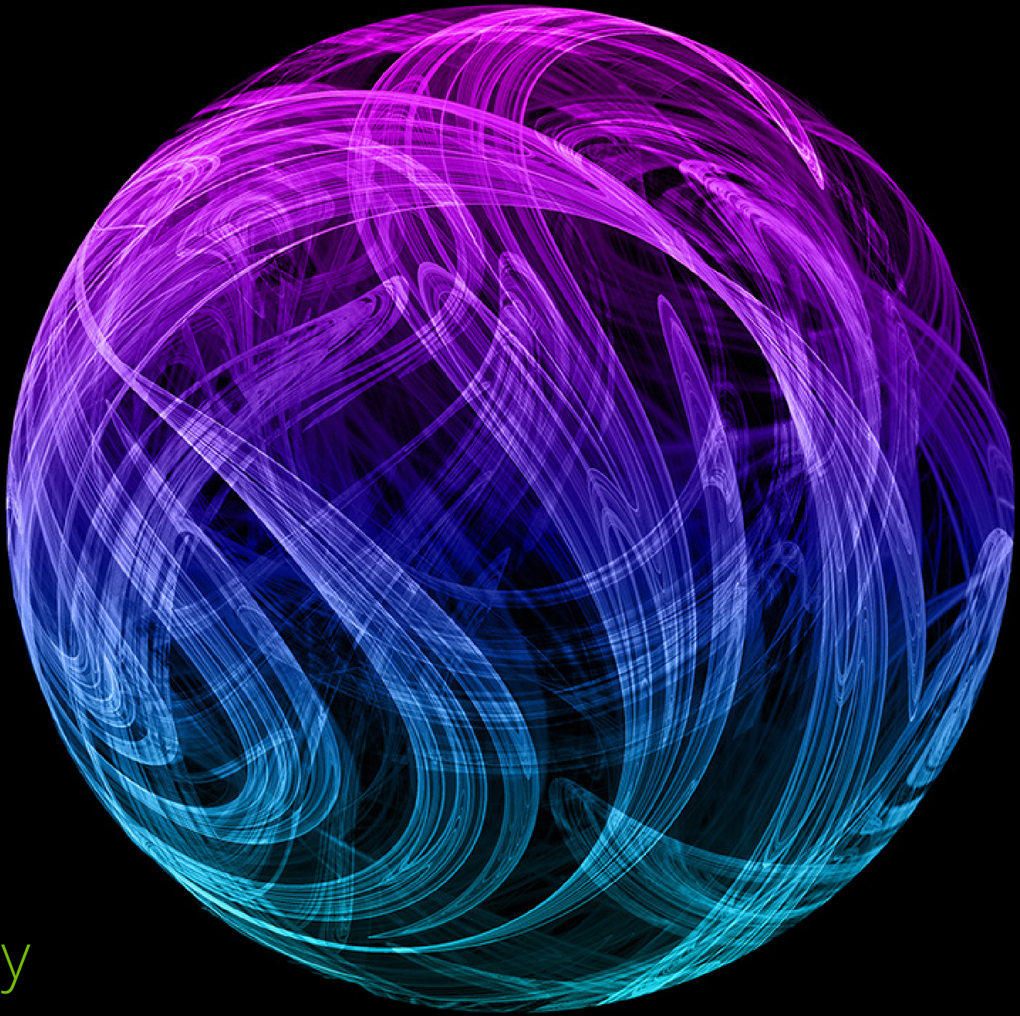
Deloitte.



Hot topics for technology and digital risk 2025

An internal audit viewpoint

Executive summary

Welcome to the 14th edition of Deloitte's technology and digital risk hot topics for internal audit.

The report offers insights into the UK technology risk landscape, derived from our survey completed by Heads of Information Technology (IT), Heads of Internal Audit, and business leaders across all sectors. We have combined qualitative insights and perspectives gained from technology, audit, risk and business leaders across all sectors along with our subject matter experience, to shed light on the latest updates in these key risk areas, whilst offering actionable suggestions for internal audit functions to consider in the next year. On that note, we wanted to extend our sincere gratitude to all survey participants for their openness and willingness to share their experiences, challenges, and strategic priorities.

We hope that this report provides you with a useful reference point from which to drive conversations and ultimately helps you enhance your risk assessment and planning processes for 2025.

We also welcome the opportunity to continue the dialogue with technology and audit leaders, to foster further discussion and collaboration across these critical topics. If there is anything you would like to discuss further, do not hesitate to get in touch.

Financial Services

Yannis Petras
Partner
Tel: +44 20 7303 8848
Email: ypetras@deloitte.co.uk

Mark Westbrook
Director
Tel: +44 113 292 1814
Email: markwestbrook@deloitte.co.uk

Non-Financial Services

Faiza Ali
Partner
Tel: +44 20 7303 7274
Email: faali@deloitte.co.uk

Kirti Mehta
Director
Tel: +44 20 8039 7437
Email: kirtimehta@deloitte.co.uk

Executive summary

Areas of focus for 2025

Technological advancements, while unlocking new organisational capabilities, also expand the scope and complexity of internal audit functions. To effectively navigate this evolving landscape, internal audit must embrace the advancements whilst maintaining a focus on the 'hygiene' factors, and fundamental risks and principles.

Embracing tools like automation and new/emerging technologies such as **artificial intelligence** is crucial for internal audit to keep pace with the evolving risk landscape. While adopting new technologies, internal audit must remain anchored to fundamental principles, ensuring robust **IT governance and risk management** remains a priority. This is particularly critical in light of recent major global incidents, that underscore the importance of sound **technology governance, resilience** and **third-party risk management**.

Technology and digital risk hot topics for 2025

ALL SECTORS

FINANCIAL SERVICES

NON-FINANCIAL SERVICES

Rank	Topic	2024 rank
1	Cyber security	1 ↔
2	Digital transformation and IT change	2 ↔
3	Technology strategy and governance	(New)
4	Artificial intelligence including GenAI	4 ↔
5	Data	3 ↓
6	Resilience	6 ↔
7	Identity and access management	9 ↑
8	Cloud	5 ↓
9	Third party risk management	7 ↓
10	Emerging technology trends	10 ↔

The following topics are key focus areas for organisations in their upcoming technology and digital internal audit plans for 2025:

Cyber security

Resilience

Artificial intelligence including GenAI

Technology strategy and governance

Digital transformation and IT change

Industry sector analysis

The 2025 hot topics for technology and digital risk survey highlights a landscape shaped by both shared priorities and sector-specific nuances. While the top 10 topics remain consistent across Financial Services and Non-Financial Services, their relative importance reveals distinct areas of focus for each sector.

- As expected, **cyber security** dominates the list, claiming the top spot in both sectors. This underscores the criticality of robust cyber security strategies as the bedrock of any effective technology control environment, regardless of industry.
- Despite this shared emphasis on cyber security, subtle yet significant differences emerge within the rankings. Financial Services organisations place a relatively increased focus on **Generative AI (GenAI)**, indicating a potential for accelerated adoption and exploration of this transformative technology within the sector. This suggests a proactive approach to leveraging GenAI for competitive advantage in areas such as fraud detection, customer service, and risk management.
- Conversely, **technology strategy and IT governance** assumes greater significance for Non-Financial Services organisations, highlighting a focus on establishing robust technology frameworks to guide innovation and growth. It also reflects the impact of the Corporate Governance Reform, as organisations seek to enhance the governance around IT in preparation for UK controls regulation (sometimes referred to as "UK SOX17 – Sarbanes Oxley"); it is vital that internal audit play a key role, particularly given the opportunity for technology to become a greater enabler for an effective control environment. This emphasis on governance also reflects the diverse nature of the Non-Financial Services landscape and the need for adaptable yet controlled technology adoption across various sub-sectors.
- By understanding the specific priorities shaping each sector, organisations can develop targeted strategies that effectively address their unique challenges and unlock the full potential of technology, innovation, and transformation.

Our survey through the years: 2012-2025

The table below presents a comparison of the top-10 technology and digital risk internal audit hot topics over the past 13 years, as identified through our annual survey of Heads of Information Technology (IT), Heads of Internal Audit, and business leaders, as well as leveraging our own insight and analysis across our extensive list of technology internal audit clients in the UK.

Topics which appear across more than two years have been colour-coded to help illustrate their movement in the top 10 over time.

Technology and digital internal audit hot topics through the years: 2012-2025

Rank	2025 (AS)	2024 (AS)	2023 (AS)	2022 (FS)	2021 (FS)	2020 (FS)	2019 (FS)	2018 (FS)	2017 (FS)	2016 (FS)	2015 (FS)	2014 (FS)	2013 (FS)	2012 (FS)
1	Cyber security	Cyber security	Cyber security	Cyber security	Cyber security	Cyber security	Cyber security	Cyber security	Cyber security	Cyber security	Cyber security	Large scale change	Third-party management	Cyber threat
2	Digital transformation and IT change	Digital transformation and IT change	Digital transformation and IT change	Cloud governance and security	Operational and IT resilience	Transformation and change	Technology Transformation and change	Strategic change	Strategic change	Strategic change	Disaster recovery and resilience	IT governance and IT risk management	Identity and access management	Complex financial models
3	Technology strategy & governance	Data management and data quality	Data governance	Operational and IT resilience	Cloud governance	Operational resilience	Data protection and Governance	Data management and data governance	Data management and data governance	Third-party management	Large scale change	Identity & access management and data security	Data governance and quality	Data leakage
4	Artificial intelligence including GenAI	Artificial intelligence	Cloud hosted environments	Data governance	Extended enterprise risk management	Extended enterprise risk management	Technology resilience	IT disaster recovery and resilience	Third-party management	IT disaster recovery and resilience	Enterprise technology architecture	Data governance and quality	Large scale change	Data governance and quality
5	Data	Cloud environ-ments – cost and sustainability	Operational and IT resilience	Transformation and change	Transformation and change	Digital technologies	Extended enterprise risk management	Information security /identity & access management	IT disaster recovery and resilience	Data governance and quality	Third-party management	Third-party management	Cyber security	Rogue trader and access segregation
6	Resilience	Technology resilience	Business critical IT controls	Digital risk	Digital risk	Data protection and data privacy	Legacy architecture	Third-party management	IT governance and IT risk management	Information security	Information security	Cyber security	Resilience	Regulatory programmes
7	Identity & access management	Outsourcing and critical third parties	Extended enterprise /third-party risk management	Extended enterprise risk management	Data governance	Cloud governance and security	Cognitive automation and artificial intelligence	IT governance and IT risk	Information security/identity & access	Digital and mobile risk	Digital and mobile risk	Digital and mobile risk	Cloud computing	Financial crime
8	Cloud	Legacy IT and simplification	IT strategy & governance	IT strategy and IT governance	IT strategy and IT governance	IT governance and IT risk	Cloud computing	Cloud computing	Enterprise technology architecture	IT governance and IT risk management	Data management and governance	Service management	Mobile devices	Third-party Management
9	Third party risk management	Identity & access management	Identity & access management/ privileged access	Payments	Payments	Application development	Application development	Digital and mobile risk	Cloud computing	Enterprise technology architecture	IT governance and IT risk management	Disaster recovery and resilience	Complex financial modelling	Social media
10	Emerging technology trends: ESG, DLT, quantum security	Emerging technology trends	Digital risk: artificial intelligence	Application/ integrated reviews	System development	Legacy environments	Payment technologies	Enterprise technology architecture	Digital and mobile risk	Payment systems	Service management	Cloud computing	Social media	Mobile devices

AS – All sectors
FS – Financial Services

1 ↔ 1 | 87% Audit planned % | 20% Audit effort % | 48% Use of analytics %

Cyber security

The ramifications of a successful cyber-attack can be disastrous for an organisation including – disruption, diversion from value-add projects, lengthy remedial work, court cases, eroded customer trust and compliance issues. The threat is constant and growing, as cyber-attacks have been weaponised and industrialised. Many people are in the crosshairs, sometimes as individuals rather than representatives of organisations. Organisations can't take their eye off the ball when it comes to meeting the challenge of maintaining security in a constantly changing threat environment. This is in part because many organisations have digitalised processes to a point where it is almost impossible for them to operate any alternative processes for any period of time.

One thing that remains unchanged is the gap between the cyber security skills requirements for organisations, and their limited supply. Last year, the UK government advised that 50% of all UK businesses had a basic cyber security skills gap, while 33% have an advanced cyber security skills gap[3]. The recruitment industry has advised that 75% of employers in the cyber security space are likely to recruit additional permanent staff throughout 2024[4]. Indeed, the government's 2024 cyber security sectoral analysis report[5] highlighted a 5% annual growth in the number of people employed by cyber security firms alongside a 13% growth in their revenue – this clearly demonstrates that supply is reaching out to meet demand.

What you should know

- We anticipate that in 2025 we will continue seeing the evolution of AI as a genuine mainstream competence that is being used to both drive new attack vectors and build defences[6]. Crucially, AI allows attacks to be scaled up in terms of speed and complexity – this includes larger and more sophisticated phishing campaigns and the use of deepfakes.
  - Attacks involving deepfakes have the potential to cause serious reputational damage. For example, misinformation and false allegations are spread online or sent in targeted communications to key stakeholders, such as clients, employees, and banks. Another use is where voice and facial imitation has been used to impersonate people to gain access to bank accounts or blackmail people into handing over sensitive commercial information.
  - Some organisations have failed to protect their own AI tools against external attacks – there have been examples of where models have been built insecurely and taken over.
  - GenAI tools have also been attacked. This can result in data being stolen, or employee sessions hijacked to attack the organisation's systems.
- There are new regulatory obligations that are driving pan-national oversight of cyber risk and privacy. These include the SEC rules on cyber disclosure that were introduced in 2023 and the NIS2 cyber security legislation now adopted for the entire European Union. This requires EU organisations to strengthen their overall level of cyber security and improve the resilience of critical infrastructures and digital services. The UK had already implemented NIS1 and it is working on its own proposals, so we can expect to see some new requirements emerging.
- Organisations are now experiencing more sophisticated targeted attacks on top of the rather 'industrialised' ones they are used to receiving. There is an increased threat from national governments and agencies as geo-politics and war plays out in parts of the world. For example, the NCA[7] reports Russian and Russian-speaking criminals behind Ransomware-as-a-Service (RaaS) platforms who continue to be responsible for most high-profile cybercrime attacks against the UK. The NCA advised that ransomware remains the most serious cyber threat in the UK. The RaaS model makes it much quicker to launch a ransomware attack and allows for the faster extraction of monies from those impacted.

Audit planned % is the percentage of respondents who have included this topic in their audit plan.
Audit effort % is the percentage of respondents' overall audit plan that was dedicated to the topic as an estimate.
Use of analytics % is the percentage of respondents who, if they have included this topic in their audit plan, currently employ analytical techniques.

What should internal audit be doing?

1. Ensure cyber security is at the top of the board agenda; understand the benefits of aligning cyber security with business direction and strategy. As the cyber risk threat environment evolves, so should the role of the Board in safeguarding against that risk. Internal audit need to ensure that cyber risk analysis and reporting is a Board level issue.

2. Review cyber threat intelligence capabilities, including how the business is modelling scenarios and what horizon scanning activities are taking place. Cyber threat intelligence itself is not a solution but it is a crucial security component. It allows businesses to optimise their cyber security resources by understanding which threats are most likely to target them.

3. Consider assessing cyber security awareness by conducting a culture review where targeted questions are used to see if the cyber security messages have been understood by employees. Prevention is always better than reaction when it comes to cyber security. A defence strategy is needed and staff are a core part of that.

4. Functions within Government and Public sector should consider alignment with the NCSC's Cyber Assessment Framework (CAF) as the new leading standard for cyber security assurance. The CAF emphasises an outcome-based approach, requiring organisations to demonstrate achievement of key cyber security outcomes rather than simply implementing specific technical controls. This represents a shift from previous years where the US-focussed NIST framework was the expected standard, highlighting the increasing importance of the CAF for UK-based organisations.

5. Continue engaging with the Institute of Internal Auditors (IIA) and provide feedback to their consultation for their "Cyber security Topical Requirements". The first draft is currently being revised by the Global Guidance Council to incorporate feedback gathered during a 90-day public comment period. The IIA's focus on issuing mandatory guidance may increase the audit burden for Internal audit functions, but at the same time elevates the topic of cyber security across industries, seeking to bring consistency and improve standards.

2 ⟷ 2 79% Audit planned % 12% Audit effort % 38% Use of analytics %

Digital transformation and IT change assurance

The increasing regulatory focus on resilience during transformation is significantly impacting how organisations approach strategic change implementation. Factoring the upcoming joint Financial Services industry consultation on incident and third-party reporting, and the cyber security and resilience bill adds complexity to existing change management practices for the wider market.

The new landscape necessitates closer collaboration between change functions, risk teams, and internal audit functions, to ensure compliance, gain insights into evolving regulatory requirements, and foster a proactive risk management culture. In modern environments, effective IT change management requires a comprehensive approach that extends beyond the technical aspects of core platforms. Organisations should consider the ethical considerations related to AI implementations, ensuring project teams possess the necessary skills and capabilities, and thoroughly evaluate the organisation's readiness to adopt the proposed changes.

Consequently, internal audit functions need to effectively prioritise change reviews and respond to the increasing demand for assurance in this evolving landscape.

What you should know

- **Increased regulatory focus on material change and material outsourcing:** In line with previous recommendations from 2022, the Prudential Regulatory Authority (PRA) has requested Financial Services internal audit functions to perform a series of reviews on IT change and outsourcing risks this year, given the frequency and materiality of those in the financial sector. While only a portion of firms have been selected for this specific review, the industry should view this as a clear signal towards robust programme execution and compliance with SS2/21 regulations.
- **Strategic alignment and value addition:** We are seeing an increase in alignment of transformation activities with strategic goals in order to enhance organisational coherence and prevent waste of resource effort on projects and products that do not add any value to colleagues or customers. Assurance engagement should be across the portfolio and coordinated with business sponsors to add value.
- **Regulatory focus on technology**: In light of recent major global incidents, global regulators are pushing for control over use of automated workflows for development, testing and deployment. It will be important that internal audit functions maintain a strong understanding of these technologies in order to develop and deliver an appropriate approach to assurance.
- **Complexity of portfolio management:** Many organisations continue to rely, at least in part, on traditional project delivery methods with fixed budgets and defined outcomes, whilst also adopting services delivered through modern methods. This often leads to a scale of complexity in portfolio management, the need for ongoing quality control, and potential resourcing challenges as teams navigate between traditional and agile approaches. For internal audit, this shift necessitates adaptability in understanding and evaluating project controls, moving beyond a traditional waterfall method, and developing the capability to effectively assess hybrid and agile practices.
- **Integrating business change and sustainability:** There is a growing emphasis on integrating business readiness into programme delivery. This shift is driven by the recognition that successful programme implementation requires more than just technical expertise. Successful execution demands a deep understanding of the human aspect of change. This integrated approach is further bolstered by the increasing alignment with sustainability goals and ESG objectives, particularly in sectors with long-term impacts like infrastructure, public health, and corporate responsibility.

What should internal audit be doing?

1 **Change prioritisation and portfolio management:** The internal audit function should challenge the approach to strategic prioritisation and portfolio management to ensure alignment with strategic objectives and regulatory compliance. This should extend beyond discussion in governance forums and should challenge bias, inconsistency, benefits realisation, and unexpected outcomes.

2 **Accountability of sponsors and leaders:** Accountability, decision-making, and financial control should reside at the portfolio level. Assurance over a lean portfolio requires proactive oversight, open structures and evidence of transparency between professionals. Assurance must be part of this structure to provide independent oversight to ensure consistent dialog and challenge from the third line. Internal audit should also assess the organisation's capacity and capability to execute transformation appropriately and robustly, through operating model and capability assessments, monitoring for overreliance on third-party expertise, 'black box' tools and product-led procurement.

3 **Regulatory impact of material change:** Internal audit's role in change assurance should include a comprehensive review of the portfolio and material changes to the business process. This should encompass regulatory compliance, programme planning, risk management, scrutinising fallback plans, "what-if" scenarios, and remediation strategies. Additionally, internal audit should focus on evaluating the testing approach, governance, the use of automated tools, and approval processes at each project stage.

4 **Embedded risk management:** While thematic reviews remain a common practice for change assurance, internal audit should consider a more proactive approach of embedding audit resources within programmes and portfolio to give real-time risk assessment, timely challenge, and value-added feedback.

5 **Measuring value:** Internal audit is becoming increasingly critical in assessing management's capability in measuring the business benefits from major transformation. For example, by assessing the decision-making criteria for shaping change ahead of mobilisation, measuring key metrics to track progress, and monitoring delivery throughout the life of the initiative.

6 **Manage complexity with enhanced skill sets:** With many organisations relying on external service providers for change delivery, they risk lacking internal standards for third-party tools and methods, which often results in an absence of challenge from project teams. Internal audit can act as the only line of defence over outsourced delivery and should be well-versed with core change frameworks and business transformation practices to assess the capabilities of teams involved with change initiatives. Internal audit can play a vital role in recommending and verifying implementation of training programs and knowledge-sharing initiatives.

3 (New) 76% Audit planned % 12% Audit effort % 39% Use of analytics %

Technology strategy and governance

Technology represents one of the biggest opportunities for organisations, but is also a source of cost and operational risk. Robust technology and digital governance can help drive continuous improvement for how an organisation manages the evolving risk landscape. Similarly, optimised governance frameworks can support the management of risks in line with appetite to enable innovation and the delivery of strategic goals. Further, they can deliver cost reductions, particularly important in a cost constrained environment.

Inadequate IT governance can lead to an unfocused strategic direction for IT, or decisions being made without a full appreciation of the impact on the organisation's broader strategy as well as risk profile and appetite. Recent major global incidents reinforce how important it is for organisations to get this right.

What you should know

- **Lack of visibility and understanding of technology by senior leadership:** A lack of technology awareness at the leadership level can create a blind spot, increasing the likelihood of strategic missteps and financial losses. The rapid pace of change challenges even IT professionals, making it crucial for Boards, executives, and senior leadership to have a grasp of emerging technologies and potential disruptions. Clear visibility and understanding at the top are essential for decision-making and strategic oversight to effectively challenge on technology strategy, investment and BAU activities.

- **Increased focus on delivering and measuring value from IT is needed:** Demonstrating tangible value from IT investments is paramount in today's business landscape. Boards need to continue to challenge Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) to ensure effective governance structures are in place, and that the service and performance of these functions are proactively and effectively managed. A clear focus on holding CIOs and CISOs accountable for establishing robust governance structure that ensures effective, efficient, and value-driven IT services should be central to help protect organisations from technology, digital and cyber risks.

- **Reporting on technology risk can be improved:** The information available to those charged with governance of technology delivery is often insufficient, particularly in key areas like technology risk management and technology risk appetite. A lack of insight can hinder effective technology governance, potentially leading to costly mistakes and missed opportunities.

- **Possibilities to enhance risk management culture and practices:** The demands of daily operations should not overshadow the critical need for robust technology governance and risk management. Activities such as lessons learned from breaches or bypassing of controls, reported by staff, should be followed up on but technology professionals are often stretched and such matters are not given appropriate attention. Thus, leaving an organisation that struggles to cultivate a culture that prioritises strong governance principles.

- **Legacy technology risks continue to grow due to the misalignment of investment and IT requirements outlined above:** Most large corporates and to an extent smaller corporates as well suffer from legacy risks because of insufficient investment down the years, and as the pace of technological change continues to accelerate and grow, the related risks associated with legacy technology continue to grow in parallel.

- **There is a lack of adherence to established IT governance frameworks:** Organisations are not always leveraging ISO/IEC 38500:2015 standard as well as Control Objectives for Information and Related Technology (COBIT) in their assessments of organisational compliance against established IT governance frameworks. Neglecting IT governance creates an environment of heightened risk, potentially jeopardising an organisation's financial stability, operational efficiency, reputation, and long-term success.

What should internal audit be doing?

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 organisational structure, value delivery and performance monitoring. Explore instances of 'shadow IT' and challenge management on the governance and control around citizen developer tools, such as platforms and tools that non-engineers or development staff can develop using 'low-code' or 'no-code' software applications.

2 **Understand how the technology risk appetite has been defined and is used for monitoring.** Internal audit must also understand how the organisation 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.

3 **Technology culture.** Assessing the culture within the organisation (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.

4 **Review technology governance on a cyclical basis.** Ensure that reviews of technology governance are considered a key component of the technology audit plan on an ongoing basis. For example, consider rotating coverage against the four IT governance pillars:

- strategic alignment (strategic IT planning and organisational structure);
- IT risk management;
- resource management including third party management;
- value delivery and performance measurement.

5 **Consider the risk profile of the organisation from a legacy technologies perspective.** Internal audit should ensure that their risk universe for technology adequately considers legacy risk and technology management, and that where audits touch upon investment decisions, risk management and risk appetite, legacy technology is adequately considered.

4 ⟷ 4 29% Audit planned % 16% Audit effort % 45% Use of analytics %

Artificial intelligence including GenAI

Generative artificial intelligence (GenAI), a branch of artificial intelligence (AI), has taken the world by storm and its ability to create original content across various modalities is revolutionising numerous industries. There is a huge opportunity to use GenAI to transform internal audit processes (please refer to recent Planning Priorities for internal audit[8]). However, the existence of such a powerful tool, if used irresponsibly, can lead to reputation damaging consequences. AI models can generate false information through hallucinations, potentially leading to the spread of misinformation, and the quality of training data used is crucial to avoid biased and/or suboptimal outputs. Firms are grappling with the right level of 'human in the loop' to ensure AI systems are not accountable for decision making. Establishing effective controls is essential to ensure GenAI services are secure, comply with laws and regulation and do not put the organisation's reputation at risk.

What you should know

- In response to GenAI risks, regulatory frameworks have been established across the globe. The EU AI Act, which was formally entered into force on 1 August, signalling the start of the implementation period, will have implications for UK businesses with ties to the EU, affecting those with customers in the EU and those developing, deploying, or marketing AI systems in the EU. The EU AI Act introduces a risk-based approach to ensure AI systems respect fundamental rights, safety, and ethical principles.

- The UK Government's planned AI regulation framework aims to promote creativity through the safe use of AI, underpinned by five principles: safety, security and robustness; transparency and explainability; fairness; accountability and governance; and contestability and redress.

- There has been a flurry of activity as part of the new Government's AI opportunities action plan activity. This activity may also feed into a new consultation on a potential new AI legislation, most likely focused on the most powerful AI models and giving a legal basis to the AI Safety Institute. Government officials have also stated that the contentious and complex topic of AI and copyright will be considered as part of this consultation.

- The Bank of England, Prudential Regulatory Authority (PRA) and Financial Conduct Authority (FCA) have responded to the UK Government's principles-based regulatory approach and are considering areas for further clarification within their regulatory framework, including data management, model risk management, governance, and operational resilience and third-party risks.

- The FCA has highlighted several of its existing rules and guidance that it views as most critical to address the UK's AI principles. The PRA and Bank of England have confirmed they will run a third instalment of the 'machine learning (ML) in UK Financial Services' survey to continue their analysis of the financial stability implications of AI/ML.

- Whilst some clarity has been provided on the regulators approach to AI, further rules, guidance and policy statements are due to be released over the comings months.

What should internal audit be doing?

1 **AI regulation readiness:** Firstly, internal audit should understand how the business has assessed and has taken action as a result of incoming and anticipated legislation; a gap analysis or horizon scanning review may be relevant here, seeking to demonstrate to audit and regulators how the execution of business strategy on AI (including GenAI) has taken into account principles of safety and risk management, as well as regulation. Further, government and public sector organisations should be aware of specific UK guidance on how to build and use AI in the public sector[9].

2 **GenAI strategy and governance:** Aside from regulation, internal audit should consider a review focused on the current state of the risk and control framework for AI. Many businesses have already defined the AI strategy and others have made progress in producing an AI inventory and assessing the current state of the business processes' adequacy in light of AI. The GenAI strategy should include whether an enterprise licenced platform will be / has been implemented, what are the associated safeguards and rules of the road for employees, definition on data classification to be processed (for e.g, public data or company internal and confidential; how personal data is treated). Accuracy and completeness before any onward use, transparency and ethical considerations in line with the organisation's code of conduct and shared values should also be key.

3 **AI risk management:** Internal audit should consider the embeddedness of AI risk within the wider risk management landscape, for example, integration in the organisations' risk taxonomy, risk appetite and risk metrics, how AI risk is monitored and reported along with clarity of roles and responsibilities. Many organisations have developed their own AI risk assessment process which can be reviewed.

4 **AI system review:** Internal audit should consider a review of any significant or high-risk AI system in the live environment, as an application review; the review focus can include a reperformance of the risk assessment performed by management, sample testing of the effectiveness of AI controls, or focus on whether expected benefits and value are being realised in practice. A regulatory lens can also be applied to the review of an AI system.

5 **Training and competence:** Internal audit should consider the skills and capabilities within the organisation to manage AI risks including how training on using / applying AI tools in a safe manner has been rolled out to all staff, and the embeddedness of this understanding.

5 ↓ 3 71% Audit planned % 13% Audit effort % 67% Use of analytics %

Data

Data governance and management remain critical for internal audit, even more so with the rise of GenAI and evolving regulations like GDPR and BCBS239 in the Financial Services sector. While many organisations initially focused on foundational setup—establishing data governance frameworks, committees, and roles—attention must now turn to addressing persistent gaps and future-proofing the organisation in light of rapid technological advancements.

Progress has been made, but many organisations are still grappling with complexities around data ownership, including third-party data, which leads to weaknesses with risk data aggregation and reporting capabilities. Accurately reporting on data quality and associated KPIs remains a struggle, and comprehensive data lineage documentation is often lacking. Crucially, employee training and awareness on data management responsibilities often fall short. This lag in data governance maturity poses a significant risk as AI adoption accelerates. Without a solid foundation, organisations risk jeopardising the effectiveness of their analytics and potentially amplifying biases inherent in poorly managed data. Internal audit must now guide organisations in bridging this gap, ensuring data governance evolves in step with technology and enables responsible AI implementation.

What you should know

- **Technology development is outpacing data governance progress:** Whilst many organisations have built good data governance foundations, there is still work to be done to stay ahead of the rapid advancement of digitalisation and technology, such as GenAI, and its impact on data governance.

- **Data lineage in a complex world:** Tracking data lineage has always been important, but the volume, velocity, and variety of data used in AI, often sourced from multiple internal and external systems, creates a new level of complexity for organisations to unravel.

- **AI governance integration:** Data governance frameworks need to be adapted to support responsible AI implementation, in line with regulatory requirements. This is new territory, requiring internal audit to assess for emerging risks related to bias, transparency, and accountability in AI systems.

- **Employee training:** With evolving regulations and the ethical implications of AI, simply delivering data awareness training is insufficient. Programmes need to be driving measurable changes in employee behaviour and decision-making related to data handling, privacy, and the ethical use of AI.

- **Regulation:** In the Financial Services sector, regulators continue to scrutinise firms' data management and data governance practices over risk data, from aggregation capabilities to internal risk reporting practices. A progress report assessing the adoption of BCBS 239, indicates that despite notable improvements, weaknesses and challenges persist in fragmented IT landscapes and deficient risk data aggregation and reporting capabilities (RDARR). We expect Financial Services regulators to intensify their enforcement to promote widespread RDARR compliance.

What should internal audit be doing?

1 **Data framework:** The focus should shift towards assessing the effectiveness of these frameworks, especially when dealing with the complexities of third-party data. This includes evaluating how well organisations identify and manage risks related to data shared with and received from external entities. This should include coverage of standardised processes and controls around access, authorisation, use, security, and sharing.

2 **Data quality reporting and KPIs:** Scrutinise the reliability of data quality reporting and the KPIs used to measure it. The focus should be on whether the chosen metrics accurately reflect the organisation's data quality risk posture, and if they are timely and effectively communicated to relevant stakeholders, including regulators, as applicable. This should include (where applicable) the measurement of data risk exposures for key RDARR metrics and reporting.

3 **Data lineage gaps:** Go beyond simply checking for data lineage documentation, and assess the level of process automation and coverage across their entire data pipeline, including subsidiary data, for example. The focus should be on evaluating the granularity, completeness and accuracy of this data. Internal audit should clearly understand and visualise the flow of data from data sources, to consumption and reporting, and whether/how it is effectively used to support data governance efforts, particularly in the context of increasingly complex data pipelines.

4 **Test the effectiveness of data management training programmes:** Assess the effectiveness of these programmes in raising employee awareness and driving behavioural change. This includes evaluating whether training content is current, relevant, and accessible to all employees handling sensitive data.

5 **Bridging the gap for responsible AI and the UK National Data Strategy:** Internal audit has a crucial role in holding management accountable for responsible AI implementation and alignment with the UK National Data Strategy. This includes evaluating the robustness of data governance frameworks in supporting ethical AI, identifying potential risks related to data quality, bias, transparency, and accountability in AI systems, and ensuring alignment with the strategy's principles, particularly within data-intensive sectors like the NHS. This focus on data-driven innovation within the public sector amplifies the need for robust data governance and ethical AI practices, areas where internal audit can provide valuable oversight.

6 ⟷ 6 55% Audit planned % 13% Audit effort % 32% Use of analytics %

Resilience

Resilience has been one of the most crucial areas of focus for firms across all industries over the past few years, in particular, for Financial Services firms; with the deadline for implementation of the Prudential Regulatory Authority (PRA) Supervisory Statement “SS1/21, Operational Resilience”[1] rapidly approaching, most firms will be in full flight implementation. Firms should also be starting to think beyond 31 March 2025 to the transition to business as usual. Early planning will help to realise efficiencies and synergies more quickly as a firm’s approach is refined. Likewise, the Digital Operational Resilience Act (DORA) is due for implementation on 17 January 2025[2], and is pushing activity at clients with exposure to EU markets.

Whilst particularly relevant in the Financial Services sector we have seen an increase in focus on operational resilience across all other industries.

What you should know

- The Financial Conduct Authority (FCA) published a webpage in May 2024[10] setting out their insights and observations for firms as they look to the 31 March 2025 deadline. This includes observations relating to important business services (IBS), impact tolerances, mapping and third parties, scenario testing, vulnerabilities and remediation, response and recovery plans, governance and self-assessment, embedding operational resilience and horizon scanning.

- Several observations made by the FCA highlight a lack of consideration both in terms of breadth and granularity of the topics in question. There is also repeated emphasis of the need for firms to continue to mature their approaches over time, rather than seeing 31 March 2025 as the endpoint.

- With this in mind, and as project teams are disbanded, the transition to business as usual will require careful consideration to ensure that the firm’s approach continues to develop. Foundational to this will be clarity around ongoing ownership, roles and responsibilities.

- All firms, but especially those who started the journey toward compliance at a later date, should have taken a risk-based approach towards compliance and should have a clear plan with well understood timelines.

- Part of the transition to business as usual will be the transferral of routine tasks such as the execution of the routine reassessment of IBS following both time and event-based triggers. Firms should ensure that the cadence of these reviews is clearly defined, planned and resourced for and appropriately communicated through governance.

- The UK government’s increasing reliance on cloud solutions like Azure and AWS, while offering advantages, necessitates a nuanced approach to operational resilience. It is crucial to dispel the misconception that cloud adoption absolves organisations of IT Disaster Recovery (ITDR) accountability. While providers maintain robust infrastructure, organisations remain responsible for data security, compliance, and business continuity within the cloud.

What is DORA? →

What should internal audit be doing?

1 **Dedicated and embedded assurance.** Beyond 2025, internal audit functions should consider how to best achieve breadth and depth of their assurance coverage through both dedicated reviews and embedding resilience considerations in other planned audits. Internal audit should also consider assessing the adequacy of provisions to support the transition to business as usual 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 towards resiliency by design, and integration with existing technology resilience processes such as disaster recovery, and incident response.

2 **Benchmarking.** Internal audit functions who understand how their firm’s approach to operational resilience compares to peers 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.

3 **Management information (MI).** The importance of management information, post the implementation deadline 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, its ability to support decision making as well as the adequacy of proposed actions for management to take where triggers are breached.

4 **Third parties.** Assurance of operational resilience is intrinsically linked to third party risk management. Internal audit may wish to undertake a review specifically focussed on the operational resilience aspects of key third parties. This includes tracking any remediation the firm has required third parties to undertake, consideration of substitutability and exit arrangements.

5 **DORA gap analysis and action plan documentation.** With many firms having completed their gap analysis, the focus of internal audit should shift to assessing the adequacy of the programme of remediation activity, how this is being tracked, whether the activity is sufficient to address the gaps identified and whether activity will be complete by the deadline. Consider reviewing the firm’s approach to proportionality and some of the mapping exercises that have been performed to ensure they are an accurate reflection of the end-to-end processes being considered. Testing plans should be examined by internal audit to ensure they appropriately cover identified critical or important functions (CIF) and the information and communications technology (ICT) services required to deliver these functions; scenarios should reflect the changing environment of ICT risk, encompassing the current and potential risk landscape.

6 **DORA governance.** Functions may also wish to examine the governance arrangements for DORA, beyond the remediation programme. This should include consideration of the target operation model for supporting compliance with DORA as business-as-usual including involvement of the correct stakeholders, ownership and oversight.

7 ↑ 9 53% Audit planned % 13% Audit effort % 75% Use of analytics %

Identity and access management (IAM)

In the last 12 months, 93% of organisations suffered two or more identity-related breaches[11].

A robust identity and access management (IAM) control environment continues to be increasingly vital in today's business environment, which is demonstrated by the rising status of cyber-attacks and data breaches, due to IAM weaknesses. IAM is a framework of policies and technologies ensuring that the right users (identities) have accurate rights regarding access to technology resources (systems, applications, networks, and data). IAM systems manage and govern user access so that only the right people can access certain resources, and proper tracking and monitoring of their acts is carried out. It could assist organisations in protecting sensitive data and systems from the hands of unauthorised personnel by making certain that only authorised employees' access whatever they need to carry out their work.

Privileged Access Management (PAM) is a specific element of IAM which manages access to critical applications and sensitive data within an organisation. PAM identifies that there are some user accounts, known as 'privileged accounts', where the holders of these elevated permissions could do significant damage to an organisations security and operations if they were somehow compromised. Good practice includes the implementation of robust methods for user-authentication, i.e., to support multi-factor authentication (MFA) in authenticating users requesting access. This also includes defining specific access controls, making sure that users are only given the least privilege needed to do their work.

What you should know

Some of the key trends likely to shape the world of IAM into 2025 include:

- Organisations move toward an "identity-first" security stance, wherein it is believed that who a user is, as opposed to their role or function, becomes important in determining privilege access to resources and systems.
- Cloud-based IAM solutions will gain momentum due to increased scalability, flexibility, accessibility, and strong security features.
- The concept of Zero Trust-namely, "never trust, always verify" continues to be important. That would also mean constant re-verification of users based on several factors, such as what, when, where, and why they access resources.
- Artificial intelligence (AI) and Machine Learning (ML) are transforming IAM technologies. Along with this transformation comes anomaly detection, threat prediction, and more sophisticated authentication mechanisms.
- With the adoption of passwordless authentication methods, including biometrics and hardware tokens, organisations are bringing down associated risks with traditional credentials.
- Business-to-Business (B2B) IAM appears as a separate product category which helps organisations meet those particular needs for safe and efficient access to external partners, suppliers, and customers.
- Behavioural biometrics has gained momentum and are being used to analyse the behavioural pattern of users with a view in authenticating their identity. This has brought another element of security and is not based on traditional credentials only.

What should internal audit be doing?

1 **Deep dive into IAM architecture:** Evaluate the IAM architecture to validate if it is aligned to business needs, is compliant with security mandates and any applicable standard or regulatory framework. Identify gaps, redundancies and opportunities for improvement present in the existing architecture that will help drive further IAM effectiveness.

2 **Identity threat detection and response:** Identify common patterns or anomalies in access activity that may otherwise suggest potential threats to an identity. Deploy strong identity threat detection to stop activity before unauthorised access even occurs and limit the damage from potential breaches.

3 **Review access lifecycle management:** Conduct a detailed review of how access to user is granted, changed, and withdrawn over its lifecycle. Ensure compliance with internal policies and external industry standards / regulations for all access-related activities. Focus on the efficacy of automation and related controls.

4 **Foster collaboration with IT and security teams:** Embed IT and security teams within the IAM environment / community to understand better joint processes, controls, and risk management and respective roles and responsibilities. Share MI around regular audits, assessments, and continuous improvement programmes to improve the organisation's security posture overall.

5 **Continuous auditing:** Many organisations explore the use of analytics to automate access reviews, role assignments and permission management that can drive continuous auditing initiatives, reduce effort, and lead to more efficient data auditing practices.

8 ↓ 5 53% Audit planned % 10% Audit effort % 40% Use of analytics %

Cloud

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

The substantial resources required for Generative AI (GenAI) have concentrated its development in the hands of major tech companies like Microsoft (Azure), Google, and Amazon Web Services (AWS). This reliance on cloud hyper-scalers 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 organisations to enhance operational resilience, it also raises concerns about over-reliance on cloud providers and third-party vendors. Cyber security risks are also heightened in this environment, demanding increased vigilance and sophisticated mitigation strategies. Internal audit teams recognise that cloud computing is an enduring aspect of the business landscape.

What you should know

- The rapid adoption of cloud technologies across industries has led to a surge in cloud spending. However, Deloitte's observations indicate that 30-40% of this expenditure can be attributed to inefficient practices and inadequate controls. Forrester estimates that, if left unaddressed, this wastage could double within the next two to three years[12]. Consequently, cloud cost optimisation is paramount, particularly as initial business cases for cloud adoption often cited potential cost savings that remain unrealised.

- As a multifaceted subject, cloud intersects with numerous other risk themes, including cyber security, data privacy, people, governance, regulatory compliance, and IT operations. Its integration into critical business processes and systems amplifies its risk profile, making it essential for internal audit to consider as part of broader technology-related risk domains. The dynamic nature of cloud security, coupled with increased investment in this domain (as highlighted by Gartner), underscores the evolving threat landscape[13].

- Traditional, one-off audits are giving way to a more cyclical approach, with more frequent assessments ensuring continuous assurance and proactive risk management. This evolution stems from the realisation that cloud environments are dynamic and constantly evolving, demanding more frequent scrutiny to keep pace with emerging risks and changing regulatory landscapes. Furthermore, cloud audits are no longer confined to high-level control assessments; they are becoming increasingly technical, demanding deeper dives into configurations and architectures to effectively identify and mitigate vulnerabilities.

What should internal audit be doing?

1 Prioritise cloud computing as a core component of all audit plans, recognising its integral role in the modern enterprise's digital ecosystem. However, a common pitfall is the lack of specialised cloud expertise during the planning process, often resulting in generic "cloud" audits that lack focus and depth.

2 While assurance over cloud environments is typically sought during the initial deployment of platforms or solutions, it's crucial to recognise that the utilisation and inherent risk profiles of these services are subject to change over time. Consequently, relying solely on point-in-time assurance can lead to outdated assessments that fail to reflect the evolving threat landscape and operational context. Therefore, consider cloud as a recurring feature in audit plans to ensure ongoing alignment with the evolving threat landscape and operational context.

3 To optimise audit coverage, organisations should adopt a more targeted approach. This involves aligning cloud audits with key technology risks and, crucially, the organisation's unique risk universe and appetite. For instance, prioritise cloud security audits for platforms critical to business operations. Integrating cloud-literate specialists into the planning process ensures the identification of specific cloud risks most relevant to the organisation, promoting a more robust and insightful audit.

9 ↓ 7 50% Audit planned % 12% Audit effort % 47% Use of analytics %

Third party risk management (TPRM)

Management of third-party risk continues to face significant scrutiny, recognising the crucial role third parties play in supporting organisations' important business services. There are known challenges firms are still facing in handling supply chains, managing visibility of extended third-party relationships, and navigating the geopolitical and macro-economic landscape.

Many organisations will have experienced disruption of business services supported by critical third-parties due to issues such as cyber-attacks, data breaches and compliance failures. Our Global TPRM survey[14] has shown that mature TPRM practices are based on deeper trust and transparency with third parties.

What you should know

- The EU and UK authorities are set to finalise their proposed approach[15] for overseeing critical third parties by early 2025. Third parties that expect to be designated as critical in both the UK and the EU can start evaluating an optimal and coordinated approach to implementation.

- In the Financial Services sector, as the Prudential Regulation Authority (PRA) and EU's operational resilience requirements transition deadline approaches in Q1 2025, organisations must strengthen the connection between operational resilience and existing third-party frameworks to ensure impact tolerance limits are not impacted by disruption at third parties.

- Prescriptive regulatory requirements and increased third-party disruptions have intensified regulatory scrutiny, prompting large-scale remediation and transformation activities that require greater collaboration across all three lines of defence.

- An organisations use of new technologies to manage third-party risk, including using Generative AI (GenAI) based tools, should prompt a review of the TPRM framework to evaluate emerging AI related risks (e.g. underlying data quality, algorithm reliability, cyber security, data privacy, and ethical considerations), as these may give rise to reputational and financial risks.

- The Corporate Sustainability Reporting Directive (CSRD) requires firms 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; recognising an increasing need to evaluate and report on sustainability risks beyond the organisation's own activities.

What should internal audit be doing?

1 **Integration and embedment of regulatory requirements:** Internal audit should consider undertaking a review to assess the level of embedment of relevant regulatory requirements. As well as testing integration of the regulatory requirements the review could consider: the adequacy of compliance reporting to management and the Board; third-party contract compliance with regulations; record-keeping; monitoring intra-group arrangements; efficacy of third-party risk assessment; and monitoring to mitigate service disrupting risks.

2 **Integrated approach to third-party management:** A common root-cause of ineffective TPRM stems from the absence of a cross functional and enterprise-wide framework. Internal audit should challenge the TPRM operating model and its integration with relevant functions to understand how silos are avoided and synergies realised. The approach here should also look at the clarity of roles and responsibilities to ensure a comprehensive risk monitoring, and consistent third-party record-keeping.

3 **Resilience across the supply chain:** Audits looking at operational resilience should include adequate coverage of third parties. Internal audit should evaluate how third-party roles are linked to the firm's operational resilience requirements and assess how the impact of third parties on the important business services has been evaluated, as well as the calibration of tolerance limits. The review could also consider how third-party failures have been incorporated in stress testing scenarios and the adequacy of BCP and exit plans for critical third parties.

4 **Concentration risk across extended supply chain:** Internal audit should look to understand how its business has ensured that appropriate metrics are in place to detect concentration risks that may exist within the supply chain, across multiple dimensions. The adequacy of mitigation actions to minimise concentration, and the processes to swiftly substitute third parties should also be considered.

5 **Emerging risks:** Internal audit may wish to consider assessing the maturity of the TPRM framework to address emerging risks, including AI-related risks from third-party use and TPRM impacts and opportunities in relation to CSRD reporting.

10 ⟷ 10

Emerging technology trends

In this section, we highlight a selection of responses from our survey under the wider umbrella of "emerging trends", topics that may not be relevant for all functions or industry sectors, however they reflect key emerging risks and areas for many organisations as well as regulators.

These topics are: **ESG technology; quantum security; digital assets and distributed ledger technology (DLT).**

ESG technology → Quantum security → Digital assets and distributed ledger technology →

Quantum security

Quantum computing promises transformative simulation and modelling capabilities across a diverse range of industries. However, these advances will also introduce significant risks via the potential threat of disruption to some widely used encryption standards, and many organisations are still unaware of that threat. We believe quantum technologies and the resultant threat to cryptography will likely not follow the "normal" linear sequential path for emerging technology as risk emerges and regulations evolve.

Today's quantum computers are not able to break cryptography, and this will likely not happen until a so-called Cryptographically Relevant Quantum Computer (CRQC) is available, which many experts believe to be ten to fifteen years away. It is widely believed, however, that threat actors may already be stealing large amounts of encrypted data in the anticipation that a CRQC will be available in the future – a so-called "harvest now, decrypt later" attack.

In terms of the regulatory environment, the US National Institute of Standards and Technology (NIST) is expected to publish final standards for quantum-secure cryptographic algorithms by the end of 2024 and has released initial drafts for comment. These documents, such as FIPS 140 in cryptography, are well-known and internationally recognised and, therefore, may serve as de facto standards worldwide.

The big question really for technology leaders and auditors is how long the transition to quantum-resistance is going to take, and what do they need to do proactively, to start getting ready. The following steps can assist organisations to be poised to adopt standards or respond to regulations in an orderly way.

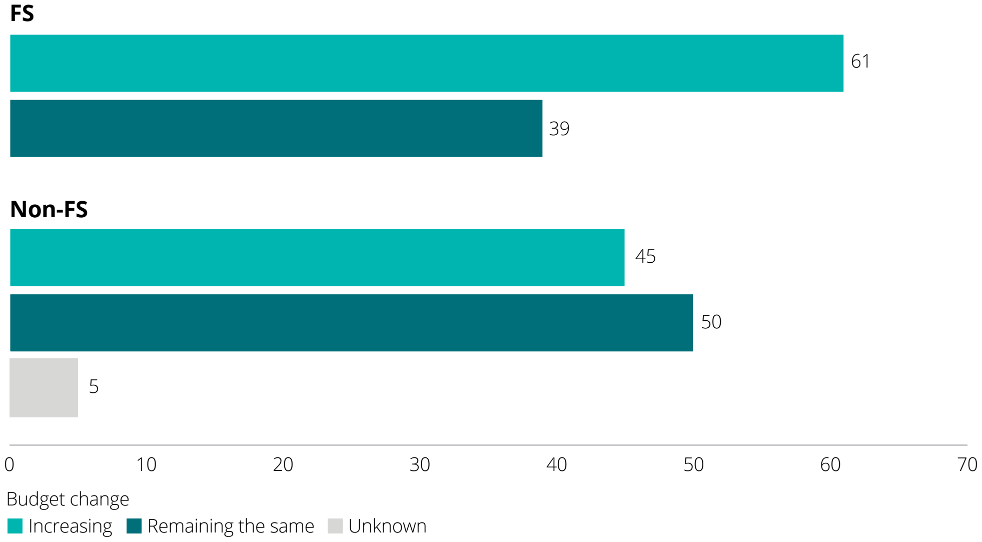
- Organisations should first understand what vulnerable cryptography they currently use, and what data would be affected by a CRQC attack. This is already being required of US federal agencies.
- Conduct an organisational cryptographic and data inventory to understand the potential exposure.
- Assess that risk alongside other organisational cybersecurity risks, leveraging a progressive framework such as the NIST Cybersecurity Framework (CSF). Reviewing organisational cryptographic hygiene can often lead to unexpected observations, which can subsequently lead to control improvements that may support and accelerate the quantum security journey.
- Develop a quantum security strategy and roadmap to achieve cryptographic agility—that is the ability to readily interchange or add cryptographic capabilities. Implement Post-Quantum Cryptography (PQC), which is designed to protect data from quantum computer attacks.

Key challenges for technology internal audit teams

Our survey showed that the number of days dedicated to technology, cyber and change audits as a percentage of the overall internal audit plan was roughly consistent across Financial Services and Non-Financial Services organisations at 20% and 25% respectively.

Budgets for technology and cyber audit teams seem to have increased in the past year, with 61% of Financial Services respondents reporting an increase in budget, versus a 39% of Non-Financial Services organisations. This is driven by increased regulatory requirements in the Financial Services sector, and indeed, the need for additional capacity / capability to cover areas such as DORA, AI, and cyber.

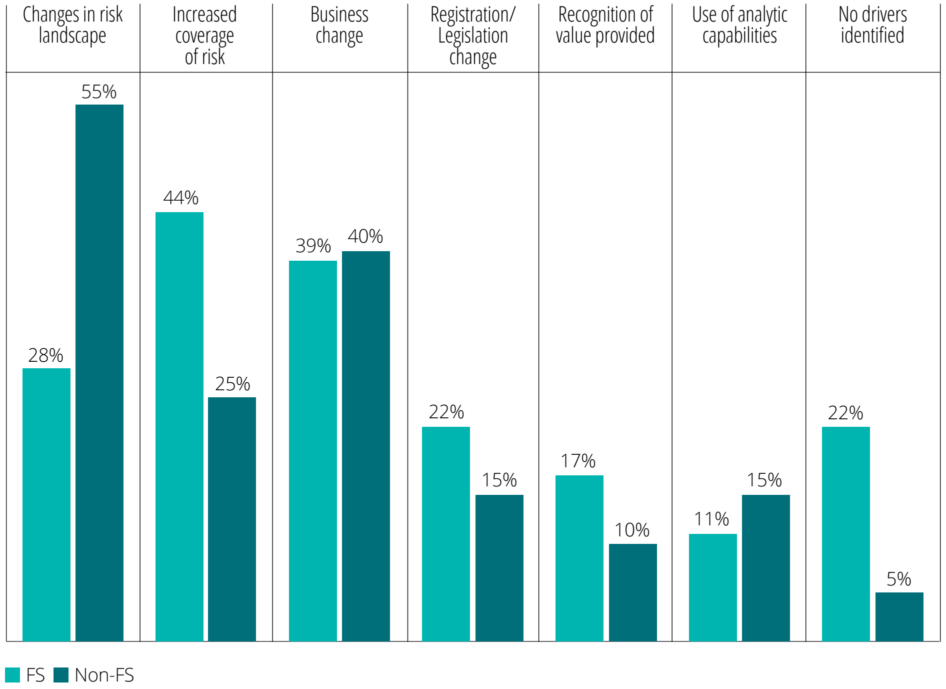
ITIA effort days increasing/decreasing



There are also clear drivers for the increased focus on technology risk that are common across sectors, with the top three drivers for the increase to technology audit budgets being:

1. Changes in risk landscape (55% Non-FS; 28% FS);
2. Business change (40% Non-FS; 39% FS); and
3. Increased coverage of risk areas (25% Non-FS; 44% FS).

Drivers for changing ITIA budget



Changes in the risk landscape are driven by emerging technologies and associated cyber threats, which we have commented on earlier in this paper. In addition, business change, which is often underpinned by supporting technology, also poses an increased risk to the technology risk landscape. More mature organisations will have mechanisms in place to ensure technology risks arising from business change are identified and discussed with technology teams, so they can be managed appropriately. The increased coverage of risk areas nods to understanding the complexity of regulatory requirements, and changes thereof, and ensuring the team has sufficient capacity and capability to cover these risks in a proportional way.

Regarding challenges for functions, capacity of the business to support the audit work was a common response across sectors, which acknowledges that increasingly organisations have been through re-organisational activities, have an increased book of work to deliver, and are being asked to deliver more with less.

Additional key challenges for Financial Services internal audit functions, include:

- Effective use of data analytics (44%)
- Building the 'function of the future' (32%)
- Pace of change (39%)

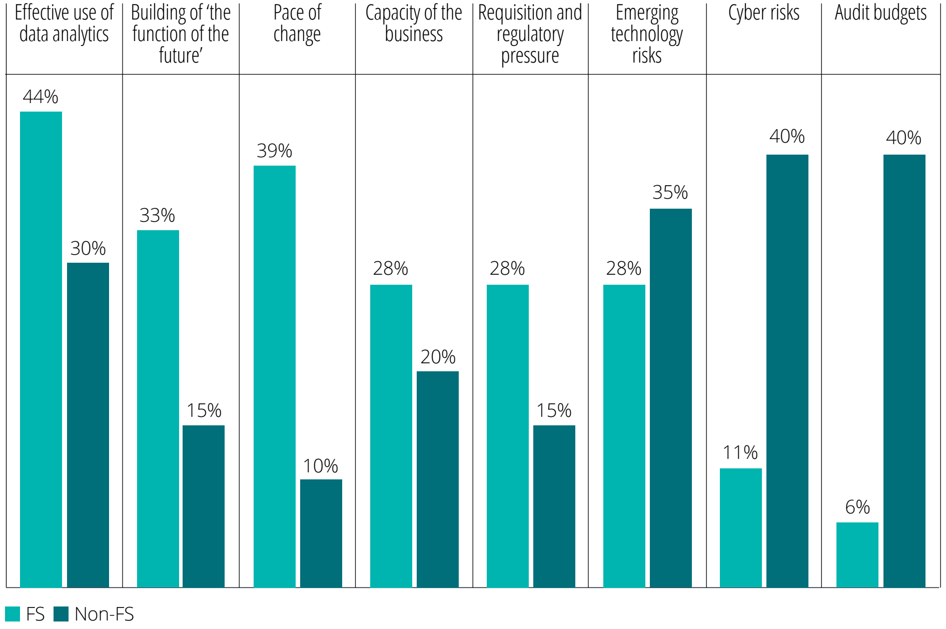
Non-Financial Services organisations cited the following:

- Cyber risks (40%)
- Audit budgets (40%)
- Other emerging technology risks (35%)

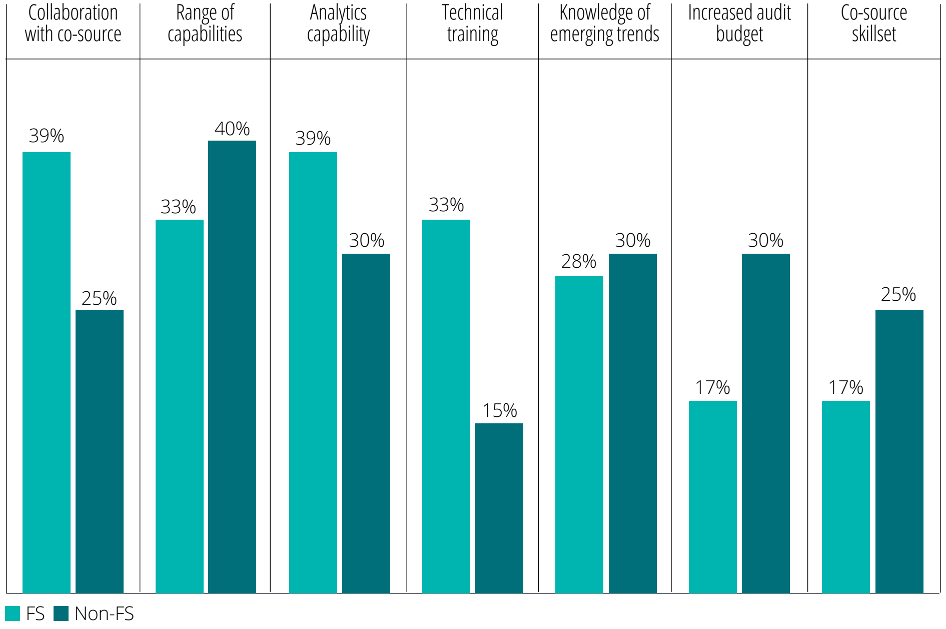
All respondents cited the capability of their internal audit teams as critical factors in being able to navigate these challenges. Collaboration with co-source partners and enhancing skills of the existing team, particularly around data analytics, are key activities internal audit functions can undertake to help manage these key challenges in upcoming years.

- Collaboration with co-source : FS - 39%, Non-FS - 25%
- Range of capabilities within the internal audit team: FS - 33%, Non-FS - 40%
- Analytics capability: FS – 39%, Non-FS - 30%

Key challenges for the IT Audit team



Key skills/resources for dealing with identified challenges



Appendices

About the survey

The aim of this survey was to understand the key areas of IT focus across internal audit functions, obtain perspectives on common challenges, and provide our insights regarding these emerging IT risks that could help support the audit planning process across industry.

We surveyed senior audit professionals from 38 organisations, across UK industry sectors. Figure A illustrates the sectors and sub-sectors of the respondents.

The size of functions in the companies we surveyed ranged from outsourced functions to those with over 100 full-time equivalents (FTEs); Figure B captures this breakdown.

The professionals that we surveyed and interviewed consisted mainly of the Heads of IT Internal Audit (or equivalent) but where appropriate, we also interviewed Chief Internal Auditors, Heads of Internal Audit, and IT Audit Directors.

This survey was commissioned by Deloitte LLP and was conducted by our senior Risk Advisory practitioners through our online survey tool; the data was collected between June and August 2024. As well as capturing the key IT internal audit risks noted by senior audit professionals, our research team has also leveraged the quantitative and qualitative data provided to understand technology and risk themes and trends developing across internal audit functions.

The output of this paper, therefore, includes technology and digital internal audit hot topics as identified by industry experts, alongside our perspectives on why these areas are important, recent developments, what internal audit functions should be doing about them, and any key challenges that must be overcome to meet these risks.

Figure A.

Sector breakdown of respondents

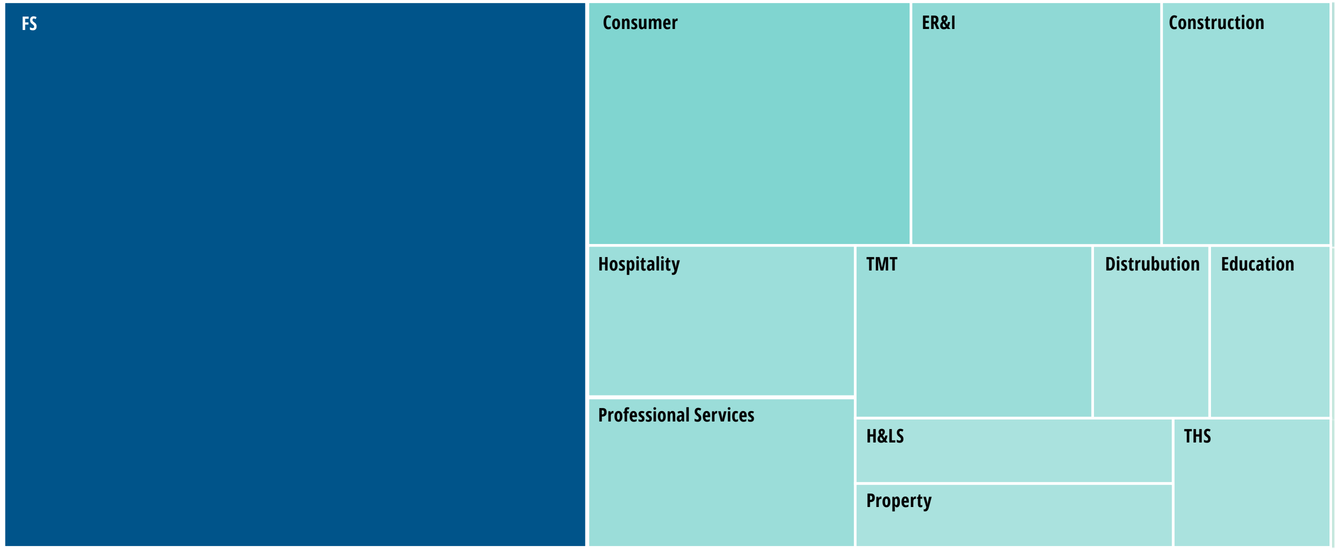
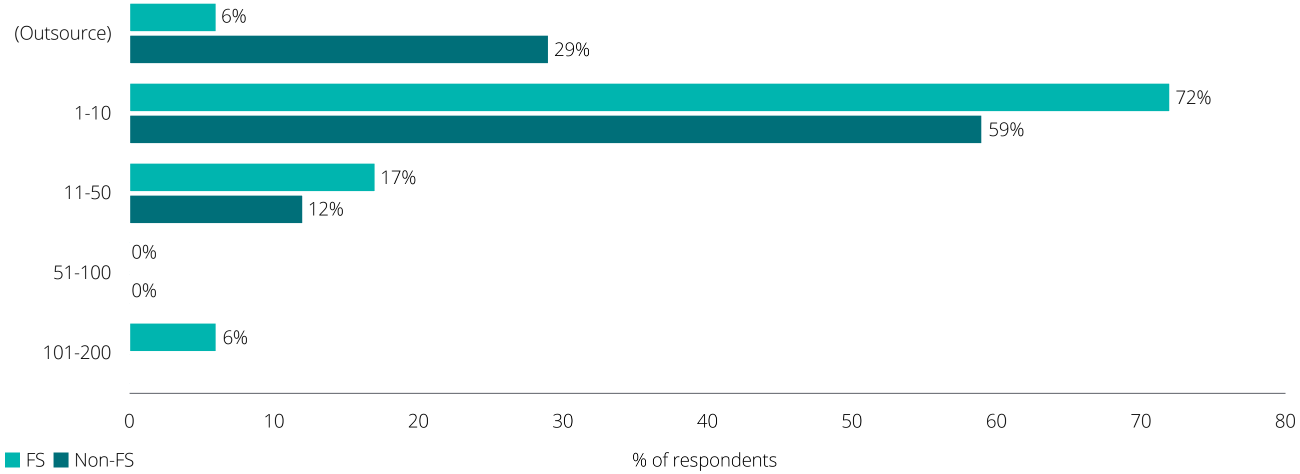


Figure B.

How many FTE work in Global ITIA Function



Additional sources and references

1 SS1/21 Operational Resilience: Impact Tolerances for Important Business Services | Bank of England

2 The Digital Operational Resilience Act (DORA) | Deloitte UK

3 Cyber Security Skills in the UK Labour Market 2023 | GOV.UK

4 The 2024 Compliance and Financial Crime Salary Survey Guide | Barclay Simpson

5 Cyber Security Sectoral Analysis 2024 | GOV.UK

6 Cyber Security Risks to Artificial Intelligence | GOV.UK

7 Overview of SOC | National Crime Agency

8 Internal Audit Planning Priorities 2025 | Deloitte UK (Section 8)

9 A Guide to Using Artificial Intelligence in the Public Sector | GOV.UK

10 Operational Resilience: Insights and Observations for Firms | FCA

11 Identity Security Threat Landscape 2024 Report | CyberArk

12 Top 10 Facts Tech Leaders Should Know About Cloud Cost Optimization | Forrester

13 The Expanding Enterprise Investment in Cloud Security | Gartner

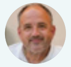
14 Third Party Risk Management Survey 2023 | Deloitte

15 Critical third parties (CTPs) – navigating the EU's and UK's new regulatory frameworks | Deloitte UK

Key contacts and contributors

Cyber security

Poppy Khan
Director
pokhan@deloitte.co.uk


David Morris
Associate Director
dmorris@deloitte.co.uk

Digital transformation and IT change

Lee Hales
Director
lhales@deloitte.co.uk

Olga Harte
Senior Manager
oharte@deloitte.co.uk

Technology strategy and governance

Mark Westbrook
Director
markwestbrook@deloitte.co.uk

Artificial intelligence including GenAI

Lewis Keating
Director
lkeating@deloitte.co.uk

Data

Nanette Scott
Associate Director
nanettescott@deloitte.co.uk

Resilience

Mark Westbrook
Director
markwestbrook@deloitte.co.uk

Adam Blair
Senior Manager
adblair@deloitte.co.uk

Identity and access management (IAM)

Poppy Khan
Director
pokhan@deloitte.co.uk

Haroon Abbas
Associate Director
haabbas@deloitte.co.uk

Cloud

Fiona Ban
Associate Director
fjban@deloitte.co.uk

Rupert Hargrave
Senior Manager
ruphargrave@deloitte.co.uk

Third Party Risk Management (TPRM)

Sonia Verbeeck
Director
sverbeeck@deloitte.co.uk

Roshan James
Senior Manger
roshanjames@deloitte.co.uk

ESG technology

Hetty van derWal
Associate Director
hevanderwal@deloitte.co.uk

Quantum security

Itan Barnes
Specialist Cyber Leader
ibarmes@deloitte.nl

Digital assets and distributed ledger technology (DLT)

Mustafa Kanchwala
Director
mkanchwala@deloitte.co.uk

With additional thanks to:

Rubal Mehta
Senior Manager
rubalmehta@deloitte.co.uk

Matt Whitfield
Manager
mwhitfield@deloitte.co.uk

Matt Brennan
Senior Manager
mpbrennan@deloitte.co.uk

Kyle Taylor
Assistant Manager
kstaylor@deloitte.co.uk

Talal Sangar Raja
Senior Manager
traja@deloitte.co.uk

Alicia Le Cheminant
Senior Consultant
alecheminant@deloitte.co.uk

Dom Hamilton
Manager
domhamilton@deloitte.co.uk

Henry Berry
Consultant
heberry@deloitte.co.uk

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please click here to learn more about our global network of member firms.

Designed by CoRe Creative Services. RITM1818465