties: Compliant processes aligned to regulatory requirements reduces the risk of fines, legal action, and reputational damage.

## What's new?

≫ Focus on enforcement: Regulators are becoming more proactive and stringent in enforcing privacy laws, issuing substantial fines for noncompliance. For example, the GDPR regulator has issued multiple fines for inappropriate direct marketing campaigns, including spam texts and emails. Organizations must be fully transparent and provide customers with sufficient information when opting in.

≫ Artificial intelligence: The use of AI and GenAI introduces new privacy risks related to bias, transparency, and automated decision-making. Organizations need to develop and embed trustworthy AI practices.

≫ Increased use of cloud computing: Storing and processing data in the cloud raises concerns about data security, third-party access, and cross-border data transfers. Organizations should understand where and how data is processed and be able to evidence this for regulators.

≫ Growing consumer awareness: Individuals are becoming more aware of their privacy rights and are increasingly concerned about how their data is being used, choosing to share their data more selectively. Organizations should openly communicate how they process data through privacy notices.

≫ Focus on data minimization and purpose limitation: Organizations are being encouraged to collect and retain only the personal data that is necessary and to use it only for the purposes for which it was collected. Individuals should have a choice in what data they share, if it is optional.

# Privacy risk management

## What internal audit should do

The local privacy regulator provides guidance and material for organizations, to support them in compliance. This may include an accountability tracker that organizations can use to evidence their compliance.

**1** Scope and coverage of key areas: Audit plans should assess the privacy framework that the organization aligns to and encompass a review of key privacy risk areas, such as data governance, privacy by design, data retention policies, vendor management, incident response procedures, and employee training programs.

**2** Privacy by design: Review whether the organization has completed Data Protection Impact Assessments (DPIAs) to determine if it has assessed the risk of its processing activity and has successfully implemented the resulting privacy controls to mitigate the risks identified.

**3** Records of Processing Activity (ROPA): Organizations are required to document their processing of personal data and legal basis for doing so. Internal audit should be able to follow samples of activity to confirm the breadth and depth of the ROPA and the reason for the processing.

**4** Data subject rights: Assess the organization's processes for handling data subject requests (e.g., access, correction, deletion) to ensure compliance and fairness.

- IAPP Privacy and Consumer Trust Report – Executive Summary
- Managing Cybersecurity and Privacy Risks in the Age of Artificial Intelligence: Launching a New Program at NIST | NIST
- Privacy Risk Management

# People strategy and coaching

## Introduction

Internal audit remains, at its heart, a people business, and therefore alongside digital transformation, there is a compelling need to amplify the focus on soft skills including critical thinking, communication, and emotional intelligence. In our 2024 Global Chief Audit Executive (CAE) survey, high-performing internal audit functions typically allocate 50–75 hours of training per auditor, yet this time is not always put to best use. The challenge of having sufficient, appropriately skilled staff is exacerbated by the increasing prevalence of burnout, which almost a fifth of functions identify as a pressing issue for their teams. The growing challenge of attracting and retaining top talent in internal audit further compounds the difficulties faced. As functions look to the future, the emphasis on people is paramount, and developing a robust people strategy and coaching framework for their own team will be critical.

## What's new?

» The emergence of GenAI will affect the operational landscape for internal audit. Functions are prioritizing the development of their people to complement AI-powered analytics and robotic process automation, enhancing risk assessment and audit procedures. However, these benefits can only be realized with digitally enabled people.

» Our CAE survey revealed that the digital skills gap has prompted 91% of functions to place a strong emphasis on training and development. We understand that many functions want to do more to develop their people, and having a clear people strategy will help enable this.

» It's crucial for internal audit to acknowledge the significance of soft skills to develop a workforce adept at navigating technology, while demonstrating empathy and sound ethical decision-making. This highlights the central role of people in the digital transformation of internal audit functions.

» High-performing functions embrace the "learn, do, teach" mindset, creating a culture that values the development and empowerment of people within the internal audit function. The challenge is to maintain this culture of continuous learning and knowledge-sharing amid resource constraints.

» The introduction of the new Global Internal Audit Standards in 2025 underscores the importance of people, requiring internal auditor learning and development plans to be closely linked to internal audit strategy. The challenge is to align the plans with the evolving needs of both the internal audit function and the broader business environment.

## People strategy and coaching

### What internal audit should do

**1** Establish a robust, forward-looking competency framework that not only focuses on short-term audit delivery but also looks to fulfill all aspects of a function's strategy, encompassing technical proficiency, industry-specific knowledge, and soft skills. The framework can be used to drive decision-making by identifying skill gaps, thereby leading to more tailored training programs, and better alignment of individual development plans with the goals of the internal audit function.

**2** Promote a holistic talent development approach by ensuring that training plans include both technical and soft skills. Encourage cross-functional collaboration through knowledge-sharing and offer opportunities for interpersonal skills development. Embrace AI as a way to alleviate staff burnout by automating tasks and providing real-time insights, as well as enabling predictive analytics to identify workload patterns. This allows functions to proactively manage workloads and better support employee well-being.

**3** Foster a culture of continuous learning and upskilling in AI-related competencies. This can empower internal audit professionals to better explore how GenAI can be used as a strategic enabler in their operational endeavors for example.

**4** Incorporate learning activities into the audit plan including knowledge-sharing sessions, cross-functional training, and post-audit debriefs. Allocate time and budget for training and coaching, promoting a culture of challenge, iteration, and innovation. This approach develops vital skills for future-ready functions.

**5** Harness people data for talent development purposes, such as performance metrics, skill self-assessment surveys, and feedback scores. Internal audit professionals can utilize this data to demonstrate the positive impact of their people strategy, help inform decision-making, and derive actionable insights for talent development and succession planning within the function.

- Global Chief Audit Executive survey

# Motivating the workforce

## Introduction

The quiet hum of automation becomes closer and more widespread, the allure of remote work lingers, and a new generation questions the meaning of "climbing the ladder." In this era of rapid change, businesses face a critical challenge: maintaining a highly motivated workforce. This isn't just about employee satisfaction; it's about ensuring the quality, innovation, and resilience of crucial delivery and oversight functions within organizations. A disengaged workforce can lead to missed risks, decreased productivity, and ultimately, organizational vulnerability. Conversely, a motivated team is more likely to exhibit curiosity, proactively identify and respond to emerging risks, and provide insightful recommendations, ultimately enhancing corporate governance and business performance. Internal audit can play a key role in helping with workforce motivation, both within the internal audit team itself and more broadly across the organization and industry in which it operates.

## What's new?

⟫ The silent threat to your bottom line: A demotivated workforce can pose significant challenges for businesses. Low morale can cripple productivity, stifle innovation, and open the door to increased errors and even fraud. Internal audit needs to sound the alarm and make sure that this hidden risk gets the attention it deserves.

⟫ Mission statements versus reality: Every company loves to push an inspiring purpose and vision, but these can often feel like empty words. When employees experience a disconnect between stated values and the daily grind, demotivation festers. Internal audit can help bridge the gap, ensuring those statements translate into a workplace where employees feel valued and engaged.

⟫ Unleashing the power of change: Internal audit is uniquely positioned to be a powerful force for positive change. By shining a light on the risks of a demotivated workforce, working hand in hand with management to develop effective strategies, and monitoring the impact of implemented changes, internal audit can help transform the organization from the inside out.

⟫ Reimagining internal audit: Many would agree that nobody likes to be audited. But what if internal audit could become a dynamic partner driving organizational success? By understanding the root causes of demotivation and collaborating with the business to find solutions, internal audit can provide invaluable support to create a more positive and productive work environment. This involves broadening its purpose to encompass not just assurance, but also advise, anticipate, and accelerate organizational learning by challenging the status quo and fostering continuous improvement.

⟫ Walking the talk: Internal audit departments must practice what they preach. By fostering a culture of open communication (promoting psychological safety), providing opportunities for professional growth, and celebrating team successes, internal audit leaders can ensure their own teams are motivated, engaged, and ready to tackle the challenges ahead.

14

# Motivating the workforce

## What internal audit should do

**1** Hit the accelerator on demotivation risk: Don't wait for low morale to snowball into a full-blown crisis. Internal audit should actively assess the risk of a demotivated workforce within the organization, using data-driven insights and employee feedback mechanisms. Elevate this risk to audit committees and business leaders, providing clear and compelling evidence to accelerate understanding and response.

**2** From the sidelines to the strategy table: Internal audit should not be a passive observer when it comes to addressing workforce motivation. Proactively engage with management in the development and assessment of plans and strategies to improve employee engagement. Offer insights from audit findings, share best practices, and advocate for solutions that address the root causes of demotivation.

**3** Measure impact, not just activities: Move beyond simply reporting on audit findings and recommendations. Internal audit should demonstrate value by measuring and showcasing the tangible impact of management actions taken in response to its work. By aligning with Principle 11 of the new Global Internal Audit Standards, and presenting findings to the audit committee and business leaders in a way that resonates with their priorities, internal audit will help demonstrate how improved employee motivation translates into tangible business outcomes.

**4** Cultivate innovation through psychological safety: A culture of psychological safety within the organization and within your own internal audit team is critical. Encourage employees to speak up, as outlined in Domain II of the new Standards, share ideas, and challenge the status quo without fear of retribution. By fostering an environment of trust and openness, you can unlock the collective creativity and problem-solving abilities of the workforce, thereby raising motivation.

**5** Time for an honest self-reflection: If we broaden the remit of what internal audit functions do, we need to look at who is doing it. This requires a critical self-reflection: Does your current internal audit strategy truly inspire and motivate your own people, or is it merely a collection of empty words? Furthermore, consider the people agenda: What capabilities and behaviors are needed within your internal audit team to effectively test and influence culture, ultimately driving positive change? Investing in the development of your people will be crucial to successfully navigate this evolving landscape.

• Internal Audit 4.0

# Risk culture

## Introduction

Organizations with a strong desirable culture overall, and risk culture more specifically, outperform those with undesirable cultures. They tend to be more trustworthy and appealing to customers and employees alike and are better placed to achieve long-term sustainability. Setting or transforming a business culture should be an active and conscious process incorporating design thinking, agile executions, culture enablement coaches, and other culture tools and accelerators.

## What's new?

» A risk-intelligent and purpose-led culture (i.e., one that has values at the forefront and is consistently driven by these) is not only a regulatory priority but also has business benefits and is critical for supporting good customer outcomes. A risk-intelligent culture means that everyone understands the organization's approach to risk, takes personal responsibility to manage risk in everything they do, and encourages others to follow their example.

» Best practice is for an organization to define a compelling cultural aspiration that is aligned to its mission, vision, values, and strategy.

» Before a business can seek to change its culture, it will need to appropriately assess the culture to understand the existing behaviors and mindsets and the shifts needed to achieve transformational culture change. There are several ways organizations can assess their risk cultures—through diagnostic surveys, focus groups, interviews, leadership labs, and risk culture gap analysis.

» Risk culture measurement metrics enable boards and executive teams to gain a better understanding of their organization's risk culture to make informed decisions on cultural matters. Defining an appropriate set of risk culture metrics will be an iterative process that organizations should be thinking about starting now.

» Trust is an organization's most valuable asset. It resides in the value proposition; in leadership; among the workforce; and in the minds of customers, suppliers, the community, and other stakeholders. Increasingly organizations are looking at their trust equity, that is, the amount of trust accumulated with key stakeholders over time. This includes internal stakeholders (e.g., employees) and external stakeholders (e.g., customers, regulators). Organizations that build trust equity typically outperform the competition, enhance workforce engagement, and build customer loyalty.

16

# Risk culture

## What internal audit should do

**1** Risk culture assessment: Consider an organization-wide risk culture infrastructure review and risk culture diagnostic survey, including industry benchmarking. This could also be considered as part of individual audits, looking at dimensions such as embeddedness of duty, governance, or board effectiveness.

**2** Tone at the top: Evaluating the influence of senior management and the board on shaping the risk culture and demonstrating ethical decision-making is another area that internal audit could consider. The influence of middle management should also be included in scope. This can be evaluated via surveys or deeper-dive activities such as focus groups or interviews.

**3** Risk culture governance: Functions may want to include a review focusing on the effectiveness of the risk governance framework in promoting a strong risk culture.

**4** Employee training and awareness: Internal audit should consider assessing the adequacy of training programs and communication strategies aimed at enhancing risk awareness.

**5** Risk reporting: Internal audit can consider a review of the metrics suite that covers key dimensions of the organization's population demographics, and which will be able to track trends over time. The range of metrics, balancing qualitative and quantitative, how they have been defined, and reporting accuracy would be important scope elements.

- Benchmark_of_Ethical_Culture_LRN.pdf

# Generative artificial intelligence (GenAI)

## Introduction

Generative artificial intelligence (GenAI) represents a groundbreaking type of machine-learning model that focuses on creating new data rather than simply making predictions. Its potential to revolutionize work processes and business data interactions, accelerating operations and uncovering innovative opportunities, has been clearly demonstrated across organizational areas, such as chatbots for customer interaction, virtual assistants, code generation, and much more.

For internal audit, the emergence of GenAI presents unparalleled opportunities for functions to enhance efficiency and quality, and to impact at all stages of the audit life cycle including risk assessment, audit planning, automated testing, working paper generation, report drafting, audit committee summaries, and issue tracking. Additional benefits beyond the life cycle exist, too, such as automated resource scheduling or curated learning paths based on skills gaps. According to our 2024 Chief Audit Executive (CAE) survey, nearly 40% of functions are planning substantial investments in GenAI within the next one to three years.

## What's new?

» The adoption of GenAI is a journey: Functions are beginning to explore use cases while simultaneously evaluating technology options and addressing challenges such as access to large language models, whether on-premises or through hyperscalers and other software-as-a-service providers; data security; and team readiness.

» Balancing risks and opportunities: Internal audit functions will need to assess the risks and opportunities associated with GenAI. The benefit of efficiencies gained from reduced manual effort needs to be balanced with the need for appropriate governance and controls over accuracy and accountability of output.

» The way we work will change: GenAI can be used to accelerate routine tasks such as drafting initial audit scopes, creating initial risk and control matrices, compiling standard reports, and tracking of open audit findings, among others. This creates space for auditors to focus on higher-level analysis, strategic thinking, and ad hoc problem-solving, leading to a more engaging and rewarding work experience.

» Data governance is increasingly important: The audit team may need to strengthen data governance practices to ensure the accuracy, security, and integrity of the data used by GenAI systems for auditing purposes. While this is already a focus area, it is often at a low stage of maturity and will need to improve at pace to ensure that functions are ready for the impact of GenAI tools and are able to deploy them safely.

» Evolving regulatory landscape: Rapidly evolving regulations around GenAI usage will require organizations and internal audit functions to pay close attention to remain compliant across all operational geographies.

# Generative artificial intelligence (GenAI)

## What internal audit should do

**1** Develop the GenAI aspect of your digital strategy: Internal audit should determine the potential of GenAI to facilitate achieving broader, functional goals. Existing strategies for digital should extend beyond GenAI to cover other areas of machine learning and existing data management systems. Common areas include report generation, methodology chatbots, audit committee summarization, or quality assurance coaches.

**2** Increase digital literacy: Internal auditors should engage with learning and development now. Although not everyone needs to become a digital expert, being familiar with the terminology and potential of GenAI tools will accelerate its adoption.

**3** Collaborate with technology teams: Functions should familiarize themselves with their organization's stance toward GenAI, from both data privacy and security perspectives. They should also understand the organization's appetite for shaping existing solutions within its environment.

**4** Clean up your data: Data quality is crucial for GenAI's efficacy. As with other departments within the organization, internal audit should revisit its data management practices and ensure that data and records held are up-to-date to realize the value GenAI can deliver.

**5** Establish good governance: Functions should consider the governance structure required to manage the risks associated with using GenAI. This should include controls around the use, development, testing, and ongoing monitoring of GenAI. Again, functions will want to consider how best to align to their organization's overall approach to GenAI governance.

- Global Chief Audit Executive survey

# Data analytics and process mining

## Introduction

Data analytics plays a critical role for internal audit by enabling the detection of anomalies, enhancing audit quality, and improving efficiency through automation. It also helps identify trends and can provide valuable insights for process improvement.

In this rapidly evolving digital era, the significance of data analytics has become even more pronounced, with 62% of functions identifying it as a key investment area over the next one to three years, according to our 2024 Chief Audit Executive (CAE) survey. However, functions are at different stages of maturity when it comes to the use of analytics, with more mature functions deploying advanced techniques, including an increased consideration of process mining.

## What's new?

⟫ Successful implementation of data analytics requires a strategic approach: A clear strategy that focuses on the end goal is key to success. Implementing data analytics, whether basic or more advanced, such as process mining, requires access to appropriate data, skills and knowledge, and appropriate tools, all of which require the right level of planning for functions to set themselves up for success.

⟫ Consider cost-benefit across the lines of defense before investing: Investment in tooling such as process mining can come with high costs, so it is important for functions to assess the benefit expected before deciding what to focus on first. Collaboration between internal audit and other lines of defense may yield a better return on investment, while also creating a more holistic approach to process improvement and risk management.

⟫ The quality and availability of data is crucial for accurate results: While more advanced techniques such as process mining can be valuable in revealing hidden insights, the benefit is better realized by functions that have access to the right, accurate data.

⟫ Advanced process mining tools are suited to complex business processes: Process mining is an advanced approach to data analytics used to analyze how processes are executed in practice. It can be helpful in identifying bottlenecks and inefficiencies. Organizations with simple processes may not get the full benefit from advanced process mining tools; however, analyzing process data is still highly valuable, and simpler techniques could be employed using more common analytics tools to achieve the same objective. We have seen functions use more traditional means to analyze data and create process flows in visualization tools to achieve the same insights but on a smaller scale.

⟫ Maturity levels vary across organizations: Our CAE survey indicated that only 23% of functions were planning to invest in process mining in the next one to three years. We believe this is largely due to the benefit of process mining being realized by mature functions only, compared to those earlier on in their journey who are choosing to prioritize building a strong foundation of analytics first.

20

# Data analytics and process mining

## What internal audit should do

**1** Develop a clear strategy: Functions should look to integrate data analytics into their broader internal audit strategy. Considerations should include how tools can facilitate more efficient and comprehensive audits, and what the function wants to achieve with these technologies.

**2** Focus on data quality and availability: Internal audit should work with relevant stakeholders to ensure that necessary data is accessible and of sufficient quality to support data analytics. This may involve collaborating with IT teams to extract and prepare data for analysis.

**3** Invest in suitable tools: Functions should consider the technological needs of data analytics and process mining to deliver desired goals. This may involve investing in new software or tools.

**4** Understand the organization's processes: Internal audit should gain a comprehensive understanding of the organization's key processes, including systems, data sources, and the end-to-end flow of activities. This understanding forms the foundation for effective data analytics.

**5** Training and skills development: Internal audit should invest in training and skills development for team members to build expertise in data analytics. This may involve formal training on process mining tools and methodologies, as well as developing data analysis and visualization skills.

- Global Chief Audit Executive survey

# Cybersecurity

## Introduction

Why is it important? In one word—cost. Organizations simply can't afford to be dealing with all the ramifications of a successful cyberattack, which can include disruption, diversion from value-add projects, lengthy remedial work, potential litigation, regulatory fines, and other compliance issues. Ensuring appropriate security has never been more important. The threat is constantly evolving and growing. Cyberattacks have been industrialized and with increased digitalization the impacts are felt across the organization. Organizations can't take their eye off the ball when it comes to meeting the challenge of maintaining security.

One thing that remains unchanged is the gap between the need for cybersecurity skills and their limited supply. For example, last year, the UK government advised that 50% of all UK businesses have a basic cybersecurity skills gap, while 33% have an advanced cybersecurity skills gap. The recruitment industry has advised that 75% of employers who operate in the cybersecurity space to provide services to organizations are likely to recruit additional permanent staff throughout 2024. This is potentially a response to the lack of in-house skills.

## What's new?

» We've seen the emergence of artificial intelligence (AI) tools as a genuine mainstream competence that is being used to both drive new attack vectors and build defenses. Crucially, AI allows attacks to be scaled up in terms of speed and complexity, due to factors such as:

- More sophisticated and elaborate phishing campaigns are possible.
- Attacks involving deepfakes have the potential to cause serious reputational damage. An example is where voice and facial imitation has been used to gain access to bank accounts or sensitive commercial information.
- Some organizations have failed to protect their own AI tools against external attack; for example, where models have been built insecurely and taken over.
- GenAI tools have also been attacked. This can result in data being stolen or your session being hijacked and used to attack your systems.

» There are new regulatory obligations that are driving international oversight of cyber risk and privacy. These include the Securities and Exchange Committee (SEC) rules on cyber disclosure that were introduced in 2023 and the Network and Information System Directive 2 cybersecurity legislation adopted by the European Union. The latter legislation requires EU organizations to strengthen their overall level of cybersecurity and improve resilience. Meanwhile the United Kingdom is working on its own proposed legislation.

» Beyond the constant threat of widespread, opportunistic cyberattacks, organizations are now facing a surge in sophisticated, targeted attacks. This alarming trend is often attributed to the escalating involvement of nation-states and their agencies, reflecting the growing influence of geopolitics and global conflicts on the cybersecurity landscape.

» The ever-expanding network of third-party relationships presents a growing challenge. A recent security scorecard study revealed that 29% of recent data breaches stemmed from third-party vulnerabilities. Furthermore, supply chains were identified as the source of a staggering 62% of system intrusion attempts. Recognizing the cascading nature of these risks, some organizations are turning their attention to fourth-party risk management. This involves scrutinizing how their third-party vendors manage their own subcontractors and agents.

» Reports indicate that cybercriminals used social engineering techniques in 20% of all data breaches last year. Worryingly, these attacks are evolving beyond opportunistic exploits, often unfolding over extended periods and utilizing technology and AI.

22

# Cybersecurity

## What internal audit should do

**1** Internal audit plays a crucial role in elevating cybersecurity to a top priority on the board's agenda. In addition, the board needs to maintain a vigilant and adaptive approach to risk oversight. Internal audit should champion this ongoing focus by ensuring that comprehensive cyber risk analysis and reporting are embedded within board-level discussions and decision-making processes.

**2** Internal audit should review cyberthreat intelligence capabilities, including scenario modeling and horizon scanning capabilities, as a critical component of the security infrastructure.

**3** Internal audit should consider assessing the effectiveness of cybersecurity awareness within the organization. Conducting a culture review that incorporates targeted questions can provide valuable insights into whether cybersecurity messages are truly resonating with employees. A comprehensive strategy is needed with staff acting as the first line of defense.

**4** Internal audit within government and the public sector should consider alignment with the National Cyber Security Centre's Cyber Assessment Framework (CAF) as the new leading standard for cybersecurity assurance. The CAF emphasizes an outcome-based approach, requiring organizations to demonstrate achievement of key cybersecurity outcomes rather than simply implementing specific technical controls.

**5** Internal audit teams are increasingly scrutinizing assurance models to gain greater confidence in their organization's management of cyber risks. These models provide a consolidated view of all internal and external assurance measures, often benchmarked against established frameworks like NIST, and they often highlight gaps. Typically, while preventive controls tend to have robust assurance coverage, reactive controls, such as incident management plans, frequently lack sufficient review.

- Cyber security skills in the UK labour market 2023 - GOV.UK
- The 2024 Compliance and Financial Crime Salary Survey Guide | Barclay Simpson
- Cyber security sectoral analysis 2024 - GOV.UK
- Cyber security risks to artificial intelligence - GOV.UK
- NSA 2024 - Overview of SOC - National Crime Agency

# Technology and digital governance

## Introduction

The establishment of an effective technology and digital framework represents one of the biggest areas of both risk and opportunity for organizations. Optimized frameworks can deliver cost reductions, support management of risks in line with appetite, and enable innovation and delivery of strategic goals. This is particularly important in the cost constrained environment in which many organizations currently operate. Recent major global incidents reinforce how important it is for organizations to get this right.

## What's new?

》》 Visibility and understanding of technology by senior leadership: With the continued fast-paced nature of technological change, even IT practitioners can struggle to maintain an adequate knowledge of the evolving technology landscape. The lack of a clear understanding and foresight of potential changes makes it difficult for boards, executives, and senior leadership to effectively challenge technology strategy, investment, and business-as-usual (BAU) activities.

》》 Increased focus on delivering and measuring value from IT: Boards should continue to challenge chief information officers (CIOs) and chief information security officers (CISOs) to ensure they can demonstrate that effective governance structures are in place, and that the service and performance of these functions are proactively and effectively managed. These teams must deliver value for money to the business and help protect the organization from technology, digital, and cyber risks.

》》 Reporting on technology risk: The information available to those charged with governance of technology delivery is often insufficient, particularly in key areas such as technology risk management and technology risk appetite.

》》 Risk management culture and practices: In many organizations the culture around technology governance is not where it needs to be. Technology practitioners are stretched on day-to-day delivery, and matters of governance and risk management may not be given adequate focus. For example, lessons learned from breaches or bypassing of controls, reported by staff, may not be followed up on.

》》 There is a general lack of adherence to established IT governance frameworks: The ISO/IEC 38500:2015 standard as well as Control Objectives for Information and related Technology (COBIT) should be leveraged by functions in their assessments of organizational compliance against established IT governance frameworks. Such frameworks center on four pillars: strategic alignment (strategic IT planning and organizational structure); IT risk management (risk management structures, policies, and processes); resource management (resource planning including capacity and capability; IT third-party management), and value delivery and performance measurement.

# Technology and digital governance

## What internal audit should do

**1** Perform a holistic review of technology governance: Internal audit should consider including a review of technology governance and risk management in their plans. Assurance should focus on key aspects of their technology environment, such as strategy, resourcing and capability, risk management, operating model and organizational structure, and value delivery and performance monitoring.

**2** Understand the technology environment and develop a tailored plan: Internal audit should invest time to understand the technology environment and the risks within it, in order to best tailor the audit plan to provide appropriate coverage of technology risks.

**3** Understand how the technology risk appetite has been defined and is used for monitoring: Internal audit must also understand how the organization is setting technology risk appetite and how it is then used by the business as a tool to measure risk profile on an ongoing basis.

**4** Technology culture: Assessing the culture within the organization (both within and outside the technology department) is another key review for the overall assessment of technology governance, which functions should incorporate in their plans.

**5** Review technology governance on a cyclical basis: Ensure that reviews of technology governance remain a key component of the technology audit plan on an ongoing basis. For example, consider rotating coverage against the four core areas:

- Strategic alignment (strategic IT planning and organizational structure)

- IT risk management

- Resource management including third-party management

- Value delivery and performance measurement

# Operational resilience

## Introduction

Resilience has been one of the most crucial areas of focus for organizations across all industries over the past few years. While the regulatory focus has primarily been in Financial Services (in the European Union and United Kingdom, for example), the business advantages of being a more resilient organization apply across all sectors.

Within financial services, firms should be starting to think beyond the current looming set of compliance deadlines (for example, the March 31, 2025, deadline in the United Kingdom for full compliance with PRA SS1/21 and FCA PS3/21, and the January 17, 2025, deadline for compliance with DORA) to the transition to BAU resilience capability. Wider industry sectors should consider the benefits and lessons learned from the financial services sector, to enhance their resiliency in a cost neutral/profit enhancing manner, when compared to their historical losses experience.

More generally, organizations should also be thinking about how to assess their organization's consideration of climate change and other environmental risks in its resilience planning, as well as evaluating preparedness for disruptions arising from geopolitical instability, including political unrest, trade wars, and sanctions. Rapid technological advancements should be acknowledged as well when addressing potential risks and opportunities, such as around artificial intelligence and cloud computing.

## What's new?

» While targeted at the financial services sector, local regulators continue to publish guidance and information that sets out their insights and observations for firms as they look to future regulatory deadlines and to support industry best practice. Organizations from all sectors can pay attention to this guidance and adjust their approach to resilience accordingly.

» Regulators continue to push for enhanced maturity of resiliency testing regimes, particularly around the variety of scenarios that are tested against, and the maturity of the testing approaches (wargaming, simulation, and live proving of resiliency capability as opposed to desktop-based reviews).

» In financial services, many organizations are grappling with the transition from project-led operational resilience to dedicated business teams, and the links to existing complementary processes for effective operational resilience (change and more traditional technical resilience for example).

» In other industries operational resilience may not yet have the profile or consideration among senior leadership it deserves or requires. However, internal audit should consider reputational, technological, geopolitical, organizational, and financial resilience and have a holistic view of these areas.

» Across all industries, effective resiliency processes while maturing still have a way to go, to provide the level of holistic, organization-wide thinking required to achieve true "operational resilience."

# Operational resilience

## What internal audit should do

**1** Dedicated and embedded assurance: Beyond 2025, internal audit functions should consider how best to get both breadth and depth of their assurance coverage through both dedicated reviews and embedding resilience considerations into other planned audits.

**2** Transition to business as usual: Internal audit should consider assessing the adequacy of provisions to support transition to business as usual from existing project teams, including clear definitions of roles and responsibilities across relevant stakeholders and with adequate ongoing oversight. Key complementary areas to consider include change delivery capabilities and methodologies and how they are moving toward "Resiliency by Design," and integration with existing technology resiliency processes such as disaster recovery and incident response.

**3** Benchmarking: Internal audit functions who understand how their organization's approach to operational resilience compares to industry peers (and organizations within financial services for those organizations sat in other sectors) will be able to add significant value in helping their firm to refine their approach to ongoing compliance in a proportionate way, aligned to the marketplace.

**4** Management information (MI): The importance of management information will become critical as metrics and data are challenged and refined. Internal audit should consider a review of the adequacy of the MI, its alignment to risk appetite, and its ability to support decision-making, as well as the adequacy of proposed actions for management to take where triggers are breached. Horizon scanning and resilience intelligence processes to feed into the operating model for resilience should support with the embedding of resiliency within the organization.

**5** Third parties: Assurance of operational resilience is intrinsically linked to third-party risk management. Internal audit may wish to undertake a review specifically focused on the operational resilience of key third parties, including the tracking of any remediation the organization has required third parties to undertake, consideration of substitutability, and exit arrangements.

- SS1/21 Operational resilience: Impact tolerances for important business services | Bank of England
- The Digital Operational Resilience Act (DORA) | Deloitte UK
- Operational resilience: insights and observations for firms | FCA

## Cloud

## Introduction

Cloud computing has become essential for organizations across all sectors, driving enterprise technology strategies for nearly a decade. Far from slowing down, cloud adoption is accelerating as organizations recognize its potential for both technological advancement and business transformation. Many now view cloud as either a disruptive force or a key enabler of new capabilities.

The substantial resources required for GenAI have concentrated its development in the hands of major tech companies like Microsoft, Google, and Amazon Web Services (AWS). This reliance on cloud hyperscalers for GenAI is directly tied to its increasing use in driving business value and transformation.

However, this dependence on cloud services also presents challenges. While cloud technology enables organizations to enhance operational resilience, it also raises concerns about overreliance on cloud providers and third-party vendors. Cybersecurity risks are also heightened in this environment, demanding increased vigilance and sophisticated mitigation strategies. Internal audit teams recognize that cloud computing is an enduring aspect of the business landscape.

## What's new?

» Multi-cloud and hybrid strategies introduce new audit challenges: Organizations are increasingly adopting multi-cloud and hybrid cloud strategies, leveraging services from multiple providers and combining public and private cloud environments. This complexity creates significant challenges for managing security, compliance, and data governance, demanding a more integrated and sophisticated approach to cloud auditing.

» Significant cloud spending is being wasted: Organizations typically waste 30% to 40% of their cloud spending due to inefficient practices and inadequate controls. This financial leakage could double in the next few years if left unaddressed (per Forrester), highlighting the critical need for robust cloud cost-optimization strategies.

» Cloud's pervasive impact amplifies organizational risk: Cloud computing's integration with critical business processes and systems significantly expands its risk profile. Its intersection with cybersecurity, data privacy, governance, compliance, and IT operations, coupled with increased investment in this domain (as highlighted by Gartner), necessitates internal audit's consideration of cloud risks within broader technology risk assessments.

» Continuous assurance vital for dynamic cloud environments: The rapidly evolving nature of cloud environments demands a shift from traditional, point-in-time audits to a continuous assurance model. Frequent assessments are crucial to proactively manage risks, address emerging threats, and maintain alignment with changing regulatory landscapes.

» Technical depth essential for effective cloud audit procedures: Cloud audits are no longer limited to high-level control assessments. The increasing complexity of cloud environments requires a more technical approach, demanding deeper dives into configurations, architectures, and security controls to effectively identify and mitigate vulnerabilities.

28

# Cloud

## What internal audit should do

**1** Recognize cloud's key role: Internal audit functions should prioritize cloud computing as a core component of their audit plans, recognizing its integral role in the modern enterprise's digital ecosystem. However, a common pitfall is the lack of specialized cloud expertise during the planning process, often resulting in generic "cloud" audits that lack focus and depth.

**2** Upskill and build cloud expertise: To this end, internal audit teams must develop cloud-specific expertise to effectively audit complex cloud environments. This includes understanding cloud service and deployment models, and key security and compliance considerations. Upskilling existing teams and/or recruiting cloud-specialist auditors should be considered.

**3** Continuous assurance is key: Cloud environments are dynamic, with evolving risks and configurations. Relying solely on point-in-time assurance, typically during the initial deployment phase, can be insufficient. Internal audit should incorporate recurring cloud audits into their plans to address evolving threats and operational context as the inherent risk profiles of these services are subject to change over time.

**4** Targeted audit approach: Align cloud audits with critical technology risks and the organization's unique risk universe. For instance, prioritize cloud security audits for business-critical platforms and leverage cloud-literate specialists in the planning process to identify and address the cloud risks most relevant to the organization.

**5** Develop specialized methodologies: Generic IT audit approaches are inadequate for complex cloud environments. Develop cloud-specific methodologies incorporating relevant risks, control frameworks (e.g., CSA CCM, NIST cybersecurity framework), and leading practices for auditing cloud configurations, access controls, and data security. Integrate cloud considerations into other relevant audit engagements for a holistic approach.

# Third-party risk management

## Introduction

Management and the board are typically focused on managing third-party risk as they play a crucial role in fulfilling strategic and operational objectives. There are known challenges in handling supply chains, managing visibility of extended third-party relationships, and navigating the geopolitical landscape.

Organizations face increasing risks from crucial business services (supported by critical third parties) being made unavailable due to issues such as cyberattacks, data breaches, and compliance failures. Deloitte's Global third-party risk management (TPRM) survey has shown that mature TPRM practices are based on deeper trust, transparency, and reliability with third parties.

Internal audit must therefore keep pace with the accelerating speed, volume, and complexity of third-party risk, as well as heightened regulatory scrutiny. As boards and management navigate the constantly changing external environment, the demand for internal audit to provide assurance and timely insights is more pressing than ever before.

## What's new?

» Integrated third-party management, as third-party risk doesn't materialize in isolation, should be evaluated holistically considering key risk domains as well as contract and performance management.

» Prescriptive regulatory requirements and increased third-party disruptions have intensified regulatory scrutiny, prompting large-scale remediation transformation that requires greater collaboration across the three lines, as well as consistent involvement from internal audit throughout the remediation program.

» The organization's growing use of new technologies, including GenAI-based tools, across various functions to manage third-party risk, and reliance on third parties using GenAI, requires an elevated TPRM framework to evaluate emerging AI risks (e.g., underlying data quality, algorithm reliability, cybersecurity, data privacy, and ethical considerations that may lead to significant reputational risks for organizations).

» The Corporate Sustainability Reporting Directive (CSRD) requires organizations to define and report on sustainability impacts, risks, and opportunities across both direct and indirect business relationships within their upstream and downstream value chains. TPRM frameworks must adapt to incorporate critical ESG considerations; recognizing an increasing need to evaluate and report on sustainability risks beyond the organization's own activities.

» Increased usage of alternative assurance mechanisms, going beyond just third-party attestation-based risk assessments, and proliferation of screening and monitoring tools for real-time risk tracking.

# Third-party risk management

## What internal audit should do

**1** Integrated third-party management: Challenge the TPRM operating model; its integration with partner functions like procurement, legal, operational resilience programs, second-line function, and subject matter experts.

**2** Integration and embeddedness of regulatory requirements: As the regulators are intensifying scrutiny, internal audit should focus on the areas where their organizations struggle to meet requirements, including early involvement in regulatory remediations.

**3** Concentration risk across extended supply chain: Ensure appropriate metrics are in place to detect concentration risks that may exist across multiple dimensions, such as service category, entities, business unit, geography, and technology service providers. Assess mitigation actions, organization's outsourcing/sourcing strategy, and third-party substitutability to minimize concentration.

**4** Emerging risks: Assess the maturity of the TPRM framework to address emerging risks including AI-related risks from third-party use and internal usage of AI-based tools, as well as TPRM facilitating the organization's ESG goals and objectives.

**5** Testing third-party risk: Assess oversight mechanisms to evaluate third-party risk and the efficacy of the risk assessment process.

- Third Party Risk Management Survey 2023

## Sustainability

## Introduction

The last 18 months have seen pivotal shifts in the landscape for sustainability reporting, at a US, European, and global level. Key reporting requirements—including the CSRD, International Sustainable Standards Board (ISSB), California Senate Bills, and the Security and Exchange Commission's (SEC) Climate Disclosure Rule—are now known, but the standards themselves continue to develop. The overall trend is toward enhanced transparency about, and accountability for, critical sustainability practices, topics and behaviors. Forward-looking organizations will take no-regret actions now to prepare for incoming regulation and will develop integrated reporting processes that span the multiple requirements.

## What's new?

» For qualifying organizations, CSRD reporting requirements are now effective with first reporting due from 2025. 2023 saw the ISSB release IFRS S1 and S2—disclosure requirements for organizations to inform investors about the sustainability-related risks and opportunities they face over the short, medium, and long term.

» The California Senate Bills 253 and 261 are the climate legislation in California and are now effective with first biennial climate risk reporting by first of January 2026 over 2025 activity, to inform stakeholders about climate emissions data and climate-related financial risks through disclosure.

» The SEC climate-related disclosures focus on climate-related disclosure as part of the financial statements and Internal Controls over Financial Reporting (ICFR) and are subject to attestation.

» In September 2023, the Taskforce on Nature-related Financial Disclosures (TNFD) published its final recommendations for nature-related risk management and disclosures. The European Financial Reporting Advisory Group and ISSB are expected to clarify how the final TNFD framework on nature-related disclosures will be adopted. More than 300 companies have already signaled early adoption and have committed to disclose in accordance with TNFD recommendations by 2025 or earlier.

» Some firms have already disclosed transition plans, but the introduction of requirements to do so in the European Union (being formalized under CSRD, CSDDD, and CRR3) will enhance scrutiny. In the United Kingdom's Transition Plan Taskforce (TPT) framework will update expectations for disclosures compared to the TCFD framework that preceded it.

# Sustainability

## What internal audit should do

**1** Internal audit strategy and position: Internal audit must apply a strategic and long-term lens in developing an internal audit plan that includes consideration of sustainability, which can provide iterative and ongoing assurance in line with the evolving risks. A coordinated approach with other lines of defense will be critical to ensure suitable coverage across the growing number of reporting requirements.

**2** Reasonable assurance: CSRD and SEC climate-related disclosures will require that firms obtain reasonable assurance in the coming years across their related disclosures. Internal audit must position itself as a strategic business partner within the organization in helping build and test the resilience of the underlying control framework.

**3** New data and processes: Many of the new ESG reporting data points, together with the data collection processes, will be new for most organizations. Internal audit should urgently identify the firm's data governance maturity and ensure third-line efforts are prioritized accordingly.

**4** Business opportunity and integration: Inherently, internal auditors are focused on the risks facing an organization. However, the third line should consider how to support and advise on the related opportunities through ESG-related reporting, in the context of market positioning and sustainability strategy. Internal audit must also capitalize on its holistic view and recommend ways to link and streamline reporting processes. This will reduce reporting silos, increase efficiency, and drive effective integration across the ESG reporting framework.

**5** Transition plan assumptions: To drive the transition plan resiliency, internal audit should independently evaluate the validity of assumptions and dependencies, help identify related sensitivities, and ensure follow-up actions are embedded.

- Internal audit planning priorities 2025 | Deloitte UK
- Deciphering the Impact of California ESG Regulations | Deloitte US
- SEC Climate Disclosure Guidance | Deloitte US
- How the TNFD recommendations and guidance support corporate sustainability reporting | Deloitte UK
- Transition Plan Taskforce consultation on "gold standard" transition plans | Deloitte UK

# Digital regulation

## Introduction

All of us enjoy the benefits of the internet, whether to work more flexibly, shop online, communicate with family and friends around the world, or spend our leisure time consuming media or playing games. But the internet comes with a cost as every day there are stories in the news about the negative impacts of the internet and other digital technologies.

Policymakers in governments globally are concerned about "online harms" that users encounter, illegal or misleading content, harmful behavior, risks to children, scams, and fraud, as well as issues for businesses around copyright, unfair competition, impacts to digital advertising, and erosion of user trust. Then there is the wide range of risks from the explosion of AI technologies in recent years. While companies seeking to innovate and deploy the digital technologies available to them have long enjoyed the benefits that these can have on revenue and exponential growth, they are now facing a paradigm shift, with a wave of complex, principles-based, and transformational regulations.

There is a sense that these new regulations will be robustly enforced, and it is no longer acceptable to hope for the best. Instead, organizations in scope will have to prove how they comply at all times—with significant increases in regulatory requests for information, independent audits, and transparency reporting. Even for industries already familiar with being highly regulated, this will cause additional complexity and drive the need for a more efficient and cost-effective compliance program. For other industries that are becoming regulated for the first time, this new regulatory regime will require a major transformational shift in how they think about business with many having to overcome a compliance backlog of many years.

## What's new?

» Regulatory challenges are on the horizon: As new innovations in technology emerge, we anticipate further regulatory obligations around quantum computing; digital identity; and virtual, augmented, and extended reality.

» Regulators take back control over the internet: With decades of unregulated growth, organizations that rely on digital communications and commerce, enabled by the internet, are seeing a global regulatory response to the potential for harm on these platforms in the areas of content, competition, and consumer protection (including EU Digital Services Act, EU Digital Markets Act, and UK Online Safety Act).

» Concerns around the risk of widespread adoption of GenAI: We are in a hype-cycle of GenAI development and deployment with organizations racing to out-compete based on early adoption. With the true unintended risk being unknown, a complex web of AI ethics, principles, codes, and regulations (including EU AI Act) is quickly taking shape across the globe.

» Resilience in the cloud: With so much of the world's data and services being processed in the cloud, many jurisdictions are asking questions around accountability when technology failures cause widespread negative social impact. New regulations such as EU DORA cover all aspects of the public cloud infrastructure layer and the legal obligations of cloud platforms and users.

» Whose data is it anyway? The EU's GDPR, introduced in 2018, set a global baseline for principles protection of personal data. As more and more data is generated, including through the Internet of Things, new regulations (e.g., EU Data Act) have had to be developed to build on these core principles—each covering different elements relating to the creation, use, sharing, and sovereignty of data.

34

# Digital regulation

## What internal audit should do

**1** Getting ready for independent audit: Many organizations going through their first regulatory independent audit would benefit from the support of the internal audit function to get audit ready, including education around audit versus investigation, audit walkthroughs, and evidence requirements.

**2** Supporting compliance culture change: Given many of these regulations are driven by the use of technology, the first line will be critical to responding to regulations and identifying business-appropriate controls. For organizations becoming regulated for the first time there may be a significant knowledge gap across the business about what effective governance risk and compliance looks like. These are concepts very familiar to internal audit, and there is a critical role it can play in educating the business and supporting compliance functions with this messaging.

**3** You can't audit what you don't understand: The technology driving these regulations is complex and not universally well understood. Internal auditors may have to upskill, so that they understand core concepts and terms across topics such as digital advertising, search rankings, and machine learning in order to ask the right questions and explain the answers to senior leaders.

**4** Looking beyond the pure compliance obligations: Many of these regulations purely list "compliance obligations" with additional obligations being principles based. It is the organization's responsibility to identify how their services could increase the risk of being regulated, often based on mandatory risk assessments, and putting in place appropriate safeguards. Internal audit can play a key role in connecting the dots between different regulations and broadening the potentially narrow focus of regulatory project teams and exploring how these regulations may affect the organization holistically.

**5** Bringing order to assurance chaos: With multiple regulations requiring monitoring and assurance activity by independent compliance functions or independent external auditors, internal audit has a critical role to play in mapping and streamlining cross-functional assurance activities and reducing the overall cost of assurance.

- The Digital Services Act is in full effect | Deloitte UK
- Online Safety Act implementation | Deloitte UK
- AI risk and approaches to global regulatory compliance | Deloitte UK
- All eyes on the cloud | Deloitte UK
- Business-to-Business data sharing under the EU Data Act | Deloitte UK
- Preparing for the Digital Markets Competition and Consumers Act | Deloitte UK

# Contacts

**Peter Astley**
**Global Internal Audit Leader**
+44 7887 633880
pastley@deloitte.co.uk

**Sarah Fedele**
**Global Transformation**
**US Internal Audit Leader**
+1 713 982 3210
sarahfedele@deloitte.com

**Mike Schor**
**Global Internal Audit Innovation Lead**
+1 212 436 6208
mschor@deloitte.com

**Neil White**
**Global Internal Audit Digital Lead**
+1 212 436 5822
nwhite@deloitte.com

**Chris Dicks**
**Global Internal Audit Growth**
**Asia Pacific**
+86 10851 25825
chdicks@deloitte.com.cn

**David Tiernan**
**Global Internal Audit Advisory Lead**
+44 113292 1520
datiernan@deloitte.co.uk

**Diego Henriquez**
**Global Internal Audit Chief of Staff**
+1 713 982 3642
dhenriquez@deloitte.com

# Deloitte.