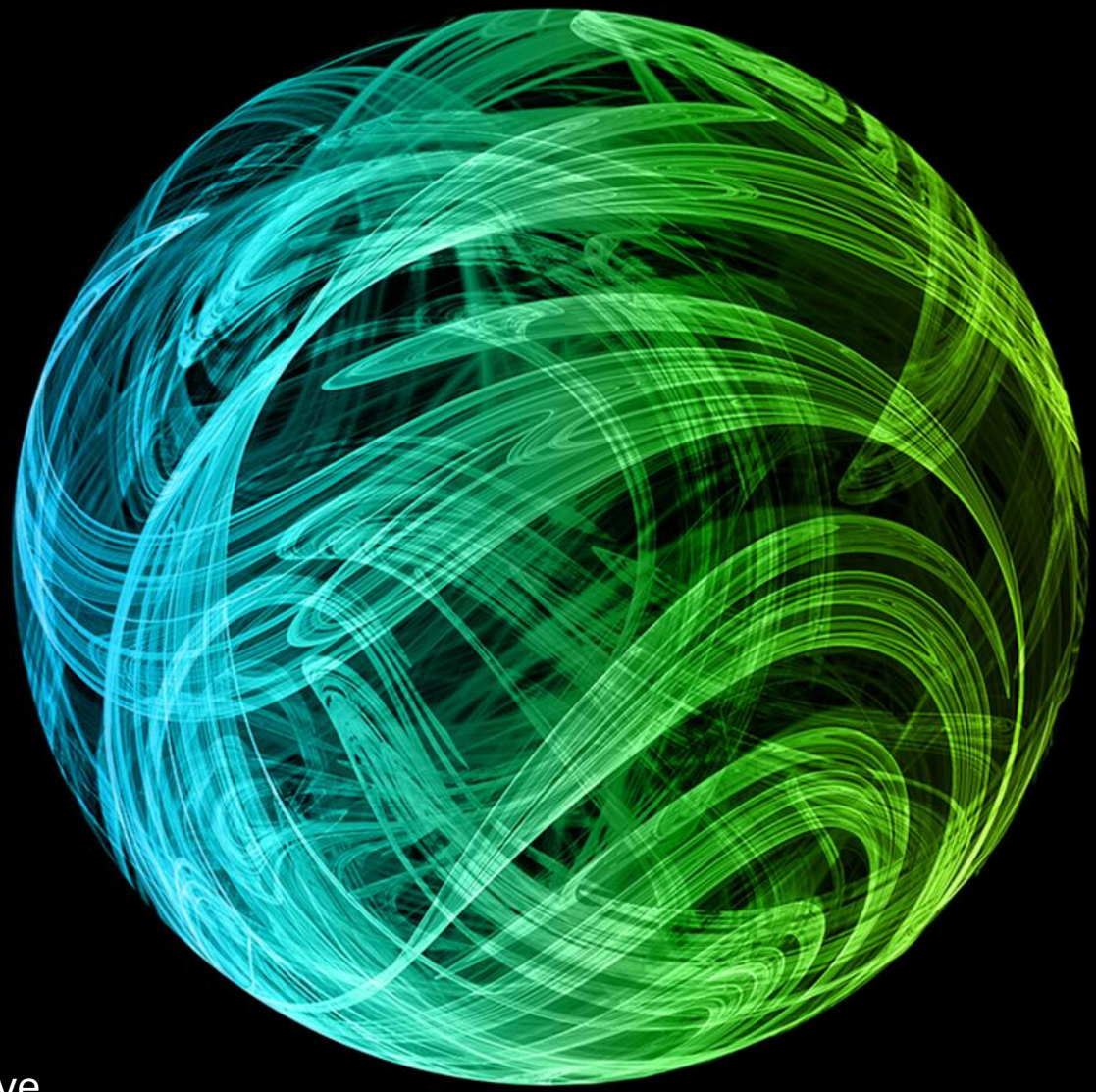
Deloitte.



Hot topics for technology and digital risk 2027

Risk at the Speed of Change: An internal audit perspective

September 2026

Foreword

Welcome to the 16th edition of our annual report on the technology and digital risk shaping internal audit and risk agendas.

Technology risk is entering a new phase. Artificial Intelligence (AI) is becoming embedded across organisations; cyber threats are accelerating and dependence on interconnected technology ecosystems continues to grow. For executives, the challenge in 2027 is not simply to adopt technology innovation, but to govern it confidently, protect critical operations and ensure assurance keeps pace.

AI has moved rapidly from experimentation to implementation to agentic scaling, with organisations seeking to harness its potential while addressing concerns around governance, accountability, data quality, regulatory compliance and operational effectiveness. At the same time, **cyber threats** continue to evolve at 'machine-speed', technology ecosystems are becoming increasingly **interconnected**, and organisations remain heavily reliant on **third parties, cloud providers** and outsourced services. No surprise that **cyber, AI** and **data** risks hold the top three places in this year's ranking.

Our survey covered organisations across UK and US, providing a broader international perspective for 2027. Whilst it highlights a strong consensus around the most significant risks facing organisations, it also reveals subtle differences in priorities across jurisdictions. These insights provide valuable context for functions operating across global organisations, while reinforcing the importance of aligning assurance activities to local regulatory expectations, market dynamics and organisational objectives.

Internal audit and risk functions face a **critical imperative to adapt and prioritise.** The regulatory landscape is characterised by a **dynamic interplay of innovation, evolving risks, and increasing supervisory expectations.** Technology risk and audit practitioners must proactively engage with these technology topics, moving beyond traditional compliance checks to provide assurance on the strategic management of these complex and interconnected risks. This requires a **forward-looking approach, robust governance, and continuous adaptation** to ensure firms can navigate this landscape effectively.

For example, as we argue in the paper, AI is no longer a discrete system to be reviewed in isolation; it is becoming a feature of the wider technology backbone of organisations and their control environment and, indeed that of the functions themselves. For 2027, the more useful ambition may be to make AI a **standing consideration** in every auditable entity / audit – both in terms of the **"what" and the "how" to audit**.

This report provides insight into the areas that technology and audit leaders consider most significant, offering a benchmark against which organisations can assess their own risk profiles and audit plans. It also includes **practical considerations and tips** on what audit executives need to do differently when evaluating each risk area, helping teams tailor their assurance efforts where they can provide the greatest value.

Finally, while the report underlines today's most pressing priorities, it also looks ahead to **emerging technology developments** that may shape future risk landscape. By maintaining a forward-looking perspective, internal audit can help organisations anticipate change, strengthen resilience and remain well-positioned to seize the opportunities presented by new technologies.

We hope this publication continues to drive meaningful discussions between internal audit, technology, risk and business leaders as they navigate an increasingly dynamic and technology-driven environment. As always, 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.

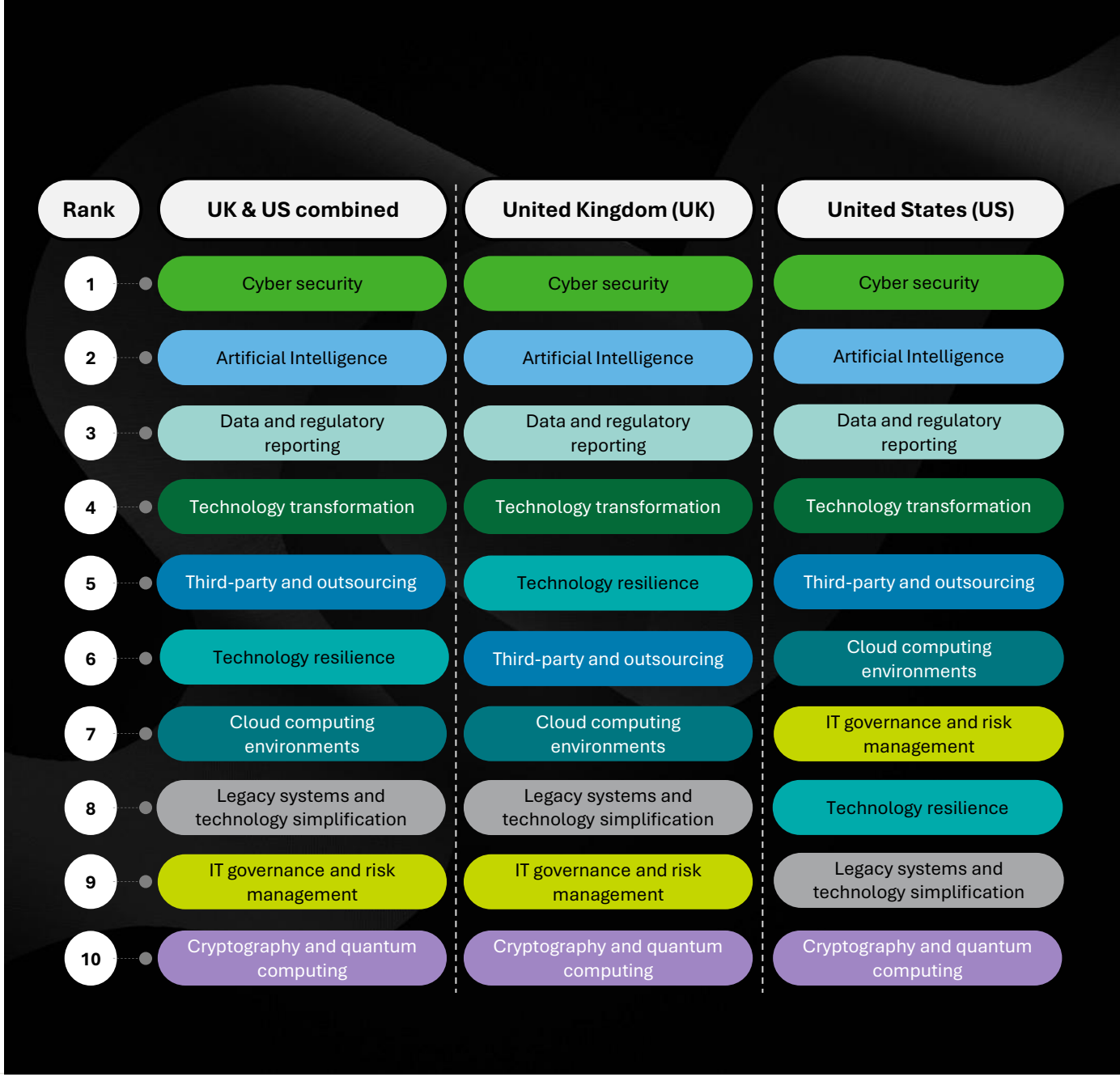
Contents

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

Analysis across regions

While the overall ranking of technology risks is broadly consistent across jurisdictions, several noteworthy differences emerge between the **United Kingdom** and the **United States.**

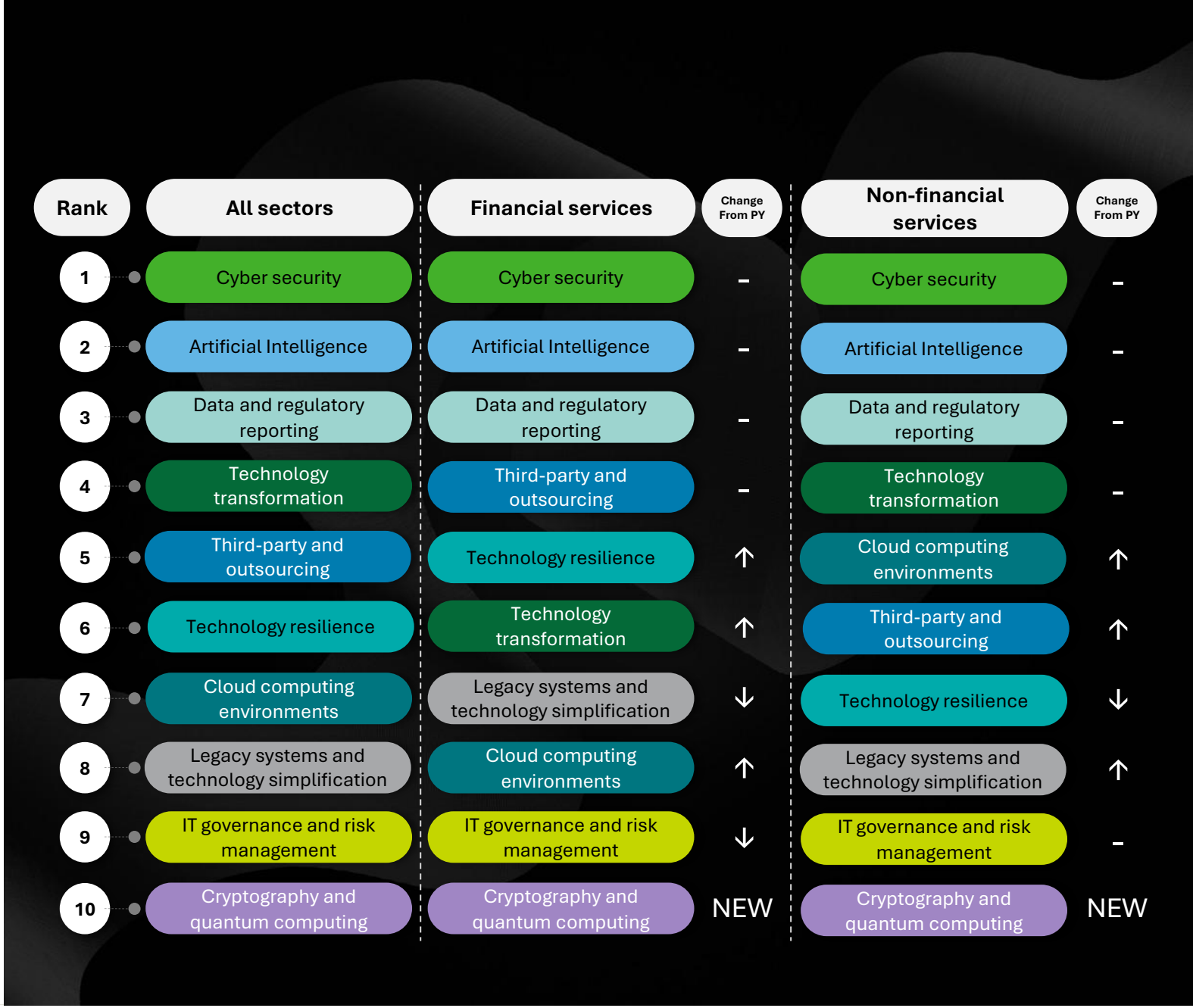
- **Cyber security**, **Artificial Intelligence**, **Data and regulatory reporting**, and **Technology transformation** occupy the top four positions across all jurisdictions, demonstrating a strong consensus on the most pressing technology priorities. This reflects the continued focus on defending against cyber threats, governing the rapid adoption of AI technologies, managing increasingly complex data environments, and delivering technology-enabled transformation successfully.
- More pronounced differences emerge in the middle of the rankings. **Technology resilience** ranks fifth in the UK but eighth in the US, likely reflecting the UK's heightened regulatory focus on operational resilience and organisations' ability to withstand and recover from disruption. In contrast, **Third-party and outsourcing** ranks slightly higher in the US (5th) than in the UK (6th).
- US firms also places greater emphasis on **Cloud computing environments** and **IT governance and risk management**, which rank sixth and seventh respectively, compared with seventh and ninth in the UK. This may indicate a stronger focus on enabling growth and innovation through technology investment, while ensuring governance frameworks evolve to support changing technology landscapes.
- Meanwhile, **Legacy systems and technology simplification** remains a common challenge across jurisdictions, ranking eighth in the UK and ninth in the US. This highlights the ongoing need to modernise ageing 'End-of-Life' or 'End-of-Support' technology estates, reduce technical debt, and improve efficiency without compromising resilience or security.
- Overall, the findings suggest that while organisations share a common set of technology risk concerns, local regulatory expectations, market dynamics and strategic priorities influence the relative importance placed on resilience, third-party management, cloud adoption and technology governance. These differences reinforce the need for technology risk and internal audit plans of global (or US/UK organisations) to be tailored to the specific environments in which organisations operate, and indeed the specific legal entity risk and regulatory profiles (where applicable).



Analysis across sectors

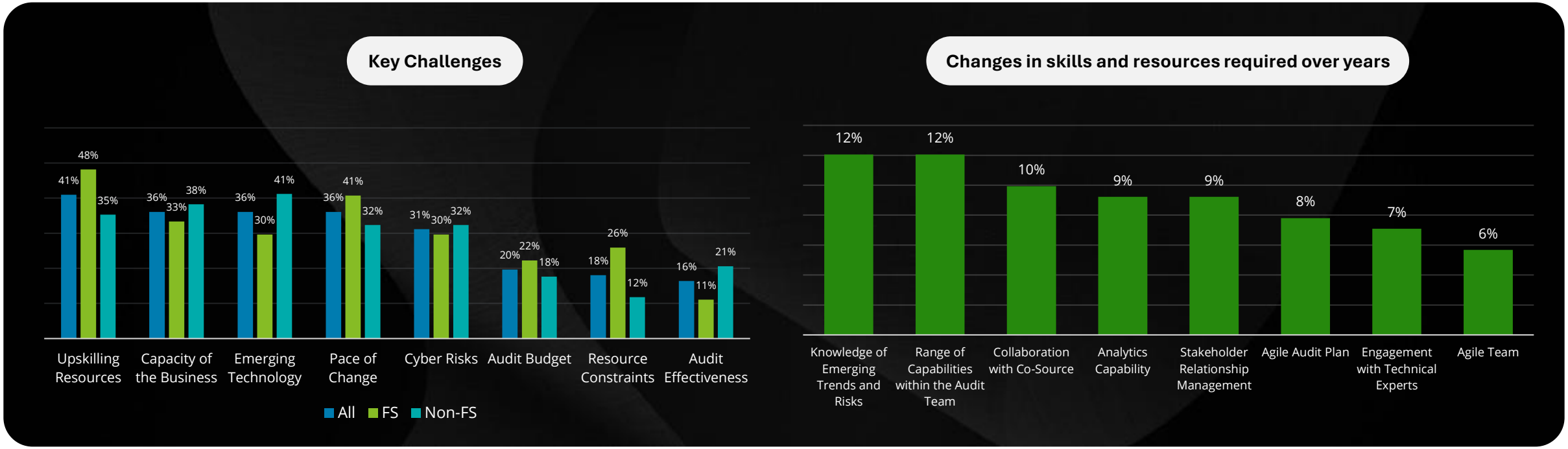
While the highest-ranked risks are broadly consistent across sectors, the results suggest different areas of emphasis between **Financial Services** and **Non-Financial Services** organisations.

- For Financial Services organisations, the rankings highlight a continued focus on operational resilience and the management of external dependencies. The prominence of **Technology resilience** and **Third-party and outsourcing** reflects increasing regulatory expectations, ongoing investment in resilience programmes and the sector's reliance on critical technology services and third-party providers to support business operations.
- By comparison, Non-Financial Services organisations appear more focused on technology-enabled transformation and modernisation. The higher ranking of **Cloud computing environments** suggests continued investment in digital platforms and cloud-based services, while **Technology resilience** and **Third-party and outsourcing** remain important considerations as organisations manage increasingly interconnected technology ecosystems.
- Across both sectors, **Legacy systems and technology simplification** continues to feature, highlighting a common challenge facing many organisations. While investment in new technologies continues, many are simultaneously balancing the need to modernise ageing platforms, reduce technical debt and improve operational efficiency without compromising security or resilience.
- Overall, the findings suggest that while organisations share a common set of technology risk concerns, sector priorities continue to be shaped by differing regulatory environments, operating models and transformation objectives.



Analysis across functions

Our survey shows that Internal Audit functions are experiencing growing pressure as technology-driven change expands in scale and accelerates at an ever-faster pace.



Across all sectors, respondents identified **upskilling resources**, **capacity of the business**, **emerging technology**, and **pace of change / innovation** as the most significant challenges. These findings reflect a technology risk landscape that continues to evolve quickly, with functions expected to provide assurance over increasingly complex and fast-moving risks while operating within constrained resource models.

While the overall challenge profile is broadly consistent, the graphs show some important differences between FS and Non-FS respondents. FS respondents reported the highest concern around **upskilling resources** and **pace of change**, as well as relatively greater pressure from **resource constraints**. This may reflect the continued need for specialist skills in highly regulated environments, where technology change, control expectations and assurance requirements are developing at pace.

Non-FS respondents placed relatively greater emphasis on **emerging technology**, **capacity of the business**, **cyber risks**, and **audit effectiveness**, suggesting that many functions are balancing the adoption of new technologies with the practical challenge of building sufficient business and audit capacity to respond effectively.

Encouragingly, the planned capability investments of surveyed functions closely align to these challenges. The highest-priority areas for future skills and resources are **knowledge of emerging trends and risks** and **broadening the range of capabilities within the audit team**[1], both identified by 12% of respondents. These are followed by **greater collaboration with co-source providers**, highlighting that functions recognise the need to access more specialised expertise and adopt more flexible delivery models.

The continued emphasis on data, the **analytics capability**, stakeholder relationship management, agile audit planning and engagement with technical experts also demonstrates a desire to strengthen audit effectiveness and deliver more responsive, insight-driven assurance. Taken together, the results suggest that successful Internal Audit functions are increasingly focusing on workforce capability, adaptability and specialist expertise as key enablers for addressing an increasingly complex technology risk landscape.[2]

A perspective on the regulatory outlook for 2027: UK / EMEA

Our latest *Digital Regulatory Outlook 2026*[1] and *Financial Services Regulatory Outlook 2026*[2] papers highlight several key technology-related areas that demand heightened attention from functions to safeguard resilience, compliance, and strategic alignment. While many regulatory developments apply across all sectors, Financial Services firms face additional obligations that often require more mature governance, control and assurance frameworks. Internal Audit functions should be prepared to provide assurance over governance, accountability and operational effectiveness as organisations adopt new technologies and operate in increasingly complex digital environments.

Artificial Intelligence Governance and Responsible Adoption

AI adoption is accelerating across financial services, promising efficiency but introducing novel risks. The implementation of the EU AI Act[3], alongside increasing scrutiny from UK regulators and government, is driving greater focus on governance, accountability, transparency and risk management for AI-enabled solutions.

- **Interplay with existing regulations**: AI use cases will be assessed through existing prudential, model risk management, conduct, operational resilience, and existing data protection frameworks. Internal audit must ensure AI systems comply with this broader regulatory landscape.
- **AI governance and risk management**: Ensuring robust frameworks are in place for AI deployment, including clear risk appetite, strong internal controls, and accountability for outcomes.
- **Data quality and governance**: High-quality data is fundamental for effective AI, underpinning transparency, model validation, explainability, fairness, and cybersecurity. Internal audit needs to assess data provenance, relevance, representativeness, and bias mitigation, especially given the EU AI Act's expectations for high-risk systems.

Financial Services: Assess readiness for evolving FCA and PRA expectations regarding AI governance, model risk management, customer outcomes and operational resilience impacts arising from AI deployment.[2]

Data Governance, Sovereignty and Digital Infrastructure

The final provisions of the UK's Data (Use and Access) Act came into force during 2026[5], creating new considerations around data sharing, automated decision-making and the governance of digital services. At the same time, organisations are becoming increasingly dependent on global cloud providers and cross-border technology infrastructure, driving greater scrutiny of data control, digital sovereignty and critical technology dependencies.

- **Data use and automated decision-making:** Assess whether governance, controls and oversight arrangements support evolving requirements relating to data use, sharing and automated decision-making, particularly where AI-enabled processes influence business outcomes.
- **Data governance and ownership**
- **Digital infrastructure and sovereignty:** Assess exposure to cloud concentration risk, cross-border data transfers, jurisdictional dependencies and the resilience of critical digital infrastructure.

Operational Resilience and Third-Party Risk

The UK's proposed Cyber Security and Resilience Bill is expected to strengthen resilience requirements across critical sectors[4], expand regulatory oversight of managed service providers and increase expectations around supply-chain security and incident reporting.

- **Third-party oversight:** Assess vendor governance, dependency mapping, contractual protections and management's ability to monitor compliance with resilience requirements.
- **Concentration and geopolitical risk:** Evaluate exposure to critical providers, cross-border dependencies and risks arising from increasingly concentrated technology and AI ecosystems.
- **Supply chain resilience:** Review resilience across third- and fourth-party relationships, including visibility of critical sub-suppliers and contingency planning arrangements.

Financial Services: Assess readiness for the March 2027 operational incident and material third-party reporting requirements, and compliance with DORA and the UK Operational Resilience framework, including resilience testing, dependency management and critical third-party oversight. Firms must ensure robust testing, auditability, transparency and continuity, particularly for concentration risks across cloud, compute, and foundation models.[2]

Technology Modernisation and Emerging Technologies

Regulators are increasingly focused on the risks arising from ageing technology estates as well as the adoption of emerging technologies. For FS organisations, the rise of stablecoins, tokenised deposits, and other digital assets is transforming the investment and payments landscape..

- **Technology modernisation and legacy risk:** Assess whether organisations understand and manage the operational, security and resilience risks arising from legacy technology, technical debt and ageing infrastructure, whilst also evaluating the governance and risk management arrangements for emerging/modernised technologies.
- **Cloud and digital transformation:** Review governance over major technology change programmes, cloud adoption and technology-enabled business transformation.

Financial Services: Monitoring adherence to evolving regimes, such as the EU's Markets in Crypto-assets Regulation (MiCA) and the UK's two-tier stablecoin regulation, which impose specific requirements on backing assets and holding limits.[2]

A perspective on the regulatory outlook for 2027: US

Additional areas below provide a summary of key US regulatory areas undergoing significant change along with associated risks for organizations. They also identify the priority focus areas that warrant management attention as organizations assess readiness, strengthen governance, and translate regulatory developments into actionable compliance and operating responses.

Privacy

Privacy is being reshaped by three converging forces — regulation, technology, and data. Each carries a rising risk and a clear call on management's attention.

Regulation is fragmenting, not consolidating. With no federal privacy law, ~20 states now enforce diverging statutes, and the bar keeps moving — new laws take effect in 2026 (Indiana, Kentucky, Rhode Island) and thresholds are falling (Connecticut to 35,000 consumers).

The implication for management: build compliance to the strictest applicable standard and treat the regulatory footprint as a moving target, reviewed continuously rather than annually.[6]

The cost of an undetected gap is climbing. Vanishing cure periods and per-violation fines of $7,500–$10,000 mean a single control failure can scale across records into material exposure — with limited opportunity to address after a regulator finds it. Management should invest in early detection, focus controls where one breakdown could replicate at volume, and treat these as board-level exposures, not operational housekeeping.

AI and privacy are now one risk. As AI scales from pilot to enterprise, regulators are targeting both how personal data flows through automated systems (new CCPA rules) and the accuracy of AI claims (Federal Trade Commission (FTC)) actions against DoNotPay and Workado). Yet most enterprises are scaling agentic AI faster than they are governing it.

Management must close that gap — verifying data provenance, controls, and both internal and vendor AI representations before deployment, not after.

California Consumer Privacy Act (CCPA)

CCPA, regulated by the California Privacy Protection Agency (CPPA) has become the benchmark for how the United States will govern **data privacy and consumer trust**.[7] In the absence of a federal law, other states are modelling their regimes on California's; the standard an organization meets there is fast becoming the standard it must meet nationwide. Alignment is therefore not a response to a single regulator, but a means of anticipating the market's direction. The benefits are tangible: organizations navigate the churn of each new state law, win where data assurance now drives purchasing, and build the baseline controls that boards, auditors, and customers expect.

The decisive change is the shift from maintaining a policy to proving it functions. The finalized rules make diligence auditable through obligations such as **formal privacy risk assessments**; extension to automated decision-making technology (ADMT), where consumers gain opt-out and appeal rights and a distinct right to access information about how the AI processed their data; and, most consequentially, a **mandatory cybersecurity audit** certified to the CPPA and signed by a board member or top executive under penalty of law. That certification places the burden of proof squarely on management, drawing security, privacy, and internal audit together behind an attestation an executive must personally sign.

Enforcement has intensified in parallel — well-resourced regulators, no cure period, and per-violation penalties that accumulate across records, with exposure now multi-state: up to $20,000 per violation in Colorado and $25,000 in Texas.[8] The risk is proven, from Tractor Supply ($1.35M) to General Motors' $12.75M settlement and extends to AI claims themselves under FTC Act Section 5(a), as the DoNotPay and Workado actions showed.[9] An undetected deficiency no longer draws a warning; it becomes board-level financial exposure and, with a signed certification, personal exposure for the executive who attested to it.

An assurance mindset demonstrates its value here. Done well, alignment lets an organization prove on demand that its controls work — a defensible inventory of automated decision-making, consumer rights that function across all systems, and documentation audit-ready ahead of deadline.

Cybersecurity Maturity Model Certification (CMMC)

CMMC is moving **cybersecurity** from a contractual expectation to an operational requirement for organizations participating in the Department of War (DoW) supply chain. Areas of focus include formal regulatory implementation, evidence-based accountability, and a reassessment of the rollout timeline with the goal of enterprise-wide readiness rather than solely an IT or compliance activity.

The regulatory framework became effective on November 10, 2025, establishing a phased approach for incorporating CMMC requirements into applicable DoW solicitations and contracts, including establishing controls, ownership, preserving reliable assessment evidence, and ensuring that cybersecurity representations remain aligned with actual operating conditions. [10]

Control focus areas include asset and data-flow mapping, access management, incident response, vulnerability management, system security planning, assessment-score governance, subcontractor oversight, and executive accountability for annual affirmations.

Implementation is now subject to a significant policy pause. In July 2026, the DoW announced the immediate suspension of Phase 2, which had been scheduled to expand mandatory Level 2 third-party assessments beginning November 10, 2026. Related future milestones have also been placed on hold while the DoD reviews the program's cost, scalability, assessor capacity, and impact on small and non-traditional defence contractors. The pause may change the timing and design of future requirements, but it should not be treated as a reason to defer existing contractual obligations to align with NIST SP 800-171.

Priorities during this period include addressing existing control gaps, validating system boundaries, improving evidence quality, and preparing for potential changes to the implementation model. Effective CMMC readiness requires organizations to demonstrate, with credible and repeatable evidence, that controls operate as intended across the enterprise and relevant supplier ecosystem.

Our survey over the years

The table below presents a comparison of the top-10 technology and digital risk hot topics over the past 10 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 colour-coded to help illustrate their movement in the top 10 over time.

Rank	2027 (all sectors)	2026 (all sectors)	2025 (all sectors)	2024 (all sectors)	2023 (all sectors)	2022 (FS)	2021 (FS)	2020 (FS)	2019 (FS)	2018 (FS)
1	Cyber security	Cyber security	Cyber security	Cyber security	Cyber security	Cyber security	Cyber security	Cyber security	Cyber security	Cyber security
2	Artificial Intelligence	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
3	Data and regulatory reporting	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
4	Technology transformation	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
5	Third-party and outsourcing	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
6	Technology resilience	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
7	Cloud computing environments	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
8	Legacy systems and technology simplification	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
9	IT governance and risk management	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
10	Cryptography and quantum computing	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

Technology and digital risk hot topics for 2027

2027 rank	Hot topic	Change	Audit	Analytics
1	Cyber security	-	92%	59%
2	Artificial Intelligence	-	74%	48%
3	Data and regulatory reporting	-	57%	46%
4	Technology transformation	↑	59%	34%
5	Third-party and outsourcing	↓	57%	44%
6	Technology resilience	-	46%	23%
7	Cloud computing environments	-	39%	25%
8	Legacy systems and technology simplification	↓	13%	15%
9	IT governance and risk management	↑	44%	28%
10	Cryptography and quantum computing	New	0%	0%

Key:

Change from 2026

Change from 2026 highlights the change in ranking of each topic from the previous year's report.

Audit planned %

Audit planned % is the percentage of respondents who have included or plan to include this topic in their 2027 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.

1 Cyber security

92% Audit planned % | **59%** Use of analytics % | **-** Change from 2026

Overview

Cyber security remains the defining technology risk for organisations in FY27, as the threat landscape becomes more complex, automated and interconnected. The rapid adoption of AI, the continued reliance on cloud services and expanding third-party ecosystems are increasing the scale and speed at which cyber risks can affect critical operations, sensitive data and customer trust. Developments of advanced AI models have highlighted the potential for AI to identify and exploit vulnerabilities at unprecedented speed, reducing organisations' ability to rely solely on traditional prevention and patching approaches. With ransomware, identity compromise and supply chain incidents continuing to test organisational resilience· cyber security remains a key area of focus for Internal Audit teams.

What's new for 2027?

Cyber security retained its 2026 position as the number one IT Internal Audit hot topic for 2027, reconfirming its role as a core assurance priority. Survey results show that 92% of participating organisations expect cyber security to feature within their Internal Audit programmes, and that 59% of organisations plan to use data analytics to assist in those planned audits.

This continued focus on the hot topic reflects the growing scale, speed and sophistication of cyber threats. Respondents highlighted AI-enabled attacks, the increased sophistication of the foundational AI models (e.g., Mythos), and the step-change in the pace of AI-powered vulnerability discovery, as key drivers for cyber security continuing being a board level risk. Indeed, the time between identifying and exploiting a cyber vulnerability is materially compressed, driving panicked responses by some organisations. Such threats also include the use of generative AI to create more convincing phishing campaigns, automate reconnaissance, accelerate malware development and support social engineering.

In parallel, organisations are embedding AI into business processes, increasing the need for assurance over data protection, secure configuration, access control and governance of AI-enabled systems.

In relation to vulnerability posture and remediation strategies, functions should continue the dialogue with cyber leadership, the board and regulators, given heightened expectations for rapid disclosure and accountability. By focusing on these areas, they can help ensure that organisations are not only keeping pace with AI-accelerated threats but are also building resilient, business-aligned cyber risk management foundations.

Identity and Access Management was also identified as a significant focus area, reflecting the prevalence of identity-based attacks and the need for robust controls over privileged access, multi-factor authentication, non-human identities and joiner-mover-leaver processes. Threat detection, incident response and recovery capabilities remain equally important, as organisations need to demonstrate that cyber incidents can be identified, contained and recovered from, before material operational, financial or reputational impact occurs.

Collectively, these drivers point to a more resilience-led cyber assurance agenda, covering prevention, detection, response and recovery across the full cyber control environment.

Key drivers for 2027

- AI-powered threats (e.g., Mythos, GPT-5.6 Sol)
- Identity and access management
- Threat detection and incident response

Top five things internal audit should do

1. **Strengthen cyber governance, regulatory oversight and Board reporting**
Internal Audit should assess whether cyber security governance aligns to risk appetite, regulatory obligations, critical services and recognised good practice, including relevant National Cyber Security Centre (NCSC)[11] guidance for the UK, such as the Cyber Assessment Framework, or National Institute of Standards and Technology (NIST)[12] guidance for the US. This should include Board oversight and reporting, cyber risk metrics, and whether governance is supported by a strong cyber security culture.

2. **Prioritise Identity and Access Management assurance**
Identity remains a primary route for cyber compromise. Internal Audit should review privileged access, multi-factor authentication, joiner-mover-leaver controls, access reviews and controls over service accounts and non-human identities. Audit teams should leverage AI-powered capabilities where appropriate to improve testing coverage and efficiency.

3. **AI-Driven vulnerability management**
AI-driven vulnerability discovery is accelerating the volume and pace of vulnerability identification. Internal Audit should assess whether organisations can rapidly identify, prioritise and remediate vulnerabilities through effective asset visibility, risk-based decision-making, escalation processes and secure-by-design development practices. Compensating controls should be in place for systems that cannot be patched quickly.

4. **Review third-party, cloud and supply chain cyber risk**
Internal Audit should assess whether cyber risks from cloud platforms, SaaS providers, managed service providers, critical vendors and outsourced services are understood and managed through vendor assurance, supplier monitoring and resilience planning for key dependencies.

5. **Embed Secure by Design, DevSecOps and AI Security Assurance**
Internal Audit should assess whether security is embedded throughout technology change and operations, including AI-enabled solutions. This should include Secure by Design practices, application security, vulnerability management, data protection and access controls. Audits should also consider AI-specific risks, including model security, data provenance, third-party AI dependencies and governance over emerging technologies.

2 Artificial Intelligence

74% Audit planned % | **48%** Use of analytics % | **-** Change from 2026

Overview

Artificial Intelligence, or 'AI', is no longer a discrete system to be reviewed in isolation; it is becoming a feature of the wider technology backbone of organisations and their control environment. It is increasingly embedded in enterprise platforms, vendor products, customer journeys, credit decisions, and the tools internal audit functions use themselves. Where organisations have not formally enabled AI, employees have often found ways to use it outside of approved channels. For internal audit, this changes the assurance approach. A single annual AI review can provide only partial comfort over a technology that may now permeate the full risk universe. For 2027, the more useful ambition may be to make AI a standing consideration in every auditable entity and audit.

What's new for 2027?

AI has retained its position as the second-ranked hot topic, signalling continued attention from audit functions. The figures are important: overall, 74% of organisations expect AI to feature in audit plans which is a great increase from 2026, but that means that over a quarter still have no current plans for a dedicated review.

For Audit Executives, the message is clear: many functions are still defining their AI assurance approach, and a single AI audit will not be enough. The survey's leading focus areas, including governance and strategy, data quality and provenance, and agentic AI, cut across multiple parts of the audit universe. A function that reports "we have audited AI" may therefore be providing narrower assurance than the Audit Committee expects.

The continued prominence of AI reflects four linked pressures: *regulatory attention; rapid business adoption / scaling; evolving compute and technology capability; and increased employee use*. Organisations are already using AI to improve productivity, service quality and decision-making, often before governance, monitoring and accountability have fully matured [13]. In parallel, employees may be using public or embedded AI tools outside approved channels, creating risks around data protection, intellectual property, output quality and transparency [14].

Regulatory scrutiny of AI continues to accelerate across both the UK and US. The implementation of the EU AI Act [3] is increasing expectations around governance, accountability, transparency and risk management for AI-enabled solutions, while global regulators are increasingly signalling that existing frameworks relating to operational resilience, conduct, model risk management and customer outcomes should be applied to AI use cases.

The audit response needs to reflect this reality. AI assurance will need to evolve beyond standalone reviews (i.e. not through traditional audits but increasingly through assurance reviews or gap assessments). Dedicated AI audits remain important, but the breadth of the identified focus areas indicates that internal audit functions should also consider how AI features within broader audits of change, data, third parties, resilience, financial crime, business strategy, customer outcomes and governance.

External auditors have also started to actively scrutinise AI governance, with the recently published COSO guidance setting clear expectations for controls and evidence. Unlike deterministic tools, GenAI is probabilistic - outputs can vary and be difficult to explain, introducing reliability and validation challenges. Relevant controls over risks relevant to 2026 year-end Financial Reporting need to be identified and scoped in accordingly.

Key drivers for 2027

- AI governance and strategy
- Data quality and provenance for AI models
- Agentic AI

Top five things internal audit should do

1. **Embed AI into audit planning and scoping**
   Treat AI as a standing consideration across the audit universe, not only as a standalone review. Each engagement should ask whether AI is used, whether it affects existing controls, what decision it influences, who approved it, what data it consumes, and whether outputs can be explained.

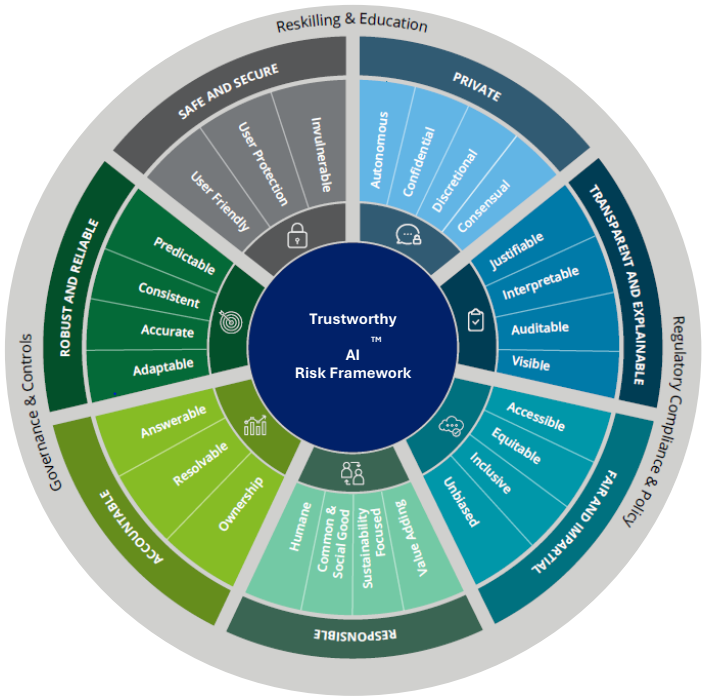
2. **Apply existing risk principles while standards catch up**
   AI regulation and standards, particularly for emerging agentic capabilities, are still developing, so internal audit should not wait for perfect guidance. AI use cases need to be assessed through existing prudential, model risk management, conduct, operational resilience, and data protection frameworks (e.g., GDPR). Existing principles around risk appetite, accountability, change control, data governance, model risk, third-party risk and customer outcomes should be applied consistently to AI use.

3. **Provide a clear AI assurance view to the Audit Committee**
   Internal audit should help the Audit Committee understand where AI is being used, where assurance has been provided, and where material gaps remain. IA teams should look to advise the business on finding the balance between risk management, governance, and efficiency – helping the business safely streamline their transformation capabilities so governance manages risk but is not a bottleneck. For both advisory and assurance reviews, IA teams should consider new AI risks, existing IT processes and digital monitoring opportunities

4. **Challenge how management responds to AI demand signals**
   Shadow AI can indicate un-met business need, but it also exposes gaps in governance, training and approved tooling. Internal audit should assess whether management has identified these demand signals and put in place proportionate routes for safe adoption, including sufficient guardrails, while challenging risks around ungoverned IT.

5. **Strengthen AI capability within internal audit**
   Audit Committees are not only asking for assurance over the enterprise but are asking IA departments to become more efficient using and enabling themselves with the capabilities. The mature IA function will be able to assure and advise the business on AI implementations and risk management. Teams need sufficient fluency to challenge how models are selected, prompted, monitored and retired. Using AI within the audit process, under appropriate governance, can help auditors understand the risks and provide more practical findings.

2 AI governance and assurance framework



Reference lenses

COSO
ICFR controls & monitoring

NIST AI RMF / Deloitte
trustworthy AI risk

EU AI Act / Other Reg Guidance
Targeted regulation & interplay with existing, e.g. PRA SS1/23

Govern & Scope

1 Governance

- Review purpose, risk profile and business impact.
- Ensure alignment with AI strategy.
- Ensure clear ownership, accountability and policy.
- Set a combination of constraints and boundary guardrails to restrict decision-making and outputs.

Trust the data

2 Data integrity & quality

- Assess data and sources – focus on integrity, quality, representativeness and bias.
- Test preprocessing and trace lineage from input to output.
- Assess source attribution, manage plagiarism and copyright risks.

Make it transparent

3 Verification & explainability

- Review architecture, training and parameters.
- Ensure explainability of decisions and auditable version control.
- Require the model / agent to provide traceable step-by-step reasoning for decisions, an auditable rationale and evidence.
- Assess deployed “auditing/validation” agents to review quality and compliance.

Challenge the risk

4 Risk management

- Design and implement AI controls to address AI-specific risks.
- Assess control effectiveness and initiate remediation.
- Test bias and fairness, adversarial security, privacy and compliance with applicable requirements.

Test & validate

5 Governance

- Validate accuracy, robustness and reliability.
- Assess code and models independently; perform threat modelling and test AI technology for malicious or environmental threats – cyber security by design.
- Stress-test edge cases and monitor drift and anomalies.

Evidence the journey

6 Data integrity & quality

- Ensure logged prompts, outputs and key actions, with evidence and records retained.
- Real-time monitoring and full-cycle tracing of actions, decisions, reasoning steps, and tool actions.

Maintain human oversight

7 Verification & explainability

- Apply risk-based human-in-the-loop approval or human-on-the-loop monitoring, based on autonomy and impact.
- Define accountability, escalation thresholds, override and stop conditions, and periodic expert review.

Improve the outcome

8 Risk management

- Challenge if the agents / models produce consistent, continuous evaluation of behaviour against performance thresholds for accuracy, security and compliance.
- Ensure agents are aligned to their purpose.

Comprehensive AI governance, risk management and assurance principles serve as the cornerstone of a sound AI risk framework. A risk management and governance AI framework (such as Deloitte’s), that balances robustness, safety with ethics provides the backdrop to a sustainable, safe, and responsible AI use environment and risk management program.

3 Data and regulatory reporting

57% Audit planned % | **46%** Use of analytics % | **-** Change from 2026

Overview

Data and regulatory reporting continues to be a critical focus for Internal Audit functions, maintaining its third-place ranking in the FY27 hot topics survey. Let's not forget, data quality is a fundamental prerequisite for any cost-effective and successful AI implementations. Data remains a core component of numerous audit programmes, reflecting its foundational importance across organisational operations and strategic initiatives. The increasing volume, complexity, and regulatory scrutiny of data necessitate robust oversight, making it an enduring priority for assurance providers in 2027.

What's new for 2027?

Organisations must recognise the critical importance of data, not only as a top supervisory priority for regulators across all sectors and jurisdictions, but also as the foundational enabler for advanced technologies such as Artificial Intelligence.

Without robust data integrity, the promise of AI cannot be fully realised, making data a strategic imperative. The survey results underscore the sustained significance of Data within Internal Audit plans. 57% of organisations anticipate including Data in their audit programmes for 2027, with 31% having already incorporated it and another 26% planning to do so in the future - a focus echoed externally by Gartner, whose 2026 survey found 94% of CAEs planning data governance activity.[15] This consistent focus highlights the pervasive impact of data across all business functions and its inherent risks. The primary drivers influencing this selection are multifaceted.

Firstly, data governance is paramount, as organisations grapple with ensuring data quality, integrity, and effective management throughout its lifecycle. Secondly, data analytics and reporting controls are crucial, given the reliance on data for strategic decision-making and performance measurement, requiring assurance over the accuracy and reliability of insights derived. Lastly, data governance and regulatory compliance remain significant focus areas. Evolving privacy laws - including the Data Use and Access Act[5] and California Consumer Privacy Act (CCPA)[7]– and sector-specific requirements demand rigorous controls and continuous monitoring of AI use, cross-border data flows and data sharing.

For financial institutions, relevant frameworks include the BCBS 239 principles[16]; the European Central Bank's (ECB) risk data aggregation and risk reporting (RDARR) expectations[17] (which many organisations continue struggling with); Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) requirements concerning systems, controls and operational resilience[2]; and the Digital Operational Resilience Act (DORA) for applicable EU entities.[2] Effective governance should address data quality, lineage and reporting, as well as AI use, cross-border flows and third-party data sharing, to mitigate legal, prudential and reputational risks. Collectively, these drivers make Data an indispensable area for Internal Audit scrutiny.

In an era defined by exponential data growth and the rapid adoption of AI and emerging technologies, the traditional reliance on manual data controls and mapping is no longer sustainable or scalable.

Internal Audit functions must recognise that future-proofing data controls necessitates a shift towards automation, with AI as a key enabler. It is no longer feasible to deploy full teams for manual data mapping and control enforcement. However, automation must not outpace data quality assurance, as AI trained on poor data scales and repeats errors.

Key drivers for 2027	Data governance (incl. data quality, data lifecycle management, etc.)	Data analytics and reporting controls	Data regulatory compliance

Top five things internal audit should do

1 Understand data's role in AI and emerging technologies

As firms embark on strategic AI scaling programmes, Internal Audit should assess data quality, provenance, lineage, and fitness-for-purpose controls, together with applicable AI-transparency, privacy, and sector-specific requirements. Testing should evidence how data is collected, processed, governed, and used in AI systems, including controls addressing bias, access, retention, and accountability.

2 Ensure data quality for operational and regulatory needs

Internal Audit should conduct holistic reviews of data quality, recognising its critical impact on both operational efficiency and regulatory reporting. With increasing reliance on data for strategic decisions, audit functions must assess the controls around data analytics processes, from data sourcing and transformation to reporting. This ensures the accuracy, completeness, and reliability of insights used by management.

3 Assess data governance frameworks

Internal Audit should evaluate the maturity and effectiveness of the organisation's data governance framework, including policies, standards, roles, and responsibilities for data ownership, quality, and lifecycle management. This includes ensuring clear accountability for data assets and a unified metadata / data-lineage capability to evidence where AI training data originated.

4 Monitor data regulatory compliance

Monitor applicable data-protection, AI, and sector-specific regulatory requirements, recognising that obligations and effective dates vary by jurisdiction, system type, and organisational role. For financial institutions, assess alignment with BCBS 239 and the ECB intensified guide on RDARR expectations[16][17], including governance, data architecture, quality, end-to-end lineage and timely risk and regulatory reporting—even where not directly mandated. Assess the organisation's compliance posture, including data handling, lawful basis and consent, data-subject rights, retention, cross-border transfers, and breach-response protocols.

5 Evaluate data security and privacy controls

Beyond governance, Internal Audit needs to scrutinise technical and organisational controls protecting sensitive data from unauthorised access, use, disclosure, disruption, modification, or destruction. including data used by AI systems and agents. This includes data encryption, access management, data loss prevention measures, data classification, and lineage controls.

4 Technology transformation

59% Audit planned % | 34% Use of analytics % | ↑ Change from 2026

Overview

Technology transformation is an enterprise-wide priority, embedded in how organisations deliver strategy, improve customer outcomes and remain competitive. Organisations ramp up investment in technology transformation at scale using AI models, cloud migration, system modernisation that ultimately drive target operating model redesign and enable new customer journeys. These initiatives create opportunities and competitive advantage but also introduce significant risks that Internal Audit must understand and address. The challenge is to move beyond traditional compliance reviews and provide assurance that digital change is delivering intended business outcomes and ROI while managing risk appropriately.

What's new for 2027?

Economic, geopolitical uncertainty and challenging markets continue to drive initiatives to optimise core operating costs, open new channels or seek strategic restructure whilst remaining compliant with evolving regulation. These changes trigger the critical need for new systems, processes and target operating models that are enabled by digital technology at the core, not as a bolt on to an existing service or way of working.

The rapid change in technology capability driven by AI agents reinforces the need for strong governance over short term portfolio prioritisation, seamless release management and functional deployment controls. Where technology enables increasing amounts of change to be delivered in the business, without the traditional structures of IT functions and change professionals, it is imperative that management, risk and Internal Audit ensure that transformation activity is well controlled, considers the impact on customers appropriately and is aligned to strategic outcomes, while also maintaining operational resilience during periods of significant change.

Additionally, Internal Audit not only need to audit and advise the business on digital transformation, but they also need to transform itself. This means integrating GRC systems, adopting new ways of working and embedding AI across the audit lifecycle. By experiencing this transformation first-hand, Internal Audit will be better positioned to act as a trusted adviser.

Technology, digital transformation and value-driven change remain high on leadership outcome measures, Board risk assessments and the Internal Audit agenda across sectors. AI is having an impact on multi-year programmes, potentially undermining viability and benefits delivered by business cases.

As many of change initiatives are non-optional, cost and time-sensitive or regulatory-driven, AI needs to be adequately considered in the design of the existing and new programmes as well as associated key performance metrics.

Key drivers for 2027

- Prioritisation and portfolio management
- Release management and deployment controls
- Change request and approval process

Top five things internal audit should do

1. **Controls and governance are playing catchup**
   Teams are under pressure to launch new products and AI capabilities quickly. Rapid prototypes and proofs of concept may be deployed before ownership, accountability and risk assessment are clearly defined. Internal Audit should assess governance pathways from ideation through operation, and in doing so should be helping business to identify opportunities to streamline governance - allowing the business and IT teams to focus more on their core responsibilities.

2. **Agentic development and vibe coding**
   Speed outpaces safeguards – Generative AI tools are transforming software development[18], enabling amateurs to build solutions unsupported. Changes may bypass existing controls and produce limited documentation. Internal Audit should assess whether Agentic coding is governed through the software development lifecycle, including access to confidential data, code review, testing, deployment and monitoring controls.

3. **Value-focussed scaled Agile**
   Industries are evolving established waterfall and agile frameworks towards custom value stream models with selected elements of DevOps, Lean and Scrum. Auditing against the framework is not sufficient, and auditors must consider how governance structures are tailored, particularly around scope control and benefits delivery.

4. **Trust is not a control**
   The growing use of open-source datasets and AI models within transformation journeys challenges how organisations map dependencies, trust outputs, and prove data sources are representative. Internal Audit should consider whether digital trust roles and specialist assurance support is in place for features built on digital supply chains beyond the enterprise.

5. **Integrated change assurance**
   With increasingly rapid change cycles, Internal Audit should align change assurance across the three lines of defence, enabling earlier identification of high-risk areas and timely intervention across complex change portfolios. Early assurance can help improve programme outcomes, reduce delivery risk and prevent costly remediation by identifying control, governance and delivery issues before they become embedded. Auditing after the event is no longer sufficient.

5 Third-party and outsourcing

57% Audit planned % | **44%** Use of analytics % | ↓ Change from 2026

Overview

Third-party risk management continues to evolve beyond traditional outsourcing oversight into a single cross-industry discipline, as organizations become increasingly dependent on cloud, technology platforms and AI-enabled services. Regulatory expectations are expanding in parallel across the UK and US – from the UK's Critical Third-Party regime and Material Third-Party Reporting rules to CISA's CIRCIA reporting rule and a wave of US state AI laws – converging around dependency mapping, concentration risk and operational resilience.

What's new for 2027?

The UK's designation of the first Critical Third Parties (CTPs) [19] — Amazon Web Services, Google Cloud, Microsoft and Oracle — in July 2026, and the UK's Material Third-Party Reporting requirements, effective 18 March 2027, are driving scrutiny of dependency mapping and concentration risk. In the US, CISA's CIRCIA final rule[20], expected September 2026, will require entities across 16 critical infrastructure sectors to report covered cyber incidents — including vendor or supply-chain compromises — within 72 hours, and ransom payments within 24 hours.

The IIA's Third-Party Topical Requirement[21], mandatory from 15 September 2026, reinforces global expectations around governance, dependency mapping, resilience and assurance across third-party ecosystems — regardless of jurisdiction.

Regulators are placing greater emphasis on understanding end-to-end dependencies across critical services, including fourth parties, offshore operations, intra-group providers and emerging AI solutions. This shift reflects growing concern that disruptions within a small number of shared providers could have widespread consequences across organisations, sectors and markets.

AI adoption is reshaping third-party risk on both sides of the Atlantic. Colorado's Automated Decision-Making Technology Act takes effect 1 January 2027[22] — the first US state regime requiring notice and human-review rights when vendor-supplied AI materially influences consequential decisions — while UK regulators are extending Critical Third Party and outsourcing expectations to cover AI-enabled services and foundation models.

Sector-specific obligations are intensifying in parallel: US federal banking agencies continue to sharpen bank-fintech and cloud-concentration expectations under the 2023 interagency guidance, HHS's proposed HIPAA Security Rule overhaul remains pending, and the Department of War's July 2026 suspension of CMMC Phase 2[10] has paused defence-sector third-party certification — even as UK financial firms prepare for the IIA Requirement and Material Third-Party Reporting deadlines.

Alongside these developments, accountability for outsourced activities remains firmly with the organisation. Regulators increasingly expect continuous oversight supported by meaningful management information, resilience testing, contingency planning and credible exit strategies.

Key drivers for 2027

- Ongoing monitoring and performance review
- Fourth-party risk (sub-contractor risk)
- Vendor due diligence and selection

Top five things internal audit should do

1. **Material Third-Party Reporting preparedness**
   Assess readiness for the UK's Material Third-Party Reporting requirements (effective 18 Mar 2027) and CISA's CIRCIA final rule (albeit not finalized and expected Sept. 2026) including the ability to report incidents within 72 hours, and ransom payments within 24 hours.
2. **Critical Third Parties, dependency mapping and concentration risk**
   Review whether dependencies on the UK's designated CTPs (AWS, Google Cloud, Microsoft, Oracle) and US cloud, core-processor and banking-as-a-service providers are comprehensively mapped, and how concentration risk is monitored and escalated to the board.
3. **AI-enabled services and emerging supplier ecosystem risks**
   Assess whether governance addresses AI vendor risk ahead of Colorado's Automated Decision-Making Technology Act (effective 1 Jan 2027) and the UK's extension of Critical Third-Party expectations to AI-enabled services, including model risk, explainability and bias testing.
4. **Operational resilience, contingency planning and exit readiness**
   Evaluate preparedness for the IIA's Third-Party Topical Requirement (mandatory 15 Sept 2026), HHS's proposed HIPAA Security Rule overhaul, and CMMC 2.0 subcontractor flow-down following the Department of War's July 2026 suspension of Phase 2 certification.
5. **Third-party governance, oversight and accountability**
   Assess whether governance arrangements, management information and escalation processes provide effective oversight of third-party risk across jurisdictions, and whether Internal Audit approaches remain aligned to evolving UK and US regulatory expectations.

6 Technology resilience

46% Audit planned % | **23%** Use of analytics % | **-** Change from 2026

Overview

Technology resilience remains a critical consideration as organisations modernise their technology estates, adopt new capabilities and rely on increasingly interconnected services. The ability to anticipate, withstand, respond to and recover from disruption is now central to maintaining operational continuity, customer trust and business performance. Resilience considerations are increasingly being embedded into strategic decision-making, change delivery and technology governance, with internal audit playing an important role in assessing whether capabilities remain effective, proportionate and fit for purpose.

What's new for 2027?

While the topic's ranking has remained stable this year, the discussion has evolved from establishing resilience frameworks to demonstrating measurable resilience outcomes, with greater emphasis on evidencing the effectiveness of resilience capabilities through testing, performance metrics, and operational results.

For UK financial services firms, this is now an ongoing supervisory expectation. The PRA and FCA have finalised new operational incident and third-party reporting requirements in March 2026[2], with the new rules coming into force on 18 March 2027, asserting that operational incident reporting rules will define operational incidents, set thresholds, introduce a standardised reporting process and require firms to submit standard or enhanced incident reports.

Organisations are increasingly recognising that technology failures, cyber incidents and disruption across the wider technology supply chain can quickly affect critical services, customer outcomes and business performance.

As a result, resilience considerations are becoming more embedded within technology strategy, architecture, change delivery and supply management, helping organisations build resilience by design rather than relying solely on reactive recovery measures.

The additional, growing complexity of environments due to the use of modern technologies such as cloud, automation and artificial intelligence further drive the need for organisations to consider their recovery methods as "disruptions" have evolved from isolated events to persistent occurrences in a constantly changing environment. Continuous, rather than static, approaches to recovery are therefore emerging as a greater focus area for organisations.

In parallel, there is growing emphasis on defining the Minimum Viable Company (MVC) - the minimum technology, people, processes and third-party services required to sustain critical operations during disruption. This is driving greater focus on dependency mapping, recovery capability and resilience testing, enabling organisations to identify vulnerabilities and validate whether critical services can continue to operate under adverse conditions. Internal audit functions are increasingly being asked to provide assurance on the MVC design (for example as part of a cyber vault programme), and that capabilities are practical, tested and capable of supporting business continuity as organisational needs evolve.

The IIA's Organisational Resilience Topical Requirement[23], issued on 30 April 2026 and effective from 30 April 2027, further strengthens the case for internal audit to apply a consistent baseline when assessing governance, risk management and control processes for organisational resilience.

Key drivers for 2027 | Cyber resilience | Supply chain resilience | Resilience testing

Top five things internal audit should do

1. **Assess whether resilience is embedded by design**
   Review how resilience requirements are reflected across technology strategy, architecture, transformation and change delivery activities. Consider the regulatory expectations and organisations' use of emerging technologies e.g. automation, AI when assessing the suitability and sufficiency of requirements defined to mitigate risks.

2. **Understand what is truly critical**
   Assess whether management understands and has defined the MVC – the minimum technology, people, processes and third parties required to sustain critical operations during disruption. Evaluate the organization's process over substantiating their minimum requirements, including their consideration of service tolerances and critical dependency mapping.

3. **Review cyber recovery and recoverability**
   Consider whether critical services can be recovered following a cyber event, including the effectiveness of backup, restoration and recovery testing arrangements. Assess whether organisations have considered scenarios and testing to address cyber risks associated with integration of information technology (IT) and operational technology (OT) systems. Test recovery from isolated, immutable cyber-vault copies.

4. **Assess technology dependency and concentration risk**
   Evaluate management's understanding of dependencies across cloud providers, technology vendors, data centres and other critical suppliers. Consider additional dependencies on automation, AI and how management incorporates the use of such technologies in their critical dependency mappings

5. **Challenge resilience testing and continuous assurance**
   Assess whether testing is sufficiently realistic and whether lessons learned are used to strengthen resilience capabilities over time. Evaluate management's process for maintaining effective resilience through continuous monitoring and improvement activities.

7 Cloud computing environments

39% Audit planned % | 25% Use of analytics % | Change from 2026

Overview

Cloud computing has become the backbone of modern organisations, enabling critical business services, digital transformation, and increasingly complex technology ecosystems. As cloud adoption matures, the focus is shifting from migration and governance to security, resilience, cost optimisation, and compliance. Organisations are now expected to demonstrate that cloud services are secure, well-governed, and resilient, while maintaining oversight of increasingly distributed environments spanning multiple cloud providers and third-party services.

What's new for 2027?

Cloud features prominently within technology risk surveys and Internal Audit plans because it underpins many of an organisation's critical business processes, rather than existing as a standalone technology capability.

The inherent complexity of these advanced cloud deployments amplifies the potential for security vulnerabilities, frequently arising from misconfigurations or inadequate identity and access management.

Concurrently, the landscape is rapidly intensifying, with a heightened focus on operational resilience, security, evolving data protection mandates, and emerging considerations around cloud supply chain resilience. Geopolitical tensions continue to increase the risk of data sovereignty constraints (i.e., data should be subject to the laws and governance of the countries of collection and storage), regional service disruption, and access restrictions, making cloud governance more complex.

This necessitates robust governance and oversight, leading to a proliferation of new security and compliance audit requirements, demanding continuous assessment of control effectiveness.

Whilst many organisations have now completed significant phases of their cloud migration programmes, cloud environments continue to evolve through increased adoption of platform services, software-as-a-service (SaaS), cloud-native applications, and multi-cloud operating models. This has shifted the risk profile from implementing cloud technologies to governing complex, interconnected environments. A significant driver for audit focus this year is the persistent issue of cloud misconfigurations, which are a leading cause of security incidents.

Internal Audit functions are therefore experiencing growing demand to provide assurance over cloud governance frameworks, identity and access management, resilience planning, third-party oversight, configuration management, and financial governance.

Boards are increasingly seeking assurance that cloud investments, including those related to AI, continue to support strategic objectives whilst remaining secure, resilient, compliant, and cost-effective. Consequently, cloud will remain a significant area of audit focus throughout 2027, with greater emphasis placed on governance, security maturity, operational effectiveness, and business resilience than on cloud adoption itself.

Key drivers for 2027

- Cloud security architecture and controls
- Cloud incident response and resilience
- Cloud governance

Top five things internal audit should do

1. **Cloud-native security assurance**
   Internal Audit should assess the integration of security into cloud-native development lifecycles (DevSecOps), evaluating automated security controls, infrastructure as code (IaC) security, and the protection of containerised and serverless workloads. This ensures security is 'shifted left' and embedded from design.

2. **Cloud recovery and resilience**
   This topics aligns with our broader Resilience topic in the report. Internal Audit must proactively assure the organisation's capability to sustain critical business operations amidst cloud service disruptions. This necessitates evaluating disaster recovery, backup strategies, Recovery Time Objectives and Recovery Point Objectives (RTOs and RPOs), the effectiveness of resilience testing (e.g., failover, chaos engineering), robust incident response plans, and strategic multi-cloud/hybrid approaches. Crucially, IA should verify third-party dependencies and their contractual resilience obligations.

3. **Identity and access governance**
   As cloud environments continue to expand, identity provisioning and management stands as the paramount security control. Consequently, Internal Audit functions should critically evaluate privileged access management, service accounts, authentication controls, and the efficacy of identity governance processes, given that IAM failures are a leading cause of cloud breaches.

4. **FinOps and AI cost optimisation**
   Internal Audit should assess whether AI-enabled cloud consumption has clear ownership, transparency and controls. AI training (using large datasets) and inference (i.e. user interaction and output generation) can create volatile, hard-to-forecast costs. Audits should evaluate anomaly monitoring, right-sizing, workload placement, and whether consumption aligns with strategic business value.

5. **Multi-cloud ecosystem governance**
   Internal Audit should assess governance across multi-cloud environments within the wider cloud ecosystem, including managed services, SaaS platforms, APIs and integrations, and other third-party dependencies. Key areas include control consistency, configuration management, and resilience to regional or cloud provider disruptions across interconnected cloud services.

8 Legacy systems and technology simplification

13% Audit planned % | 15% Use of analytics % | ↓ Change from 2026

Overview

Legacy systems often support critical business operations, but they can constrain agility where they are difficult to integrate, poorly documented or no longer fully supported. They may also increase operational and security risk where processes depend on manual workarounds or knowledge held by a small number of individuals. As organisations look to use AI more effectively, these limitations become more significant. AI relies on good-quality data, clear ownership, reliable interfaces and adequate performance. Where legacy environments cannot provide this foundation, initiatives may be harder to deliver and may not achieve the expected benefits.

What's new for 2027?

Recent survey results show that Legacy IT and Simplification remain important areas of focus for organisations, and many functions still struggle with the topic. It continues to be a consistent priority rather than a short-term concern.

Additionally, only 13% of organisations expect to include it in their audit plans. This apparent disconnect may reflect the fact that legacy technology risks are often assessed indirectly through cyber security, resilience, transformation or cloud reviews rather than through standalone audits. However, respondents increasingly recognise that legacy technology is not simply a technical concern, but a business issue that can increase operational costs, constrain transformation, create technical debt and limit the benefits organisations can realise from emerging technologies such as AI.

Although legacy technology risks are well established, regulatory expectations continue to rise. The EU DORA[2], alongside wider UK and US resilience requirements, increase the focus on understanding critical technology assets, managing information and communications technology risks and ensuring important business services can withstand disruption.

Survey respondents identified key drivers including modernisation, decommissioning and improved technology inventories. In the age of agentic artificial intelligence and models with advanced cyber related capabilities, unsupported systems, technical debt and poor visibility of assets can increase cyber, operational and resilience risks.

Organisations are therefore focusing not only on technology refresh, but also on simplification and resilience, including whether critical legacy services can meet recovery requirements. Ageing and fragmented environments may also restrict the value organisations can realise from data, automation and AI initiatives.

This creates a clear role for Internal Audit to provide assurance over the governance, resilience and management of legacy technology risks, and the effectiveness of modernisation and simplification programmes in supporting business, regulatory and transformation objectives.

Key drivers for 2027	Modernisation strategy and execution	Decommissioning	Inventory and risk assessment

Top five things internal audit should do

1. **Assess senior leadership visibility and risk acceptance**
   Assess whether management and the Board have a clear view of material legacy technology risks, including unsupported systems, concentration risk, cyber exposure, resilience constraints, funding gaps, and accepted risk positions.
2. **Validate the legacy technology inventory**
   Review whether the organisation maintains a complete inventory of legacy systems, including ownership, business criticality, support status, data dependencies, interfaces, manual workarounds, and links to important business services.
3. **Review modernisation and decommissioning plans**
   Assess whether modernization, replacement, and decommissioning activity is risk-based, funded, prioritised, and aligned to resilience, security, regulatory, and business objectives.
4. **Assess resilience and recoverability of critical legacy services**
   Test whether legacy systems supporting critical operations can meet recovery requirements, incident response requirements, backup/restoration needs, and operational resilience tolerances.
5. **Evaluate whether legacy environments constrain AI and data strategy**
   Consider whether legacy platforms provide reliable, accessible, secure, and well governed, quality data to support automation, analytics, and AI use cases.

9 IT governance and risk management

44% Audit planned % | **28%** Use of analytics % | ↑ Change from 2026

Overview

Of the 44% of participating organisations that have indicated that IT governance and risk management will be included in their audit plans, only 13% of organisations have already included the topic whilst the other 31% expect to do so in future, suggesting that governance and risk management capabilities are becoming an increasingly important area of assurance. Respondents identified IT strategy and business alignment, policy and standards enforcement, and enterprise architecture governance as their primary areas of focus. The IIA topical requirements (as covered elsewhere in the paper) underline the importance for Audit functions sufficiently covering governance and risk management areas, treating them as foundational components for any technical domain.

What's new for 2027?

As organisations accelerate the adoption of AI, cloud technologies and digital transformation initiatives, effective technology governance is becoming increasingly important. Many organisations are discovering that emerging risks cannot be managed through specialist governance frameworks alone, but instead require strong foundational governance over technology strategy, decision-making, risk management and accountability. Weak governance in these areas can undermine even the most mature cyber, resilience or AI-specific control frameworks.

Similarly, as there is an acceleration in adoption of AI-enabled services, cloud technologies, and digital transformation initiatives, governance frameworks should track applicable regulatory obligations and implementation timelines by jurisdiction, AI-system category, and organisational role.

Organizations must balance innovation with appropriate oversight, ensuring that technology decisions remain aligned to business objectives, risk appetite, regulatory expectations, and clear accountability. As technology environments become more decentralised and business-led, effective governance is increasingly relied upon to provide consistency, transparency, risk management, and control.

At the same time, senior stakeholders continue to demand greater visibility of technology risk and investment outcomes. This is driving increased focus on technology strategy execution, enterprise architecture governance, policy compliance and management information that supports informed decision-making.

As a result, Internal Audit functions are increasingly being asked to provide assurance that governance frameworks remain effective as organisations adopt new technologies and evolve their operating models.

Key drivers for 2027	IT strategy and alignment	IT policy and standards enforcement	IT risk assessment frameworks (e.g., ISO 31000, NIST RMF)

Top five things internal audit should do

1. **Technology strategy and business alignment**
   Assess whether technology investments, transformation programmes and emerging technology initiatives are aligned to organisational objectives, risk appetite and long-term business strategy and are delivering intended value. Review whether governance forums provide sufficient oversight and challenge over technology decision-making.

2. **AI, 'Shadow IT' and 'citizen development' governance**
   Evaluate whether governance frameworks have evolved to address increasing use of AI tools, low-code/no-code platforms and business-led technology solutions. Review controls over approval, oversight, accountability and monitoring to ensure innovation does not create unmanaged technology risks. Internal Audit should also test discovery and monitoring of AI usage, AI-literacy training and the provision of approved, secure alternatives.

3. **Policy, standards and control compliance**
   Review whether technology policies, standards and governance requirements are clearly defined, communicated and consistently enforced across the organisation. Assess whether exceptions are appropriately approved, monitored and reported. Assess evidence of operating effectiveness, not just policy existence, and avoid over-reliance on third-party vendor assurances.

4. **Enterprise architecture and technology change governance**
   Assess whether enterprise architecture principles are effectively embedded within technology decision-making and change programmes. Review whether architecture governance promotes standardisation, reduces technical debt and supports long-term technology objectives across cloud, AI, and other platforms.

5. **Technology risk governance and reporting**
   Evaluate whether technology risks are identified, assessed and escalated effectively, and whether management information provides leadership with a clear view of technology performance, emerging risks and governance effectiveness. This includes governing AI adoption as a material risk change within the enterprise risk framework rather than as a siloed technology initiative. Internal Audit should also consider whether governance and risk management arrangements align to the principles set out in the IIA Topical Requirements and support consistent assurance across the technology risk landscape.

10 Cryptography and quantum computing

0% Audit planned % | 0% Use of analytics % | New Change from 2026

Overview

Cryptography and quantum computing has entered the 2027 rankings for the first time as a standalone topic, having been included under 'emerging risks' in our 2026 report, highlighting growing awareness of the opportunities and risks associated with emerging technologies. While practical quantum computing capabilities remain at an early stage, the potential impact on current cryptographic protections is driving increased focus on data security and long-term resilience. The transition to post-quantum cryptography (PQC)[24] is expected to be a complex, multi-year undertaking, requiring organisations to better understand their cryptographic dependencies, prioritise critical assets, and develop proportionate migration strategies across both internal and external entities.

What's new for 2027?

Despite entering this year's rankings, no respondents indicated that cryptography and quantum computing is currently included within their audit plans. This suggests that awareness of the topic among security professionals is developing more rapidly than formal assurance activity, with many organisations either unaware of the risk or still viewing quantum-related risks as a future concern rather than an immediate audit priority. Respondents are preparing, however, for inclusion in the next 3 years. This view may be challenged over the next couple of years as FSI regulators rally to generate new regulations, and an increasing number of peer organisations convert to the new quantum safe cryptography.

Respondents identified data security and transactional integrity as the primary drivers behind their interest in the topic, termed together as cryptographic resilience.

As investment in quantum computing continues to accelerate globally, organisations are increasingly considering the potential implications for the confidentiality of information and the integrity of transactions. Modern cryptography underpins much of the technologies and services relied upon by organisations today, including secure communications, digital identities, and trusted digital transactions. A loss of confidence in these capabilities and controls could have significant implications for security, resilience and trust across the digital ecosystem.

This growing focus on cryptographic resilience reflects a broader recognition that the cryptography at risk from the quantum computing threat is currently supportive of many business functions.

Although dedicated audit activity remains limited, growing awareness of future cryptographic challenges is prompting increased discussion amongst risk, security and technology leaders regarding the actions required to maintain trust and resilience in a rapidly evolving digital landscape. Internal audit has a significant role to play in this conversation.

Key drivers for 2027 | **Data security and cryptographic resilience**

Top five things internal audit should do

1. **Perform a cryptography audit, to assess the business implications of compromised asymmetric cryptography**
   Many organisations lack understanding of where cryptography is used. Assess which business services, controls and legal or regulatory obligations depend on public-key cryptography. Determine the operational, financial and reputational impact if encryption, authentication or digital signatures can no longer be trusted, and confirm that management has identified the most critical dependencies and owners.

2. **Review third- and fourth-party dependencies**
   Map where cloud providers, software, managed services and other suppliers embed cryptography, including dependencies beyond direct vendors. Test whether third- and fourth-party risk, procurement and contracting processes capture quantum exposure, migration timelines, accountability, exit plans and concentration risk across the extended supply chain.

3. **Protect at-risk and long-retention data**
   Identify sensitive data that must remain confidential for years, confirm that it is stored in secure repositories, and prioritise it for migration to quantum-resistant protection. Include data held by third parties and exposure to "harvest now, decrypt later" attacks, with clear ownership and retention requirements.

4. **Test audit evidence integrity and chain of custody**
   Review whether digital and automated controls, signed artefacts and evidence-handling processes preserve authenticity, completeness and traceability from creation through retention. Assess how quantum threats could weaken chain of custody or undermine the reliability of evidence used by Internal Audit and other assurance functions.

5. **Reassess audit methodologies that rely on digital evidence**
   Identify audit procedures that assume digital signatures, system logs and electronic records are inherently reliable. Define alternative evidence, corroboration and testing approaches for scenarios in which those assumptions weaken, and keep audit methodology and practitioner skills under review as quantum capabilities and standards mature.

About the Survey

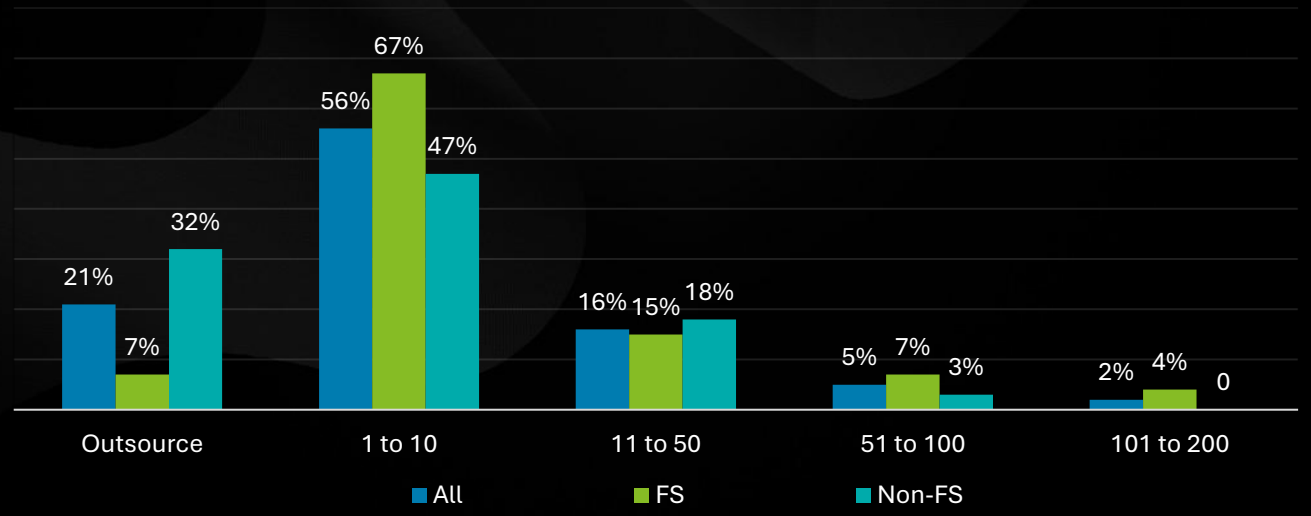
The survey respondents were Heads of IT Internal Audit or held equivalent roles, with additional input from Chief Internal Auditors, Heads of Internal Audit, IT Audit Directors and other IT/Business Leaders. Deloitte LLP commissioned the online survey, which our senior Technology and Transformation practitioners conducted between May and July 2026.

The survey captured the most significant IT internal audit risks identified by senior audit professionals. We also analysed the responses to identify emerging technology and risk themes across Internal Audit functions.

This paper sets out the key technology and digital internal audit topics raised by industry experts. For each topic, it explains why it matters, summarises recent developments, recommends actions for internal audit functions and highlights challenges to effective risk mitigation.

Industry breakdown of respondents

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



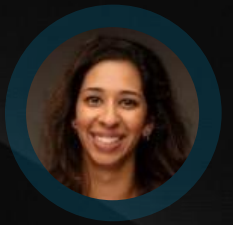
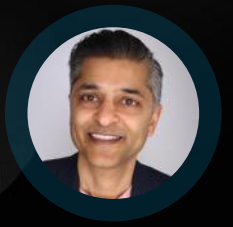
Key contacts and contributors

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

We hope this report serves not only as a source of insight, but as a catalyst for discussion - helping you strengthen risk assessment and planning for the year ahead.

We encourage you to use it to spark conversations across your organisation, and, as always, we look forward to continuing the dialogue.

Please get in touch if you would like to explore any of these topics further.

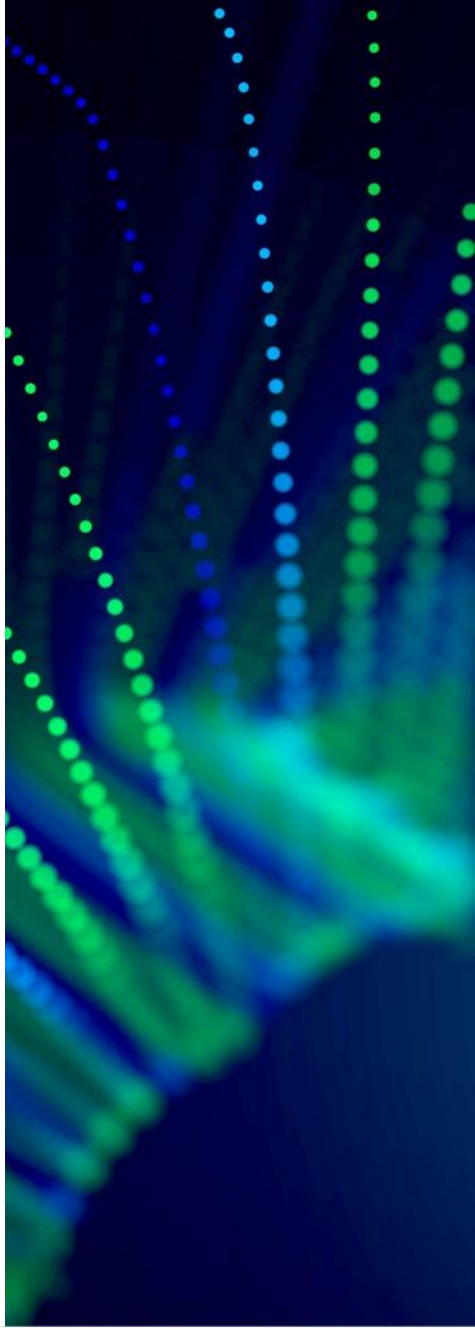
	Financial services	Corporates	Government and public services
UK	 **Yannis Petras** **Partner** ypetras@deloitte.co.uk	 **Faiza Ali** **Partner** faali@deloitte.co.uk	 **Helen Cutting** **Partner** hcutting@deloitte.co.uk
	 **Mark Westbrook** **Director** markwestbrook@deloitte.co.uk	 **Kirti Mehta** **Director** kirtimehta@deloitte.co.uk	 **Matt Davis** **Associate Director** mattxdavis@deloitte.co.uk
US	 **Mike Schor** **Partner** mschor@deloitte.com	 **Vipul Patel** **Managing Director** vbpatel@deloitte.com	 **Gregory Boehmer** **Managing Director** gboehmer@deloitte.com

Key contacts and contributors

Topic		Contributors			
		UK		US	
1	Cyber security	**Haroon Abbas** haabbas@deloitte.co.uk	**Poppy Khan** pokhan@deloitte.co.uk	**Phil Klebba** pklebba@deloitte.com	**Dillon Bromley** dbromley@deloitte.com
2	Artificial Intelligence	**Billy Bond** billybond@deloitte.co.uk		**Siddarth Damle** sidamle@deloitte.com	**Greg Nicholson** gnicholson@deloitte.com
3	Data and regulatory reporting	**Katie Hibbert** kehibbert@deloitte.co.uk	**Oscar Lowe** oslowe@deloitte.co.uk	**Patrick Girling** pgirling@deloitte.com	**Piali Sinha** pisinha@deloitte.com
4	Technology transformation	**Lee Hales** lhales@deloitte.co.uk	**Olga Harte** oharte@deloitte.co.uk	**Thomas Kancyan** tkancyan@deloitte.com	**Greg Nicholson** gnicholson@deloitte.com
5	Third-party and outsourcing	**Roshan James** roshanjames@deloitte.co.uk		**Bezhan Tayebi** btayebi@deloitte.com	
6	Technology resilience	**Adam Blair** adblair@deloitte.co.uk	**Matt Whitfield** mwhitfield@deloitte.co.uk	**Alice Pickering** alice@deloitte.com	
7	Legacy systems and technology simplification	**Carol Mucherahowa** cmucherahowa@deloitte.co.uk		**Seth Connors** sconnors@deloitte.com	
8	Cloud computing environments	**Dom Hamilton** domhamilton@deloitte.co.uk		**Twinkle Patel** twipatel@deloitte.com	**Stefan Unertl** stunertl@deloitte.com
9	IT governance and risk management	**Mark Westbrook** markwestbrook@deloitte.co.uk	**Kirti Mehta** kmehta@deloitte.co.uk	**Greg Boehmer** gboehmer@deloitte.com	
10	Cryptography and quantum computing	**Ella Lewis** elewis@deloitte.co.uk		**Scott Buchholz** sbuchholz@deloitte.com	**Colin Soutar** csoutar@deloitte.com

Additional Contributions

Zuhaib Ahmed, Henry Berry, Veronica Pralea, Marcus Jolly, Dominic Janik-Browne, Katy Sobodos, Mark Ward, Reha Iqbal, Harvey Finnegan, Shade Obele, Max DeMeola



Resources and references

[1]	Deloitte, *Digital Regulatory Outlook 2026*, Deloitte, (2026).
[2]	Deloitte, *Financial Services Regulatory Outlook 2026: The Regulatory Remix*, Deloitte, (2026).
[3]	European Parliament and Council of the European Union, *Regulation (EU) 2024/1689 laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)*, Official Journal of the European Union, (2024).
[4]	Department for Science, Innovation and Technology, *Cyber Security and Resilience Bill*, GOV.UK, (2025).
[5]	Department for Science, Innovation and Technology, *Data Use and Access Act 2025: Plans for Commencement*, GOV.UK, (2026).
[6]	Koley Jessen., *New State Privacy Laws Effective January 1, 2026: Indiana, Kentucky, and Rhode Island*, (2025).
[7]	California Privacy Protection Agency, *CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Regulations*, (2025).
[8]	*CommLaw Group, Multi-State Privacy Enforcement Sweep Targets Global Privacy Control Noncompliance: California, Colorado, and Connecticut Launch Joint Investigation, (2025).*
[9]	FTC, *FTC Approves Final Order against Workado, LLC, Which Misrepresented the Accuracy of its Artificial Intelligence Content Detection Product*, Federal Trade Commission, (2025).
[10]	United States Department of Defense, *Cybersecurity Maturity Model Certification (CMMC) Program*, (2025-2026).
[11]	National Cyber Security Centre, *Cyber Assessment Framework (CAF)*, NCSC.
[12]	National Institute of Standards and Technology, *Cybersecurity Framework (CSF)*.
[13]	UK Civil Aviation Authority, *UK Civil Aviation Authority Unveils New AI Strategy*, (2026).
[14]	PRA and Bank of England, *Strategic Approach to Artificial Intelligence in Letter to Government*, (2026).
[15]	Gartner, *Chief Audit Executive Survey 2026*, Gartner Research, (2026).
[16]	Basel Committee on Banking Supervision, *Principles for Effective Risk Data Aggregation and Risk Reporting (BCBS 239)*, Bank for International Settlements, (2013).
[17]	European Central Bank, *Guide on Risk Data Aggregation and Risk Reporting (RDARR)*, European Central Bank, (2024).
[18]	Keyhole Software, *Vibe Coding Trends 2026: Adoption, Productivity, and Code Quality Data*, Keyhole Software, (2026).
[19]	HM Treasury / UK Regulators, *Critical Third Parties (CTP) Regime*, (2026).
[20]	Cybersecurity and Infrastructure Security Agency (CISA), *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)*, (2026).
[21]	Institute of Internal Auditors, *Third-Party Topical Requirement*, (2026).
[22]	State of Colorado, *Colorado Automated Decision-Making Technology Act*, (2026).
[23]	Institute of Internal Auditors, *Organisational Resilience Topical Requirement*, (2026).
[24]	National Institute of Standards and Technology, *Post-Quantum Cryptography*, NIST, (2024-2026).

Deloitte.

Together makes progress