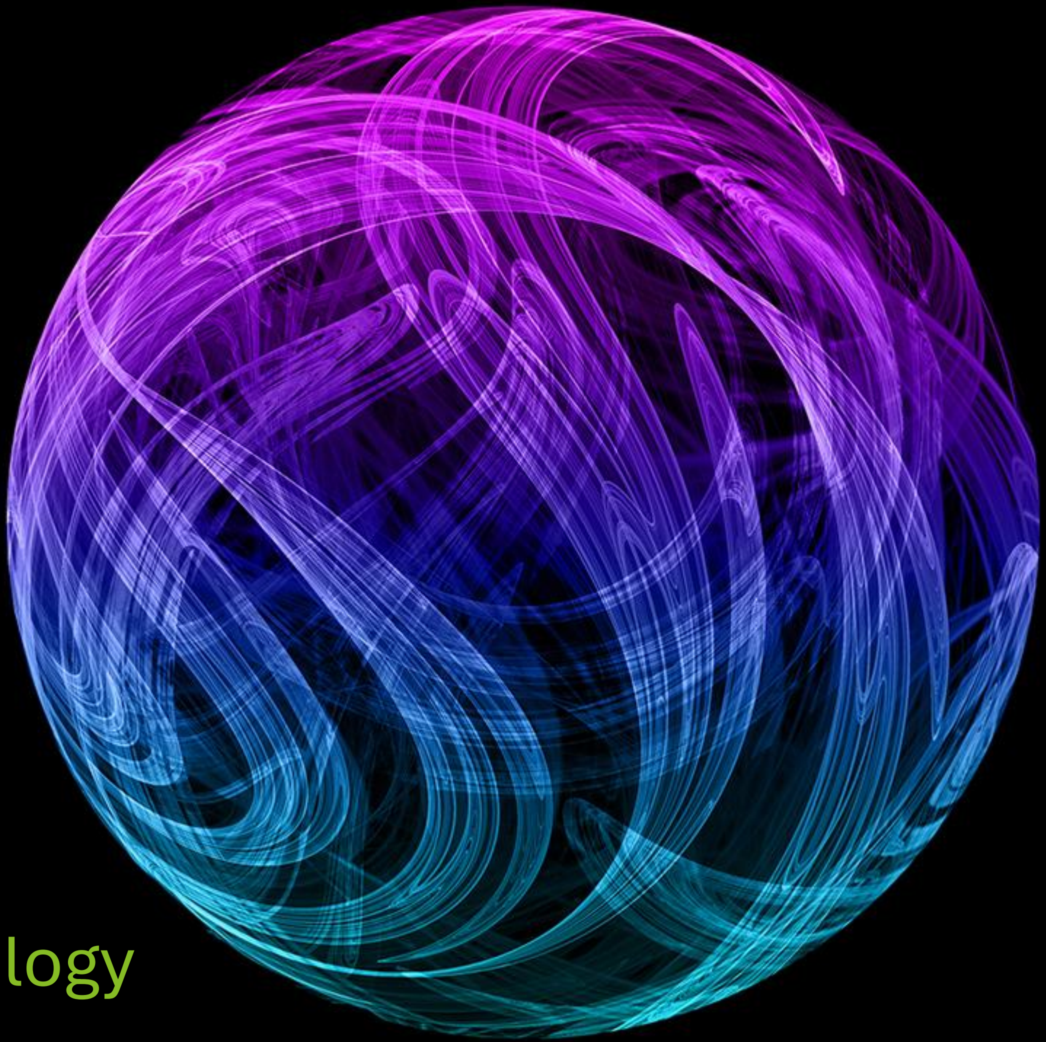
Deloitte.



Hot topics for technology and digital risk 2026

Navigating uncertainty: An internal audit perspective

Executive summary

Welcome to the 15th edition of our annual paper on the hot topics in technology and digital risk.

The report's release is timely, given the unprecedented challenges facing organisations. Rapid technological advancements, particularly the ultra-rapid acceleration of artificial intelligence (AI), are creating a volatile digital risk landscape, exacerbated by increasing system interconnectedness, evolving regulations, and ongoing global uncertainty and geopolitical disruption. Key technological shifts in 2025-26 include the rise of generative and agentic AI (GenAI), the proliferation of Internet-of-Things (IoT), increasingly sophisticated cyberattacks, and vulnerabilities within global supply chains.

Successfully navigating this complex landscape requires a dual focus: leveraging technological advancements, such as automation and AI, to foster competitiveness, reap the business rewards and enhance efficiency, while simultaneously strengthening foundational risk management practices. Robust IT governance, resilience, and effective third-party risk management are paramount. Recent high-profile cyber incidents serve as stark reminders of the criticality of these foundational elements.

This year's paper advocates once again the crucial role of internal audit in mitigating these risks, protecting the business and safeguarding regulatory compliance. It explores how functions can effectively integrate innovation and established principles to create a comprehensive and future-proof risk management strategy, enabling organisations to confidently seize the business opportunities presented by emerging technologies while mitigating the associated risks.

The survey data hopefully provides a valuable benchmark for organisations to assess their own preparedness and identify areas requiring immediate attention. As always, our report aims to offer practical guidance and recommendations for functions, outlining the key actions they can take to address key risks by domain, and ensure compliance with evolving regulations, such as the Institute of Internal Auditors' (IIA) new cybersecurity topical requirements.

Finally, we also tried to look beyond the immediate concerns and open the discussion on emerging technology risks. By highlighting these future challenges, we hope to equip internal audit functions - as well as CIO and IT risk functions - with the foresight needed to proactively address emerging threats and ensure the long-term sustainability and success of their organisations in an increasingly complex and dynamic technological landscape.

We hope this continues to be a valuable resource to inform discussions and enhance your 2026 risk assessment and audit planning. We welcome ongoing dialogue and collaboration with technology and audit leaders on these critical topics, so please do not hesitate to contact us if you'd like to discuss any aspect of this report further.

Table of contents

Click on each section to navigate through the report and use the home button on the right to return to this page.

Sector analysis

Rank	All sectors	Financial services	Corporates and public sector
1	Cyber security	Cyber security	Cyber security
2	Artificial intelligence (AI) risk management	Artificial intelligence (AI) risk management	Artificial intelligence (AI) risk management
3	Data governance and risk management	Data governance and risk management	Data governance and risk management
4	Supply chain risk: third-party and outsourcing	Supply chain risk: third-party and outsourcing	Digital transformation and IT change
5	Digital transformation and IT change	Digital transformation and IT change	Supply chain risk: third-party and outsourcing
6	Technology, cyber, and operational resilience	Unsupported infrastructure and legacy technology	Technology, cyber, and operational resilience
7	Cloud computing and sustainable technology	Technology, cyber, and operational resilience	Cloud computing and sustainable technology
8	Unsupported infrastructure and legacy technology	Cloud computing and sustainable technology	Identity and privileged access management
9	Identity and privileged access management	Identity and privileged access management	Unsupported infrastructure and legacy technology
10	Strategy and governance	Strategy and governance	Strategy and governance

Subtle yet notable differences emerge when comparing financial services responses with other corporates and public sector organisations. The ranking variations reflect differing regulatory landscapes, business models, and technological priorities.

Cyber security dominates the list, claiming the top spot across respondents and sectors. This underscores the concerns around the threat environment across the industry, and the criticality of robust cyber security strategies as the bedrock of any effective technology control environment.

Artificial intelligence (AI) features prominently across top risks, reflecting the rapid adoption of generative AI technologies in recent months across all industry sectors, and the associated challenges in managing the risks and opportunities they present. There was a notable upwards move from 4th to 2nd place this year.

Third-party risk and outsourcing show a difference in prioritisation between sectors. Financial services organisations rank third-party risks higher than corporates and public sector, highlighting the significant concern around managing risks associated with external vendors in a highly regulated environment, whereas the prioritisation of **digital transformation and IT change** by corporates and public sector organisations, compared to financial services organisations, is reflective of the concern of the pace, governance and success of technology-driven change initiatives. Industries such as retail and manufacturing face fast innovation cycles making IT change a core business driver.

Technology, cyber and operational resilience, while important to both sectors, holds the 6th position for corporates and public sector but drops to 7th in financial services. This difference might reflect the varying approaches to risk mitigation and the maturity of resilience strategies within each sector e.g. financial services, with a rather more stringent regulatory environment, already has relatively more robust resilience measures in place.

These nuanced differences highlight the importance of tailoring technology risk and internal audit strategies to specific organisation and sector contexts. While core risks remain similar, the priorities and approaches to mitigation should reflect the unique challenges and opportunities within each sector.

A perspective on the regulatory outlook for 2026 | Financial services

Deloitte's 2025 Financial Services Regulatory Outlook[1] report highlights a challenging market landscape marked by uncertainty. Geopolitical instability, economic volatility, and rapid technological advancements, particularly in terms of AI and GenAI adoption, create a complex environment.

While a soft economic landing is predicted, significant downside risks, including increased trade tariffs and geopolitical tensions, necessitate a dual approach for organisations in the sector: *vigilant short-term management* and *bold, long-term strategic transformation*.

Key trends and areas of focus to highlight:

1. **Global regulatory trends:** A global trend prioritises economic growth and national security, potentially influencing financial services deregulation. However, maintaining financial stability, combating financial crime, and responsible technology integration remain paramount. Increased interconnectedness within the financial system, especially between traditional firms and Non-Bank Financial Institutions (NBFIs), adds complexity. Central bank interest rate adjustments impact profitability, requiring firms to explore alternative strategies like fee income generation and strategic acquisitions. Reinsurers face challenges from interest rate volatility and rising "social inflation". Strategic decision-making here is crucial.

2. **EMEA regulatory landscape:** The EMEA region faces a demanding year. While major regulatory changes are unlikely in 2026, as policymakers prioritise economic growth and removing regulatory barriers, the UK's emphasis on "informed and responsible risk-taking" signals a growth-oriented approach. Streamlining existing regulations is likely, but firms should anticipate compliance costs.

3. **Sector-specific priorities:** The report highlights key regulatory priorities. Retail and commercial banks face increased scrutiny on data quality, risk culture, and governance. Investment banks must navigate CRD6 implementation, T+1 settlement transitions, and the EU's active account requirement. General insurers face intensified scrutiny on consumer protection under the Consumer Duty Act, emphasising vulnerable customer outcomes. Robust data frameworks and technological solutions are essential. Life insurers face a demanding implementation agenda, including Solvency UK reforms, liquidity reporting, and stress tests. Investment management and wealth firms face increased scrutiny on consumer protection, focusing on vulnerable customers and product value. Private market investments face greater scrutiny due to systemic risk concerns, leverage, and valuation processes.

4. **Cyber security:** UK financial services firms face a complex web of cyber security regulations. The Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) demand robust cyber security practices to protect consumers and market stability. The Digital Operational Resilience Act (DORA), though EU-originated, significantly impacts UK firms operating within EU jurisdictions, mandating operational resilience against IT disruptions. The UK GDPR and Data Protection Act 2018 govern personal data handling, requiring stringent security measures and incident reporting. The SEC mandates that public companies disclose material cybersecurity incidents within four business days of determining materiality, detailing the incident's nature, scope, and impact (Form 8-K). Annually, these companies must also disclose information regarding their cybersecurity risk management, strategy, and governance.

5. **AI and data:** There is a tension between open data ecosystems and intensified AI scrutiny. The EU AI Act necessitates proactive compliance. Firms must align data and AI strategies with a cohesive digital vision, integrating risk and compliance. Robust data governance, addressing data quality, privacy, security, and bias, is crucial. Third-party AI risk management is a key concern. Please refer to our AI-dedicated topic, in section 3.2 of the report, where we elaborate on the above and what it means for functions.

6. **Payments and digital assets:** The payments and digital assets sector faces numerous compliance deadlines. Firms must adapt to new regulations like the EU's PSD3 and the UK's safeguarding rules, considering open banking implications. The report addresses the evolving regulatory landscape for new forms of money and payments, including stablecoins and CBDCs.

7. **Sustainable finance:** The report emphasises the urgency of the sustainability transition. Policymakers prioritise industrial strategy and fiscal policy to drive economic growth. Corporate sustainability reporting under the CSRD is highlighted, along with the need for robust risk management frameworks to address climate change and nature degradation risks. The report also discusses the challenges and opportunities in sustainable finance, including scaling finance for the transition and mitigating greenwashing risks.

A perspective on the regulatory outlook for 2026 | Corporates and public sector

In 2026, organisations across sectors will face an environment of heightened regulatory scrutiny, increased vulnerability due to interconnected systems and new threats to customer and service user trust and service continuity.

Internal audit teams will need to focus on how governance, resilience and ethical safeguards are being built into technology strategy from the outset in a connected, AI enabled world.

Key trends and areas of focus to highlight:

1 **Data protection regulation enhancements:** The Data (Use and Access) Act 2025 (DUAA) necessitates a reassessment of data access controls, data usage policies, and Subject Access Request (SAR) handling procedures to ensure alignment with the amended UK GDPR, Data Protection Act 2018, and the Privacy and Electronic Communications Regulations (PECR). IT internal audit teams should focus on verifying the effectiveness of implemented changes, particularly concerning the new "recognised legitimate interests" lawful basis, the relaxed cookie consent rules and the revised requirements for automated decision-making and Subject Access Request (SAR) responses, to ensure that in relaxing processes organisations have not become non-compliant. This is especially key given the impact of increased fines for non-compliance with the PECR, bringing them in line with those for GDPR breaches.

2 **Future of AI regulation:** Delays in the UK to the artificial intelligence (Regulation) Private Members Bill and the Labour government's promised AI Bill have left significant judgements on the ethical use of AI technologies in the hands of the judiciary. Judgements to date have been grounded in broader existing laws and regulations on public rights and freedoms and use of technology. Use cases such as live facial recognition technology in policing have already been scrutinised by the courts. For example, in 2020, the UK Court of Appeal ruled that South Wales Police's use of automated facial recognition (AFR) technology was unlawful, citing "fundamental deficiencies" in the legal framework and a lack of proper oversight. Organisations would do well in the interim to look to such court rulings, combined with industry leading frameworks such as Deloitte's Trustworthy AI Framework[2] in determining a proportionate, ethical approach to leveraging AI in their workflows.

3 **Online Safety Act considerations:** Ofcom's enforcement of the Online Safety Act[3] for providers of person-to-person services (such as social media, online marketplaces, online gaming platforms and messaging apps) has been in place since 2023. As of March 2025, this includes assessing the effectiveness of systems and processes designed to identify and remove illegal content, and the robustness of mechanisms for handling user reports and complaints. Organisations need to ensure proactive risk assessments are in place, are regularly reviewed and updated, and that appropriate safety measures are implemented and monitored for effectiveness.

4 **Cyber security legislation:** NIS2[4], the European Union's (EU) updated Network and Information Systems Directive (NIS), aims to enhance the resilience of essential services and digital infrastructure. While EU member states are establishing compliance measures, the United Kingdom's (UK) Cyber Security and Resilience Bill (CSRB) has been adapted and has similarities to NIS2 for the UK context. This Bill introduces key changes and expansions, impacting organisations operating within the UK. Enforcement of these changes is anticipated in late 2025 or early 2026, although the precise date is subject to the legislative process. Both NIS2 and the CSRB impact a wide range of sectors, including Energy and Utilities, Transport, Manufacturing, Telecommunications, Healthcare, and other essential services and their supply chains, emphasising operational resilience and the security of digital technologies, including Operational Technology (OT). Organisations in both regions must understand the specific requirements applicable to their operations.

Our survey over the years

The table below presents a comparison of the top-10 technology and digital risk hot topics over the past 15 years, as identified through our annual survey of Heads of Technology Audit, Heads of Internal Audit, CIOs and business leaders, as well as leveraging our own insight and analysis across our extensive list of clients in the UK.

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

Rank	2026 (all sectors)	2025 (all sectors)	2024 (all sectors)	2023 (all sectors)	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	Cyber security	Large scale change	Third-party management	Cyber threat
2	Artificial intelligence (AI) risk management	Digital transformation and IT change	Digital transformation and IT change	Digital transformation and 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	Data governance and risk management	Strategy and 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	Supply chain risk: third-party and outsourcing	Artificial intelligence and 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 & quality	Large scale change	Data governance and quality
5	Digital transformation and IT change	Data	Cloud environments – 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 management and data governance	Third-party management	Third-party management	Cyber security	Rogue trader and access segregation
6	Technology, cyber, and operational resilience	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	Cloud computing and sustainable technology	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 management	Information security / identity & access management	Digital and mobile risk	Digital and mobile risk	Digital and mobile risk	Cloud computing	Financial crime
8	Unsupported infrastructure and legacy technology	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	Identity and privileged access management	Third party risk management	Identity and 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	Strategy and governance	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

Technology and digital risk hot topics for 2026

2026 rank	Hot topic
1	Cyber security
2	Artificial intelligence (AI) risk management
3	Data governance and risk management
4	Supply chain risk: third-party and outsourcing
5	Digital transformation and IT change
6	Technology, cyber, and operational resilience
7	Cloud computing and sustainable technology
8	Unsupported infrastructure and legacy technology
9	Identity and privileged access management
10	Strategy and governance

Keys:

Audit planned %

Audit planned % *is the percentage of respondents who have included this topic in their audit plan.*

Use of analytics %

Use of analytics % *is the percentage of respondents who, if they have included this topic in their audit plan, either currently employ or are planning to employ analytical techniques as part of that audit.*

2025 report rank

2025 report rank *highlights the rank of each topic in the previous year's report.*

1 Cyber security

89% Audit planned %

66% Use of analytics %

1 2025 report rank

In an era defined by digital acceleration and systemic unpredictability, cyber security has transcended its traditional boundaries to become a cornerstone of enterprise resilience. The cyber security landscape is in constant flux, with an increased number of cyber-attacks this year, and new threats and vulnerabilities emerging daily.

Our paper highlights five key cyber security trends expected to dominate this year and outlines five crucial actions IT internal audit functions should take to address them. The cyber security challenges facing organisations are constantly evolving. IT internal audit teams play a critical role in identifying and mitigating these risks. By focusing on the key areas highlighted here, IT internal audit can contribute significantly to the organisation's overall cyber security posture and ensure its long-term resilience. Proactive review and challenge of internal security controls, and continuous monitoring are essential for navigating the complex and ever-changing cyber security landscape.

Five things you should know about the topic:

- **Artificial intelligence (AI) is rapidly transforming the cyber threat landscape**[5]. Attackers are leveraging AI for automated phishing campaigns, sophisticated malware development, and the rapid identification of vulnerabilities. This necessitates a shift towards AI-driven security solutions for detection and response.
- **Human error remains a significant cyber security vulnerability**, despite technological advancements. The 2025 attacks on major retailers highlight this, showcasing sophisticated techniques such as SIM swapping to large-scale ransomware, using advanced social engineering, custom malware, and modified leaked ransomware code. Robust security measures, including multi-factor authentication, endpoint detection and response (EDR), data loss prevention, and comprehensive security awareness training, are vital for mitigating these threats.
- **Cyber-attacks targeting the supply chain are becoming increasingly prevalent**. Organisations need to assess and manage the cyber security risks associated with their third-party vendors and suppliers. This requires robust due diligence processes and ongoing monitoring of vendor security practices.
- **The expanding attack surface of Internet of Things (IoT) and Operational Technology (OT) devices** presents significant cyber security risks. The sheer number and diversity of these devices, often lacking robust security features, creates numerous entry points for attackers. Legacy systems, outdated protocols, and insufficient network segmentation exacerbate vulnerabilities. The potential for cascading effects from a single compromised device necessitates a comprehensive and proactive approach to security.
- **The Institute of Internal Auditors (IIA)** released their cyber security topical requirement in Q1 2025, providing a baseline approach for assessing cyber security governance, risk management, and control processes. Refer to the next page for more information.

Five things internal audit should do

1 **Assess the maturity of cyber security programs**

Internal audit should evaluate the maturity of the organisation's cyber security program against recognised frameworks such as the NIST Cyber Security Framework. This assessment should focus on the effectiveness of people, process and technology in mitigating identified risks.

2 **IIA cyber security topical requirement compliance**

The IIA's cyber security topical requirement (released in Q1 2025) will become mandatory for audit engagements. Internal audit should prioritise achieving and maintaining compliance with this requirement. This involves collaborating with information/cyber security teams to improve cyber security risk assessments, enhance the controls environment, and develop a robust technology strategy. The focus should be on aligning audit processes with the new standards and ensuring ongoing conformance.

3 **Artificial intelligence (AI) attacks**

Internal audit should assess the organisation's readiness for AI-powered attacks. This involves evaluating AI-powered threat detection systems, deepfake detection technologies, and employee awareness training. A crucial aspect is reviewing the security implications of AI deployment across all systems and processes, ensuring robust AI-related security practices are in place to mitigate risks.

4 **The evolving threat of ransomware**

Internal audit should verify security awareness training effectiveness (including phishing simulation results), assess security culture, and confirm robust access controls (least privilege, privileged account management, and effective lifecycle management). A comprehensive vulnerability management program (patching, scanning, penetration testing) and data security measures (classification, encryption, DLP) are crucial. The incident response plan requires regular testing and updates, ensuring effective communication and recovery.

5 **Supply chain security**

Third-party vendor reliance significantly expands cybersecurity risk. Internal audit should continue to review supplier risk assessments, enforcing robust cybersecurity clauses in contracts, and monitoring the entire supply chain's security posture, but consider that assurance should be based on evidence such as direct internal audit reviews of suppliers or SOC reports where appropriate, supplementing or replacing reliance on security questionnaires.

1 Cyber security

Institute of Internal Auditors' cyber security topical requirement

The Institute of Internal Auditors' (IIA) first set of specific requirements around a topic / risk domain was released earlier in the year and is around cybersecurity. The aim of the Topical Requirements is to improve the consistency, quality, and reliability of internal audit services related to cybersecurity. They provide a minimum baseline and relevant criteria for assessing governance, risk management, and control processes in this critical area.

What they are:

The Topical Requirement are a mandatory element of the IPPF to be used with the Global Internal Audit Standards.

- The cyber security requirements will become effective for audits conducted from February 2026, but early adoption is encouraged.
- They provide an approach to assessing the design and implementation of cyber security governance, risk management, and cyber control processes (such as internal and vendor-based controls to protect systems and data; controls for monitoring threats and integrating cybersecurity in IT asset management; network, endpoint communication, and software development controls).
- It contains 17 requirements (four governance; six risk management; seven controls) which are mapped against widely adopted frameworks such as NIST and COBIT. The cyber security requirements apply when cyber risk is identified as part of the risk assessment and annual planning, identified during engagements, or specifically requested.
- Applicability assessments and any exclusions must be documented, with conformance reviewed in external quality assessments.

What they are not:

- They are not comprehensive work programs. They form minimum baseline requirements to review when performing a cyber security audit – internal audit functions can, and should, cover other aspects of cyber security relevant to the risk profile of their organisation.
- They do not require internal audit functions to audit the specific risk area, unless it is identified as part of a risk assessment or specifically requested by the business / regulators. They are subject to applicability, as determined by a risk-based plan. They are not designed to circumvent legal or regulatory requirements.

1 **Timelines for implementation:**

The requirements take effect on 5 February 2026, triggering mandatory implementation. Conformance with the Topical Requirement will be assessed during quality assessments conducted after the effective date. We believe organisations should aim to adopt the Topical Requirement as early as possible to ensure a smooth transition and proactive risk management.

2 **Implementation guidelines**

- **Collaboration**: Internal audit should proactively engage with IT and security departments, sharing the cyber security Topical Requirements to foster a collaborative approach to implementation. To effectively adopt these requirements, organisations should conduct an initial assessment, update policies and methodologies accordingly, implement periodic employee training sessions, and perform periodic audits to ensure ongoing compliance with the requirements. The function can test and evaluate these requirements using the helpful documentation tool included within the IIA's user guide[6] for this topical requirement.
- **Documentation**: Coverage of the Topical Requirement can be documented in either the internal audit plan or engagement workpapers based on the auditors' professional judgment. One or more internal audit engagements may cover the requirements. In addition, not all requirements may be applicable. Evidence that the Topical Requirement was assessed for applicability must be retained, including a rationale explaining any exclusions.

The IIA released a public comment draft on **Third-Party Risk** Topical Requirements in March 2025, with a view to releasing in early 2026. The IIA is also hard at work developing new guidance for 2025/2026 on these critical topics: **culture; business resilience and anti-corruption/bribery.**

2 Artificial intelligence (AI) risk management

69% Audit planned %

56% Use of analytics %

4 2025 report rank

AI is no longer an emerging trend. It is becoming a foundational element of how businesses operate, compete and scale. In FY26, the focus is shifting to how to deploy AI that can be trusted; how to generate return on AI investment; how to govern AI; and how to align it to enterprise objectives.

The challenge is not just model risk or data quality. Integrating AI has introduced new complexities as responsibility is diffused across external developers, deployers, business owners, technical owners, data owners and users. This stratified accountability, coupled with rapidly evolving AI technology and an evolving regulatory landscape (e.g., the EU AI Act), creates novel risks requiring adaptive risk management strategies. It is therefore essential that oversight evolves alongside the technology. For internal audit, this creates a moving target.

Five things you should know about the topic:

- **Widespread AI integration:** AI is increasingly being embedded in enterprise and business systems (in many cases, by default), augmenting core operations across Financial Services, Corporates and the Public Sector. From forecasting to customer service, the risks associated with AI are now prevalent in sectors that have not historically developed and deployed AI/ML systems at scale. For Corporates and the Public Sector, in particular, governance and oversight structures have not matured at the same pace as AI adoption.
- **Governance gaps are common in AI adoption:** As businesses scale AI use cases, few have developed or uplifted governance frameworks to effectively coordinate existing risk and control areas, clarify key accountabilities, and define ethical boundaries. Ineffective governance and risk management is becoming a significant barrier.
- **Heightened AI scrutiny and regulation:** Regulators, investors, and boards are demanding greater transparency on AI risk, resilience, and compliance. Internal audit is increasingly called upon to comment on the evolving risk profile for AI within organisations and the robustness of their controls. The key question is, 'How can we demonstrate confidence in our management of AI-related risks?' This scrutiny is further amplified by the proactive efforts of UK regulators (PRA, FCA, CAA) to shape industry requirements for safe AI use, fostering dialogue and developing practical regulations tailored to the specific challenges faced by different sectors[7, 8].
- **AI risks are dynamic and interconnected:** AI related risks can evolve along the lifecycle and interact in subtle ways, potentially requiring trade-offs to be made (e.g., reliability vs explainability or cyber security vs transparency). Static AI risk assessment is not enough; appropriate monitoring, guardrails and human oversight are essential.
- **Agentic AI complexity:** Agentic AI systems (that is AI systems that can independently accomplish defined goals or tasks) are capable of multi-stepped, autonomous actions and decision-making that can create real world outcomes. This introduces another new layer of complexity for auditors. There is a need to consider not just the output of the AI but also the opaque reasoning for actions taken and decisions made by agentic AI systems, as well as potential consequences.

Five things internal audit should do

1 **Inventory and visibility of AI usage**

Internal audit should assess the completeness and accuracy of the organisation's AI systems inventory, documenting their purpose, data sources, controls, and the effectiveness of observability mechanisms. This ensures sufficient visibility to manage AI-related risks.

2 **AI in the internal audit plan**

Integrate AI audits into the internal audit schedule, tailoring scope to the organisation's AI strategy and governance maturity. Audit the governance framework (AI Policy, risk management, roles, etc.), testing against relevant frameworks (e.g., NIST AI RMF, ISO 42001, Deloitte's Trustworthy AI2) and diverse AI use cases. This provides a clear view of practical gaps in holistic risk management and evaluates overarching AI strategies.

3 **Regulatory awareness and compliance**

Identify and understand relevant AI regulations (e.g., EU AI Act[9]). Conduct a gap analysis comparing organisational practices against these requirements. Develop a plan to address any gaps, aligning regulations with the internal audit control framework. EU-based organisations should conduct regulatory readiness assessments for EU AI Act compliance, noting prohibited systems (e.g., those inferring workplace emotions).

4 **Controls framework for agentic AI**

Internal audit should assess the controls framework for agentic AI, ensuring it touches on appropriate agent evaluation, constrained actions, understood defaults, traceable activity, real-time monitoring, attributable outcomes, and team control. It should also address third-party risks and cyber security considerations related to external tool access.

5 **AI literacy capability and training**

Assess organisational AI fluency across various personas (aligning with EU AI Act Article 4), determining sufficient expertise for risk management. Include a self-assessment of the audit capability needed to support the organisation's long-term AI ambition.

3 Data governance and risk management

61%	Audit planned %
77%	Use of analytics %
5	2025 report rank

Data remains a strategic asset, but inadequate governance creates a significant competitive disadvantage, hindering innovation and efficiency while raising costs and reputational risks. The rapid growth of data and accelerating technological change (e.g., changes in the AI landscape) exacerbate this challenge[10], further amplified by the increasing reliance on data-driven decision-making across all business functions. This is reflected in data's rise as one of the critical topics for internal audit functions, moving up to the third place. Internal audit must therefore play a proactive role, guiding organisations towards sustainable data maturity and fostering a culture of data responsibility from the top down.

Five things you should know about the topic:

- **Sustained and accelerated technological change**: The rapid pace of technological innovation creates a significant challenge for organisations to keep pace with evolving data security threats and best practices. This widening gap necessitates a more urgent focus on embedding data management practices and data governance frameworks. The migration of data to the cloud introduces new risks related to data security, privacy, and compliance. Internal audit needs to evaluate the security and governance controls in place for cloud-based data.
- **Data management, privacy, and security regulations**: The regulatory landscape surrounding data privacy and security is dynamic, requiring organisations to adapt quickly and maintain ongoing compliance. While UK law relies on existing legislation to help govern the changing technology landscape, there is increasing principles-based guidance which organisations need to navigate which can create uncertainty around compliance. Regulations like GDPR in EU, CCPA in the USA, and others are constantly evolving and becoming more stringent. Internal audit needs to ensure the organisation complies with these regulations, and data management and governance are central to compliance. Failure to comply can result in substantial fines and legal repercussions.
- **Sustainable data maturity**: Achieving robust data governance is a journey, not a destination. Organisations are starting to focus on sustainable maturity, building capabilities incrementally and fostering a culture of continuous improvement; underinvestment in data architectures is a key cross-sector structural problem, and internal audit can play their role in signposting this. "Walking before running" is key.
- **Digital savviness and leadership**: A strong commitment to data governance must be driven from the top. Successful organisations set the tone at the top to champion digital literacy and foster a culture of data responsibility throughout the organisation.
- **Data resilience and business continuity**: Organisations need to build data resilience into their operations to ensure business continuity in the face of disruptions, whether caused by cyberattacks, natural disasters, or other unforeseen events.

Five things internal audit should do

1 **Prioritise and guide data governance initiatives**

Collaborate with the business to identify and prioritise key initiatives, offering practical guidance and risk assessments to bridge capability gaps and achieve sustainable maturity. Internal audit can help by highlighting lack of resources, funds, and strategic focus on the enterprise architecture to fully achieve corporate strategy and aims. The focus should be on incremental, achievable improvements.

2 **Champion a culture of continuous improvement**

Internal audit should promote the implementation of a continuous monitoring program for data quality and governance, including regular data quality assessments and process reviews. Based on the findings, specific improvement recommendations should be developed and implemented iteratively. A feedback loop should be established to track progress and ensure ongoing improvement.

3 **Promote data literacy and digital savviness**

Internal audit should champion data literacy training programs, starting with senior leadership, to foster a culture of data responsibility and informed decision-making at all levels.

4 **Proactively assess emerging data risks**

The use of emerging technologies, automation, data analytics, and AI for decision making requires strong data quality and data management processes. Internal audit needs to assess the risks associated with automated systems and ensure data quality throughout the automation lifecycle.

5 **Strengthen data resilience and business continuity**

Internal audit should assess the organisation's data resilience by evaluating its data protection and recovery mechanisms. This includes reviewing data backup and recovery procedure, disaster recovery plans, and incident response strategies for data-related incidents. This should include consideration of adherence to recovery time objectives (RTOs) and recovery point objectives (RPOs).

4 Supply chain risk: third-party and outsourcing

58% Audit planned % | 57% Use of analytics % | 9 2025 report rank

The escalating complexity of global supply chains, coupled with unpredictable macroeconomic and geopolitical shifts, has amplified the vulnerability of organisations reliant on third-party services. Cyber attacks, data breaches, and compliance failures are no longer hypothetical threats; they are frequent occurrences crippling businesses. The lack of reliable, accurate information from third and fourth parties further exacerbates the problem, leaving many TPRM programs struggling to keep pace. This is underscored by the significant rise in TPRM's ranking in this year's hot topics publication from ninth to fourth highlighting its growing importance.

Internal audit’s role is not merely to identify and report on weaknesses; it's to encourage and support the business to use TPRM in a safe and controlled way as a catalyst for improved organisational performance and therefore proactively evolve its approach. The sheer speed, volume, and complexity of emerging risks, combined with intensifying regulatory scrutiny, demand a proactive and insightful response. The Institute of Internal Auditors (IIA) is expected to finalise their topical requirements on Third-Party risk, later this year, which will be mandatory for all internal audit functions. The requirements reflect the importance of this area for the Institute and will provide practitioners with a set of baseline requirements and a consistent and comprehensive approach to assessing the design and implementation of third-party governance, risk management, and control processes.

Five things you should know about the topic:

- **Intensified FS sector regulation:** The UK's CTP Regime and EU's DORA (effective early 2025) increase FS regulatory complexity, demanding navigation of overlapping requirements for managing critical third-party relationships, focusing on business continuity (UK) and ICT (EU). Large-scale remediation is driven by stringent regulations and disruptions. The IIA's standardised TPRM audit requirements (expected September 2025) aim to improve assessments and resilience.
- **Emerging AI risks in third-party relationships:** Increased GenAI use necessitates a sophisticated TPRM framework addressing data quality, algorithm reliability, cybersecurity, data privacy, and ethical considerations to mitigate operational disruption and reputational damage.
- **Operational resilience and TPRM:** Integrating operational resilience with TPRM capabilities (e.g., BOE CP26/23, FCA PS24/16, PRA SS1/21) ensures third-party disruptions remain within acceptable impact thresholds.
- **Risk Intelligence over attestation:** Moving beyond self-reported data, risk intelligence leverages external data and analytics for a more comprehensive, objective view of third-party risks. This enables proactive threat identification, shifting from reactive compliance to predictive risk management.
- **Fourth-party risk:** Assessing fourth-party risks requires a structured approach, understanding ecosystem interconnectedness and cascading disruption effects. Critical fourth parties should be prioritised based on business service importance and data sensitivity, with dependencies mapped and broader impact appropriately considered. Assurance should be obtained through contracts, suitable monitoring, and communication practices, and through integrating into business continuity and disaster recovery plans, including exit strategies.

Five things internal audit should do

1 **Intensified regulatory requirements**

Effective collaboration across all three lines of defence and consistent internal audit involvement are crucial to ensure the business and risk areas have considered the changes in the regulatory environment and uplifted policies and processes accordingly. Effective TPRM programmes require strong senior oversight. Internal audit plays a crucial role as the third line of defence, proactively planning audits and clarifying key roles and responsibilities within the TPRM governance framework. Internal audit functions should align their TPRM audits with the IIA topical requirements once issued.

2 **Managing emerging AI risks in third-party relationships**

Internal audit may provide independent assurance on the effectiveness of controls mitigating AI-related risks within third-party relationships, encompassing data governance, cybersecurity, and compliance; this includes evaluating due diligence processes, monitoring performance, and reporting on emerging threats to management and the board.

3 **Operational resilience and TPRM**

Internal audit may evaluate the impact of third parties on the organisation's ability to remain within its impact tolerance limits by assessing the consideration of third-party failures in stress testing scenarios and reviewing the robustness of business continuity plans (BCPs) and exit strategies for critical third parties, ensuring alignment with the organisation's overall BCP.

4 **Evidence-based assurance of third-party risk intelligence over traditional attestation-based assurance**

Internal audit should test the effectiveness of risk intelligence outputs including feeding into the effectiveness of large-scale technology implementations in third-party risk management by reviewing data sources and methodology, comparing results with traditional attestation methods, testing predictive capabilities, assessing alerting mechanisms, reviewing governance and controls, and interviewing key personnel. This multifaceted approach helps determine the reliability and value of the organisation's risk intelligence program.

5 **Fourth-party risk management**

Internal audit plays a crucial role in ensuring effective fourth-party risk management. This involves assessing the organisation's TPRM framework for its coverage of fourth-party risks, particularly concerning over-reliance on specific providers; evaluating the methodology for identifying material fourth parties and assessing their risks; reviewing third-party contracts, due diligence and monitoring processes to ensure adequate fourth-party risk coverage.

5 Digital transformation and IT change

44% Audit planned %

50% Use of analytics %

2 2025 report rank

The global technology landscape is evolving rapidly, driven by the accelerated adoption of GenAI solutions, the continued automation of organisational processes and controls, ever-increasing cloud adoption, required uplifts in legacy technology to stay competitive and relevant, and a surge in market consolidations and reorganisation particularly within the insurance and banking sectors. Furthermore, ongoing geopolitical uncertainty has introduced considerable volatility into global markets, increasing risk profile, impacting investor confidence and forcing boards to refocus investment on short term and defensive capabilities.

Internal audit functions should continue to challenge the change strategy, focussing on the effectiveness of return on investment and cost reduction for major changes, strategic alignment of change objectives during transition to BAU and the effective integration of GenAI technologies.

Four things you should know about the topic:

- **A cost-effective approach to change management:** Uncertainty in market performance leads to a focus on more controllable elements of business performance, such as the prudent management of costs. Focus on controllable elements like cost management, integrating diverse resource models (e.g., offshore), lean delivery, and leveraging technology to streamline processes and improve efficiency. Risk managers and change assurance teams should identify and track the critical success factors, such as achieving clear outcomes for customers, employees, and regulators.
- **Navigating the challenges of as-a-service transition:** The rapid adoption of "as-a-service" solutions can leave customers and support unprepared, leading to change programmes not meeting their objectives during the transition to live operations. The internal audit insights and recommendations must align with integrated programme assurance teams that aim to not only provide oversight, but to advocate for customer experience, challenging the practicality of new solutions.
- **Balancing agile delivery with talent retention:** While agile and value stream change delivery methods drive innovation, retaining in-house expertise remains a challenge. Avoiding over-reliance on third parties, coupled with consistent agile application, can help to avoid wasted resources and drawn-out implementation timescales.
- **Change programme pitfalls and transitions to BAU:** Many change programmes struggle to fully realise their objectives during the transition to business-as-usual (BAU). Old problems resurface, hindering the intended benefits and highlighting the need for improved handover processes and more robust change management strategies.

Five things internal audit should do

1 **Strategic approach**

When auditing change, consider a strategic approach including the timing of key milestones and applying proportionate controls assessment based on the nature of the change; functions should challenge themselves on whether change assurance coverage is fit for purpose.

In line with the CIIA Code of Practice, internal audit activities should align on key corporate events (e.g., business process changes, new products/services, M&A activity).

2 **Governance**

Internal audit should expand its role beyond assessing the change execution. It must actively evaluate risks at portfolio-level to provide assurance over the business strategy, challenge existing practices, and to proactively assess the risks of inaction, with a stronger emphasis on governance oversight.

3 **“Skills versus skilled”**

Digitisation increased reliance on external expertise for business transformation. Future-proof skills include using tools and GenAI technologies to automate development and other processes. Internal audit should review talent management and challenge future workforce strategies.

4 **Quality of reporting and data**

Cost-cutting on change initiatives drives the need for internal audit to evaluate the appropriateness of objectives and key results (OKRs), quality of management information, stakeholder awareness, and risk management.

5 **“Never a failure, always a lesson”**

Post-implementation reviews often prioritise large transformations, but continuous improvement, like DevOps, is key for long-term sustainability. Internal audit should ensure the organisation benefits from a centralised lessons-learned repository.

6 Technology, cyber, and operational resilience

47% Audit planned % | 47% Use of analytics % | 6 2025 report rank

Technology is a critical enabler for conducting business in the digital world and therefore technology resilience is crucial in enabling organisations to operate and maintain an expected level of service, even when faced with navigating or recovering from disruptive events. The increasing sophistication of cyber-attacks[11], evolving regulatory landscape and reliance on legacy systems and/or third parties to host key services, highlight some of the key challenges that can threaten a firm's operational resilience and thus, standing in the market. This section highlights the important role that internal audit functions can play in strengthening technology resilience. While the UK regulatory deadlines have now passed, operational resilience remains a key area of focus for FS firms and internal audit functions alike. Recent large scale disruptive events highlight the continued importance in building a resilient business that can respond to and recover from a range of expected disruptions. Geopolitical instability, sanctions, trade wars, and unforeseen global events impact the organisation's ability to operate, requiring a more sophisticated approach to scenario planning than previous years.

Five things you should know about the topic:

- **Evolving threat landscape:** All organisations are having to deal with more acute, severe and frequent disruptions than ever before. This is because the threat landscape continues to evolve with climate change, geopolitical shifts and technological advancements presenting new and emerging risks. For example, cyber attacks are becoming increasingly sophisticated, utilising AI and advanced techniques to target users, exploit vulnerabilities and disrupt services. An organisation's ability to withstand or recover critical systems and data is imperative and therefore anticipating failure and building resilience by design should be a key area of focus.
- **Legacy system challenges:** Outdated systems and end-of-life support can pose significant resiliency and security risks and are expensive to maintain. A phased approach to modernisation often through increased cloud adoption strategies can reduce these vulnerabilities and improve efficiency.
- **Business alignment:** Technology resilience should directly support business continuity objectives. Resilience and recovery strategies enhance operational continuity, agility, and the ability to adapt to and recover from IT related disruptions[12]. As a result, effective strategies require close collaboration between IT and business units.
- **Third-party dependencies:** Understanding and assuring the resilience of third-party suppliers and providers within the supply chain is more crucial than ever and many organisations and internal audit functions struggle in this area. Failures in this ecosystem (including fourth and fifth parties) can lead to severe financial and reputational consequences for all involved[13].
- **Regulatory scrutiny:** There is increased regulatory scrutiny on operational resilience within Financial Services. Simply this means the bar has been raised and regulations such as the Digital Operational Resilience Act (DORA)[14] and UK Operational Resilience is demanding attention of those at Board level, driving standards and focus towards 'customer outcomes' as opposed to individual assets (e.g. building or data centres).

Five things internal audit should do

1 **Recovery objectives, capabilities and testing**

Evaluate the comprehensiveness and completeness of business continuity and disaster recovery plans, assessing their alignment with critical business functions and technology recovery strategies. Confirm a shared understanding of potential downtime and data loss across various disruptive events and assess the organisation's ability to recover critical systems and data. This includes verifying data backup/recovery procedures, effectiveness, frequency, security, alignment with criticality, and RTOs/RPOs, including regular testing.

2 **Legacy system risk mitigation**

Identify and assess the risks associated with end-of-life/end-of-support legacy systems from a resiliency standpoint. Evaluate the organisation's plans and controls for mitigating these risks, including system upgrades, replacements, or alternative solutions. Assess the impact of these systems on overall resilience, including data security and recovery.

3 **Transitioning to BAU assurance**

Be actively involved in the transition to BAU assurance following operational disruptions. This involves independently assessing the effectiveness of recovery actions and the subsequent restoration of normal operations, evaluating the long-term impact of the disruption, reviewing and updating operational resilience plans based on lessons learned, and continuously monitoring key controls and emerging risks.

4 **Third-party resilience assurance**

Assess controls in place to manage third-party resilience within the technology supply chain, both at on-boarding and as part of periodic assurance over the contract term. Evaluate the organisation's third-party risk management processes, including due diligence, contractual agreements, and ongoing monitoring. Confirm robust oversight mechanisms are in place at senior level, including data security and recovery provisions.

5 **Alignment with regulation and good practice**

Though focused on Financial Services, operational resilience regulation prompts internal audit teams across all sectors to assess organisational alignment with best practices. This includes gap analysis against requirements, control environment maturity evaluation, and risk identification for continuous improvement. Internal audit should also challenge management information (MI) quality, particularly the use of data-driven insights (KRIs/KPIs) for proactive risk identification and moving beyond reactive reporting.

7 Cloud computing and sustainable technology

33% Audit planned %

42% Use of analytics %

8 2025 report rank

While cloud adoption continues unabated, the landscape is evolving rapidly. With a significant proportion of UK organisations' IT estates still hosted in on-premises environments, there is still some way to go in many organisations' journeys to migrate to cloud.

This year's focus should be on two key evolving trends significantly impacting risk management. Firstly, rise of data sovereignty and national security concerns is leading to a more fragmented cloud landscape. Increasing regionalisation of the cloud market, driven by geopolitical factors and specific regulations like GDPR, CCPA, and CDSA, creates potential vulnerabilities. This includes risks of service disruptions, vendor lock-in, and difficulties ensuring data compliance across multiple jurisdictions. Secondly, environmental, social, and governance (ESG) factors are gaining significant traction in cloud strategies. Organisations must now consider the environmental impact of their cloud consumption (e.g., carbon footprint), ethical sourcing of technology, and the broader societal implications of their cloud deployments. These interconnected trends demand a proactive and comprehensive approach from internal audit to ensure organisations effectively mitigate associated risks and maintain compliance.

Five things you should know about the topic:

- **Data sovereignty risks:** Increased geopolitical tensions are driving a trend towards regionalisation of cloud services. This necessitates a thorough assessment of data sovereignty implications, including compliance with varying national regulations (e.g., GDPR, CCPA, CDSA) and the potential for data breaches or restrictions on access. Furthermore, organisations must consider the risks of vendor lock-in, limiting flexibility and potentially increasing costs, and the potential for service disruptions stemming from escalating international relations or geopolitical instability. A robust risk mitigation strategy should address these interconnected challenges, ensuring business continuity and data security in a volatile global landscape. This strategy should include diversification of cloud providers, robust data governance policies, and comprehensive incident response plans.
- **Cloud sustainability imperative:** ESG is a business imperative and organisations must integrate ESG factors into their cloud strategies, considering energy consumption, carbon footprint, and ethical sourcing of cloud services. This includes due diligence on cloud providers' sustainability initiatives.
- **Evolving regulations:** With increased cloud adoption comes increased responsibility for data security and privacy. Regulations like the UK GDPR and NIS2 continue to evolve, demanding robust security controls and compliance frameworks.
- **Supply chain risks:** Organisations must assess the resilience of their cloud supply chains. Dependencies on specific providers can create vulnerabilities. Diversification and robust vendor management strategies are crucial.
- **Effective management:** Cloud costs can escalate rapidly if not managed effectively. Organisations need to implement robust cost management processes, including regular cost analysis, right-sizing resources, and leveraging cloud cost optimisation tools.

Five things internal audit should do

1 **Assess geopolitical risks**

Internal audit should assess the organisation's exposure to geopolitical risks related to cloud providers. This includes evaluating data sovereignty compliance, vendor concentration, and potential service disruptions.

2 **Integrate ESG into audits**

Internal audit should incorporate ESG considerations into its cloud audits, evaluating the organisation's cloud strategy against its ESG goals and assessing the sustainability of its cloud providers.

3 **Enhance data security and privacy reviews**

Internal audit should strengthen its data security and privacy reviews, ensuring compliance with evolving regulations like the UK GDPR and NIS2. This includes testing access controls, data encryption, and incident response plans.

4 **Review supply chain resilience**

Internal audit should assess the resilience of the organisation's cloud supply chain, identifying potential vulnerabilities and recommending mitigation strategies. This includes evaluating vendor diversification and contract terms.

5 **Monitor cloud costs**

Management should be challenged on how they monitor cloud costs, identifying areas for optimisation and recommending cost-saving measures. This includes reviewing resource utilisation, identifying inefficiencies, and leveraging cloud cost management tools.

8 Unsupported infrastructure and legacy technology

11% Audit planned % **75%** Use of analytics % **New** 2025 report rank

Legacy and unsupported technology presents a significant risk to organisations, with the technical debt accrued as a result of deferred technology investment and uplift typically resulting in a sizeable associated "interest" burden. Though the use of modern cloud hosted products is increasing (see hot topic seven), many organisations are struggling to prioritise the investment in this modernisation. This is leaving organisations, many of whom are responsible for critical national infrastructure (CNI), struggling with the operational costs and security risks associated with aging on premises infrastructure. Outdated systems lack security updates, increasing vulnerability to cyberattacks and operational disruptions. Maintaining these systems is costly and inefficient, hindering innovation and agility.

This section highlights the critical role of internal audit in assessing and mitigating the risks associated with legacy technology, paving the way for a more secure and efficient IT environment. Organisations all face decisions of whether to replace, upgrade, or maintain legacy systems; this requires careful consideration of the associated costs, risks, and benefits. A comprehensive assessment of the current state of the legacy systems and a well-defined modernisation strategy are crucial for mitigating the risks and ensuring the long-term success of the organisation; Internal audit functions have a clear role to play in this exercise.

Five things you should know about the topic:

- **Security vulnerabilities:** Unsupported systems may lack crucial security patches, making them prime targets for cyberattacks. Exploiting these vulnerabilities can lead to data breaches, financial losses, and reputational damage. The absence of vendor support further exacerbates this risk.
- **Operational inefficiencies:** Legacy systems often lack integration with modern technologies, leading to inefficient workflows and increased operational costs. Maintaining these systems requires specialist skills, which can be difficult and expensive to find.
- **Compliance risks:** Outdated systems may not comply with current data privacy regulations (e.g., GDPR, CCPA) or industry-specific standards, leading to significant fines and legal repercussions. Auditors may need to assess compliance gaps and recommend remediation strategies.
- **Business disruption:** Failures in legacy systems can cause significant business disruption, impacting productivity, revenue, and customer satisfaction. A robust plan for migration or replacement is crucial to minimise downtime and maintain business continuity.
- **Hidden costs:** The total cost of ownership for legacy systems often exceeds the initial investment due to ongoing maintenance, support, and security challenges. A cost-benefit analysis comparing the cost of maintaining legacy systems versus migrating to modern alternatives is essential.

Five things internal audit should do

1. **Review and challenge management's security risk assessment**

   Evaluate management's assessment of security risks associated with legacy systems. Determine if the assessment considers all relevant threats and vulnerabilities, and if the identified risks are appropriately prioritised. Review the methodology used for the risk assessment against industry frameworks (e.g., NIST CSF, CAF).

2. **Review of management's deprecation plan**

   Assess the adequacy of management's plan for deprecating and replacing legacy systems. Evaluate the plan's feasibility, considering timelines, resource allocation, and potential disruptions. Also consider longevity; adequately dealing with legacy technology can be a multi-year, significant investment which requires strong continuity of purpose. Determine if the plan includes appropriate risk mitigation strategies, contingency plans and is formally aligned to target architecture and environment planning documents.

3. **Testing of management's asset visibility**

   Test the design and operating effectiveness of management's controls designed to ensure technology is successfully inventoried across the organisation, and that these inventories are proactively maintained, to support in the identification of legacy assets across the estate.

4. **Evaluation of management's continuity planning**

   Evaluate the adequacy of management's business continuity and disaster recovery plans for addressing potential disruptions caused by legacy system issues. Assess the plans' alignment with business objectives and the effectiveness of testing and training activities.

5. **Analysis of management's cost-benefit analysis**

   Review management's cost-benefit analysis comparing the cost of maintaining legacy systems versus migrating to modern alternatives. Assess the completeness and accuracy of the analysis, considering all relevant costs and benefits. Determine if the analysis supports management's decision-making process.

9 Identity and privileged access management

56% Audit planned %

70% Use of analytics %

7 2025 report rank

Recent high-profile cyber attacks targeting retailers have dramatically highlighted the critical importance of Identity access management (IAM) solutions. Organisations are significantly increasing their focus on IAM controls to protect organisational systems and data, reflecting the heightened risk in the current macro-environment. Weak IAM practices include lack of, or insufficient, multi-factor authentication (MFA); inadequate security in help desk password reset procedures (allowing resets based on single interactions); and vulnerabilities in privileged access management (PAM) that facilitate lateral movement within the network. These weaknesses may result in devastating consequences such as data breaches, substantial financial losses, and severe reputational damage.

Effective IAM is crucial for any organisation's cyber security posture and digital transformation and remains a critical area requiring ongoing attention despite its consistent ranking as a top IT internal audit risk. The survey highlights the persistent relevance of IAM, particularly given the increasing sophistication of cyber threats and the growing reliance on digital assets and outlines key actions internal audit teams should take. While IAM's ranking may fluctuate slightly year-on-year (from seventh to ninth in our survey), its underlying importance remains unchanged.

What you should know about the topic:

IAM encompasses the policies, processes, and technologies used to manage digital identities and control access to organisational resources. This includes:

- **Identity Governance and Administration (IGA):** The overarching framework for managing user identities throughout their lifecycle, from provisioning to de-provisioning. This includes processes for user account creation, modification, and deletion, as well as role-based access control (RBAC).
- **Authentication:** Verifying the identity of users attempting to access systems or data. This can involve various methods, such as passwords, multi-factor authentication (MFA), biometrics, and single sign-on (SSO).
- **Authorisation:** Determining what actions authenticated users are permitted to perform. This is often based on roles, responsibilities, and data sensitivity.
- **Access control:** Implementing mechanisms to restrict access to sensitive data and systems based on the principle of least privilege. This ensures that users only have access to the information and resources necessary to perform their jobs.
- **Privileged Access Management (PAM):** Managing and controlling access for users with elevated privileges e.g. administrators. This is crucial for mitigating the risk of insider threats and lateral movement by attackers.
- UK IAM regulation is complex and evolving. Organisations must comply with multiple frameworks, including UK GDPR (strong access controls, data minimisation), NIS2 (robust cybersecurity for essential services), and FCA regulations (stringent data security for financial institutions). Effective IAM is crucial. Continuous alignment with NCSC guidance on best practices (PAM, MFA, Zero Trust) is also vital for strong security.

Five things internal audit should do

1 **Assess IAM maturity**

Conduct a comprehensive assessment of the organisation's IAM maturity, aligning with relevant regulations and industry good practices (e.g., NIST Cybersecurity Framework). Identify gaps in security controls and compliance.

2 **Focused reviews on PAM practices and tooling**

Focus on auditing privileged access management practices and tooling (e.g., CyberArk, SailPoint, Beyond Trust), ensuring robust logging and monitoring to detect and respond to suspicious activity. This is critical for mitigating insider threats.

3 **Evaluate MFA implementation**

Verify the effectiveness of MFA implementation, assessing the types used, user/system coverage, and overall security posture. Identify gaps and recommend improvements to enhance security.

4 **User access reviews**

Examine the frequency and effectiveness of user access reviews, ensuring alignment with data retention policies and regulatory requirements. Verify timely reviews and appropriate access revocation.

5 **Test IAM controls**

Simulate real-world attacks targeting IAM capabilities. Assess the organisation's incident response plan and its ability to effectively address IAM-related breaches, ensuring compliance with breach notification requirements. This includes testing the resilience of authentication mechanisms, authorisation processes, and access control measures.

10 Strategy and governance

44% Audit planned %

56% Use of analytics %

3 2025 report rank

Effective information technology strategy and appropriate governance structures are crucial components for CIO functions navigating today's complex digital landscape. Robust frameworks mitigate operational risks, support innovation aligned with strategic goals and deliver cost efficiencies. Conversely, weak governance leads to strategic misalignment, uninformed decisions, and increased vulnerability to significant incidents. Prioritising strong IT governance is paramount for organisational success and resilience, and yet across sectors we continue to see underinvestment and a lack of focus on good governance and risk management of technology.

Four things you should know about the topic:

- **Formalisation of technology performance reporting and KPIs:** Many organisations still struggle to provide robust and transparent reporting on the performance of their technology capabilities, hampering the ability to make effective strategic decisions. Whilst significant progress has been made in the investment and management of cyber risks over the past decade, the formalisation of technology risk management more generally, remains a challenge for many organisations. However, recent advances in AI in continuous monitoring capabilities and the automation of testing technology controls, offers opportunities for low cost and scalable improvements to be made.
- **Cultural challenges relating to IT governance:** Many organisations continue to operate under a counterproductive culture both within and outside the technology function in relation to IT governance. This often leads to lack of traction and ownership for managing the organisation’s technology risk and controls, or formalising reporting of technology function performance appropriately. Outside the technology function it tends to be through a lack of understanding of division of responsibilities between teams for technology delivery, or at senior levels effective understanding of the technology risk profile of the organisation.
- **Longer term approach to technology investment:** It is well documented that investment in technology remains one of the key areas of capital expenditure at most organisations, and over time, organisations often fail to adequately invest in technology to achieve the benefits associated with appropriate technology investment.
- **Governance of key emerging challenge areas:** Alongside more holistic technology governance challenges, there are key areas where governance is typically immature even when broader governance of technology is effective. Typical areas seen are in relation to emerging technologies (such as AI), and in an increasingly cloud and vendor driven technology environment, governance of vendors and those third parties.

Five things internal audit should do

1 Holistic, dedicated reviews on IT strategy and governance

There is a tendency to focus technology reviews on more operational risk areas, and this means internal audit teams are often failing to assess and reflect the bigger picture. Including more holistic reviews of technology strategy and governance is increasingly important and should be considered for regular rotation alongside other key risks already subject to mandatory reviews on many internal audit plans, such as cyber.

2 Review of technology risk management and reporting

Consider specific reviews of technology risk management capabilities at organisations; the implementation of the technology risk service model, and key elements of risk management such as setting risk appetite for technology, setup and curation of a technology risk and control framework, related risk and control self-assessment and management testing processes, and other key elements of technology risk management.

3 Culture reviews

An assessment of the culture within and outside the technology function of the organisation can highlight structural challenges in ways of thinking around how the organisation manages its technology.

4 Technology target operating model and service model

Looking at the operating model for technology, resourcing levels, skills and capabilities, and highlighting shortages or gaps can provide an important independent view, on how well equipped the organisation is to deliver the expected services to the wider enterprise and external stakeholders.

5 Supplementary deep dives on key areas

Internal audit teams should consider when conducting broader reviews of technology governance if specific areas of governance could be catered for either as part of the review, or in follow up reviews in response to findings. In this way a review of technology governance can often act as part of the planning process for future audits of risk areas.

Emerging topics

Effective internal audit functions are looking ahead to scan the horizon and identify emerging technology risks that may threaten the organisation's assets, reputation, and long-term sustainability. The focus should be on continuous learning, adaptation, and collaboration to navigate the ever-evolving technological landscape.

Our core topics for 2026 highlight some risks areas that were part of the 'emerging' banner a few years ago, such as the risks of GenAI or artificial intelligence powered cyberattacks. This section outlines a selection of such emerging developments and associated risks that functions should start monitoring in 2026.

1 Digital assets:

The increasing regulatory scrutiny and inherent complexities associated with digital assets demand robust internal audit oversight. The digital asset landscape is evolving, with notable growth being seen in stablecoins, decentralised finance (DeFi), and non-fungible tokens (NFTs), alongside the continued development of cryptocurrencies. Recent developments, including the FCA's crypto-asset regime and the Bank of England's stablecoin regulations, are introducing new compliance obligations. Draft statutory instruments and FCA Consultation Papers (CP25/14, CP25/15, CP25/16) bring further considerations around CASS, the Prudential Regime, and retail access to crypto-asset exchange-traded notes (cETNs).

Immature frameworks could raise significant data independence concerns, increasing the risk of misreporting, fraud, and regulatory breaches. Failures to manage conflicts of interest in the digital asset sector have led to significant customer losses and market instability. Recent high-profile collapses, such as that of FTX, in the sector have underscored the tangible consequences of inadequate conflict management, highlighting the importance of clear governance, segregation of duties, and independent oversight.

2 The metaverse:

The metaverse is a persistent, shared, 3D virtual world where users can interact with each other, with digital assets, and experiences. While still in its nascent stages, its potential impact on businesses is substantial and may present unique challenges for traditional audit methodologies. The regulatory landscape surrounding it is also still at very early stages, but we expect it will start evolving soon. Auditors need to monitor regulatory developments and ensure the organisation's activities comply with existing and emerging regulations. It generates vast amounts of user data, including biometric information, location data, and behavioural patterns. Protecting this data from breaches and misuse is paramount. Auditors need to assess the organisation's ability to protect its intellectual property in this new environment and to ensure compliance with relevant licensing agreements. The potential for counterfeiting and infringement is high.

3 Quantum computing:

The development of quantum computers poses a long-term threat to current encryption methods. This allows them to theoretically crack existing encryption algorithms. Internal audit should monitor advancements in quantum computing, stay informed about the timeline for the development of practical quantum computers and their potential impact on the organisation's security posture.

Many nation states are investing heavily in quantum computing, and assuming these developers overcome current challenges soon, most traditional public key cryptography (PKC) algorithms in use today will be highly vulnerable to attack. For those trusted with safeguarding the most sensitive data assets in the country, in defence, intelligence services and critical national infrastructure (CNI) providers, rapid adoption of post-quantum cryptography (PQC) safe algorithms is of paramount importance to national security.

Internal audit functions should support the business and security teams in assessing the organisation's reliance on vulnerable cryptographic algorithms, planning for a transition to quantum-resistant cryptography for the organisation.

4 Weaponised AI and misinformation:

GenAI enables the creation of convincing deepfakes and targeted disinformation campaigns. These increase fraud and misrepresentation risks, misleading stakeholders in the corporate world, and most worryingly can erode public trust in democratic government systems.

It is of critical importance that public service organisations implement clear mechanisms for the public to identify and validate trusted sources of public service information.

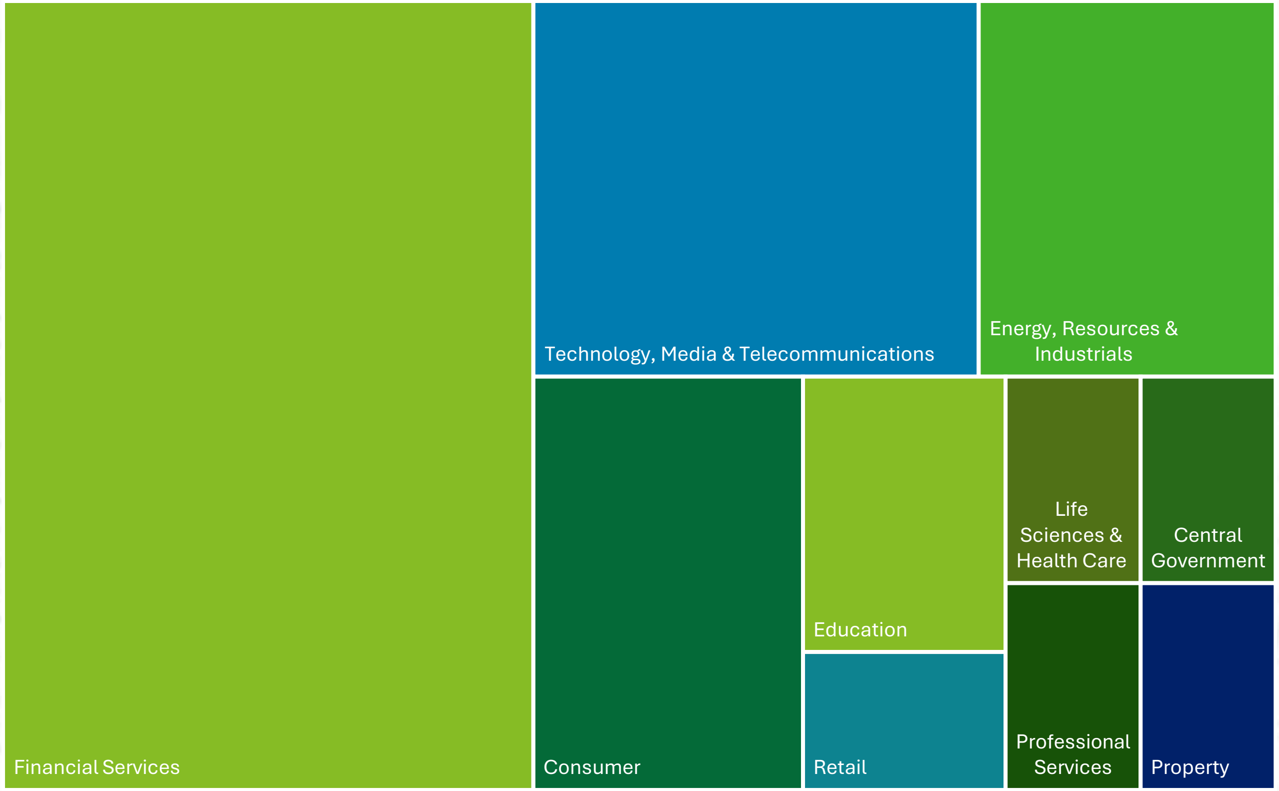
Appendices

About the survey

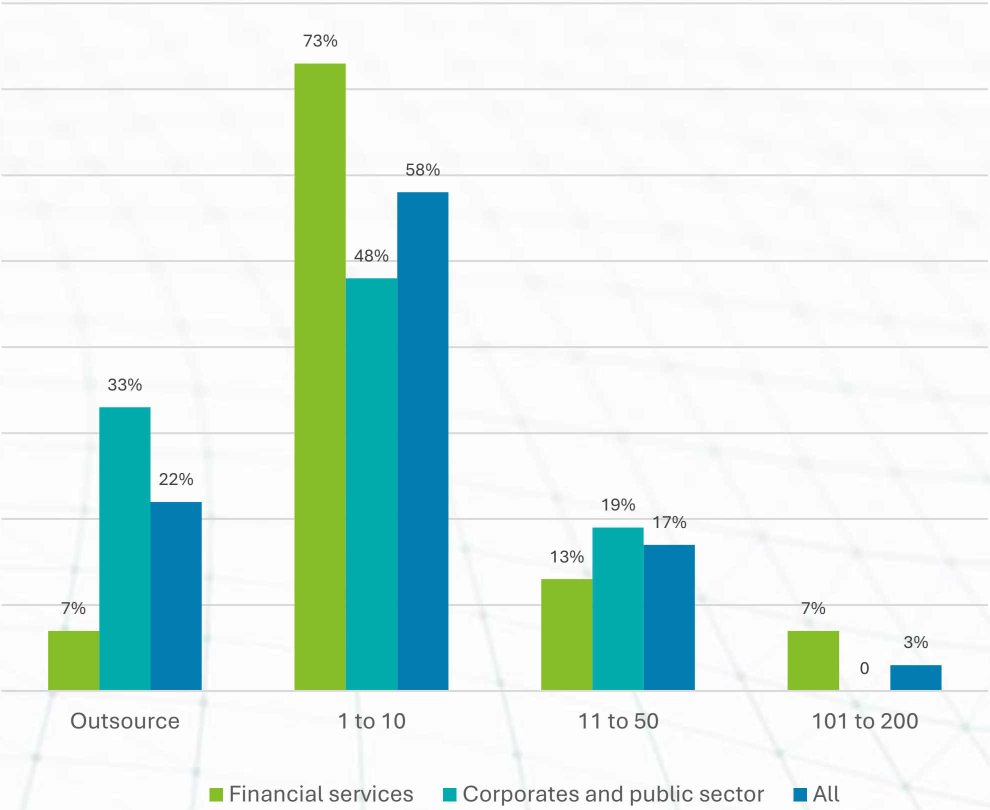
Respondents primarily comprised Heads of IT Internal Audit (or equivalent roles), with additional input from Chief Internal Auditors, Heads of Internal Audit, and IT Audit Directors. Deloitte LLP commissioned this survey, conducted by our senior Technology and Transformation practitioners via an online tool between May and June 2025. As well as capturing the key IT internal audit risks noted by senior audit professionals, our research team has also leveraged the data provided to understand technology and risk themes and trends developing across internal audit functions.

Our research analysed the results to understand technology and risk trends within internal audit. This paper highlights key technology and digital internal audit topics identified by industry experts, explaining their importance, recent developments, recommended actions for internal audit functions, and key challenges to effective risk mitigation.

Industry breakdown of respondents



Number of full-time employees in the IT internal audit team



Additional sources and references

1. Financial Markets Regulatory Outlook | Deloitte UK
2. Deloitte's Trustworthy AI Framework
3. Online Safety Act | Deloitte UK
4. Cyber Resilience Bill | Deloitte UK
5. The near-term impact of AI on the cyber threat - NCSC.GOV.UK
6. Cybersecurity topical requirement user guide | IIA
7. UK Civil Aviation Authority unveils new AI strategy - Airport Suppliers
8. PRA and BoE set out strategic approach to AI in letter to Government | Global Regulation Tomorrow
9. AI Act Regulation (EU) 2024/1689 - Publications Office of the EU
10. Chief Data Officer survey 2024 | Deloitte UK
11. Is Your Business Prepared for a Major Cyber Incident? Proactive Security Measures
12. Risk and resilience: bringing risk management and resilience closer together
13. Enhancing Supply Chain Resilience: key strategies from risk to resilience
14. The Digital Operational Resilience Act (DORA) | Deloitte UK

Key contacts and contributors

We extend our sincere thanks to all survey participants and clients for their invaluable contributions, openly sharing their experiences, challenges, and strategic priorities.

This report aims to be more than just an informative publication; it is designed to be used as a catalyst for discussion, helping you to refine your risk assessment and planning strategies for the year ahead. We encourage professionals to use it as a springboard for conversations within your organisation and we look forward to continuing the dialogue.

Please do not hesitate to reach out if you would like to explore any of these topics further.

Financial services

Yannis Petras

Partner
ypetras@deloitte.co.uk

Mark Westbrook

Director
markwestbrook@deloitte.co.uk

Corporates

Faiza Ali

Partner
faali@deloitte.co.uk

Kirti Mehta

Director
kirtimehta@deloitte.co.uk

Government and public services

Helen Cutting

Partner
hcutting@deloitte.co.uk

Matt Brennan

Associate Director
mpbrennan@deloitte.co.uk

Key contacts and contributors

Data governance and risk management

Nanette Gardos
Associate Director
ngardos@deloitte.co.uk

Katie Hibbert
Senior Manager
kehibbert@deloitte.co.uk

Cyber security

Poppy Khan
Director
pokhan@deloitte.co.uk

David Morris
Associate Director
dmorris@deloitte.co.uk

Supply chain risk: third-party and outsourcing

Roshan James
Associate Director
roshanjames@deloitte.co.uk

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

Cloud computing and sustainable technology

Rupert Hargrave
Senior Manager
ruphargrave@deloitte.co.uk

Dom Hamilton
Senior Manager
domhamilton@deloitte.co.uk

Identity and privileged access management

Poppy Khan
Director
pokhan@deloitte.co.uk

Haroon Abbas
Associate Director
haabbas@deloitte.co.uk

Technology, cyber, and operational resilience

Adam Blair
Associate Director
adblair@deloitte.co.uk

Matt Whitfield
Manager
mwhitfield@deloitte.co.uk

Artificial intelligence (AI) risk management

Lewis Keating
Director
lkeating@deloitte.co.uk

Kirsty Maund
Senior Manager
kmaund@deloitte.co.uk

Digital transformation and IT change

Lee Hales
Director
lhales@deloitte.co.uk

Olga Harte
Senior Manager
oharte@deloitte.co.uk

Unsupported infrastructure and legacy technology

Matt Brennan
Associate Director
mpbrennan@deloitte.co.uk

Ermias Workayehu
Manager
etworkayehu@deloitte.co.uk

Strategy and governance

Kirti Mehta
Director
kirtimehta@deloitte.co.uk

Mark Westbrook
Director
markwestbrook@deloitte.co.uk

Additional contributions

Nicola Hicks
Director
nhicks@deloitte.co.uk

Carol Mucherahowa
Associate Director
cmucherahowa@deloitte.co.uk

Kevin Macnish
Associate Director
kmacnish@deloitte.co.uk

Darren Samuel Lawton
Senior Manager
dslawton@deloitte.co.uk

Rubal Mehta
Senior Manager
rubalmehta@deloitte.co.uk

Ritvik Mehra
Manager
ritvikmehra@deloitte.co.uk

Kyle Taylor
Assistant Manager
kstaylor@deloitte.co.uk

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

Henry Berry
Consultant
heberry@deloitte.co.uk

Veronica Pralea
Senior Analyst
veronicapralea@deloitte.co.uk

Reha Iqbal
Senior Analyst
riqbal@deloitte.co.uk

Mik Oludairo
Industrial Placement
moludairo@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 see www.deloitte.com/about to learn more about our global network of member firms.