

## Innovating responsibly

Hot topics in technology and digital risk 2024

An internal audit viewpoint

# Contents

- 01** Executive summary
- 06** Our survey through the years: 2012-2024
- 09** Technology and digital risk hot topics 2024: a viewpoint
- 43** Unlocking the power of digital through Generative AI for internal audit
- 48** Appendices
- 51** Contacts



Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics  
2024: a viewpoint

Unlocking the power of digital through  
Generative AI for internal audit

Appendices

Contacts





# Executive summary

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics  
2024: a viewpoint

Unlocking the power of digital through  
Generative AI for internal audit

Appendices

Contacts



# Executive summary

We are delighted to present our annual viewpoint on the technology and digital risk hot topics for internal audit functions.

Our publication presents the results of a survey conducted across all UK sectors, completed by Heads of Information Technology (IT) Internal Audit/Heads of Internal Audit, combined with qualitative insights and perspectives from interviews held with IT internal audit practitioners, as well as Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Chief Technology Officers (CTOs), and business leaders across sectors.

We would like to thank all participants who took part in this survey, either via interviews, or by using our online survey tool. Your openness and candour, particularly when highlighting weaknesses, challenges and strategic priorities, was greatly appreciated. We hope this paper offers insights for your ongoing conversations with technology, digital and business leaders, while also supporting your risk assessment and planning process for 2024.

As always, we look forward to discussing our paper further with technology and audit leaders, hearing their views on the key points underlined by the survey and continuing the conversation.

## Areas of focus for 2024

The continuous evolution in technology comes with great opportunities for organisations but also new and unknown risks. Across the industry we have seen significant in-flight transformation aiming to modernise legacy infrastructure, improve customer experience and deliver better margins through the adoption of cloud, artificial intelligence (AI) and 'big data' technologies that can help improve efficiency and reduce cost. Transformation may take the form of upgrade to, or innovation in, their technology environment, including leveraging the tools to improve efficiency and effectiveness.

With this opportunity for innovation comes challenges and risks which organisations across all sectors will need to effectively manage, in order to realise the upside potential and build and maintain a competitive advantage.

Technology, digitisation, and resilience are central themes seen by organisations as underpinning future business success. Technology internal audit continues to play an important role in assuring risks and advising technology functions on how best to balance priorities around fast delivery of change and accelerated time to market, with appropriate levels of governance and control. That's why our key theme this year is centred around safe and responsible innovation.

As we move forward, it is crucial for technology internal audit leaders to stay ahead of the curve and proactively familiarise themselves with this emerging technology landscape to provide valuable predictive insights, assurance and advice to their respective organisations.

Our 2024 survey covered organisations across all UK sectors and despite there being a small disparity between the Financial Services (FS) sector and Non-Financial Services sectors (non-FS) in the prioritisation of challenges faced, internal audit functions, and indeed organisations, continue to face very similar burdens and challenges when it comes to technology, cyber and digital risk domains.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts







# Hot topics top 10 for 2024

Figure 1: Technology and digital risk hot topics 2024

Rank	Across all sectors	Financial Services	Non-Financial Services
1	Cyber security	Cyber security	Cyber security
2	Digital transformation and IT change	Cloud environments	Data management and data quality
3	Data management and data quality	Digital transformation and IT change	Artificial intelligence
4	Artificial intelligence	Technology resilience	Digital transformation and IT change
5	Cloud environments	Outsourcing and critical third parties	Legacy IT and IT simplification
6	Technology resilience	Data management and data quality	Cloud environments
7	Outsourcing and critical third parties	Artificial intelligence	Technology resilience
8	Legacy IT and simplification	Identity and access management	Outsourcing and critical third parties
9	Identity and access management	Legacy IT and IT simplification	Identity and access management
10	Emerging technology trends: digital assets and blockchain, UK controls regime, responsible marketing and digital channels	Emerging technology trends: digital assets and blockchain, responsible marketing and digital channels	Emerging technology trends: UK controls regime, responsible marketing and digital channels



Cyber security continues to be top of our list as cyber threats become increasingly sophisticated.”

The following topics are key focus areas for organisations in their upcoming technology and digital internal audit plans for 2024:

**Cyber security** continues to be top of our list as cyber threats become increasingly sophisticated. Organisations are faced with the on-going challenge of keeping pace with threat actors through enhanced threat detection and response, and ensuring their critical infrastructure and data is protected. This year, our paper discusses trends such as Ransomware-as-a-Service, AI-powered attacks, supply chain ecosystem-targeted attacks as well as evolving threats from a challenging geopolitical environment.

**Data management and data quality, digital transformation and IT change, and cloud environments** continue to be in the top five hot topics, demonstrating the on-going focus of organisations to keep pace with technology developments, innovate their technology landscapes, and ensure that their organisational data is secure, and its integrity is maintained as it is migrated into new systems and tooling. The appetite for enhanced usage of organisational data, for example through data analytics, continues to grow, and is facilitated by good data quality. Let’s not forget that one of the critical challenges and the core foundation of effective generative AI (GenAI) implementations would be the quality, integrity and security of the underlying data.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



This year, **artificial intelligence** (AI) has jumped into the top five hot topics given the growth trajectory of this technology, boosted further by wide-spread attention in the market. We found that several functions have already started to perform reviews in this area, and for many others, the Executive and Audit Committee Chairs have started engaging with Chief Audit Executives on the topic, expecting them to stay close to the associated risk and regulatory landscape to protect the organisation. GenAI has truly captured the imagination of the world, fuelling discussion among businesses and policymakers. AI controls are managing data privacy and security risks, as well as ethical considerations and concerns about the reliability of outputs created by GenAI. Internal audit functions are looking at the developing regulatory landscape and assuring that their organisation is preparing for the arrival of this regulation in 2024 and beyond. The paper touches on all the above.

**Resilience** remains a hot topic within Financial Services as organisations work towards meeting regulatory expectations set by the UK regulators ahead of the 31 March 2025 transition deadline. This has been reinforced by the EU Digital Operational Resilience Act (DORA). Against a backdrop of increasingly common and impactful cyber incidents, a frequently asked question by the board, regulators, shareholders and customers is “could our business recover from a catastrophic cyber attack?”. Our paper discusses technology, cyber resilience and enterprise recovery, recognising that organisations need to ensure resilience and recovery mechanisms are robust to protect against catastrophic loss and are aligned to broader operational resilience requirements.

**Outsourcing and critical third parties.** The financial and wider business implications of a failure in this ecosystem through operational losses, fines or reputational damage can be severe. The increased regulatory scrutiny, and prescriptive requirements (as a part of the third-party and operational resilience regulations), have rapidly increased focus on third-party risk, as organisations have seen accelerating digitisation across entire operations, with traditional services and operating models requiring unprecedented changes to new ways of working in a short space of time. We discuss the challenges for internal audit functions and priorities going into 2024.



...internal audit functions – and indeed organisations, continue to face very similar burdens and challenges when it comes to technology, cyber, and digital risk domains.”

**Key challenges in 2024:**  
The key challenges that internal audit functions are, or will be facing this year, are illustrated in a word-cloud on page 5, based on survey responses.

**People, skills and capabilities.** Given the pace of change and associated emerging trends across technology and digital, and the wide range of tools and technologies in the market, functions are concerned that their in-house teams may not have adequate skills and capabilities to assess risks, and perform audits of some of these emerging technology risk areas. From conversations with internal audit leaders, it is difficult to identify and recruit key technology and digital skills in the market, but also to retain existing talent. They try to be inventive and resourceful in terms of providing the right opportunities, upskilling their people, investing in talent and wellbeing. They also consider opportunities to upskill team members through training and access to external resources on emerging trends, some of which are outlined in this publication.

**Cost pressures.** We noted 40% of survey respondents stated that their FY24 budget will remain the same, however, expectations of what the function delivers continued to grow. While the ‘doing more for less’ principle can prove a key challenge for organisations, especially in a difficult environment for skills and with increased regulatory expectations, it may also be a catalyst for innovation and transformation for the functions. Refer also to section 4 of our paper.

Executive summary
Our survey through the years: 2012-2024
Technology and digital risk hot topics 2024: a viewpoint
Unlocking the power of digital through Generative AI for internal audit
Appendices
Contacts





40% of survey respondents stated that their FY24 budget will remain the same, however, expectations of what the function delivers continued to grow.”

Figure 2. Top challenges faced by internal audit functions/teams in the next 12-18 months



Executive summary

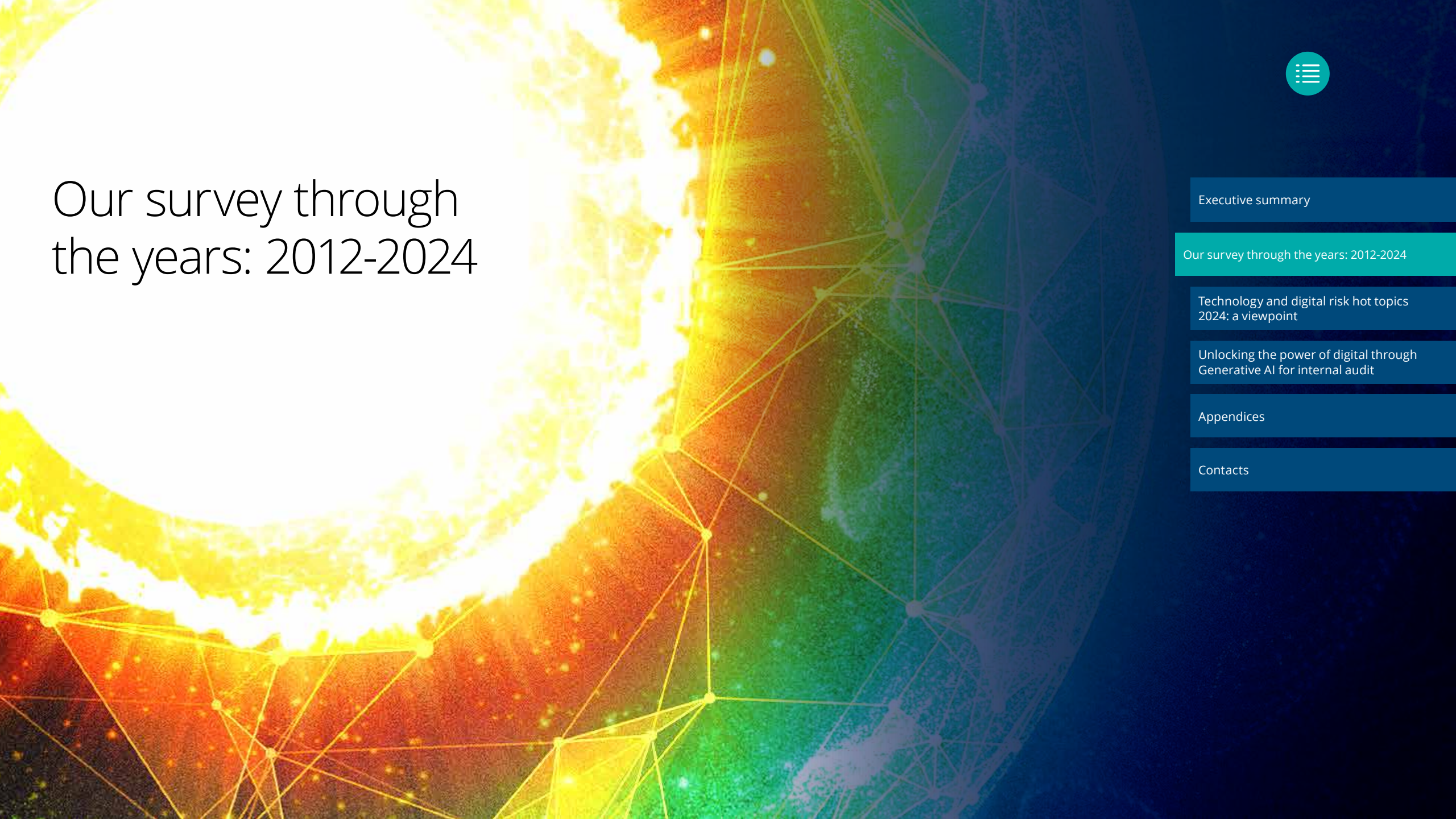
Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



# Our survey through the years: 2012-2024



[Executive summary](#)

[Our survey through the years: 2012-2024](#)

[Technology and digital risk hot topics  
2024: a viewpoint](#)

[Unlocking the power of digital through  
Generative AI for internal audit](#)

[Appendices](#)

[Contacts](#)





# Our survey through the years: 2012-2024



The table overleaf presents a comparison of the top 10 technology and digital risk hot topics over the past twelve years, as identified through our annual survey of Heads of Technology Audit.

**Cyber security** continues to dominate the top position in our list, having maintained its place for the past decade, driven by the elevated complexity of the threat environment, the increasing scope and frequency of cyber-attacks, combined with new and pending regulations.

While **cloud** continues to be an important focus area, organisations have started to develop more mature approaches to address its challenges as business-as-usual, leading to a shift in focus towards other areas in our study. Nevertheless, the importance of cloud governance and risk management in cloud hosted environments remains.

In more recent years, **resilience** and **data** have moved up the rankings, indicating that as organisations grapple with the increasing volume and complexity of data, the focus on effective data management and governance has become paramount.

Following the emergence of **artificial intelligence** as a distinct hot topic in last year’s publication, we noted it has gained significantly more attention in this year’s survey, owing in part to the ‘hype’ of GenAI. As the introduction of disruptive technology accelerates, organisations are increasingly compelled to address areas such as AI, blockchain, and robotic process automation (RPA).

In this publication we have also included a separate theme around **emerging technology trends**, covering **digital assets** and **blockchain**, the **new UK controls regime**, and **digital channels** and **responsible marketing**.

These technologies bring new challenges and opportunities, requiring IT internal audit functions to adapt and ensure effective risk management and control in these rapidly evolving fields.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



Figure 3. Technology and digital risk hot topics through the years: 2012-2024

Rank	2024 (All Sectors)	2023 (All sectors)	2022 (FS)	2021 (FS)	2020 (FS)	2019 (FS)	2018 (FS)	2017 (FS)	2016 (FS)	2015 (FS)	2014 (FS)	2013 (FS)	2012 (FS)
1	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Large Scale Change	Third-Party management	Cyber Threat
2	Digital Transformation and IT Change	Digital Transformation and Change	Cloud Governance and Security	Operational and IT Resilience	Transformation and Change	Technology Transformation and Change	Strategic Change	Strategic Change	Strategic Change	Disaster Recovery and Resilience	IT Governance and IT Risk Management	Identity and Access Management	Complex Financial Models
3	Data Management and Data Quality	Data Governance	Operational and IT Resilience	Cloud Governance	Operational Resilience	Data Protection and Governance	Data Management and Data Governance	Data Management and Data Governance	Third-Party Management	Large Scale Change	Identity and Access Management and Data Security	Data Governance and Quality	Data Leakage
4	Artificial Intelligence	Cloud Hosted Environments	Data Governance	Extended Enterprise Risk Management	Extended Enterprise Risk Management	Technology Resilience	IT Disaster Recovery and Resilience	Third-Party Management	IT Disaster Recovery and Resilience	Enterprise Technology Architecture	Data Governance & Quality	Large Scale Change	Data Governance and Quality
5	Cloud Environments – Cost and Sustainability	Operational and IT Resilience	Transformation and Change	Transformation and Change	Digital Technologies	Extended Enterprise Risk Management	Information Security/ Identity & Access Management	IT Disaster Recovery and Resilience	Data Management and Data Governance	Third-Party management	Third-Party management	Cyber Security	Rogue Trader and Access Segregation
6	Technology Resilience	Business Critical IT Controls	Digital Risk	Digital Risk	Data Protection and Data Privacy	Legacy architecture	Third-Party Management	IT Governance and IT Risk Management	Information Security	Information Security	Cyber Security	Resilience	Regulatory Programmes
7	Outsourcing and Critical Third Parties	Extended Enterprise/ Third-Party Risk Management	Extended Enterprise Risk Management	Data Governance	Cloud Governance and Security	Cognitive Automation and Artificial Intelligence	IT Governance and IT Risk Management	Information Security/ Identity & Access Management	Digital and Mobile Risk	Digital and Mobile Risk	Digital and Mobile Risk	Cloud Computing	Financial Crime
8	Legacy IT and Simplification	IT Strategy & Governance	IT Strategy and IT Governance	IT Strategy and IT Governance	IT Governance and IT Risk	Cloud Computing	Cloud Computing	Enterprise Technology Architecture	IT Governance and IT Risk Management	Data Management and Governance	Service Management	Mobile Devices	Third-Party Management
9	Identity and Access Management	Identity & Access Management/ Privileged Access	Payments	Payments	Application Development	Application Development	Digital and Mobile Risk	Cloud Computing	Enterprise Technology Architecture	IT Governance and IT Risk Management	Disaster Recovery and Resilience	Complex Financial Modelling	Social Media
10	Emerging Technology Trends	Digital Risk: Artificial Intelligence	Application/ Integrated Reviews	System Development	Legacy Environments	Payment Technologies	Enterprise Technology Architecture	Digital and Mobile Risk	Payment Systems	Service Management	Cloud Computing	Social Media	Mobile Devices

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts





Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics  
2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through  
Generative AI for internal audit

Appendices

Contacts

# Technology and digital risk hot topics 2024: a viewpoint





# 1. Cyber security



## Why is it important?

Cyber risk remains one of the most important topics in the agendas of business leaders and regulators alike. This has reached the top of our survey for 2024, with respondents quoting the evolving threat landscape (with nation-state threats particularly prominent), the increased reliance on technology, regulatory requirements, and the ever-expanding attack surface. Chief amongst the areas of concern, are ransomware attacks. This has developed from an operationally disruptive phenomenon to a sophisticated suite of attack vectors that block systems, extract data and provide opportunities for further blackmail and extortion.

Organisations continued to reference the need to manage changes to their risk profile through increased digitisation of processes and activities, which provide efficiency and cost reduction, but also expose poorly designed processes and systems to many attack vectors.

There is also a very clear desire for constant hardening in the cyber security environment and to ensure that there is a level of consistency across the organisation's wider control environment, with no divisions or subsidiaries dragging down the overall maturity level for the organisation.



Cyber risk remains one of the most important topics in the agendas of business leaders and regulators alike. This has reached the top of our survey for 2024."

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

\*\*Use of analytics % is the percentage of respondents who, if they have included this topic in their audit plan, will employ analytical techniques.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



**What's new?**

Cybercriminals are developing more complex strategies, utilising cutting-edge technology, and taking advantage of weaknesses in digital systems. By using the most recent technological developments, such as AI and automation, cloud security, and cyber threat intelligence, data can be protected from malicious attacks, such as hacking.



Cybercriminals are developing more complex strategies, utilising cutting-edge technology, and taking advantage of weaknesses in digital systems.”

**01. Ransomware-as-a-Service (RaaS)**

In recent years, the number of ransomware attacks, where cyber criminals encrypt a victim's files and demand a ransom, has increased. In fact, they affected 66% of organisations in 2021, an increase of 78% over 2020, according to Sophos “The State of Ransomware 2022” report. We can anticipate a rise in the use of RaaS platforms in 2024. Additionally, organisations must develop a strong security policy and robust cyber hygiene if organisations want to safeguard from RaaS risks. These procedures will become even more crucial as we proceed through the coming years as RaaS is anticipated to rank among the top cyber security trends during 2024.

**02. AI-powered attacks**

Criminal groups are attempting to use AI and GenAI to create more advanced attacks, and we anticipate an increase in AI-powered attacks that elude conventional security measures in 2023. For instance, AI can construct malware that adapts its behaviour to evade detection by security software or make realistic phishing emails that easily trick consumers.

**03. Supply chain attacks**

Attacks on the supply chain aim to access the systems and data of customers by targeting third-party vendors and service providers. The likelihood of a supply chain attack rises as organisations depend more on a network of partners and suppliers. Supply chain attacks are likely to increase in 2024 as cybercriminals look for ways to weaken an organisation's security. To reduce the danger of a supply chain assault, organisations must also evaluate the security posture of their partners and put in place robust access controls.



Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



**What should internal audit be doing?**

**Maturity assessments**

Internal audit functions should be performing cyber maturity assessments against industry recognised standards such as the National Institute of Technology (NIST). Once a full assessment has been completed, deep dive areas across people, process and technology should be included within internal audit plans as we continue to see a focus on driving improvements to maturity scores.

**Culture reviews**

Internal audit should perform audits of security culture. These are not as common as you might expect, but they can be immensely valuable in gauging what users really know about security risks and their own role in addressing them. It can also show what Executives – including Non-Executive Directors– really understand about the severity of cyber risks and their own roles in keeping their organisation's data and information safe.

**Red teaming and penetration testing**

Internal audit have not traditionally performed such exercises, but we are increasingly seeing internal audit teams leading red teaming simulations and cyber preparedness initiatives, in most cases by engaging third parties to carry this out on their behalf. Audit and Risk Committees (ARCs) have general concerns about the quality of cyber defences and how these can best be tested. However, ARCs are not always fully aware of what red teaming exercises are or how they can help organisations. There is a new opportunity for internal audit functions to help inform or upskill them in this space.

**Security configuration assessments, reviewing security of key systems, networks and technologies**

Internal audit should assess the security tooling landscape, for example, Data Loss Prevention (DLP), Security Information and Event management (SIEM), and firewalls. All of these reviews typically cover both process and governance as well as the technical aspects.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



## 2. Digital transformation and IT change



### Why is it important?

The continuous evolution in technology comes with great opportunities for organisations, but also new and unknown risks. Across the market there is significant in-flight transformation aiming to modernise legacy infrastructure, improve customer experience and deliver better margins through the adoption of cloud, AI and big data technologies that can help improve efficiency and reduce cost. However, organisations face challenges when it comes to monitoring the benefit realisation and the outcomes these initiatives drive for the business.



We see significant transformation...to modernise legacy infrastructure, improve customer experience and deliver better margins through cloud, AI and big data technologies.”

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts

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

\*\*Use of analytics % is the percentage of respondents who, if they have included this topic in their audit plan, will employ analytical techniques.





Most of the transformation we are seeing is driven by:

- M&A activity which leads organisations to want to streamline their services and product offerings while wanting to provide better and faster services
- digital initiatives that continue to be the main conduit for organisations to deliver their strategic priorities
- organisations which continue to face regulatory pressures and often come with a large technology and data remediation components
- the need to keep up with competition and ever-increasing customer demands

In order to respond quickly to market demands, organisations are looking to engage third parties in their transformation activities while moving to Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) solutions. This increases third-party risk and shifts the focus to more robust third-party oversight.

Organisations also see the creation of a common, strategically linked language and methodology for digital transformation as a means for achieving digital advantage and adaptability. They also continue to digitally transform their business models with more hybrid working and fewer face-to-face interactions, although a number of organisations have recently asked their staff to return to the office and change keeps adapting to these trends.

**What's new?**

In 2023, the market has been operating under significant uncertainty which leads organisations to more conservative spending and a cost constrained environment. This means that a large part of the change portfolio is delivered internally with limited resources and there is greater scrutiny on priorities and budgets.

The ongoing adoption of new digital technologies, including GenAI and increased use of cloud, has led to a need for organisations to establish how to best integrate them within their current environment and service offering, manage their risk and potentially develop new value propositions and use cases for existing and new customers and markets.

Agile methodology and tools continue to be popular, and we're seeing more and more organisations adopting these not just in their operations but also their audit functions. These tools are targeted to improve collaboration across the organisation, and the use of agile, combined with continuous monitoring, is effective in making programme delivery quick and efficient.

There are still large regulatory initiatives that drive strategic decisions for organisations (i.e. the Consumer Duty Act, Digital Services Act, Environmental Social and Governance (ESG) and DORA) which necessitate the need for robust change frameworks that enable cross functional delivery and effective management oversight.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



What should internal audit be doing?

Skills and capabilities

Internal audit should invest in building the right skills and capabilities that align to the technologies being introduced into their organisation (GenAI, cloud and others) as part of their digital transformation journey. This is a key part of understanding the risks and being able to assess if the business has established effective mitigation strategies.

Business strategy, execution priorities and portfolio assessment

Internal audit should, alongside standard planning activities, take a top-down view of the business strategy and execution priorities at a board, ExCo and then portfolio level. Internal audit should take a view of the impact and potential risks, to manage capacity and resource planning and effective prioritisation of change initiatives. In addition, internal audit should assess if the selected resources have the relevant skills and knowledge to deliver the required initiatives including third parties.

Focused reviews

Internal audit teams should be assessing which areas they need to focus for digital change and IT reviews, and which would be adding more value to the business as a result of the competition for talent and current cost pressures. They will then need to work alongside first and second line risk teams to make sure that all relevant risks are covered. Internal audit should also be carefully allocating resources to those focused reviews so that they get comfortable that risk is appropriately managed across the organisation.

Benefit realisation evaluation

Functions should focus on whether change benefits are clearly identified, owned by the business, and that key programme decisions are made based on these benefits. This includes making sure that programmes are set up to succeed with high quality benefits, and that they are actually used when making decisions on programme changes. Internal audit should also assess if the current process of tracking benefits and value delivery is aligned with delivery methods with expectations that some benefits should be realised earlier using Agile programme delivery.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



### 3. Data management and data quality



#### Why is it important?

Data governance, data management, and data quality are wide-ranging disciplines and processes across organisations that ensure that data is an asset, and not a liability. Data continues to be a core focus area for internal audit functions. We've seen various instances in the news where poor data governance resulted in fines and reputational damage. Indeed, data governance and quality are critical components of global regulatory requirements such as GDPR with steep penalties for non-compliance. Recent years have seen some hefty fines levied against large organisations with a maximum penalty of £17.29m or 4% of global revenue. The biggest fines seen are above £17.29m with the highest recorded so far being £43.2m.

Data is, and will remain, crucially important across all businesses and industry sectors. Good data governance, sound processes and robust data management are key enablers of using data to make informed business decisions and remain compliant with regulation.



Good data governance and robust data management are enablers of using data to make informed business decisions."

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts

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

\*\*Use of analytics % is the percentage of respondents who, if they have included this topic in their audit plan, will employ analytical techniques.



What's new?

Data governance is not a new area for many organisations, it has been a frequent feature in our IT internal audit hot topics list for many years, however we have seen increased focus on data quality, data governance, and stewardship over the past year.

Many functions have been called on to review data strategies and data governance frameworks and these are fast becoming standard features in most annual internal audit plans. From our interactions with clients and discussions with subject matter experts, we have also noted the following:

Increased number of businesses have mentioned data strategy implementation or refresh with a focus on tooling, resourcing, and skills. This is in part due to the continued move from legacy to modern solutions, particularly where legacy tooling is going out of service.

There has been an increase in the definition of roles and responsibilities regarding data ownership across sectors. However, this is still in its early stages with challenges around data requiring multiple teams to have access, and, in many cases, limited understanding of who is using their data and how.

For many organisations, the focus is still on short term activities and setting up a data governance framework, writing policies, establishing ways of working and building the foundation for successful data governance going forward. While this is encouraging, we see many organisations potentially caught up in delivery of short-term objectives rather than focusing on longer-term strategic data goals, with the current cost-conscious corporate environment often driving this behaviour.

Additionally, we notice organisations continually struggle with designing and implementing data strategies and overarching effective governance. Attrition in key data roles often impacts this with multiple attempts to improve data governance being undertaken without much progress seen.

While more advanced from a technology standpoint, some businesses are using sophisticated analytics like machine learning for continuous monitoring and automation. Barriers such as low data quality and challenges with access are slowing or preventing progress. The speed at which technology is moving and the adoption of GenAI solutions means organisations may need to accelerate their data governance activities to ensure they optimise the value from GenAI and remain future-fit.

Internal audit functions are increasingly using analytics to aid the audit process and provide improved data-driven insights. However, our recent digital and analytics survey<sup>1</sup> shows data access and quality is still a blocker with 69% of functions reporting access to appropriate data being their biggest barrier, and data quality also recognised as a key challenge across 56% of survey respondents. This is one indicator of the impact of immature data governance and data quality processes on utilisation of data.

In the Financial Services sector, one of the key topics defined by the European Banking Authority (EBA) for banking supervision in 2023 is the aggregation of risk data and data governance. The current status is far from satisfactory. Therefore, there is renewed supervisory focus on this aggregation of risk data and the principles for effective risk data aggregation and risk reporting as defined in BCBS 239<sup>2</sup>. It is expected that this focus will significantly impact banks, so adequate focus from internal audit functions will be required.



Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts

1 Internal audit digital and analytics survey 2023 | Deloitte UK  
2 BCBS 239 resurfaces on the EBA regulatory agenda | Deloitte Netherlands



**What should internal audit be doing?**

**Data quality reviews**

Internal audit should focus on data quality, allowing a better understanding of the extent of poor-quality data, and where such data may be used to influence business decisions. Functions should perform thematic reviews on the topic, leveraging analytics techniques, to allow senior management to gain a substantiated and clear view of the potential issue and exposure. The review could also assess management's approach to safeguard data quality for example assessing their use of technology to set data quality rules and assess compliance. This will be a key enabler for analytics use and improved efficiency across functions.

**Focus on data ownership**

Internal audit functions should be assessing how governance forums such as data governance committees are utilised to improve data ownership. Mastering data ownership is a crucial element of understanding and improving data, data quality and how data is used. They should also assess how data assets are stored and managed throughout their lifecycle.

**Prioritisation of data governance**

Internal audit should challenge the business to assess the prioritisation of data governance as part of their strategy. Dedicated focus and resourcing are needed to get this right and functions should assess whether data governance is getting the required level of attention at senior levels and that programs are appropriately run with longer term objectives set and tracked.

**Keep pace with change, and incorporate data reviews within other audits**

Internal audit should support the business is assessing these risks and managing them proactively. As technology is moving at a rapid pace, there is a risk of data loss, errors, and costly remediation being required where change is driven by tooling or the decommission of legacy systems. The advent of GenAI will bring about additional regulatory expectations on how data will be managed and used amplifying the need for robust data governance frameworks to be in place. Internal audit should integrate data considerations within such audits.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



## 4. Artificial intelligence: risks, ethical considerations, and controls



### Why is it important?

Enterprise adoption of AI systems has been growing for a number of years, and during 2023 GenAI has truly captured the imagination of the world fuelling discussion among businesses and policymakers. It is incredibly rare for any emerging technology to achieve these levels of adoption and frequency of usage so rapidly. While initial use was mainly by individuals Deloitte's research also found just under a third<sup>3</sup> (32%) or approximately 4 million people in the UK who have used GenAI have done so for work, and organisations are investing heavily in enterprise use cases.

With the rapid acceleration and integration of GenAI into business functions, AI and accordingly GenAI risk management, will continue to be a hot topic for internal audit teams throughout 2024 and beyond.



...the interest around GenAI has increased with organisations and individuals exploring how they can utilise the tools."

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

\*\*Use of analytics % is the percentage of respondents who, if they have included this topic in their audit plan, will employ analytical techniques.

<sup>3</sup> Digital Consumer Trends 2023 | Deloitte UK

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts





GenAI is a subset of artificial intelligence in which machines create new content in the form of text, code, voice, images, videos, or processes. Large Language Model (LLM) capabilities are powering an easily accessible interface that enables GenAI to have its breakthrough moment and surprise even specialists in the field.

To mitigate and minimise potential risks posed by GenAI and other AI systems, organisations are actively investing in the development of controls to enable them to innovate with confidence. AI controls are managing data privacy and security risks, as well as ethical considerations and concerns about the reliability of outputs created by GenAI. Internal audit functions are also looking at the developing regulatory landscape and assuring that their organisation is preparing for the arrival of this regulation.

In conjunction with the publication of regulations and guidance, the pace of AI development and deployment for the UK is expected to intensify, as the UK government pushes to be a global leader in AI development<sup>4</sup>.

What’s new?

With the recent release of GenAI systems such as ChatGPT in November 2022, Bard by Google in March 2023, and Amazon’s release of its open source LLM called Falcon in June 2023, the interest around GenAI has increased with organisations and individuals exploring how they can utilise the tools. Further there have been changes this year to the AI regulatory landscape, and guidance has been published to aid people and organisations as they navigate the use not only of GenAI, but all forms of AI.

- **EU AI Act<sup>5</sup>** (latest development from June 2023) – the European Parliament AI Act, which is expected to come into action in Q1 2024, is a regulatory risk-based approach to classify AI systems and manage the development, distribution, and use of AI systems.
- **AI Regulation: A pro-innovation approach white paper<sup>6</sup>** (published in March 2023) – following the collaboration of multiple UK government departments, the National AI Strategy outlines an innovation focussed approach to AI development. Investing in the long term needs of AI ecosystems, and supporting the transition to an AI enabled economy, can establish the correct national and international governance of AI technologies. The white

paper outlines the Government’s plans to regulate artificial intelligence, identifying AI as a critical technology. A new framework will encourage innovation in a responsible manner to drive growth and public trust making the UK a global leader in AI.

- **ISO AI Risk Management Framework<sup>7</sup>** (published in February 2023) – ISO published risk management guidance for organisations that are developing and deploying AI.
- **NIST framework<sup>8</sup>** (published in January 2023) – the NIST has collaborated with organisations from both public and private sectors to develop the NIST AI risk management framework. The guidance is voluntary and aims to help organisations understand the considerations that should be made during the design, development, use, and evaluation of AI systems.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts

4 Regulating AI: Can the UK’s proposed approach achieve both flexibility and clarity? | Deloitte UK  
5 Navigating the EU AI Act: a guide for Chief Data Officers | Deloitte UK  
6 A Pro-Innovation Approach to AI Regulation | GOV.UK  
7 ISO/IEC 23894:2023 Artificial Intelligence – Guidance on risk management  
8 Artificial Intelligence Risk Management Framework | NIST



**What should internal audit be doing?**

While GenAI technology is still developing, it is already being adopted by organisations at pace. Internal audit functions are understanding to what extent their organisation is using this technology, and to what extent they are planning to invest in it. Internal audit teams are upskilling themselves to understand the risks associated with GenAI, which include the full suite of existing risks associated with IT, but also GenAI specific considerations such as ‘hallucinations’, ethical AI, transparency and AI accountability.

As AI technology advances, internal audit teams must stay abreast of developments and ensure they have the required skills and capabilities to provide the necessary insight to senior leadership teams.

**Understand the organisation’s AI strategy**

Internal audit should consider their organisation’s approach to governance of AI. This should include a review of the organisation’s strategy that defines the road map of AI adoption, detailing desired research areas, mapping the development process, and the business areas which will pilot developing systems. Considerations can include the business case and value proposition, alignment to organisational strategy and to what extent AI risks have been considered.

**Review internal policy, standards, and guidelines**

Internal audit should consider reviewing any AI policy the organisation has developed, including acceptable usage guidance and/or policy which defines parameters of AI system development and deployment. Many policies align to specific standards and/or guidelines and many organisations are creating their own AI risk management framework.

**Determine whether an AI Inventory exists**

Internal audit should consider whether an AI Inventory has been developed by the business. The development of an AI inventory records active and developing AI projects with details on their status, and risk management considerations so they can be monitored or managed effectively. Organisations are taking differing approaches to this but ultimately AI risks cannot be managed unless there is clarity over AI use.

**Determine which external regulations or industry guidance applies to the organisation**

Internal audit should understand how the organisation is staying up-to-date with new and changing regulations and the processes and controls in place to assess how a regulation will impact AI development or current deployment of AI systems, which is vital to prepare actions to ensure future compliance.

**Assess the extent to which AI risk management practices and cultural behaviours considers AI risks**

Internal audit should also consider AI in the context of risk management. AI should be integrated with the current risk management processes and procedures to ensure systems utilising AI are effectively managed, governed, and monitored. Current risk management processes may need to be amended to ensure that risks associated with AI are proficiently covered. Risk appetite statements may also require updating for this new risk. Many organisations are adapting existing governance arrangements to be fit for AI, such as AI Ethics councils and the creation of AI Centre of Excellences.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts





# 5. Cloud environments – cost and sustainability optimisation



## Why is it important?

The power of cloud continues to be a key driving force in accelerating digital transformation. It allows for agility, scalability, and availability, as well as security and compliance, all of which are crucial to successful transformation, allowing organisations to operate more efficiently and effectively.

There is a risk that poorly governed cloud adoption can lead to an inefficiently designed and operated cloud. This can raise both cloud costs and carbon usage, causing a negative impact on an organisation's overall sustainability strategy.

This can be observed in practice: as cloud adoption has soared (Gartner predicts that by 2025, 95% of all new workloads will be based in the cloud<sup>9</sup>), and as a result the size and complexity of enterprise cloud estates, along with the related cost, has duly increased. Tied with the fact that many



There is a risk that poorly governed cloud adoption can lead to an inefficiently designed and operated cloud."

\*Audit planned % is the percentage of respondents who have included this topic in their audit plan.  
\*\*Use of analytics % is the percentage of respondents who, if they have included this topic in their audit plan, will employ analytical techniques.  
9 Cloud Will Be the Centerpiece of New Digital Experiences | Gartner

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts

current cloud estates are often a result of earlier organic and ungoverned adoption (with surveys suggesting that 30% of cloud spend is wasted<sup>10</sup>), some of the above noted benefits of cloud haven't been fully realised, notably that of efficiency.

From the perspective of sustainability, pressure from both regulators and increasing consumer preferences for sustainable and carbon-efficient outcomes has led many organisations to develop sustainability strategies. Often included are dedicated investments, net zero targets and carbon reduction initiatives. These have further accelerated many organisations' moves to the cloud. Cloud is primarily a 'greener' IT model due to the economies of scale available to vendors, therefore establishing an enterprise's cloud estate as an essential component of its broader sustainability strategy. However, the increasing demand for cloud has in turn led to concerns about the size of organisations' cloud carbon footprint, which is often larger than is necessary as sustainability objectives may not have been taken into account.

**What's new?**

Entering 2023, many organisations reported that their cloud usage and spend were higher than planned, with 'managing cloud spend' ahead of 'security' as the top cloud challenges across all organisations<sup>11</sup>. At a high level, by taking steps to improve and maintain their cloud architecture, reduce service and resource wastage and implement cloud best practices, organisations can reduce their cloud costs, energy usage and carbon footprint.

These objectives are facilitated by the increasing availability of native toolsets, such as Amazon Web Services (AWS) 'Customer Carbon Footprint Tool' and 'Cost Explorer', Google Cloud Platform's (GCP's) 'Carbon Footprint' and 'Cloud Billing Reports', and Azure's 'Emissions Impact Dashboard' and 'Cost Manager'. The tools allow organisations to gain visibility over their cost and carbon overheads, and to take remediating steps. However, the responsibility lies with the consumer to take these actions.

Through the datasets these tools provide, there is the opportunity to apply analytics to cost and carbon trends, leading to more informed sustainability decision-making, and therefore allowing for greater and more impactful changes to be made. Organisations need to ensure that any steps taken are sponsored by senior leadership and supported through education to ensure that relevant cloud stakeholders understand the link between cloud usage, cost and carbon and how these tie back to broader enterprise and IT strategies.

The increasing focus on cloud cost optimisation and sustainability sits alongside a range of existing cloud challenges that still need to be actively managed to minimise risk in the cloud, such as ensuring a safe and effective cloud migration, building effecting cloud controls, and the integration of cloud controls into existing IT risk frameworks. Ensuring these significant challenges are effectively managed and governed is key to laying the groundwork for a safe and efficient cloud environment.



Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts

10 State Of The Cloud Report | Flexera  
11 Flexera 2023 State of the Cloud | Report





What should internal audit be doing?

Cost and optimisation maturity

Functions should assess whether proactive steps have been taken to ensure appropriate maturity and ownership over cloud cost and carbon optimisation as well as whether the organisation has the right skills, sponsorship and accountability to tackle these challenges as part of the broader cloud governance framework and estate. It is also worth establishing whether right-sized governance is in place across multi-cloud estates, and that ownership is well-defined.

ESG strategy alignment

Internal audit should ensure that any steps taken to optimise cloud cost and carbon are effectively aligned with the organisation's overall ESG strategy and targets, as well as with those across the relevant IT/digital and cloud strategies. As such, cloud should be a consideration when planning and performing reviews into broader ESG governance.

Cloud architecture practices

Internal audit should evaluate whether relevant architectural and design principles and patterns underpinning sustainable and cost optimised cloud usage are baked into existing IT and cloud management frameworks, notably those around cloud design and build practices as well as ongoing operations.

Cloud audit integration

Internal audit should build considerations around cloud cost and carbon integration alongside traditional cloud risks, such as high cost or unsafe cloud migrations, inappropriate data storage, and insecure cloud configurations. These are still key areas for audit to ensure cloud usage is secure and compliant.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



# 6. Technology resilience



### Why is it important?

Operational and technology resilience is integral to an organisation’s ability to prepare, respond to, recover and learn from disruptive events. ‘Operational resilience’ remains a hot topic within financial services as organisations’ work towards meeting regulatory expectations set by the Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA) and Bank of England ahead of the 31 March 2025 transition deadline.

Resilience regulation is demanding the attention of banks, building societies, and insurance organisations, and financial services firms are leading the way. Despite this, minimising the impact and likelihood of crises, disruptions and major changes in working conditions is industry agnostic and we see this as a key focus area for all UK organisations and internal audit functions.

Resilience sits at the heart of every organisation across all sectors with operational disruption having the potential to cause significant enterprise-wide financial and reputational damage. With digitisation continuing to drive technology into the core of all business processes, the unavailability of critical technologies can prevent the delivery of important business services, severely impacting key areas or the entirety of the organisation.



Resilience sits at the heart of every organisation across all sectors”



Executive summary

Our survey through the years: 2012-2024

### Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts

\*Audit planned % is the percentage of respondents who have included this topic in their audit plan.  
\*\*Use of analytics % is the percentage of respondents who, if they have included this topic in their audit plan, will employ analytical techniques.





To keep pace, we see many organisations looking to strengthen their security controls and looking for ways to uplift their cyber and technology resilience maturity. Against a backdrop of increasingly common and impactful cyber incidents, a frequently asked question by the board, regulators, shareholders and customers is “could our business recover from a catastrophic cyber attack?”<sup>12</sup>. Most of them, however, are still on their journey of implementing adequate risk mitigation to enhance the resiliency of key services, including against catastrophic cybersecurity events.



We have continued to see an increase in high-profile major cyber incidents across 2023, challenging the organisations’ technology and cyber resiliency capability.”

### What’s new?

We have continued to see an increase in high-profile major cyber incidents across 2023, challenging the organisations’ technology and cyber resiliency capability. Some of the recent key trends that we see at the top of our clients’ priorities are as follows:

**01. Advanced tactics:** ransomware groups continue to advance their data exfiltration tools and techniques to carry out extortion. These tools help ransomware groups more efficiently steal data from target organisations before encryption. The threat of publishing this stolen data is then used to extort victims.

**02. Remote working:** Initial Access Brokers (IABs) are cyber threat actors (CTAs) that sell access to corporate networks to other CTAs as a service. With the continued increase in remote working, IABs are now increasingly targeting remote accesses for onward sales. The insurance sector is perceived to be of particularly high value, given the sensitivity of information which is attractive to a variety of threat actors.

**03. Supply chain:** as organisations increasingly shift operations and applications to the cloud, attackers continue to exploit weaknesses in third-parties, supply-chain, and cloud hosting solutions to gain access to networks. For example, Russian state-sponsored Advanced Persistent Threat groups are likely to continue targeting organisations by attacking third-parties.

**04. Phishing attacks:** we have seen Phishing-as-a-Service platforms that are capable of bypassing Multi-Factor Authentication (MFA) are being increasingly used in attacks. These platforms help threat actors gain initial access to target organisations with strict MFA policies in place without needing to develop sophisticated capabilities themselves.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



Financial Services

Operational resilience remains a hot topic within financial services as organisations work towards meeting regulatory expectations set by the FCA, PRA and Bank of England.

A deadline was set at 31 March 2022 where organisations were expected to have identified important business services, mapped operational dependencies, set impact tolerance thresholds, commenced scenario testing and produced a self-assessment.

Organisations are now required to demonstrate that all important business services can operate within impact tolerance limits by no later than 31 March 2025 in order to comply with UK regulations, following the remediation of vulnerabilities identified throughout the transition period. This date will mark the end of a three-year transition period which means organisations are now in a crucial period, and this is likely to mean a shift away from identifying operational vulnerabilities towards the timely design, implementation and acceleration of remediation plans and activities.

This focus on the resilience of financial services has also been reinforced by the European Union (EU) Digital Operational Resilience Act (DORA). EU DORA impacts virtually all regulated organisations within the financial services sector that operate legal entities in the EU, and consideration needs to be given in determining the impact of EU DORA requirements, including linkages and synergies with its UK counterparts. EU DORA entered into force on 16 January 2023 and full application is required by 17 January 2025<sup>13</sup>.

During this time, the European Supervisory Authorities (ESAs) will develop a broader set of secondary technical standards that will be crucial for the implementation of EU DORA. This means organisations are facing a relatively tight timeline to interpret and comply with EU DORA requirements. EU DORA can be broken down into five key pillars: (1) ICT risk management, (2) ICT incident classification and reporting, (3) Digital operational resilience testing, (4) Third-party risk management and (5) Critical third-party oversight. While areas of the UK regulation are aligned with the EU objectives, EU DORA represents new and significant implications for those impacted. However, the experience of implementing the operational resilience framework of their UK counterparts should provide helpful lessons.

Other sectors

Other key areas of focus by respondents to our survey include IT disaster recovery, capacity management, testing and exercising. While these concepts are not new, the importance that technology can be recovered in line with expectations of end-users is fundamental to an organisation’s operational and technology resilience. This includes the design of appropriate recovery strategies, whether hosted on-premise, with third party service providers or with cloud vendors. Understanding interdependencies within the IT estate and configuring (or procuring) appropriate IT resilience arrangements, with recovery priorities fully aligned and tested to meet the expectations of end-users remains a key challenge for

organisations across all sectors.

While regulatory requirements specifically relate to those operating in the financial services sector, there should be a focus across all sectors on the operational and technology resilience of the organisation. We are seeing an increase in organisations across all sectors looking to align and apply financial service principles within their resilience approach. For example, the adoption of a holistic service led approach to resilience, placing customers and key services at the heart of their programmes where failure could cause either intolerable harm to the end-user or threaten the viability of the organisation. This can refocus priorities and alter the mindset from ‘building’ and ‘data centre’ resilience, towards specific outcomes delivered to end users.

This is highlighted by ongoing discussions by the Financial Reporting Council (FRC) to include a ‘Resilience Statement’ as a legislative requirement for all companies over a particular size. This consultation which is part of the ‘Audit and Corporate Governance Reform’ would see relevant companies required to report on matters that they consider a material challenge to resilience over the short and medium term. The proposed changes would apply from accounting period beginning or after 1 January 2025.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts

13 Implementing the DORA: What EU financial services firms can learn from the UK’s path to implementing operational resilience | Deloitte UK



**What should internal audit be doing?**

Internal audit should also be mindful of regulatory deadlines during annual planning exercises and consider timelines for (1) audit scheduling and (2) developing management action plans. It is important to conduct timely assessments to enable organisations to incorporate and act on audit feedback.

**Digital Operational Resilience Act (DORA)**

Internal audit should review the organisation’s ICT risk management framework, a key requirement within the EU’s DORA. This should include the systems deployed to detect anomalous activities, and appropriate incident response, recovery and testing strategies.

**Scenario testing**

Testing is a key area of both UK and EU regulation, helping organisations to understand how resilient their operations are in their current state, and where vulnerabilities exist that require remediation efforts. This includes the appropriateness of test design (e.g. desk-based discussions, live testing and simulations) through to test criteria (e.g. involvement of third parties) and the appropriateness of the scenarios modelled, which should be covered in the scenario library.

**Remediation plans**

Internal audit should aim to understand how effectively organisations are managing plans to meet their resilience objectives (including those prescribed by the regulator). Internal audit need to ensure they are providing their opinions at the right point to enable the business to have sufficient time to complete remediation activities.

**Embedding into BAU**

Internal audit should review how operational resilience has been embedded across the business. Resilience outcomes need to be delivered in a sustainable manner which can be maintained and, where applicable, comply with regulation long term.

**Management information and reporting**

Internal audit should evaluate the design of management information provided to the Board and management committees pertaining to operational and technology resilience, considering whether it is adequately robust and sufficient to enable Senior Leadership to make informed decisions that may impact the delivery of important business services.

**Cyber incident response**

Review incident response capabilities of the organisation. This includes the ability to prevent, detect, mitigate, and respond to major incidents, and exercising such processes.

**Technology resilience**

Internal audit should understand the systems and data that is critical to the organisation and review the provisions (e.g. disaster recovery, backup and archiving policies) that are being implemented. This should consider the classification of systems and data and its criticality to the business. This should include whether capabilities and security controls are sufficient and aligned to the expectations of those that depend on the technology (end-users). This may include a consideration as to whether organisations are required to invest in cyber vaulting capabilities to protect against a “catastrophic cyber attack”.

**Third-party risk and resilience**

Internal audit should review the management of, and relationships with, third parties. Given the increasing complex nature of supply chains and use of third parties, understanding, and managing the risk posed by third party organisations is crucial.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



# 7. Outsourcing and critical third parties



## Why is it important?

In recent years we have seen a trend of organisations becoming increasingly reliant on their third and fourth parties. Reasons for this include the nature of the relationships, how bespoke the services are, thus making substitutability challenging, and even how ‘close to core’ the services are, all of which heighten the need to manage these relationships proactively and effectively.

The financial and wider business implications of a failure in this ecosystem through operational losses, fines or reputational damage can be severe. In addition, the increased regulatory scrutiny, and prescriptive requirements (as a part of the third party and operational resilience regulations) have rapidly increased focus on third-party risk, as organisations have seen accelerating digitisation across entire operations, with traditional services and operating models requiring unprecedented changes to new ways of working in a short space of time.



In recent years we have seen a trend of organisations becoming increasingly reliant on their third and fourth parties.”



Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts

\*Audit planned % is the percentage of respondents who have included this topic in their audit plan.  
\*\*Use of analytics % is the percentage of respondents who, if they have included this topic in their audit plan, will employ analytical techniques.

We anticipate that global regulators will provide more clarity and greater harmonisation of third-party risk regulations in 2024 and beyond, offering clearer direction for organisations operating across multiple jurisdictions, greater linkages to third-party management and operational resilience across group level entity structures, better guidance on data security requirements, including use of the cloud and IT providers.

Our research has shown that organisations which acknowledge the cross-functional nature of third-party risks, implement third-party oversight in a holistic manner and in a technology-enabled manner, achieve far greater clarity and consistency compared to organisations that assess third-party risks in individual siloed teams.

### What's new?

In July 2022, the HM Treasury introduced a discussion paper<sup>14</sup> articulating a new regulatory oversight regime for the supervisory authorities to set resilience standards, a testing approach and enforcement powers for Critical Third Parties. While non-regulated, these Critical Third Parties can still pose a systemic concentration risk to the financial services sector.

The EU DORA was published in the EU's Official Journal on 27th December 2022 and entered into force on 16th January 2023. A 24-month implementation period will precede full application in 2025. The EU DORA introduces a unified regulatory and supervisory rulebook for Information Communication Technology (ICT) operational resilience in the financial sector, pushing organisations to make substantial investments to improve their resilience to digital and cyber risk disruptions. One of its main objectives is to harmonise Financial Services organisations' management of ICT third-party risks through mandatory contractual terms for outsourcing and the requirement to assess concentration risks when outsourcing affects Critical or Important Functions (CIFs).



Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



**What should internal audit be doing?**

For internal audit functions considering performing an audit in the area of outsourcing or third-party risk management, we recommend the following topics be considered for inclusion in the scope:

**Proportionality**

Internal audit should assess how the organisation has applied the regulatory expectations around proportionality for example the materiality, complexity and risk associated with their outsourced or third-party services. This should also include consideration of how the organisation applies the concept of proportionality to non-outsourcing third-party arrangements.

Internal audit should assess how the organisation approaches intra-group outsourcing, the regulators do not consider intra-group outsourcing to carry less risk than external outsourcing services, but they acknowledge that organisations may adjust due diligence requirements and adapt contractual clauses.

**Governance and record-keeping**

Internal audit should assess how the organisation’s governance supports ultimate responsibility sitting with the board, for example through the setting of the risk appetite or approval of relevant policies.

It’s also important to assess how the organisation has approached roles and responsibilities relating to outsourcing including allocation of senior management functions responsibility.

Finally, internal audit should assess whether the organisation maintains an up-to-date register of information in line with regulatory expectations and the content and detail of this register.

**Pre-outsourcing phase**

A consideration for internal audit is how the organisation assesses a third party’s materiality and the requirements around periodic or trigger-based re-assessment. How the organisation has assessed any sub-outsourcing risk and the capacity and ability of the outsource provider to appropriately oversee any material sub-outsourcing on a continued basis.

Internal audit should assess whether the organisation understands and adheres to regulatory notification requirements.

Internal audit should consider how the organisation assesses concentration risk including consideration of third and fourth parties and/or geographies.

**Outsourcing agreements**

Internal audit should assess whether the organisation has met minimum requirements in terms of contractual safeguards and monitoring arrangements to be included in written agreements. Do the agreements provide organisations auditors, the PRA and the Bank of England with full and unrestricted access to information and to audit. How outsource arrangements are being audited/covered by internal audit.

**Data security**

Internal audit should assess whether there is clear consideration for data security where a third-party agreement involves the transfer of data, including the recognition of different classes of data and a risk-based approach to managing these.

**Business continuity and exit plans**

Internal audit should assess whether the organisation has developed, documented, maintains and routinely tests a business continuity plan and exit strategy for each material outsourcer. This should also be included as part of the risk assessment conducted before they enter into an outsourcing agreement with clear roles and responsibilities in the event of both stressed and unstressed exits.

**Environmental and social considerations**

Internal audit should assess how environmental and social considerations of the business are reflected in outsourcing policy and its application, as well as the alignment of this policy to the sustainability ambitions and compliance obligations of the business.

In order to facilitate more comprehensive sustainability reporting, internal audit should assess how outsourcing arrangements support routine access to relevant third-party data.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts





Financial Services

While Financial Services internal audit functions will already be aware of some regulatory requirements, there have been significant new regulatory developments in 2022/23 on third-party risk that have broadened requirements for almost all organisations. Since 31 March 2022, PRA regulated organisations are required to comply with the PRA's Supervisory Statement (SS) 2/21, 'Outsourcing and Third-Party Risk Management' which makes it more explicit that organisations are expected to assess the risks and materiality of all third-party arrangements, including those that do not fall within the definition of 'outsourcing'. It clearly articulates that materiality, outsourcing and risk must be independently assessed and considered as part of a proportionate and risk-based approach and it also implements the European Banking Authority (EBA's) guidelines on outsourcing arrangements and expands on certain sections such as data security, business continuity and exit plans.

For Financial Market Infrastructures (FMIs), supervisory statements were issued on the topic of outsourcing and third-party risk management to provide guidance as to how the Bank of England expects FMIs to meet their regulatory obligations under the Code of Practice and sets out more specific requirements and expectations than are contained within the Principles for Financial Market Infrastructures (PFMI). There are separate supervisory statements for Recognised Payment System Operators (PRSO) and Specified Service Providers (SSPs), Central Counterparties (CCPs) and Central Securities Depositories (CSDs).

Other sectors

Due to recent supply chain disruptions and their unforeseen organisational impact, including third party cyber-attacks and concerns over dominant or non-substitutable service providers in the market, organisations outside the financial sector are turning their attention to third party risk management practices.

These industries have directed their attention primarily towards three key areas of third party and outsourcing risk:

- identifying and assessing concentration risk across the supply chain, such as understanding their reliance on third parties in the same geographical region or the use of the same subcontractors
- evaluating their most critical third-party relationships to gain a holistic view of relevant risks
- establishing effective internal business continuity plans and robust exit strategies for their most critical third parties to prepare for the unexpected.

We anticipate that these industries will increasingly prioritise these areas, driven by various factors such as financial instability, geopolitical risks, natural disasters and the evolving regulatory landscape.



We anticipate that even industries outside the Financial Services sector will increasingly prioritise these areas, driven by various factors such as financial instability, geopolitical risks, natural disasters and the evolving regulatory landscape."

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



# 8. Legacy IT and IT simplification



## Why is it important?

Two key focal points that have gathered significant attention this year within organisations are legacy IT systems and the simplification of the IT environment. These topics, although not new, continue to be of paramount importance due to their direct impact on an organisation's agility, cost-effectiveness, and ability to innovate. Internal audit teams play a critical role in ensuring that organisations address these issues effectively, understanding key trends, mitigating risks, and implementing strategic actions.

Legacy IT systems refer to outdated technologies, software, or hardware that an organisation continues to use, often due to perceived complexity in replacement or integration with newer solutions. These systems can hinder an organisation's growth and flexibility, making it challenging to keep up with market demands and technological advancements.



...continue to be of paramount importance due to their direct impact on an organisation's agility, cost-effectiveness, and ability to innovate."

\*Audit planned % is the percentage of respondents who have included this topic in their audit plan.  
\*\*Use of analytics % is the percentage of respondents who, if they have included this topic in their audit plan, will employ analytical techniques.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts

We found that respondents from more established companies reported a greater proportion of legacy IT within their estate, which is not surprising. Interestingly while legacy IT can increase maintenance costs, organisations reported that they often lacked the budget to invest in new technologies to replace the ageing estate.

IT environments consist of a complex web of interconnected systems, applications, and infrastructure, with a combination of both old and new technologies. Simplification involves streamlining this environment by reducing redundancies, eliminating unnecessary processes, and optimising resource allocation. A simplified IT environment enhances operational efficiency, reduces costs, and provides a foundation for innovation and agility. Fundamentally, it enables organisations to respond quickly to changes and seize opportunities that arise in the fast-paced digital landscape.



...the pace of technological innovation has accelerated, making legacy systems even more obsolete.”

The following are key risks to consider:

Loss of data integrity

Inadequate security measures and lack of data backup procedures can lead to data corruption or loss, disrupting critical business operations and potentially impacting customer trust.

Dependency on individuals

If the knowledge about how to operate and maintain legacy IT resides with specific individuals, the business becomes dependent on them, creating a single point of failure.

Long-term viability Legacy or complex IT solutions might not have a clear roadmap for development and updates, leading to obsolescence and technical debt.

Compliance violations

Using old technology or operating across a complex environment might result in non-compliance with industry regulations and data protection laws (e.g., GDPR, HIPAA). This can lead to legal actions, fines, and reputational damage.

Inadequate support and maintenance

Legacy IT solutions can often lack proper support channels and maintenance, making it challenging to address technical issues promptly. This can lead to extended downtimes and loss of productivity.

Lack of scalability

Legacy IT solutions might not be designed to scale with the business’s growth, leading to scalability issues as demand increases.

Financial implications

While legacy IT might appear cost-effective in the short term, it can result in higher costs over time due to inefficiencies, security incidents, and the need to address technical debt. Overly complex IT environments will cost more to maintain.

Business continuity risks

In the event of system failures or disasters, relying on legacy or complex IT solutions can complicate disaster recovery and business continuity efforts.

Data breaches and security vulnerabilities

Legacy IT tools might lack the necessary security controls, leaving sensitive business data vulnerable to unauthorized access, breaches, and cyber-attacks. This risk is amplified when critical processes involve sensitive customer information or proprietary data.

Operational inefficiencies

Different departments using different tools can lead to inefficiencies in processes, communication breakdowns, and duplication of efforts.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



What's new?

In 2023, several factors have heightened the significance of legacy IT systems and the simplification of IT environments:

Technology evolution

The pace of technological innovation has accelerated, making legacy systems even more obsolete. Emerging technologies such as AI, blockchain, and the Internet of Things (IoT) demand modern, integrated IT infrastructures to unlock their full potential. Organisations that cling to legacy systems risk falling behind competitors who have embraced the latest advancements.

Remote work reality

The global shift to remote and hybrid work models has highlighted the importance of agile IT systems. Organisations require flexible, cloud-based solutions that empower employees to collaborate seamlessly regardless of their location. Legacy systems can impede remote work capabilities, hindering productivity and creating frustration among employees.

Cybersecurity concerns

Legacy IT systems are often more vulnerable to cyber-attacks due to outdated security measures and lack of ongoing support from vendors. As cyber threats continue to evolve, organisations must prioritise security by modernising their IT environments. Ransomware attacks and data breaches can have significant financial and reputational consequences.

Greater demands on profitability

The current economic climate has focused the attention of organisations onto the economic viability of their business models more so than in previous years. This re-focus on the bottom line has caused a reduction in some investments in technology such as legacy IT. We noted that organisations who were successful in making the cases for legacy IT replacement and IT environment simplification were those who made the business case around reducing maintenance costs and improving the security of the systems. Others focused on removing legacy IT as part of business wide process improvement projects aimed at simplifying business models and/or improving customer experience.

What should internal audit be doing?

Assess technology alignment

Internal audit should assess how well an organisation's IT strategy aligns with its business objectives and technological trends. This involves identifying opportunities for digital transformation and evaluating the integration of emerging technologies.

Review cloud adoption

Internal audit should evaluate the organisation's cloud adoption strategy, ensuring that it promotes scalability, security, and cost-efficiency. They should also assess how well cloud solutions are integrated with existing systems.

Assess security vulnerabilities

Internal audit teams should assess the cybersecurity measures in place, including patch management, access

controls, and data encryption. Outdated systems can expose an organisation to security breaches.

Identify operational inefficiencies

Internal audit teams should identify processes that could benefit from simplification and automation, because legacy systems can lead to inefficiencies, impacting productivity and customer experience.

Assess compliance and governance

Internal audit should ensure that the organisation adheres to industry regulations and internal governance policies. This includes data protection regulations and best practices for IT management.

Review the modernisation roadmap

Internal audit should collaborate with IT and business units to develop a comprehensive roadmap for modernising the IT environment. This includes prioritising legacy system replacement, cloud migration, and integration of new technologies.

Perform regular risk assessments and reporting

Internal audit should assess whether regular risk assessments are conducted to identify vulnerabilities associated with legacy systems and the complexity of the IT environment, mitigation strategies are developed and monitored, and whether reporting particularly on risks presented by legacy IT risk and the risk mitigation strategies in place, are produced and shared with the Board on a regular basis.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



# 9. Identity and access management



### Why is it important?

Identity and access management (IAM) is a core area of information security and digital transformation that is constantly evolving, recently being influenced by new technologies and emerging threats. Privileged Access Management (PAM) is a methodology employed to safeguard an organisation against cyber-attacks by regulating and administering access to crucial resources and systems. PAM facilitates the monitoring, detection, and prevention of unauthorised access through the implementation of policies, tools, and good practices. Every organisation's employees and executive team needs to have access to critical business applications, the authentication information for these applications needs to be properly protected as malicious individuals gaining unauthorised access may cause the organisation a significant amount of damage.



Every organisation's employees and executive team needs to have access to critical business applications"

\*Audit planned % is the percentage of respondents who have included this topic in their audit plan.  
\*\*Use of analytics % is the percentage of respondents who, if they have included this topic in their audit plan, will employ analytical techniques.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



Some of the common challenges of implementing PAM are:

**Lack of visibility and control**

Many organisations do not have a clear picture of how many privileged accounts they have, who owns them, what they are used for, and how they are secured. As a result, managing and auditing privileged access becomes challenging, and the organisation is exposed to potential security breaches and compliance violations.

**Overly restrictive or permissive privileges**

Finding the right balance between security and productivity is a key challenge for PAM.

**Credential theft and misuse**

Privileged accounts are attractive targets for cybercriminals, who can use stolen or compromised credentials to access sensitive data, install malware, or escalate privileges. Credential theft can occur through phishing, malware, social engineering, or insider threats. Users who discuss their passwords, make use of default or weak passwords, or don't change their passwords frequently run the risk of having their credentials misused.

**Innovation and transformation support**

As organisations adopt new technologies and trends in IAM, such as zero trust, passwordless authentication, decentralised identity, and AI and Machine Learning (ML), they need to ensure that their PAM solutions are compatible and integrated with these innovations. PAM systems must be updated and tested frequently, and users must be informed and trained.

To overcome these challenges, organisations need to implement a comprehensive and robust PAM strategy that covers the entire lifecycle of privileged access, from identification and provisioning to monitoring and revocation.

**What's new?**

**IAM modernisation**

As more organisations move to the cloud and adopt remote work models, they need to modernise their IAM solutions to provide secure and efficient digital experiences for their users and customers. Consolidating several IAM products into a single suite, adopting good practises and standards for IAM governance and management, and transitioning from old systems to cloud-based or hybrid solutions are all components of IAM modernisation.

**Zero trust architecture**

Zero trust is a security paradigm that assumes no trust between any entities, whether they are users, devices, applications, or networks. Zero trust requires continuous verification of identity and context before granting access to any resource. Granular policies, micro segmentation, multifactor authentication, encryption, and monitoring are all implemented as part of Zero Trust architecture across the whole IT ecosystem.

**Passwordless authentication**

Passwords are the weakest link in IAM, as they are often easy to guess, steal, or compromise. Passwordless authentication eliminates the need for passwords and replaces them with stronger methods of verifying identity, such as biometrics, tokens, or certificates. User satisfaction, usability, and security are all improved by passwordless authentication.

**Decentralized identity ecosystem**

Decentralised identity is a concept that empowers individuals to own and control their own digital identities, without relying on centralised authorities or intermediaries. Decentralised identity ecosystems involve using blockchain, self-sovereign identity, verifiable credentials, and decentralized identifiers to enable secure and privacy-preserving identity transactions across different domains and platforms.

**Artificial intelligence (AI) and machine learning (ML) integration**

AI and ML are playing an increasing role in IAM, as they can help automate and optimise various IAM processes, such as identity lifecycle management, access provisioning, risk assessment, anomaly detection, and incident response. AI and ML can also enhance user experience and personalisation by providing adaptive authentication, intelligent recommendations, and conversational interfaces.

**SaaS and consolidating solutions**

Software-as-a-service (SaaS), hybrid cloud solutions, or self-hosted cloud solutions are becoming more popular among IAM vendors at an accelerated rate. Organisations will gain from this change in a variety of ways, including fewer server and infrastructure maintenance needs, improved preparation for the coming decade, and the availability of a complete IAM suite in a single package.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



What should internal audit be doing?

Assessing the IAM maturity and effectiveness

Internal audit should evaluate the current state of the organisation's IAM processes, policies, and tools, and compare them with good practices and standards in the industry. They should also identify the gaps, risks, and opportunities for improvement, and provide recommendations for enhancing IAM performance and security.

IAM governance and strategy

Internal audit should review the IAM governance structure, roles, and responsibilities, and ensure that they align with the organisation's objectives and risk appetite. Functions should also consider assessing the IAM strategy, roadmap and co-organisation, to ensure that that they are aligned with the business needs and IT capabilities of the organisation.

IAMs automation, innovation and transformation

Internal audit should assess any automation of IAM processes through relevant tooling, off the shelf or not, such as provisioning, authentication, authorisation, and deprovisioning, including reviewing any detective monitoring controls (such as logging, auditing, reporting, and alerting on IAM activities and events) as an approach of improving the efficiency, security, and compliance of an organisation's IAM system. They should monitor the adoption and integration of new technologies and trends in IAM, such as Zero Trust, passwordless authentication, decentralised identity, and AI/ML.



Internal audit should evaluate the current state of the organisation's IAM processes, policies, and tools, and compare them with good practices and standards in the industry."



Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



# 10. Emerging technology trends

Rank Previous

10 — —

In this section, we highlight a selection of responses from our survey under the wider umbrella of “emerging trends”, topics that may not be relevant for all functions or industry sectors, and won’t necessarily make the top 5, however they reflect key focus areas for many organisations as well as regulators.



When risks are managed well, responsible marketing creates enormous opportunities to strengthen consumer loyalty, brand value and achieve digital marketing growth with confidence.”

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



## I. Responsible marketing and digital channels

### [Sectors: All]

Consumer confidence and digital trust are at the heart of responsible marketing, social media and e-commerce. That confidence is fragile, with less than a quarter of consumers stating they are 'highly confident' when using digital technologies, which is understandable given over 70% of consumers experienced a digital incident in our latest digital risk survey<sup>15</sup>, trust is hard to earn, and quickly lost.

When risks are managed well, responsible marketing creates enormous opportunities to strengthen consumer loyalty, brand value and achieve digital marketing growth with confidence. The breadth of channels is growing across social media, entertainment, retail and the metaverse. In line with this growth, investment is also on the rise as brands seek to build deeper and more meaningful relationships with their customers and better understand and respond to their preferences. As these channels develop, the need to grow responsibly whilst being mindful of key risk areas such as privacy, data security, regulation, and compliance, is more important than ever to protect brand reputation, value and customer confidence.

Key considerations for technology audit leaders include:

### Data protection

Direct access to customer data is critical to gaining competitive advantage, and must be done within the limits of data protection laws and data privacy controls. A key area of current focus is around underage access prevention and ensuring accounts have appropriate age safeguards in place (e.g. disclaimers and age-verification mechanisms).

### Compliance

Regulation across digital commerce, marketing and social changes rapidly, the Digital Services Act, for example, resulted in companies coming under increasing scrutiny in relation to regulatory change. Brands need to keep up with these requirements and track and implement obligations accordingly to ensure any content and campaigns are compliant with regulation and marketing standards.

### Metaverse

The metaverse and immersive experiences (Virtual Reality, Augmented Reality, AI, Chatbots) have extensive potential and implications across responsible marketing, social and commerce, making experiences more immersive for customers before they buy to engage with and try items. This will change how consumers and businesses engage across channels, but also the risks arising from them. It will be key for internal audit functions to understand how organisations are using these experiences and identifying and managing these risks appropriately.



As these channels develop, the need to grow responsibly whilst being mindful of key risk areas such as privacy, data security, regulation, and compliance, is more important than ever.”

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts





**II. The new UK controls regime and the role of technology [Sectors: All]**

As many organisations start to consider how they enhance their control environment (including digital and technology) in preparation for complying with the proposed UK controls regulation<sup>16</sup> (sometimes referred to as “UK SOX<sup>17</sup> – Sarbanes Oxley”), following the Department for Business, Energy & Industrial Strategy (BEIS) white paper<sup>18</sup> published in March 2021, it is vital that internal audit play a key role, particularly given the opportunity for technology to become a greater enabler for an effective control environment. From this perspective we explore certain key considerations for IT internal audit leaders.

**What is the relationship and integration between business and technology functions?**

One of the key challenges facing internal audit should be whether there is a governance structure that clearly defines shared accountability, for example. One of the most commonly identified pitfalls and root causes for control deficiencies is a lack of understanding, accountability, and integration between business and technology functions which leads to failure around digital controls.

**How business leaders could use technology to enhance the control environment?**

Technology will form a significant part of how organisations respond to the proposed regulation, and there is a real opportunity to use digitisation and technology as an enabler

to improve automation, as well as cost efficiency and effectiveness of control. Again, internal audit can play a key role here, advising and supporting management in assuring risk and implementing fit-for-purpose control.

**How does management define a proportionate and right-fit scope?**

Understanding financial processes is key to correctly identifying the systems and technology that support complete and accurate financial reporting and may therefore be in scope to comply with the proposed regulation. All too often, relevant technology is overlooked during the scoping process which can mean issues with the reliability of financial information, or with the controls that help to ensure reliability of financial information, go unnoticed. Internal audit should advise management to start at the initiation of data and flow through to financial reporting and identify all systems, technology, digital capabilities, and tools that appear in the process for scoping consideration.

**Does the business know what they really need to control?**

A comprehensive risk assessment will lead to a more complete risk and control register, which is central to the effectiveness of the chosen framework in meeting current or future requirements to attest on the operating effectiveness of Internal Controls. A comprehensive risk assessment will actively enable the accurate and complete identification of the principal technology and digital risks in relation to financial reporting.

**Does the organisation have the right technology controls?**

Some of the factors that influence the scale of effort required to implement and comply with a new control regulation include the current technology estate, maturity of the risk and control framework, and effectiveness of the control environment. In addition to considering the maturity of the control environment, business and technology leaders should consider whether there is an opportunity to streamline the IT control environment and consider other risks (cyber, resilience, change) as part of the journey to readiness. This drives value by creating a sustainable, value add environment while also addressing applicable compliance requirements.

Following the BEIS white paper, the assurance requirement over a new regulation is still unknown, but whether internal audit or other form of assurance is needed, management will still need to be able to support their statement that their controls are effective. From our experience of US SOX, technology and business functions at US registrants, they speak to the challenges of the early SOX implementations and highlight that where controls are implemented purely to satisfy a compliance requirement then the business is missing an opportunity to take control and safeguard value for their own purposes. While the timelines for complying with the future legislation are currently unknown, the experience of the US SOX implementation tells us that deploying a control environment that is efficient, effective, technology driven, and value adding takes time. Many organisations find that when they start this process, they uncover challenges that will take time to resolve. Audit can be a supporting partner in that journey, that can truly add value.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts

16 Future of Controls | Deloitte UK  
17 New UK controls regime | Technology enablers | Deloitte UK  
18 BEIS White Paper: Corporate governance | UK SOX | Deloitte UK

III. Digital assets and distributed ledger technology  
[Sectors: Primarily Financial Services, Investment Banking, Asset Management, Financial Markets Infrastructure]

Distributed ledger technology (DLT) has the power to re-platform Financial Services across the value chain, transform capital markets and impact traditional market structure in custody. There is wide variety of custody offerings across jurisdictions owing to technological, regulatory and legal standards.

Digital asset custody is the safe keeping of digital assets. Digital asset custody providers are often third parties who provide safekeeping of assets for institutions, who in turn offer digital asset services to their clients.

The use of DLT is not limited to cryptocurrencies, it also includes a wide variety of assets that are being represented on-chain in the tokenization of existing asset classes and digitally native assets such as equity and debt instruments, and other representations of tokenized real-world assets.

Custody is important as private keys which are used to conduct transactions or access crypto holdings are complex and thus difficult to remember and can be hacked or stolen. For individual holders of digital assets the risk lies in losing one's own assets, but for institutions, the risk is of losing the assets of a number of clients.

When entering the world of custody of digital assets, the underlying new technology continues to affect existing risk domains in the business of custody as we know it today. In parallel, many existing risk domains will undergo fundamental changes as DLT comes into play, and entire new risks will emerge.



Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

- 1. Cyber security
- 2. Digital transformation and IT change
- 3. Data management and data quality
- 4. Artificial intelligence
- 5. Cloud environments
- 6. Technology resilience
- 7. Outsourcing and critical third parties
- 8. Legacy IT and IT simplification
- 9. Identity and access management
- 10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



#### Key crypto custody regulatory framework developments:

- the EU's Markets in Cryptoassets (MiCA) regulation entered into force in June 2023 [see our in-depth analysis here<sup>19</sup>]. Organisations will need to be MiCA-compliant from 30 December 2024, subject to certain transitional measures
- in February 2023 the UK Government published a consultation roadmap to develop a comprehensive regulatory framework for cryptoassets [you can also refer to our in-depth analysis blog<sup>20</sup>]. This includes an activity-based regime to bring custodians and other key crypto entities (e.g. exchanges, lending platforms) within the UK regulatory perimeter

- in December 2022 the Basel Committee on Banking Supervision (BCBS) published its final proposals on the prudential treatment of cryptoasset exposures<sup>21</sup>. Also contained within the regulation are specific provisions for the regulator to continue exploring quantitative approaches to measuring the risk profile of a cryptoasset. This is likely to lead to internal audit work given organisations may have to undertake significant efforts to evidence compliance with future quantitative testing.

#### Internal audit can play a key role by:

- **reviewing the organisation's risk assessment processes** to understand the implications of relying on digital assets third-party custody providers and the third-party's risk
- **perform a Digital Assets Controls review**, focusing on the mechanisms and controls in place to ensure they adequately mitigate risks from digital asset custody related activity. Suggested controls for a review in this space could be around key management, storage of digital assets in wallets, reconciliation of digital assets on-chain vs off-chain records, proof of reserves assurance where applicable, amongst others

- consider the following, as part of any **review of the organisation's third-party risk** and oversight framework:

- definition, responsibility and capabilities to oversee digital assets custody services from third-party providers
- key components of the third-party oversight programme, which should include vendor's risk management practices, ongoing financial and operational resilience, controls and reporting including that the custodian organisation documents and addresses any identified weaknesses, and that these are monitored.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

1. Cyber security
2. Digital transformation and IT change
3. Data management and data quality
4. Artificial intelligence
5. Cloud environments
6. Technology resilience
7. Outsourcing and critical third parties
8. Legacy IT and IT simplification
9. Identity and access management
10. Emerging technology trends

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts

<sup>19</sup> Markets in Cryptoassets (MiCA) – A New Cryptoasset Regime For The EU Finalised | Deloitte

<sup>20</sup> A Comprehensive Roadmap for UK Cryptoassets Regulation | Deloitte

<sup>21</sup> Capital Treatment of Cryptoassets – a heavy price to pay? | Deloitte UK





Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics  
2024: a viewpoint

Unlocking the power of digital through  
Generative AI for internal audit

Appendices

Contacts

# Unlocking the power of digital through Generative AI for internal audit



# Unlocking the power of digital through Generative AI for internal audit

## Why should I digitalise my function?

Over the past twelve months, business leaders have experienced a sudden awakening to the potential of GenAI. Large Language Models (LLMs) have sent shockwaves through the business landscape by demonstrating the transformative power of how these technologies could redefine how organisations work. Whether interacting with vast sources of knowledge and business data through human-like interactions, accelerating how people work, or revealing new opportunities that were not previously possible through manual efforts, the benefits AI could bring are broad and far reaching.

We believe the integration and use of enabling technologies, such as Artificial Intelligence, is critical to helping functions maximise their impact and value. Digitalising internal audit's ways of working **can improve quality, provide greater levels of assurance, achieve new levels of productivity, and increase the function's impact.** Yet it remains a significant gap and 'number one' opportunity for many functions.



We believe the integration and use of enabling technologies, such as Artificial Intelligence, is critical to helping functions maximise their impact and value.”



Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



The digital landscape is broad, covering artificial intelligence, automation, audit management systems, cloud-based solutions, visualisation, data analytics, and tools such as process mining. While they can be deployed in isolation, the power of digital is in their combination. Digitalisation requires a holistic and coordinated approach across the function, and internal audit lifecycle. And therein lies the challenge...

Digitising the internal audit function **requires a level of digital fluency to start exploring the art of the possible, coupled with a deep understanding of internal audit practice and a mindset of experimentation, innovation and challenging the status quo.** It's a cultural shift as much as a technology lift.

#### And why now?

Most people are already using forms of AI in their daily life without realising it. For example, tools like autocomplete, spellcheck, smart calendar scheduling, and suggestions on the most effective ways to visualise data in applications such as Power BI, are all powered by forms of AI.

But since Open AI unleashed ChatGPT to the public, business leaders have been looking at how to harness these more sophisticated capabilities on their own business data (but within the safety of their environments).

Consequently, very few internal audit functions have jumped 'two footed' into GenAI, and those who are exploring it, are largely still in their proof-of-concept phase or using these tools as general aids. For example, using tools like ChatGPT as research aids to inform an auditor's understanding on risks, controls, etc., to help accelerate creation of general content, or access knowledge resources through a more interactive and human-like conversation enabled user interface.

But much like how the invention of cars forced us to pave the way for better roads, the rise of artificial intelligence will compel businesses to build a robust infrastructure of privacy and security, allowing them to create specific organisational contexts where their data can be combined with broader world models.

Whether companies invest in fine-tuning foundation models or access existing services through APIs or integrated functionality in current applications, AI is coming and quicker than you think. The genie is out of the bottle at it's not going to return inside any time soon.

Whether this is driven by growing stakeholder expectations, necessity to help drive efficiencies, or your function's appetite to innovate and improve, there is a sense in the industry that **those functions who do not engage with the digitalisation agenda now, and specifically AI/ GenAI, will quickly find themselves left behind in their ability to deliver the value.**

The good news is that it's not as big and scary as you think. Enabling technologies are becoming increasingly accessible and this is only being accelerated through the wider efforts of organisational IT functions looking at the same challenge question. You don't need to become digital experts overnight or start replacing your auditors with teams of data scientists (although increasing your digital fluency is key).

As we like to say, **digital isn't the goal. It's what it can help you achieve.** The most important thing is to understand what digitisation could do for your function in **helping you deliver your function's purpose and desired impact.** That means exploring how digital could help you **re-imagine traditional ways of working, reveal new possibilities, and give your teams a superpower to accelerate and scale their capacity to add value.**

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts





**Where do I start with GenAI?**

Generative AI is impressive. The ability of technologies such as large language models to provide coherent and insightful responses, in a human like dialogue, can quickly lead to high levels of trust being placed in their output. Functions who choose to ignore these technologies will fall behind, but the adoption of them must be managed and considered.

**Increase your digital fluency**

Start engaging with learning and development now. You don't need staff to become data scientists, engineers, or digital experts. However, being familiar with the terminology, types of capability and potential for these tools will help accelerate adoption and get your function thinking about the use cases.

**Determine your digital strategy and potential**

Determine how Generative AI can help you achieve your broader functional strategy and outcomes. Systematically review your ways of working to identify potential use cases. Some common instances and proof of concept opportunities may include:

**Performing continuous auditing and automating risk assessment processes.** Utilising natural language processing capabilities to gain insights from data by analysing unstructured datasets in a sophisticated way, such as risk events, customer complaints, issue and risk registers, as well as external sources such as social media posts and customer reviews. This enables audit functions strengthen their future-focused, horizon scanning and 'anticipate' capabilities, while allowing them to provide richer assurance and advisory insights.

**Automating audit tasks,** such as key audit execution/ testing procedures, including content creation: such as controls testing procedures and creation of checklists, QA and methodology adherence assessments, compilation of reports, working papers, audit opinion, audit files.

**Improved and automated communication,** including creation of Audit Committee papers and presentations, audit findings and recommendations could be enriched by industry best practices across relevant geographies, as well as applicable regulatory implications and requirements.

**Not limiting your digital strategy to just Generative AI,** there are many applications and use cases relating to other areas of machine learning such as natural language processing, sentiment analysis, topic modelling, linear regression and neural networks that can already be harnessed and provide opportunities for experimentation.

**Engage with your technology teams**

Understand your organisation's stance toward AI, both from a data privacy and security perspective for open solutions, and it's appetite for shaping existing solutions within the safety of your organisation's environment.

**Clean up your data**

The quality of AI both in terms of its training and its output will be a product of the quality of data it is given and looking at. Many organisations (including internal audit) have poor data quality, version control or out of date versions of documents that haven't been removed from intranets for years. While you're waiting for some of the tools to become

more accessible, getting your house in order will pay dividends to the value AI can deliver. Refer also to our "Data Governance and Data Quality" topic.

**Work through, and manage the risks**

As mentioned earlier, the invention of cars forced us to build better roads, there is no better time to really consider the risks associated with Generative AI while still considering the opportunities it brings. Good governance is critical, and functions should be challenging both themselves and the business to put in robust governance processes and controls around the use, development, testing, access, and ongoing monitoring of AI within the organisation.

**Develop a culture of innovation**

Organisational culture can make or break the success of new technology and new ways of working. Functions that have a culture of innovation, curiosity and the willingness to experiment have usually fared better than those that were less willing to embrace change. Functions should consider innovation programmes, encourage experimentation and reward the right behaviours.

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



### What do the next 6 months look like?

The race is on, and the pace has been set.

Technology houses and software companies are rapidly developing tools and models that will soon be accessible to any organisation. Change is coming and it's coming fast, here is what we expect to see.

LLMs are likely to become **more accessible** with enterprise licences and on-premises models becoming available, resolving the current security concerns associated with the current online models, enabling functions and users to properly leverage for their businesses or functions, including for customer facing solutions.

It is likely that Generative AI will start to become a standard tool for many industries, primarily through smart and efficient **integration** with desktop and collaboration tools we use every day to support our work, such as **text editors, collaboration tools, search engines and chat bots** (to name a few). Microsoft's Copilot GenAI in particular is a tool that is expected to build on the success of 365 to transform productivity and our ways of working.

Traditional ways of working will change, not only will we gain higher levels of efficiency, but **organisational transformation journeys will be accelerated**

**Increased innovation** with new products and new ideas entering the market. Gen AI creates a catalyst for innovation, if embraced, it opens up countless options and new opportunities.

**New security and regulation requirements** are coming our way. The ethical use of AI and data will be at the forefront while we move forward and is certainly not an area we can afford to neglect. Organisations are likely to encounter more expectations and be expected to provide evidence of compliance. Our topic 4 above "Artificial intelligence risks, ethical considerations, and controls" highlights the regulatory developments, as well as the challenge in managing risk appropriately and innovating responsibly.



The race is on, and the pace has been set...  
Change is coming and it's coming fast..."

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics  
2024: a viewpoint

Unlocking the power of digital through  
Generative AI for internal audit

Appendices

Contacts





Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics  
2024: a viewpoint

Unlocking the power of digital through  
Generative AI for internal audit

Appendices

Contacts

# Appendices



# Appendices

## About the Survey

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

We surveyed senior audit professionals from 54 organisations, across UK industry sectors. Figure A illustrates the sectors, and sub-sectors of respondents.

The size of IT audit teams in the companies we surveyed ranged from less than 10 full-time equivalents to those with over 20. Figure B captures this breakdown.

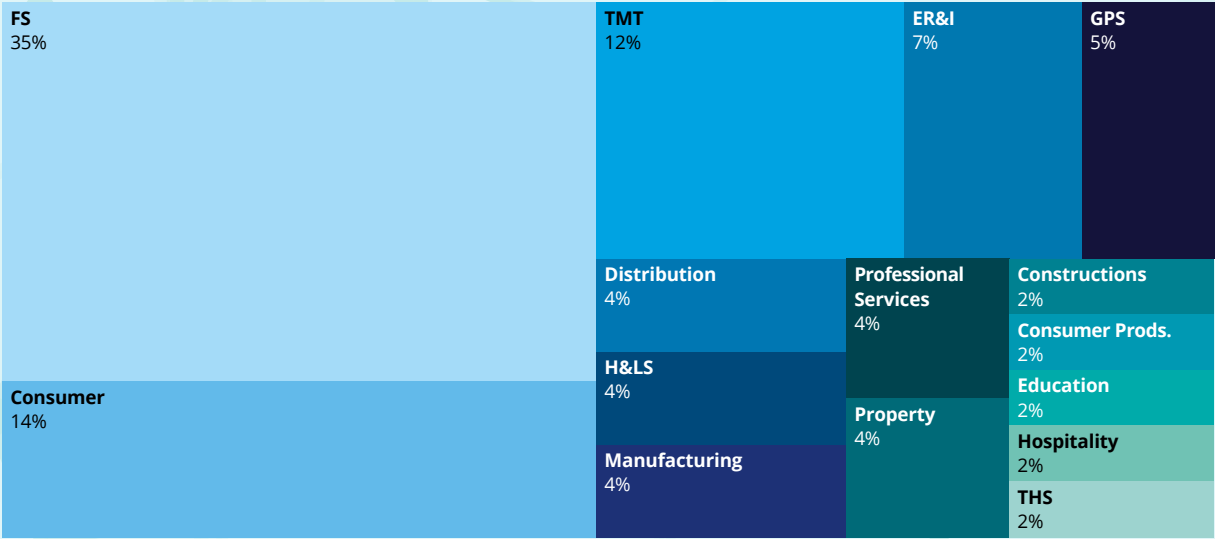
The trend of internal audit budget in the companies we surveyed has mainly increased with 40% of organisations surveyed seeing an increase in their overall budget for the function compared to the previous year. Figure C illustrates the changes in internal audit budgets.

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

This survey was commissioned by Deloitte LLP and was conducted by our senior Risk Advisory practitioners either via direct interviews or through our online survey tool. The data was collected between June and August 2023. As well as capturing the key IT internal audit risks noted by senior audit professionals, our research team has also leveraged the quantitative and qualitative data provided to understand themes and trends developing across internal audit functions.

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

Figure A. Demographic split of survey respondents by Sector



Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



Figure B. How many FTE work in your Global IT internal audit function?

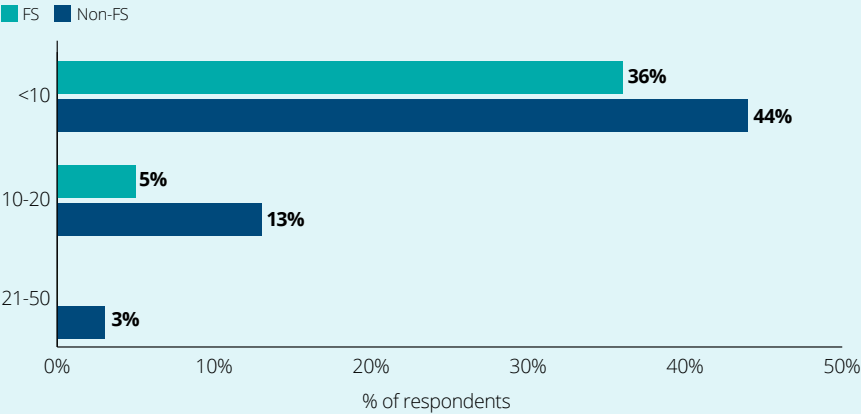
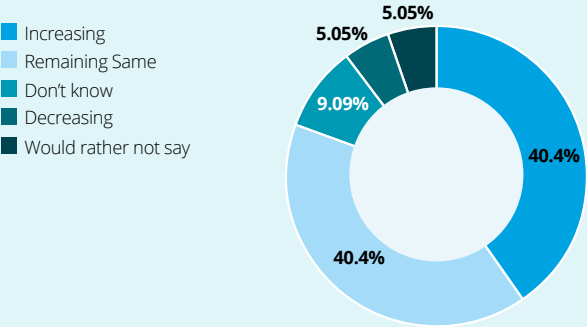


Figure C. Budget trend



Additional sources and references

1	Internal audit digital and analytics survey 2023   Deloitte UK
2	Digital Consumer Trends 2023   Deloitte UK
3	Regulating AI: Can the UK's proposed approach achieve both flexibility and clarity?   Deloitte UK
4	Navigating the EU AI Act: a guide for Chief Data Officers   Deloitte UK
5	Digital Resilience and Enterprise Recovery: Would your business survive a catastrophic cyber attack? Deloitte, 2023
6	Implementing the DORA: What EU financial services firms can learn from the UK's path to implementing operational resilience   Deloitte UK
7	UK financial regulators propose oversight regime for Critical Third Parties: key takeaways and implications   Deloitte UK
8	Consumer experience – the biggest digital risk to your business?   Deloitte UK
9	Future of Controls   Deloitte UK
10	New UK controls regime   Technology enablers   Deloitte UK
11	BEIS White Paper: Corporate governance   UK SOX   Deloitte UK
12	Markets in Cryptoassets (MiCA) – A New Cryptoasset Regime For The EU Finalised   Deloitte
13	A Comprehensive Roadmap for UK Cryptoassets Regulation   Deloitte
14	Capital Treatment of Cryptoassets – a heavy price to pay?   Deloitte UK

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts





Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics  
2024: a viewpoint

Unlocking the power of digital through  
Generative AI for internal audit

Appendices

Contacts

# Contacts





# Contacts

## Financial Services



**Yanniss Petras**  
Partner

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



**Mark Westbrook**  
Director

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

## Corporates and Public Sector



**Faiza Ali**  
Partner

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



**Pete Balmforth**  
Director

Tel: + 44 113 292 1894  
Email: pbalmforth@deloitte.co.uk



**Kirti Mehta**  
Director

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

### We would like to thank the following Deloitte practitioners for their contribution to our paper:

- |                       |                       |
|-----------------------|-----------------------|
| Adam Blair            | Lewis Keating         |
| Alex Mullineaux       | Mackenzie Hobby       |
| Catalina Reyes Magnet | Madeleine Thirsk      |
| David Coldwell        | Maria Eugenia Morales |
| David Morris          | Nanette Scott         |
| David Tiernan         | Olga Harte            |
| Dimitar Milanov       | Roshan James          |
| Haroon Abbas          | Rubal Mehta           |
| Joseph Preston        | Rupert Hargrave       |
| Katie Hibbert         | Sofia Triantafyllou   |
| Kirsty Maund          | Sonia Verbeeck        |
| Konstantin Litvak     |                       |

Executive summary

Our survey through the years: 2012-2024

Technology and digital risk hot topics 2024: a viewpoint

Unlocking the power of digital through Generative AI for internal audit

Appendices

Contacts



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

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

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

© 2023 Deloitte LLP. All rights reserved.

Designed and produced by 368 at Deloitte. J31428