Deloitte.

Riding the wave
2023 Hot Topics for IT Internal Audit

An internal audit viewpoint

MAKING AN IMPACT THAT MATTERS since 1845

Contents

1 Foreword

2 Executive Summary

3 Our survey through the years: 2012-2023

4 IT Internal Audit Hot Topics 2023: A viewpoint

5 Where next for Internal Audit?

6 Appendices

7 Contacts

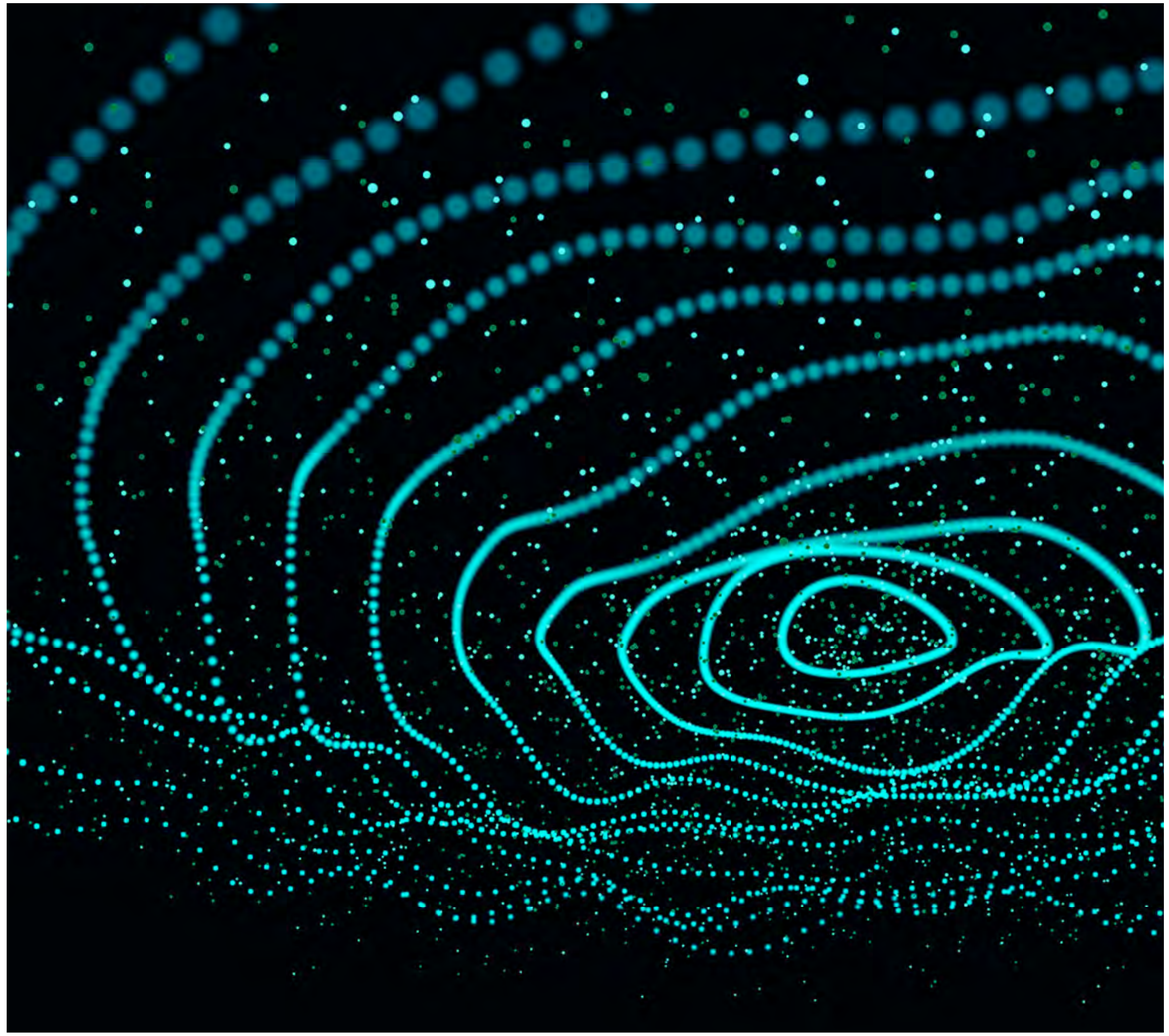
1 Foreword

We are pleased to welcome you to our annual viewpoint on the information technology hot topics for Internal Audit functions.

We are delighted that this year's publication presents the results of a survey run across all UK Industry sectors. The survey is based on an online questionnaire completed by Heads of IT Internal Audit/Heads of Internal Audit, combined with qualitative insights and perspectives from interviews held with IT Internal Audit practitioners, as well as CIOs, CISOs, CTOs and business leaders across sectors.

We would like to thank our clients who took part in this survey, either via interviews, or by utilising our online survey tool.
Their 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 and business leaders, whilst also supporting your risk assessment and planning process for 2023. As always, we look forward to hearing your views on the key points underlined by the survey and continuing the discussion.



2 Executive Summary

In the past two years our survey has been completed in a period defined by one of the most significant global events in decades, the COVID-19 pandemic, that transformed business models, ways of working, and the technology and data environment for many organisations. As with all periods of significant change, business leaders were required to act quickly to respond to the uncertainty unleashed by the pandemic. Internal Audit functions were also called upon to provide well-needed assurance over risks, as decisions were made at pace, many of them with technology at their heart.

This year, the repercussions from these events continue to play out, in the wider context of continued uncertainty and a challenging macro-economic environment. The impact of the pandemic, geopolitical changes and rising cost of living has driven, and perhaps even forced, business models to become more agile and innovative. It appears clear that technology, digitisation, and resilience are central themes seen by the organisations as underpinning future business success. IT internal audit continue 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.

- Our survey was performed across all UK sectors, but one thing that transpired was that – except for in a couple of domains – we did not notice a significant disparity amongst priorities and areas of challenges across functions surveyed.

Table 1. IT Internal Audit Hot Topics 2023

Rank	Across UK sectors	Financial Services	Corporates and Public Sector
1	Cyber Security	Cyber Security	Cyber Security
2	Digital Transformation and Change	Digital Transformation and Change	Digital Transformation and Change
3	Data Management and Governance	Cloud Hosted Environments	Data Management and Governance
4	Cloud Hosted Environments	Operational and IT Resilience	Business Critical IT Controls
5	Operational and IT Resilience	Data Management and Governance	Third-Party Risk Management
6	Business Critical IT Controls	Third-Party Risk Management	IT Strategy and Governance
7	Third-Party Risk Management	IT Strategy and Governance	Cloud Hosted Environments
8	IT Strategy and Governance	Identity and Access Management/Privileged Access	Identity and Access Management/Privileged Access
9	Identity and Access Management/Privileged Access	Business Critical IT Controls	Operational and IT Resilience
10	Digital Risk: Artificial Intelligence	Payments	Digital Risk: Artificial Intelligence

- **Cyber security** remains the number one 'hot topic', continuing the trend over the past few years; we notice how organisations continue to evolve their thinking around managing this risk as the broader cyber risk landscape continues to mature and diversify. Cyber-attacks in the form of data theft, compromised accounts, ransomware, social engineering attacks is "top-of-mind" across organisations and industry sectors. Topics such as ransomware and incident response were popular across all sectors in our survey, while FS organisations also raised topics such as data leakage prevention, threat intelligence, and insider threat. Other corporates highlighted a focus on cyber strategy and maturity, vulnerability management, security operations.

- The post-pandemic activity around **digital change and transformation** has resulted in heightened risks around change delivery, strategy, and planning, where greater integration between business and IT strategy will be paramount – more than ever before. Organisations are embracing digital transformation as a key driver for growth. With the uncertainty in the economic environment, we're seeing a lot more interest in technology spend that will impact the bottom line, whether that's driving additional operational efficiency through cloud, analytics, and cyber risk management. This creates new areas of risk, as well as opportunities to streamline governance and control processes, making it increasingly important that Internal Audit engage with the programme teams early on in and continually throughout the lifecycle to help organisations manage risks appropriately and proactively.

- FS regulation has continued to intensify and evolve, touching on key technology areas such as **cyber security, cloud, resiliency, and third-party risk**. It is interesting to explore how these IT risk disciplines coalesce across the organisations' control environment, as well as being key hot topics in their own right, that need to be suitably risk assessed and assured against. This also requires IT Internal Auditors to stay close to the changing regulatory environment around these areas, and Internal Audit leaders to ensure the combination of skills in the team is keeping pace with emerging risk themes.

- On the other hand, non-financial services organisations placed hot topics around **business-critical controls** (in the context of recent UK reforms), higher in the ranking. This is driven by the journey of reforming and re-emphasising UK corporate governance, whereby companies and auditors are expected to face even tougher obligations that will re-shape the approach to internal controls. These recommendations (also known as UK SOX) reflect a wider, global sentiment from society that stronger internal control environments are needed to prevent material fraud and unexpected company failures. With technology environments both being ever pervasive and becoming more complex, it will be important for Internal Audit to ensure senior management demonstrate they understand how these core controls are implemented across the technology estate, how their effectiveness and suitability is being monitored and how they can support compliance.

The two key challenges that Internal Audit functions are, or will be, facing this year, are illustrated below in word-cloud, based on survey responses.

01. People, skills and talent: resourcing remains a challenging area, as the desirable skills (or combination of skills) are hard to find and retain, against a backdrop of an exceptionally competitive market for skills. From conversations with Internal Audit leadership, it is very difficult to identify and recruit key technology and digital skills in the market, but also to retain existing talent. Functions try to be inventive and resourceful in terms of providing the right opportunities, upskilling their people, investing in talent and wellbeing. At the same time, they are exploring the optimum mix of alternative delivery and resourcing models such as contingent staff, guest auditors, contractors, and third-party co-source.

02. The ability to appropriately harness the pace of change: we live in an environment of constant change, particularly in the technology and digital domain, accompanied by relentless regulatory attention and intervention in many sectors. The macro-economic environment of uncertainty, and indeed the expected headwinds to business performance, certainly exacerbates the concern. We see functions continuing to explore transformation and innovation options to stay relevant, continuing to add value in a cost-effective way, so that they effectively "*ride the wave*" of uncertainty and constant change. We see functions adopting automation, experimenting with data analytics or tech-enabled approaches to transform the way they operate, provide their services, or modernise their core processes, such as risk assessment or horizon scanning.

The core focus of Internal Audit functions should remain on increasing their impact and influence in their respective organisations, by not only providing assurance, but also educating and advising management and anticipating risks. The sections of our report that follow cover the 'hot topics' for 2023 in more detail, aiming to provide perspectives and insights on how functions can best achieve that.

Figure 1. Word cloud of responses: challenges facing Internal Audit functions in 2022-2023

3

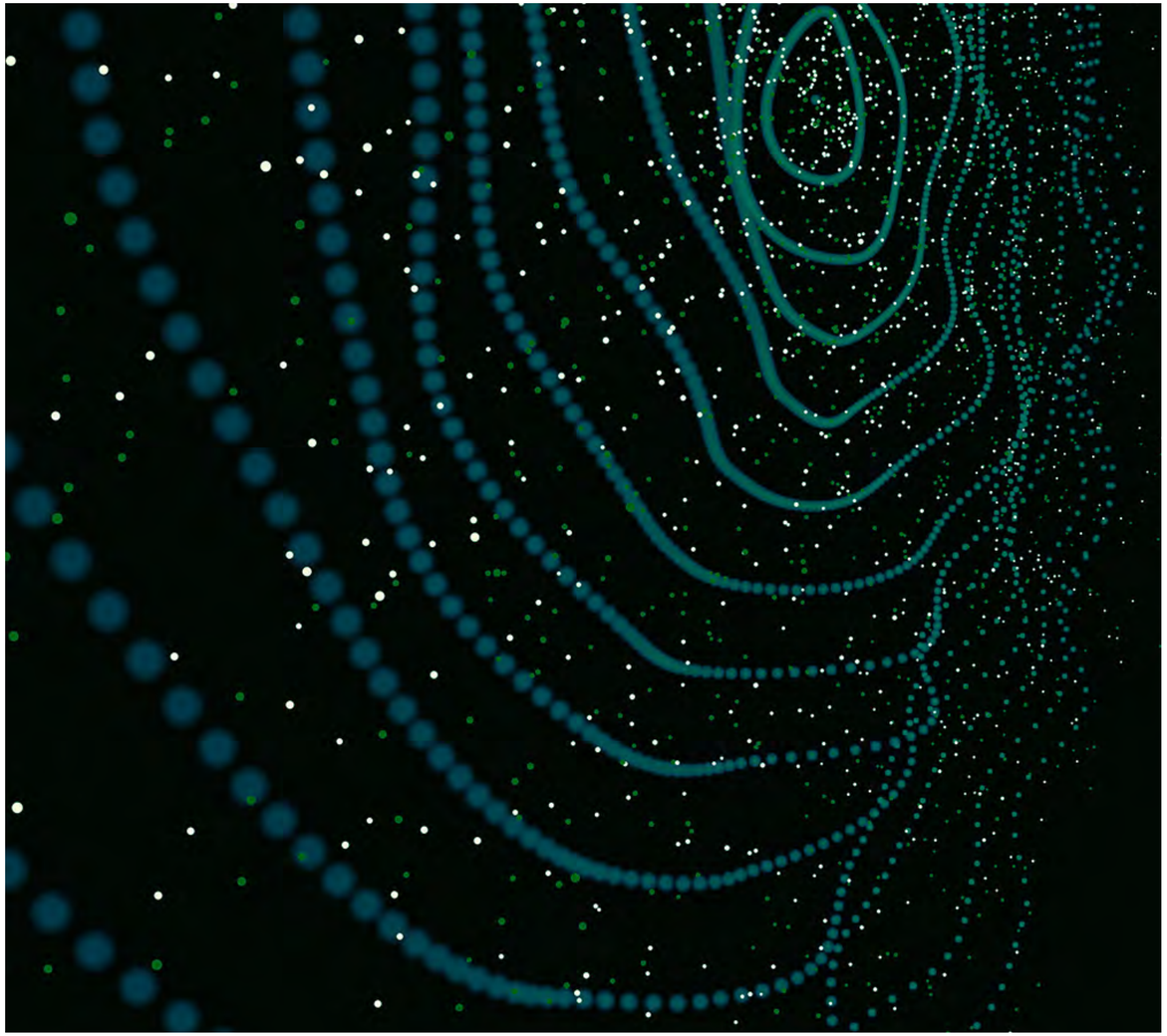
Our survey through the years: 2012 – 2023

Our survey through the years: 2012 – 2023

The table overleaf presents a comparison of the top-10 IT internal audit hot topics over the past eleven years, as identified through our annual survey of Heads of IT Internal Audit.

We noted the continued presence of 'Cyber Security' at the top of our list for the best part of a decade now, as well as the continued focus from functions on 'Cloud' (and what it means from an internal audit coverage standpoint), 'Digital Transformation', 'Third-Party Risk', 'Operational and IT Resilience'. The final two boosted in the ranking by a recent emphasis, particularly in the financial services sector in response to FS regulation.

We also observe the impact from the post-pandemic drive to introduce disruptive technologies enabling digital business models and transformation initiatives. On the other hand, the presence of more traditional areas, such as "Data Management" and "Privileged Access", reflect the ongoing struggle of organisations across sectors to improve their internal control environment in those, undoubtedly very complex, areas.



Our survey through the years: 2012 – 2023

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

Table 2. IT Internal Audit Hot Topics through the years: 2012-2023

Rank	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	Large Scale Change	Third-Party management	Cyber Threat
2	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 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	Cloud Hosted Environments	Data Governance	Extended Enterprise Risk Management	Extended Enterprise Risk Management	Technology Resilience	IT Disaster Recovery and Resilience	Third-Party Management	IT Disaster Recovery and Resilience	Enterprise Technology Architecture	Data Governance and Quality	Large Scale Change	Data Governance and Quality
5	Operational and IT Resilience	Transformation and Change	Transformation and Change	Digital Technologies	Extended Enterprise Risk Management	Information Security/ Identity and 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	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	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 and Access Management	Digital and Mobile Risk	Digital and Mobile Risk	Digital and Mobile Risk	Cloud Computing	Financial Crime
8	IT Strategy and 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/ 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	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

4

IT Internal Audit Hot Topics 2023: A Viewpoint

1 ◀▶ (1) Cyber Security

Audit Planned %	Min % of Audit Plan Days	Max % of Audit Plan Days	Use of Analytics %
74%	11%	83%	36%

Why is it important?

We have seen cyber-attacks increasing significantly in the wake of the pandemic era, with fraud, social engineering attacks, blackmail, and email compromise particularly heightened.

Many organisations would potentially suffer numerous and substantial consequences from a successful attack or security event that could include breach of regulations and any resultant significant fines for loss of data, loss of confidential information, loss of key operational systems and a reduction in customer confidence. The reputational impact from a cyber-attack can be very high with any loss of trust having significant business repercussions, particularly for those businesses with a high reliance on on-line presence for sales, distribution and/or back-office operations.

This has also called attention to long-standing cyber security – as well as information security more broadly – challenges facing many organisations, particularly in relation to their capability across various domains to prevent, detect, mitigate, and respond effectively to a significant cyber incident.

Footnote

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

Min % of Audit Plan Days is the lowest percentage of audits days that a respondent noted they will spend on this topic in relation to their total audit plan.

Max % of Audit Plan Days is the highest percentage of audits days that a respondent noted they will spend on this topic in relation to their total 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?

- Ransomware continues to present a significant risk across all sectors. We are seeing the prevalence of (double and triple) extortion which can be particularly damaging, owing to the exfiltration of sensitive data in addition to the ceasing of operations. After encrypting victim networks, threat actors use double or triple extortion by threatening to (1) release stolen data, (2) disrupt access and/or (3) inform victim's customers, employees, partners, or suppliers about the incident.
- There has been a notable increase in the implementation of artificial intelligence technologies to aid detection efforts and identify fraud, identity theft, and other suspicious activities in real time.
- Social engineering remains a common infiltration tactic. Staff, customers, and employees are falling victim to targeted phishing attacks at ever increasing rates.
- There is an increasing concern over the potential use of 'deep fake' technology to identity theft. This is a technology seeing rapid development with slower deep fake detection technology development.
- While many companies rely heavily on remote working technologies and capabilities, including the use of BYOD (Bring Your Own Device), personal laptops or other devices are typically not held to the same security standards as corporate assets, increasing the risk of infiltration by hackers and other threat actors.

1 ◀▶ (1) Cyber Security (continued)

What should Internal Audit be doing?

Potential areas for Internal Audit functions to consider as part of their 2023 annual planning, include:

- Review of the "incident response" capability of the organisation, which would include their assets and capability across various domains to prevent, detect, mitigate, and respond to ransomware incidents.
- Indeed, the focus on cyber resilience more generally by functions is heightened this year.
- The ability of the organisation to detect and pull back/recover from major cyber security incident or breach (not ransomware).
- Evaluate and opine on the overall cyber security awareness at executive management and board level. 40% of boards of directors will have a dedicated cyber security committee overseen by a qualified board member, up from less than 10% today, according to research by Gartner, Inc[1]. Cyber security should be a Board-level issue and responsibility.
- Review the organisation's cyber security strategy in the context of operations, environment, and current organisation; this could include alignment to future business, people, and organisational plans.
- Review the ability to perform adequate and sufficient levels of cyber due diligence across third-party services (in a risk proportionate manner); this should include initial take-on, contracts, relationship management and review. Consideration also needs to be given to the agents and suppliers that they also rely upon – the subcontractors, or "fourth party" services. Refer also to the "Third-Party Risk Management" hot topic.
- Evaluate the ability of the organisation to conduct simulation or war-gaming exercises to 'test' their cyber incident response capability more holistically and ensure subsequent observations/outputs are being tracked and remediated where required.

[1] **Source:** https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-

Sector perspectives:

Financial Services

- The financial services sector seems to be one of the most targeted for cyber-attacks because of its extensive access to financial accounts, large databases of sensitive data on individuals, businesses and governments and access to funds.
- The sector continues to be at the forefront of new cyber risk defences with technologies such as Multi Factor Authentication (MFA), biometrics, electronic authentication.
- Cloud adoption continues at a high pace, leading to an all-time-high in terms of the number of financial services institutions availing of cloud services with often inadequate effort being placed on cloud security.
- There is still a balance to be struck between customer convenience e.g., app payments and banking, with that of regulation and security.
- Other topics that were raised in our survey include data leakage prevention, threat intelligence, and insider threat.

Corporates and Public Sector

- Ransomware remains a significant concern mainly due the number of organisations that are not keeping up to date with vulnerability patches and/or not securing legacy systems.
- Securing remote access connections for those working from home, remains a key area of concern and focus.
- Lack of investment within developing cyber security capabilities.
- Other topics that were raised through our survey include cyber strategy and maturity, vulnerability management, security operations.

2 ▲ (5) Digital Transformation and Change

Audit Planned %	Min % of Audit Plan Days	Max % of Audit Plan Days	Use of Analytics %
72%	5%	63%	16%

Why is it important?

Investment in strategic change and digital transformation in all industry sectors has rebounded post-pandemic. Many organisations are investing in projects designed to achieve long-term growth and looking at ways to create new revenue opportunities. This is opposed to the previous emphasis of reacting to operational challenges and the need to protect colleagues, customers, and services. Management are looking at how they attract new customers and better engage with existing ones through new digital services offerings.

The competition for talent and the evolving skills landscape is forcing organisations to look at new and faster ways to deliver change without key dependency on internal experts. This creates new areas of risks, as well as opportunities to streamline governance and control processes, making it increasingly important that Internal Audit engage with the business early on in the lifecycle to help organisations manage risks proactively.

What's new?

- Focus on strategy, product design, digital consumer engagement and innovation. The main driver for change programmes is not only to reduce the operational costs, but to attract new customers and increase engagement with existing customers through new digital services and better customer journeys and experiences.
- Increase in partnership. Due to high competition for talent, organisations are looking to collaborate with best of breed partners (including new, nimble and non-traditional service providers) to support internal capabilities with specialist expertise and knowledge.
- Investing in, and enhancing project management processes, tooling and capabilities, building and developing internal QA and Risk Functions.
- Embracing new technologies quickly through experimentation and iteration with new consumer value propositions and use cases
- The introduction and use of data analytics tools for transparency, visibility, and better management of dependencies across the programmes, as well as having the appropriate level of resources that can interpret and make decisions based on the data.
- The use of agile tools continues to gain popularity, with a focus to improve collaboration and cohesiveness across the project teams. Adoption of Agile and Continuous monitoring methodologies is seen as one of the most effective ways to reduce delays in the programme delivery.

2 ▲ (5) Digital Transformation and Change (continued)

What should Internal Audit be doing?

- Internal Audit functions need to be proactively assessing the organisation's innovation and digital transformation strategy and approach to ensure it would benefit the business long term. The key is not to penalise for single product or delivery failures but look at the overall programme potential.

- Internal Audit should assess the appropriateness of levels of governance for agile delivery and review of organisation's control environment to ensure the right level of controls are in place for Agile programme delivery, leveraging continuous monitoring solutions to minimise delay.

- Internal Audit should work more closely with first and second line risk and control function to support the organisation in its transformation journey and get involved early on in and continuously throughout the programme lifecycle.

- It is critical that effective MI and adequate reporting is in place to allow relevant senior stakeholders to provide right level of governance and oversight. Effective stakeholder management and governance at senior levels can help foster an operationally effective environment throughout a programme lifecycle. We see a lot of organisations moving into a variety of "business partnering" models to embed risk management skills directly into programme delivery teams or product delivery pipelines.

- As organisations adopt new analytical tools, there is a danger for the business to have too many systems in pursuit to accelerate the digitalisation without proper assessment of performance and benefits. Internal Audit should plan an assurance review of how these tools are embedded across the organisation to ensure they deliver value for money. A holistic approach is needed where the reviews include systems, structures, skills, and capabilities.

Sector perspectives:

Financial Services

- Most Internal Audit functions we engage with across the financial services sector have already performed various reviews across the topic, and we see on an average 10-20% of their audit plan dedicated to change and transformation auditing – including technology and digital transformation.

- Some of the focus areas, as identified in our survey are: Agile Change Delivery; Core Banking System/Legacy Technology Upgrades; DevOps; Digitisation of customer journeys; Change Governance.

Corporates and Public Sector

- Large corporates are continuing to invest in new technologies to improve the efficiency of internal processes and to develop the services they provide in response to the demands of consumers who are expecting increasingly digital offerings. Internal Audit's role in these transformation and change programmes will require a shift away from traditional internal audit approach, towards an agile assessment of risks throughout the lifecycle of the programme.

3 ▲ (4) Data Management and Governance

Audit Planned %	Min % of Audit Plan Days	Max % of Audit Plan Days	Use of Analytics %
74%	4%	57%	61%

Why is it important?

Data management and governance reviews are increasingly common across all IA functions. Good data governance and data management processes are key to managing the risk of unreliable, missing, or inaccurate data across an organisation. Where data quality is robust, it can add value to an organisation through providing increased efficiency and business opportunities.

Despite the strategic importance of data, many firms (across sectors) have been slow to implement data governance and accountability frameworks, which could enable a better coordinated and more effective approach in the use of data. This, in turn, increases the risk of regulatory fines or poor decision making that can lead to the misallocation of critical resources or missed business opportunities – in leveraging data capabilities of new digital technologies, for instance.

What's new?

- There has been increasing use of data and digital technologies and this is a trend we believe will continue. Many functions have been moving from legacy to modern solutions such as S4 Hanna, cloud, and big data platforms due in part to the limited support available for legacy systems.
- Following Covid-19, we have seen a sustained increase in remote working. This makes the use, storage, and security of data a more prevalent concern. Businesses are seeing the need for increased focus on the governance and management of data particularly in instances where data is being accessed from different countries.
- While regulations such as BCBS239 or GDPR have been seen as the driving force behind functions investing time and resources into their data governance programmes there is an increased understanding that data, when managed correctly, can lead to efficiencies. Businesses across all sectors are recognising that data privacy and security is crucial and are no longer adopting standards solely to ensure compliance with regulation.
- Businesses, particularly those in financial services, are taking concerted efforts to automate processes where possible or using platforms to reduce the risk of human error and allow for real time monitoring of data anomalies or issues. They are using a combination of machine learning, natural language processing (NLP), and platforms which are targeted at improving data quality, security, and adherence to regulations.

3 ▲ (4) Data Management and Governance (continued)

What should Internal Audit be doing?

- Internal Audit functions should be challenging the business and assessing the foundations of the data strategy in place and the governance and management processes that align with this. An effective data strategy should align to business aims and outline a narrative of how data will help the business achieve their objectives. They should also detail who will be responsible for these actions, when they should be completed, and how success will be measured. Data governance strategies should be regularly updated, particularly as business needs change.
- Functions should consider the overall attitudes towards data within the business which includes the levels of ownership, data literacy training, and stakeholder engagement. Data culture is largely what can make adoption of policies succeed or fail. Mandatory training should be provided to the business which ensures a basic understanding of key data principles and how these should be applied. Where there are skills or knowledge gaps identified, measures should be designed to help bridge the gap between the current state and the desired state.
- A recurring area of focus should be around data ownership and responsibilities. Without a data ownership framework and detailed data or information asset registers it is not clear to the business what data is held, where the data is stored, the quality of the data, and who should have access to that data. Once there is an understanding of the data landscape it will help inform key business decisions as there is a clearer understanding of what data is available and how it could be used. Additionally, with a better understanding of the data, remedial actions can be taken, such as a plan to improve data quality and help get the best out of the data available.
- Data quality is a key challenge for every organisation and should be an ongoing area of focus. Internal Audit functions should assess and opine upon data quality including processes to safeguard quality, and business initiatives or controls around appropriate root cause analysis and remediation.
- Timely investment to upgrade from legacy systems is key to ensuring effective data management. Support for legacy systems is often patching up issues rather than addressing them and eventually investment will be required where this support is no longer offered. Functions should challenge the business to be proactive and upgrade legacy systems in good time with a plan for how to perform the migration so that critical data is appropriately managed and retained.

Data management and governance reviews are increasingly common across all IA functions. Good data governance and data management processes are key to managing the risk of unreliable, missing, or inaccurate data across an organisation. Where data quality is robust, it can add value to an organisation through providing increased efficiency and business opportunities.

4 ▼ (2) Cloud Hosted Environments

Audit Planned %	Min % of Audit Plan Days	Max % of Audit Plan Days	Use of Analytics %
73%	1%	60%	18%

Why is it important?

Cloud-hosted environments have been widely adopted across all UK sectors with many organisations having started their strategic cloud migration journey 2-3 years earlier. Cloud is now both an integral part of corporate strategy and day-to-day operations; however, Risk and Control functions are continuing to struggle to keep pace with the rapid transition and scaling risk management activities, enabling organisations to adopt cloud at pace and with confidence. There are significant regulatory pressures around cloud use, and these are increasing globally, while many organisations that have embraced cloud are yet to realise the full benefits of use.

There are significant regulatory pressures around cloud use, and these are increasing globally, while many organisations that have embraced cloud are yet to realise the full benefits of use.

What's new?

- As cloud environments become more commonplace, the modification and adoption of existing enterprise-wide IT risk and control frameworks is increasingly important. False 'baseline' assurance is often placed over fresh migrations to the cloud where it is assumed that due assessment of the controls and risks in the cloud environment has already been undertaken, but as organisations have moved gradually to the cloud, it is highly likely that the underlying risk profile and exposure have changed since the cloud environment assessment.

- Many organisations started their cloud transition journey as a key part of their broader digital transformation 2-3 years earlier and are now looking to understand the benefits realised from investment – so, demonstrating added value, objectives/benefits realisation, and tangible service performance improvement would be key priorities.

4 ▼ (2) Cloud Hosted Environments (continued)

What should Internal Audit be doing?

- Internal Audit functions need to reflect on the increasing adoption of cloud and treat it as a new "technology environment" or part of their "digital universe", rather than an application or a component to be audited in isolation.
- Functions should consider implementing an approach of looking into cloud environment components or thematic areas on a cyclical basis and assess proper coverage as part of planning.
- Furthermore, cloud should also be considered as a broader trigger point during business audit planning. For example, planning for each audit should raise key questions around cloud usage (as well as third-parties more broadly) in the delivery of a given business service or process.
- Enterprise use of cloud should be reviewed holistically to evaluate concentration risk and how the organisation is able to manage the potential impact on operational resilience and associated tolerances.
- It is also sensible for functions to reflect on the assurance that is provided over cloud service providers, and whether a piecemeal adoption of cloud solutions, has resulted in an overarching control framework which lags the prevalence of cloud usage. Focussing on management's understanding of cloud usage across the enterprise and the controls which prevent the procurement of cloud capabilities outside of established governance/procurement processes can be a high-risk area of focus here.
- Internal Audit functions need to evaluate and truly understand the risks in the context of cloud and how this should be controlled, for example access to production environments should be controlled through comfort over the configuration of cloud pipelines and controls over changes to code, rather than traditional controls such as review of user access list.

Sector perspectives:

Financial Services

- Many emerging areas of regulation across the financial services sector are often heavily impacted by cloud, and so it is increasingly important to ensure strong linkage between an organisation's cloud team and regulatory and compliance specialists. For example, the Operational Resilience Supervisory Statement (effective as of March 2022) requires organisations to consider their cloud usage and understand the implications of these services for their operational resilience.
- This has led to regulators requesting FS Internal Audit functions to review cloud related submissions such as cloud outsourcing register completeness and accuracy.
- Key areas of focus by FS organisations in our survey include cloud outsourcing, regulatory requirements, operational resilience and cloud.

Corporates and Public Sector

- Key areas of focus by respondents to our survey include cloud governance, cloud security and cloud migration.

5 ▼ (3) Operational and IT Resilience

Audit Planned %	Min % of Audit Plan Days	Max % of Audit Plan Days	Use of Analytics %
70%	3%	38%	25%

Why is it important?

This remains a particular hot topic for the financial services industry. The recently published Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) Business Plans for 2022/23 demonstrate that Operational Resilience remains a top UK supervisory priority. By 31 March 2022 firms were expected to identify and map their Important Business Services, set Impact Tolerances, commence scenario stress testing programmes to identify vulnerabilities, produce 'Self-Assessments', and ensure appropriate governance arrangements are in place.

Whilst the past 12 months have been very demanding, the resilience journey is only just beginning. The three-year 'transition period' for the policy runs until 31 March 2025, and the actions that firms take in that time will be critical to their success. Their focus must now shift to addressing the initial operational vulnerabilities identified, expanding the depth and breadth of mapping and testing to detect and address additional vulnerabilities, and embedding Operational Resilience into the whole operating model to withstand severe but plausible disruptions.

What's new?

- Amongst the broader suite of activity required to continue the Operational Resilience journey, the following areas are likely to be key areas of focus and challenge for Boards and senior Management over the next three years:

- **Scenario Stress Testing**: Testing is likely to be the key area of Operational Resilience policy expectations which continue to evolve throughout the period up to 31 March 2025, as firm's gain experience in the stress testing necessary, and the Regulators assess and feedback on the approaches being followed.

- **Third Party Risk Management**: Third party dependencies pose a significant threat to a firm's operational resilience. Visibility, oversight, and assurance is imperative to adequately understand and manage the risks posed by third party and outsourced arrangements (including technology giants and those responsible for providing IT services). Boards and senior Management cannot outsource their ultimate accountability and responsibility for their Operational Resilience and therefore need to gain assurance over the risks posed by the web of third and fourth parties in the service chain, especially when the service being provided is critical in providing a firm's Important Business Service.

- **Transition to Business As Usual (BAU)**: As firms look to build longevity in their Operational Resilience framework and transversal capabilities, embedding Operational Resilience across the organisation will transform meeting the 2025 policy requirements and expectations into sustainable BAU activity.

5 ▼ (3) Operational and IT Resilience (continued)

What should Internal Audit be doing?

The key areas of focus for FS Internal Audit functions moving forward should be as follows:

- Providing robust challenge on the inputs and outcomes of scenario testing, challenging the approach undertaken to ensure that it is sufficiently detailed and enables identification of vulnerabilities for remediation.
- Challenging the approach to third party risk management (TPRM), alignment with the outcomes of the PRA's Supervisory Statement SS2/21 on 'Outsourcing and TPRM' and consideration of current key areas of TPRM such as engagement with Cloud service providers and the linkage to Operational Resilience e.g. the sophistication of mapping to enable delivery of Important Business Services.
- Assessing management's ability to monitor and report on the performance of Important Business Services along with the ability to remain within Impact Tolerance limits, with consideration over the firms understanding of remedial actions and the plans in place to remedy these over the transitional period ending 31 March 2025.
- Monitoring the embedding and ownership of the Operational Resilience requirements within the First Line of the business (i.e. has a resiliency culture been achieved), as well as the links from a process and technology perspective to existing related disciplines (change management, disaster recovery, business continuity planning, and risk management).

Sector perspectives:

Financial Services

- Most Internal Audit functions we engage with across the financial services sector have already performed several reviews on the topic.
- There is a need to now move from programme readiness assessments reviews to broader engagement with the business including progress against management's remediation of vulnerabilities (including more in-depth reviews of technology, cyber resiliency remediation programmes for example), further embedding of the framework and continued development of scenario stress testing.

Corporates and Public Sector

- Operational Resilience regulation in Financial Service has shifted the mindset of clients in the CPS, with many organisations choosing to adopt a business services-aligned perspective.
- While the regulatory requirements above specifically relate to those operating in the financial services sector, functions across industry sectors should focus on challenging management on their business and technology resiliency of the organisation.
- The pandemic is a timely reminder that organisations need to be able to manage disruption and challenging circumstances and events effectively, focusing on timely prevention, response, and recovery.
- Key areas of focus by respondents to our survey include disaster recovery, IT resiliency and business continuity, as well as assessments over cyber resilience of the organisation including the monitoring, alerting, and incident response.

6 * * Business Critical IT Controls

Audit Planned %	Min % of Audit Plan Days	Max % of Audit Plan Days	Use of Analytics %
56%	5%	50%	40%

Why is it important?

As the UK continues the journey of reforming corporate governance, companies and auditors are facing even tougher new obligations that will re-shape the approach to internal controls. These recommendations (also known as UK SOX) reflect a wider, global sentiment from society that stronger internal control environments are needed to prevent material fraud and unexpected company failures.

As part of this guidance, the board should monitor the company's risk management and internal control and, at least annually, carry out a review of their effectiveness, and report on that review in the annual report. IT controls are among the most important elements of daily business operations, and not only for effective compliance, and security.

With technology environments becoming more complex, it is important for senior management to demonstrate they understand how these core controls are implemented across the technology estate, how their effectiveness and suitability is being monitored and how they can support compliance.

The focus from IT Internal Audit should be to address core technology and cyber risks, and assure controls designed to safeguard the confidentiality, integrity, and availability of information. All aspects of the technology estate are important to consider, including business-critical applications, databases, operating systems, wider infrastructure, as well as core IT processes defined under frameworks such as COBIT, ITIL and ISO etc.

What's new?

- Many organisations have started considering their roadmap towards stronger internal controls, and we see many Internal Audit functions seeking to undertake both a gap analysis and readiness assessment. As such, the concept of integrated assurance over technology enabled, automated, and core manual business process controls around business-critical processes will be of increased importance.

- Only a few Internal Audit teams have started to move away from solely thematic IT internal audit reviews to dedicate time on the plan to business-critical IT controls. Teams that do dedicate this time are finding new issues, previously never understood, that have been remediated ahead of potential business failure. IT failures can arise from any system across the estate. When assessing the root cause for IT failure it can often be traced back to the interconnections between systems breaking down, or the reliance on legacy, heavily customised, out of support infrastructure components or applications. The many interfaces between systems in today's world can easily cause a business issue in a short amount of time and having robust controls in place, with continuous monitoring, can help a business become more resilient.

- Organisations are utilising industry good practice frameworks such as COSO, COBIT, ITIL, ISO27001 and NIST, to drive the initial design or improvements on their key process and controls. They are also using these to report progress on their maturity to stakeholders, including to the board and sub-committees.

6 * * Business Critical IT Controls (continued)

What should Internal Audit be doing?

- Whilst Internal Audit functions will be a key stakeholder for the new proposed controls regulation and a rich source of information and insight, we believe they should not be tasked with implementation but should instead assist organisations with readiness by helping to bring challenge and drive accountability. Functions should continue to have a role to play in:
  - Challenging management's financial risk assessment, to show the breadth of areas likely to be in-scope
  - Help agree the in-scope IT systems. Failure to identify in-scope systems early enough is still one of the top causes of non-compliance with US SOX as it leaves insufficient time to assess essential IT controls. As part of that, it is important to assess the complexity of the IT environment (e.g. 'shadow IT', multitude of relevant systems, third-party dependency etc), the architecture, and interdependency of relevant controls.
- Internal Audit should be looking to understand the technology estate at their organisation, how it is structured from a process perspective and how the technology landscape is designed. Given the dependency on technology to run business-critical processes many technology controls are automated and embedded within systems themselves (e.g., configurations, tolerances and limits, segregation of duties, enabled/ disabled functionality etc).
- Internal Audit should establish and apply a risk assessment and audit planning process that ensures suitable risk-based cyclical coverage across business-critical technology areas. Using industry recognise frameworks, or regulatory guidance (for example, in the case of the FS sector, EBA guidelines on ICT and the Technology Risk Taxonomy) Internal Audit can assess the technology function's maturity within defined process areas to help the organisation keep pace with industry standards and expectations.

7 ◀▶ (7) Third-Party Risk Management

Audit Planned %	Min % of Audit Plan Days	Max % of Audit Plan Days	Use of Analytics %
55%	7%	50%	36%

Why is it important?

In an increasingly digital world, organisations are reliant on third-parties to manage core business and IT processes and drive growth. Our latest third-party risk management (TPRM) survey revealed a growing level of organisational interest and focus on third-party risk management by executive leadership and members of the board. Alongside benefits such scalability, efficiency gains and cost optimisation, outsourcing has expanded the universe of risks organisations can be exposed to. This now encompasses domains ranging from operational to cyber and business continuity to sustainability risk and, if critical services fail, this could affect financial stability or cause harm to consumers. The need to develop more resilient supply chains was highlighted during the pandemic and it continues to be a priority for organisations.

Regulators have provided more clarity over third-party risk regulations in 2022, providing increased direction for firms operating via intra-group arrangements, focus on governance and senior executive accountabilities, greater linkages to third-party management and operational resilience across group level entity structures and heightened data security requirements, including use of the cloud.

7 ◀▶ (7) Third-Party Risk Management (continued)

What's new?

- **Managing third-party resilience:** Organisations recognise the need to improve the resiliency of their supply chains. This need is particularly strong for critical third-parties and lower tiers of the third-party ecosystem (i.e., beyond those with direct contractual relationships). The focus on resilience has emphasised the relationships with critical cloud service providers (CSPs). It has also underlined the importance of developing capabilities to manage evolving challenges, such as traceability and geographic concentration risk.

- **Integrated/holistic third-party management:** Executive leadership and members of boards aspire to implement a more integrated approach to TPRM that leverages synergies across third-party management processes. Consequently, integration of contract/legal management processes with TPRM appears to be a common initial milestone on this journey.

- **Key post-pandemic TPRM trends:** Increased leadership focus and investment in TPRM continues to drive transformational change. This is characterised by smarter third-party segmentation and integrated technology solutions that improve efficiency and reduce cost.

- **Regulatory focus:** While financial services Internal Audit functions will already be aware of a number of regulatory requirements, there have been significant new regulatory developments in 2021/22 on third-party risk that have broadened requirements for firms.

7 ◀▶ (7) Third-Party Risk Management (continued)

What should Internal Audit be doing?

- Internal Audit should consider if the firm has an *adequate Outsourcing* and *Third-Party Risk Management (TPRM) framework* embedded across the business.

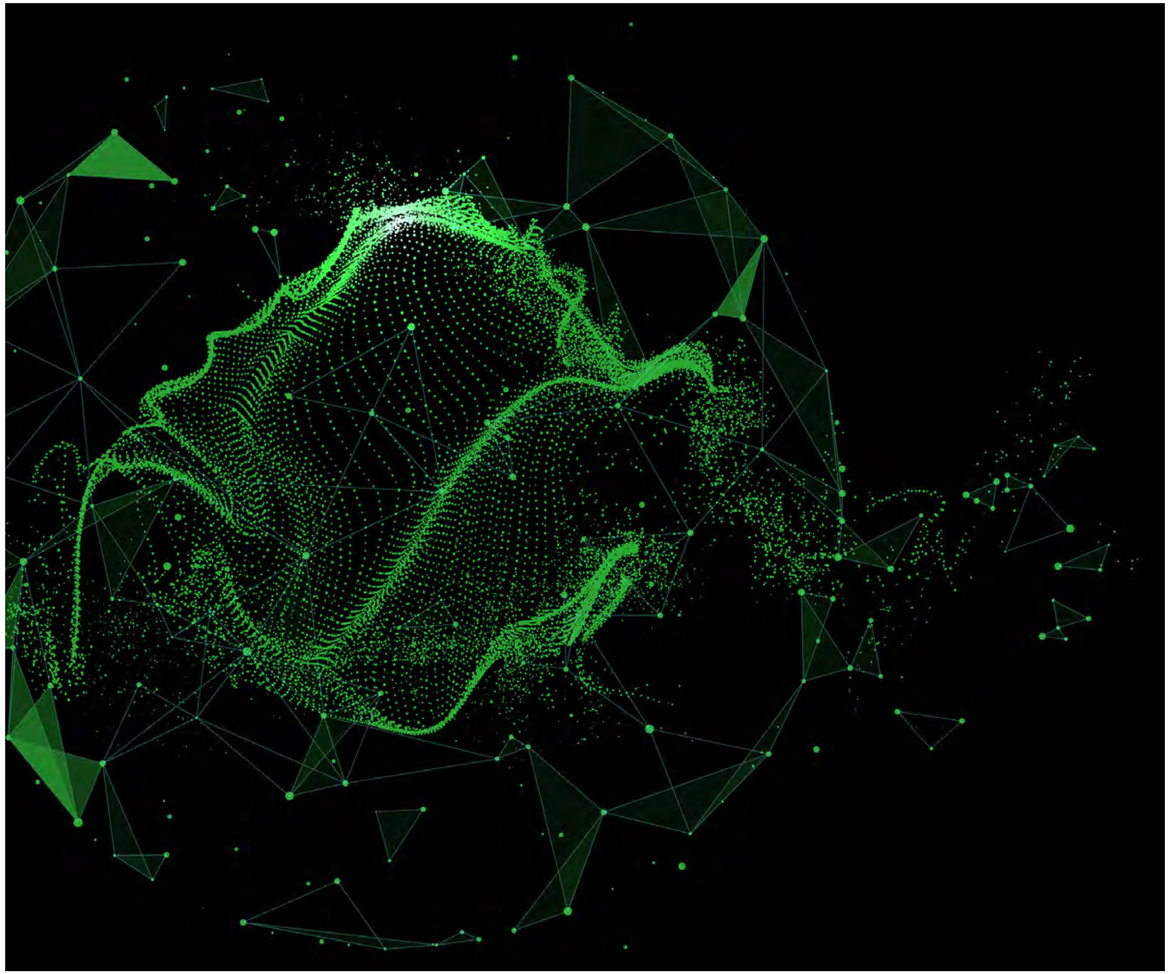
- Assess how organisations are obtaining assurance on third-party resilience via periodic reviews of third-party business continuity plans and assessing their level of alignment with organisational business continuity plans. One of the evolving considerations in such reviews is the need to 'scenario stress test' existing third-party relationships and their business continuity plans. In addition, evaluating exit plans to cover stressed and unstressed exit scenarios, as well as establishing testing programmes for periodic testing of these processes and artefacts.

- Assess due diligence activities and robustness of ongoing monitoring in place. Especially with the increasing levels of dependence on Cloud Service Providers, together with the preference for engaging with a smaller pool of providers, functions should be looking into how management is assessing concentration risk.

- Assess adequacy of the overarching governance model, and clear allocation of roles and responsibilities to manage third-party risks throughout their lifecycle.

- Assess the appropriateness of metrics and reporting used consistently across the organisation to drive improved performance and to measure risk appetite and remain within tolerance thresholds.

- Given the increased regulatory scrutiny, particular focus should be given to understanding how the TPRM framework is designed to address resiliency requirements, including around subcontracting risk and digital risk. For example, Internal Audit should be looking into how management is utilising tools that enable access to real-time information to supplement the more traditional 'point-in-time' data that is collected.



7 ◀▶ (7) Third-Party Risk Management (continued)

Sector perspectives:

Financial Services

- His Majesty's Treasury (HMT) published a policy statement on 8 June 2022 proposing the approach to mitigate risks from critical third-parties, such as cloud-based service providers, to the UK finance sector. Under this proposal, HMT, in consultation with the financial regulators and other bodies, will designate certain third-parties that provide services to firms as "critical". Once a third-party service provider has been given a 'critical' status, the financial regulators can exercise a range of powers over the provider.

- The Financial Conduct Authority (FCA), in collaboration with Bank of England and Prudential Regulation Authority's (PRA's), published a joint discussion paper on 21 July 2022 to set out potential measures to oversee critical third-parties in a move to increase resilience of the financial services sector. This paper proposes an oversight regime for the supervisory authorities to set resilience standards, a testing approach, and enforcement powers for Critical Third-Parties. The responses will be used to inform a consultation in 2023.

- The PRA's Supervisory Statement (SS) 2/21, 'Outsourcing and third-party risk management', was published in March 2021 and has come into effect since 31 March 2022. The statement makes it more explicit that firms are expected to assess the risks and materiality of all third-party arrangements, including those that do not fall within the definition of 'outsourcing' and have clearly articulated that materiality, outsourcing and risk must be independently assessed and considered as part of a proportionate and risk-based approach.

- As per 2022 FCA Business Plan, there is an increased focus on improving oversight of Authorised Representatives (AR). An AR carries out regulated activity under the responsibility of an authorised firm. The authorised firm (the Principal) is responsible for making sure that the AR is fit and proper and complies with rules. The FCA is consulting (CP21/34) on changes to their current regime and the final rules were published during August 2022 via Policy Statement (PS) 22/11 with implementation due in December 2022.

- Internal Audit should consider if the firm has an adequate Outsourcing and Third-Party Risk Management (TPRM) framework embedded across the business, and assess adherence to key regulatory requirements, including the

  – FCA's SYSC 8.1 general outsourcing requirements;

  – FCA's Senior Managers and Certification Regime;

  – PRA's SS2/21 Outsourcing and third-party risk management; and

  – Outsourcing guidelines published by European Banking Authority, European Securities and Markets Authority and others.

Corporates and Public Sector

- Organisations have made incremental improvements to the way they manage third party relations, from an efficiency, cost effectiveness and decision-making perspective. Hindered by functional silos and decentralised systems, they aspire to develop a more holistic and integrated approach. Greater alignment between risk management and legal and contract management processes represents a critical milestone in the journey towards fully integrated third-party management.

8 ◀▶ (8) IT Strategy and Governance

Audit Planned %	Min % of Audit Plan Days	Max % of Audit Plan Days	Use of Analytics %
63%	7%	28%	8%

Why is it important?

IT Strategy remains a significant area of focus, particularly as the economic and social shifts of the last two years continue to upend operating models of organisations across all sectors.

With the continued trend to digitise, the increasingly important role of automation, the move away from manual processes, and the acceleration of change delivery, this has placed a greater importance on operations and decisions being made by IT. Therefore, the need to have effective, streamlined IT governance, with the right capabilities and experience is more important than it has ever been before.

Businesses rely more heavily on IT than ever before and ensuring that IT can create the value that the business requires to grow and prosper is critical. Organisations who fail to keep their foundations up to date, and business friendly, are finding that they cannot pivot quickly enough or harness the benefits that technology should provide to the business, customer facing teams, but also support/operational functions.

What's new?

- Over the course of 2022 it has been difficult for IT organisations to attract and retain the necessary talent due to the rise in demand for IT and digital skills across the economy. This in turn has influenced the ability for IT to support the increasing demands that are now made typically across business functions who are seeking the support of IT to further business strategies. We have seen a rise in the number of functions looking to automate and/or outsource operations due to the supply issues in the market.

- Some businesses have started to move away from the concept of having separate strategies for technology and business aims. These organisations are now producing corporate strategies which include digital and technology components as a core integrated element of the main strategic outputs.

- As more parts of the business look to technology to enhance operations it is becoming more important for IT to have governance that allows the business to interact and engage with IT. Never has it been more important to ensure that core IT disciplines are in place and operating effectively. Notable focus areas include having an up-to-date enterprise architecture, as well as effective demand, asset, change, and release management processes. More organisations are revisiting these areas to ensure that IT is built on a solid, business-aligned, foundation.

- From a governance point of view, challenges remain around management of IT risk holistically, including 'shadow IT', Key Risk Indicators (KRI) and, reporting, as well as the ownership of IT controls, to name a few. In the face of accelerated strategic change, the pressure to digitise, automate the IT control environment, and establish continuous controls monitoring procedures, will only increase.

8 ◀▶ (8) IT Strategy and Governance (continued)

What should Internal Audit be doing?

Harmonisation of IT and Business Strategies

- Internal Audit's role to assess and challenge IT governance and strategy continues to remain important following the increased digitisation of business service delivery following recent global events. Internal Audit should continue to examine whether processes and practices followed to set IT strategy, and provide appropriate governance and oversight, continue to be aligned to the needs of the business.

- In an increasingly digital world, having a separate business and IT strategy looks like an outdated methodology for the delivery of corporate strategy. Internal Audit should continue to play a key role in monitoring strategy setting processes and whether these are fit for purpose in the digital age, and adequately consider emerging technologies.

- Internal Audit should look at how successful IT has been previously in delivering on strategies set and how the achievement of strategy is being monitored in the present to demonstrate delivery.

IT Foundations

- Internal Audit should assess whether IT has solid foundations in place that support effective IT and wider business demands and execution.

- Areas that Internal Audit should explore include enterprise architecture, shadow IT, and demand, asset, change and release management. Common frameworks that can help internal audit scope audits include COBIT 2019 and ITIL.

- Key questions to consider include:

  – Are the core IT disciplines in place to support the business in its growth ambitions? How does IT demonstrate these are in place and subject to regular review and improvement?

  – Does IT have a view of the technology architecture across the entire business, including shadow IT, and is this maintained and up to date?

  – Are IT foundations designed in a way to support the business needs and the pace for change?

  – Can the benefits from technology be demonstrated and measured?

Agile and Lean Project and Portfolio Management

- Internal Audit should examine whether emerging schools of thought in relation to Agile and Lean portfolio management are being adopted when setting strategy.

- Use of product and value chain orientated expenditure decisions may be desirable, and wider Agile principles around portfolio planning and expenditure should also be considered. Consideration of scaled agile models in the delivery of the strategic level of the value chain (SAFE for example) may also be desirable to apply the relevant levels of governance.

9 * * Identity and Access Management/Privileged Access Management

Audit Planned %	Min % of Audit Plan Days	Max % of Audit Plan Days	Use of Analytics %
53%	2%	60%	78%

Why is it important?

One of today's biggest cyber security risks is privilege misuse, which frequently causes high losses and may place companies in danger of failure. It's also one of the most widely used attack vectors by hackers since, if successful, it allows free access to an organisation's information and data, frequently without raising any red flags until the damage is done. Key personnel of every company have access to vital business applications. These applications' login credentials must be carefully safeguarded as they contain important information and data, and illegal access may cost the company a significant amount of money.

While business privileged user accounts are frequently given to specific people, many other privileged account types are typically shared by several administrators. This popular tactic presents a number of challenges:

- It can be difficult to hold each person accountable for the actions they take using the privileged account.
- Local administrator accounts frequently share the same password throughout a platform or the entire organisation due to weak password management.
- Account deprovisioning can be overlooked where local admin accounts are created for maintenance which are often not deleted, which leaves the accounts open for attackers to exploit them.

The more privileges and access a user, account, or process amasses, the greater the potential for abuse, exploit, or error. Particularly, this issue can be seen for legacy systems which are at times unable to be brought into a single Privileged Access Management (PAM) solution due to lack of system functionality and vendor support. Reducing the legacy footprint within the IT infrastructure will drive down the opportunity for threat actors to target these types of system/accounts, which if exploited, could lead to the unavailability of critical systems.

What's new?

Digital transformation is expanding the privileged attack surface across new privileged threat vectors from Internet of Things (IoT), DevOps, and cloud environments and use cases, for example:

- Despite the pervasiveness of IoT, IT teams still struggle to discover and securely onboard legitimate devices at scale. Compounding this issue, IoT devices commonly have severe security drawbacks, such as hardcoded, default passwords and the inability to harden software or update firmware. Furthermore, they may not have enough processing capability on which to run Anti-virus (AV) software. PAM has a pivotal role to play in IoT.
- The DevOps emphasis on speed, cloud deployments, and automation presents many privilege management challenges and risks such as organisations may lack visibility into privileges and other risks posed by containers and other new tools. Inadequate secrets management, embedded passwords, and excessive privilege provisioning are just a few privilege risks that are widespread across typical DevOps deployments.
- AWS, Microsoft 365, Google Cloud etc. provide nearly boundless superuser capabilities, which enables users to rapidly provision, configure, and delete servers at a massive scale. Within these consoles, users can spin-up and manage virtual machines. Organisations need the right privileged security controls in place to onboard and manage all of these newly created privileged accounts and credentials at massive scale.

9 * * Identity and Access Management/Privileged Access Management (continued)

What should Internal Audit be doing?

- Internal Audit functions need to review the PAM policy, approach taken, and ensure the solution is fit for purpose and meet the requirements of the company. The company may include pragmatic processes of provisioning/de-provisioning, identifying privileged accesses, procedure on approval/dismissal of privileged access requests, amongst other processes.

- Internal Audit should also review the approach taken to deploy a PAM solution, so that it is designed to suit the company.

- The function should review and assess if all privileged accounts are under one repository. It is always viable to keep privileged accounts under a single repository as this helps in governing the access. Also, once the function starts to review the accounts, the team may start identifying privileged accounts, which are dormant and/or orphan accounts. Internal Audit should take necessary measures to highlight these accounts to the organisation as they may provide a gateway to potential attacks.

- Internal Audit should assess if the organisation is regularly monitoring privileged accounts. Although privileged accounts are secured, they should be subject to constant monitoring and audits. This gives the organisation a clear picture of who is accessing the account and immediately prompts them if there is a suspicious activity.

- Internal Audit should assess if there are any compliance requirements for the organisation to implement a PAM solution as part of a comprehensive security and risk management strategy.

- Internal Audit should assess what strategic plans are in place for organisations that continue to use legacy systems such as Zero Trust Privilege that builds on traditional legacy PAM by enforcing a 'never trust, always verify, enforce least privilege' approach.

- Internal Audit should assess what Cyber Threat Intelligence the organisation receives covering new PAM risks/threats, which is relevant to the organisations sector, and what (if any) mitigating controls can be applied to the PAM solution.

- As part of PAM migration activities, some accounts can only be managed in a static way, i.e., onboarded to a PAM tool but passwords are not automatically changed after use possibly due to application limitations or hard coding of scripts etc. and the Internal Audit team should take this into account when assessing migration plans and actions.

One of today's biggest cyber security risks is privilege misuse, which frequently causes high losses and may place companies in danger of failure...

10 ▼ (6) Digital Risk: Artificial Intelligence

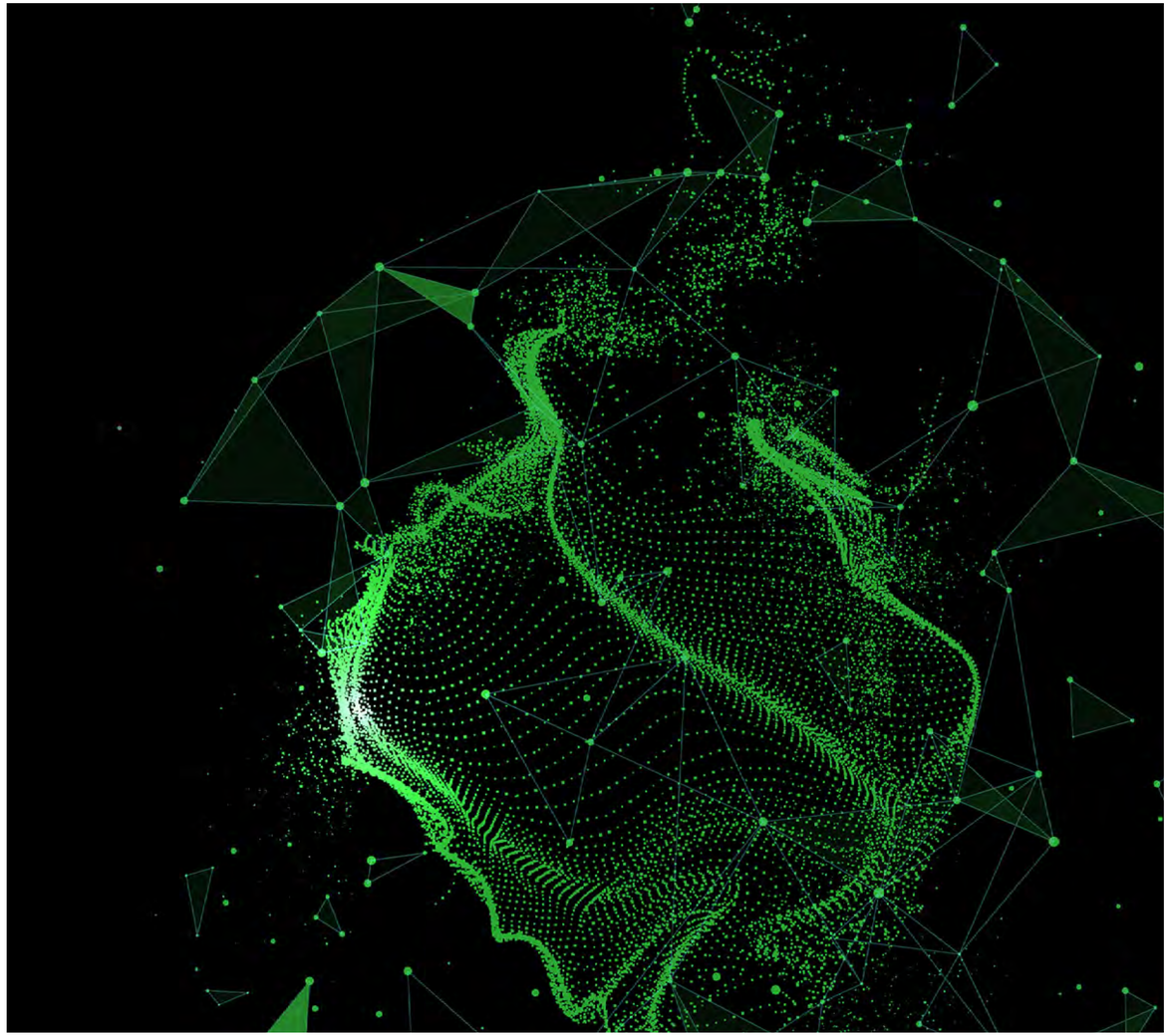
Audit Planned %	Min % of Audit Plan Days	Max % of Audit Plan Days	Use of Analytics %
25%	19%	31%	100%

Why is it important?

Organisations' adoption of Artificial Intelligence (AI) is growing rapidly, with companies seeking to capture the opportunities and value associated with AI. As organisations start to realise these benefits, alongside the improvement of AI systems functionality and reduction in their cost, it is expected that the rate of AI adoption will continue to increase. However, with opportunity comes risk, specifically that AI systems make decisions which lead to sub-optimal outcomes or unethical decisions which are not aligned with an organisation's values.

There are also serious considerations around the processing of personal data, ethical training of AI systems and the requirement for transparency, human oversight, and accountability. Public consciousness of these risks, and the associated risk of severe reputation also impact, is driving organisations to better understand their usage of AI.

Organisations' adoption of AI is growing rapidly, with companies seeking to capture the opportunities and value associated with AI.



10 ▼ (6) Digital Risk: Artificial Intelligence (continued)

What's new?

- There has been a notable increase of adoption of AI technology; as well as an increase in the complexity of algorithmic decision making by AI systems.
- More "off the shelf" AI solutions are available in the market, such as CV screening tools. These solutions can act as a "black box" whereby the underlying algorithms are not accessible to the organisation using them.
- The availability, and reduction in cost of AI systems can lead to 'shadow AI' existing in an organisation, whereby IT, Security and Risk are not aware AI systems are being used.
- There is increasing awareness from the public of the ethical risks associated with AI which is leading to organisations taking steps to understand their use of AI systems and put in place processes to ensure AI is used responsibly.
- Decision making over the trade-offs associated with AI use, for example between privacy and personalisation, is being defined by organisations with ownership and accountability of these decisions being discussed at board level.
- To ensure transparency of customer impacting decision making, some organisations are turning towards a human centric AI approach. "Human in the Loop" AI is becoming common place in high risk areas.
- The regulatory landscape for AI is emerging. Various guidance and frameworks exist (e.g., Alan Turing Institute, ICO, NIST) but the approach to regulation is still being worked through globally. The widely anticipated finalisation of the European Commission's Artificial Intelligence Act (AI Act) is expected in the coming year and when passed into law, it is positioned to function as a new global standard for AI regulation, given its extraterritorial application, with a newly founded enforcement body expected to operate in a similar fashion to the GDPR oversight operation. It aims to introduce a common regulatory and legal framework for artificial intelligence, with a scope that encompasses all sectors, and to all types of artificial intelligence. The proposed regulation classifies artificial intelligence applications by risk and regulates them accordingly.

There has been a notable increase of adoption of AI technology; as well as an increase in the complexity of algorithmic decision making by AI systems.

10 ▼ (6) Digital Risk: Artificial Intelligence (continued)

What should Internal Audit be doing?

- Naturally, the rate of adoption of disruptive technologies may be different for each company, and the approach and maturity levels of each Internal Audit department to respond to the risks posed will vary. The challenge remains however: auditors need to accept that the business will be 'disrupted' and need to stay ahead of how to deliver quality reporting, insightful assurance, and impactful advice.
- Check the organisation has a strategy for AI adoption, with appropriate governance processes to identify and manage the risks associated with AI usage.
- Work with the technology and risk functions to support the use of appropriate controls over the use of AI, and any underlying tools and technologies used to support AI.
- Where appropriate, especially regarding the use of "high risk" AI, Internal Audit functions should start incorporating such technologies into their Audit Universe. Periodically plan and validate that AI systems being used are in line with appropriate control standards, and in an ethical manner, commensurate to the organisation's objectives and risk appetite.
- Support the organisation in terms of raising awareness for both the opportunities and risks associated with AI usage.
- Evaluate as to whether the organisation is prepared to comply with expected regulation.

Financial Services

- The pace of adoption of AI by Industry players is closely related to the nature of services they provide.
- We see the application of Artificial Intelligence technologies rapidly transforming financial services organisations. They reshape business models and enable innovation in terms of productivity and operational efficiency and, critically, in the way they connect with, and offer products and services to, their customers.
- Where AI is already in use, we see organisations (including Internal Audit functions) quickly maturing their understanding and their own capabilities in this area, by building processes and frameworks to better managed associate risks.

Corporates and Public Sector

- Industries such as healthcare and public sector have large ambitions for the use of AI due to their scale and impact on society. In turn they are making significant investment in controls and insights (such as focus groups) to help navigate appropriate use of AI in their services provided.
- Technology organisations are often deemed as leaders in this area and find themselves under scrutiny for using AI and are making investments to help build societal trust in areas where AI use cases benefit society.

11 ▼ (9) Payments (Financial Services)

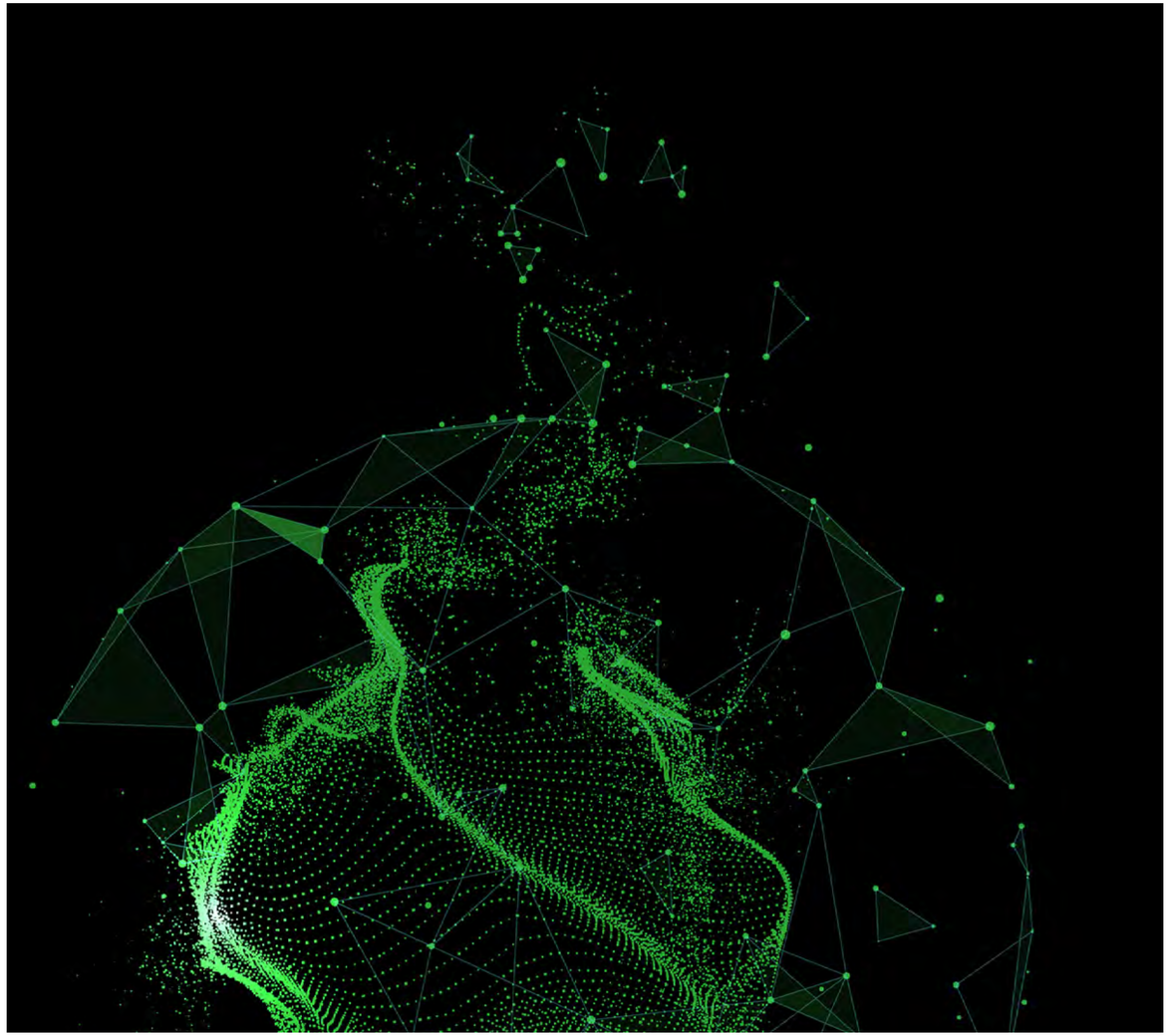
Audit Planned %	Min % of Audit Plan Days	Max % of Audit Plan Days	Use of Analytics %
50%	16%	28%	100%

Why is it important?

Significant technology, regulatory and infrastructure developments are driving major change, growth and innovation in payments. There is significant regulatory focus across a variety of areas for both incumbents and new providers, where there is significant potential to expand into new markets (for example, payments are being increasingly intermediated by BigTech and other non-traditional parties). Fees are also being reduced through regulation and competition and banks' historic data advantages are being diminished by Open Banking and the Payment Services Directive 2 (PSD2), with this set to increase with the future introduction of Open Finance.

At the same time, growth in the payments industry is increasing at a significant rate and interoperability is increasing through use of common standards which are also delivering richer data. There are also fundamental infrastructure changes occurring, requiring structural changes to the payment ecosystem, and requiring changes to the payment plumbing and data flows for ecosystem participants.

Significant technology, regulatory and infrastructure developments are driving major change, growth and innovation in payments.



11 ▼ (9) Payments (Financial Services) (continued)

What's new?

ISO 20022

- The ISO 20022 messaging standard is replacing the existing SWIFT messaging standard. From November 2022 SWIFT messages will start to be replaced for cross-border payment and reporting messages.

- In the UK, this is also impacting CHAPS payments, where the Bank of England is moving to a new Real Time Gross Settlement (RTGS) system utilising ISO 20022. Direct participants in CHAPS have been required to start sending messages in the new format from June 2022 and use the full enhanced message set from February 2023. The Bank of England is continually assessing CHAPS participants' readiness for these key dates.

- There will be further impacts for other payment types through the future introduction of the New Payments Architecture (NPA). Other non-UK high value payment schemes will also be migrating and will have their own deadlines for this, e.g. November 2022 for TARGET2 (the RTGS system owned and operated by the Eurosystem) and Euro high value payments. Indirect participants will also be impacted and will need to discuss with their provider as to what steps they must take.

Strong Customer Authentication/Transaction Risk Analysis:

- Mandatory annual audit requirements persist around Strong Customer Authentication (SCA), with this now having gone live in the UK from March 2022, bringing e-commerce transactions into scope. All Banks and payment service providers (PSPs) should be utilising SCA for payment transactions.

  In addition, an increasing number of banks are now adopting Transaction Risk Analysis (TRA) which requires fraud rates to be below a certain level for a bank to exempt the usage of SCA. SCA requirements apply across any channel offering access to 'payment accounts' (including cards) across any customer segment (i.e., Retail, Business, Corporate, Private Banking etc.)

- The scope of the audit requirement extends across all electronic customer channels, such as internet banking, mobile apps, firm provided software, enterprise software integrations, other software integrations embedded through Application Programming Interfaces (APIs) or other interfaces, and 'Open Banking' channels.

There will be further impacts for other payment types through the future introduction of the New Payments Architecture (NPA).

11 ▼ (9) Payments (Financial Services) (continued)

What should Internal Audit be doing?

ISO20022

- Internal Audit should perform a detailed review of ISO 20022 programme activities to ensure that regulatory deadlines will be met and how changes to adopt the new messaging standard are being implemented and tested. Additional investigation may also be performed to determine how enriched messaging data may provide key benefits and how these are realised.

- ISO 20022 migration is inherently complex, posing significant challenges for impacted firms, in particular Internal Audit should understand the controls in place around the following areas:

  - Appropriate training is in place for the new messaging standard.

  - Upgraded messaging appropriately interfaces to the new standard.

  - Robust and detailed testing of In-flow translations, including the receipt of multi-format messages takes place.

- The impact on banks will be significant across business operations and technology stacks which will require careful and comprehensive consideration with significant pressure being placed on technical resources.

Strong Customer Authentication/ Transaction Risk Analysis:

- Both SCA and TRA must be audited annually by operationally independent internal or external auditors. The audit should include an evaluation and report on the compliance of the firm's security measures with the Regulatory Technical Standard (RTS) requirements, and the report must be made available upon request by the Financial Conduct Authority (FCA).

- For the first year when TRA is adopted, and every three years thereafter, the audit must be performed by an independent external auditor. (i.e., Internal Audit can only perform this work in intervening years).

5

Where next for internal audit?

Looking ahead, the breadth of demands on Internal Audit functions, and the pace and scale of innovation in the profession, point to the need for an update of our vision of the Internal Audit function of the future. We call this Internal Audit 4.0 (IA 4.0).

Ongoing disruption is here to stay:
We have all moved beyond "change is the only constant" to an environment of ongoing disruption. Over recent years we've observed several key lessons from functions who have successfully embedded a culture of continuous improvement and innovation, and our updated IA 4.0 framework brings three new features to the forefront.

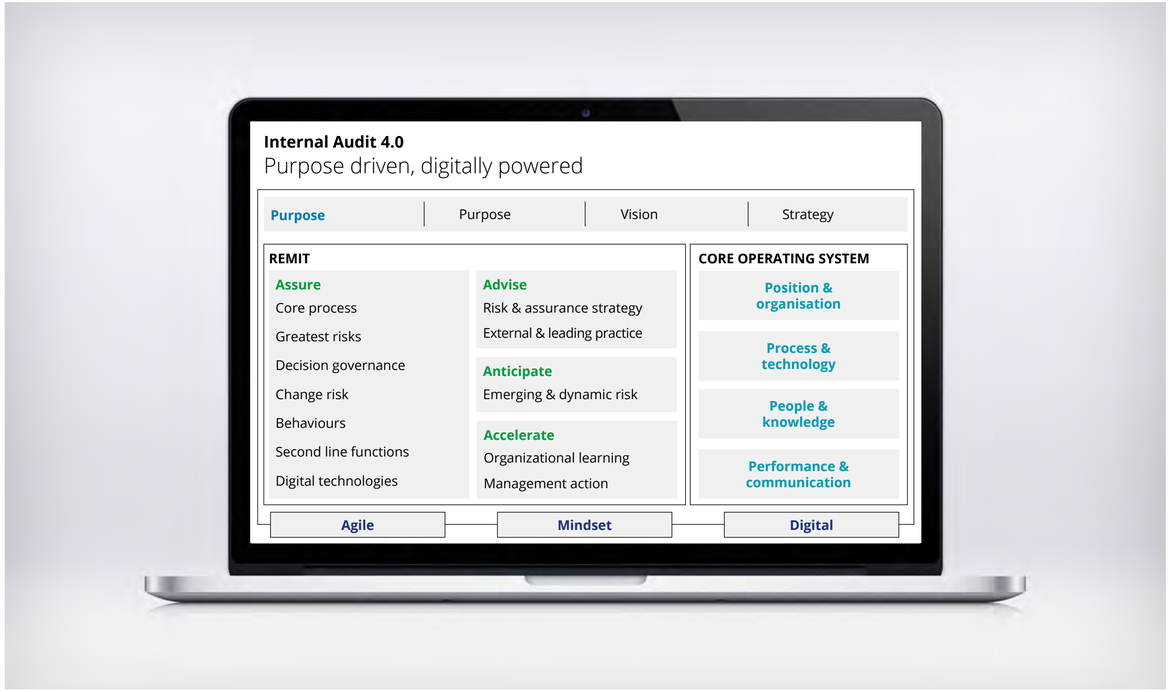
By aligning Internal Audit's outcomes with the organisation's purpose, helping accelerate organisational change and learning, and further embracing digital and technology enablement, we believe Internal Audit can upgrade and maximise its impact and the value it delivers.

We believe the next evolution Internal Audit is for it to be purpose-driven and digitally powered. A high-level diagram of the refreshed model can be found right.

You can read more about the Deloitte perspectives on the function of the future and our 4.0 framework in the recently released publication that can be found on our website[2].

We believe IA should embrace digital-enabled transformation, foster innovation, explore the power of automation and analytics, as a way of decreasing costs, embedding agility, and adding value. A deeper digital transformation and the use of data-driven auditing will not be merely required by Audit Committees as a nice-to-have, but in our view, would be core for the development of a resilient and a high functioning function of the future.

[2] Deloitte Internal Audit 4.0 | Purpose driven, digitally powered: Internal Audit 4.0 | Deloitte Global



6

Appendices

Appendices

A. 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 cross the industry.

We surveyed senior audit professionals from 66 organisations, and for the first time the survey was not focused on the financial services sector only but was extended to the wider private sector as well as the public sector. **Figure A** illustrates the sectors, and sub-sectors of respondents.

The size of functions in the companies we surveyed ranged from than 10 full-time equivalents to those with over 200; **Figure B** captures this breakdown.

The roles of the professionals that we interviewed consisted mainly of the Heads of IT Internal Audit, but where appropriate, we 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 May and July 2022. 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

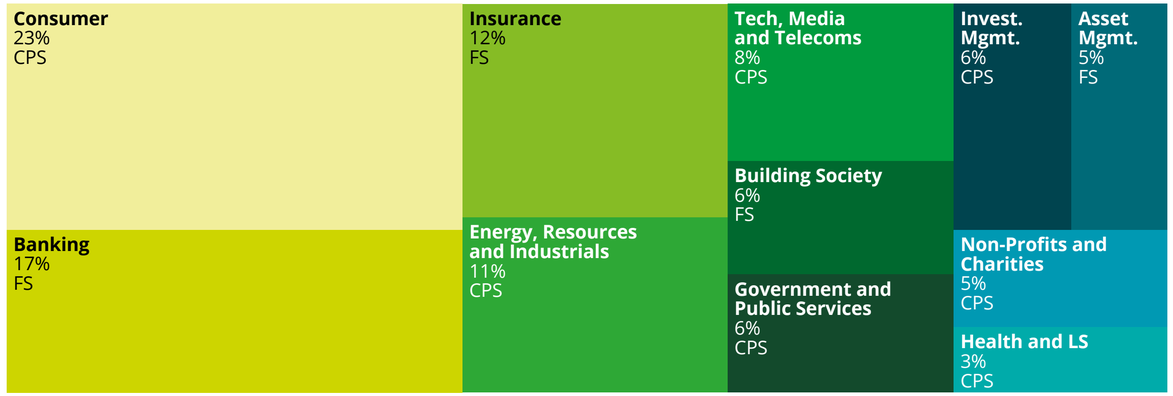
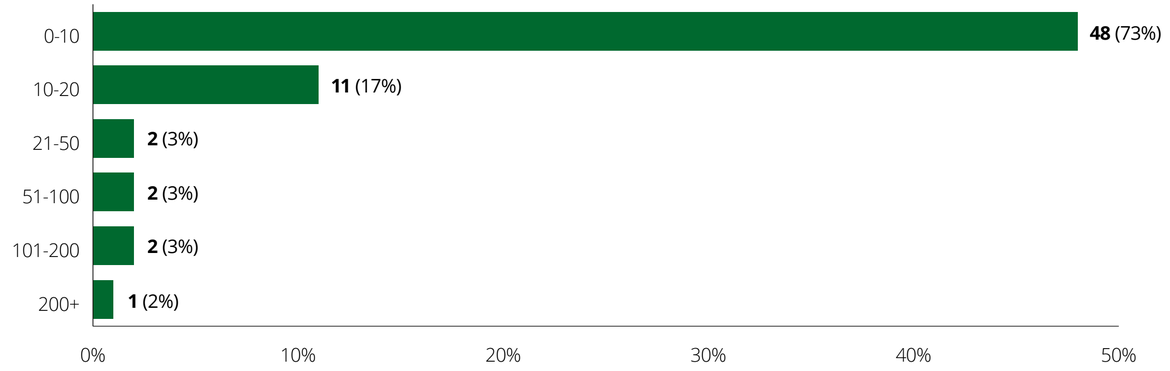


Figure B. Demographic split of survey respondents by FTEs in the IT Internal Audit function

Number of IT internal audit FTEs



Appendices (continued)

B. Additional sources and references

01. Cyber Security

- Future of cyber survey: Deloitte Future of Cyber survey | Global
- Deloitte CISO programme: Deloitte CISO programme | Deloitte UK

02. Digital Transformation and Change

- Tech Trends 2022: Tech Trends 2022 Deloitte

03. Data Governance

- Do businesses require additional support to construct and deliver on data governance?: Effective data governance | Deloitte Insights
- Data governance for next-generation platforms: us-big-data-governance.pdf (deloitte.com)
- Modernising data infrastructure with data management tools, the CFO guide to data management strategy: Data Management Strategy | Deloitte US

04. Cloud Hosted Environments

- Closing the cloud strategy, technology, and innovation gap | Deloitte Future of Cloud Survey Report: Future of Cloud Strategy Survey Report | Deloitte
- Taking a Cloud Journey Without Risky Detours: Taking a Cloud Journey Without Risky Detours (deloitte.com)

05. Operational and IT Resilience

- Operational Resilience: The opportunity for Internal Audit to support Operational Resilience implementation: Operational Resilience: The opportunity for Internal Audit to support Operational Resilience implementation | Deloitte UK

06. Third-Party Risk Management

- Emerging stronger: The rise of sustainable and resilient supply chains | Global third-party risk management survey 2022: Third Party Risk Management Survey 2022 | Deloitte UK

07. IT Strategy and Governance

- Tech Trends 2022: Tech Trends 2022 Deloitte

08. Identity and Access Management/ Privileged Access

- Future of cyber survey: Deloitte Future of Cyber survey | Global

09. Business critical IT controls

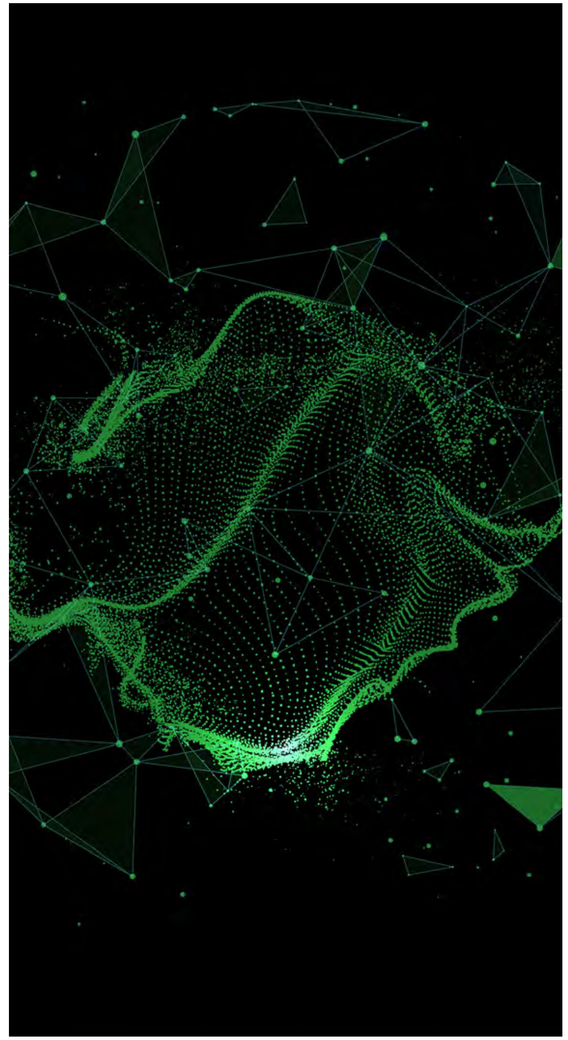
- Deloitte Future of Controls: Future of Controls | Deloitte UK

10. Digital Risk: Artificial Intelligence

- Tech Trends 2022: Tech Trends 2022 Deloitte

11. Payments

- Payments trends 2022: Payments Industry Trends | Deloitte US



7

Contacts

Contacts

Financial Services

Mike Sobers
Partner
Tel: +44 20 7007 0483
Email: msobers@deloitte.co.uk

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

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

Corporate and Public Sector

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

Pete Balmforth
Director
Tel: +44 11 3292 1894
Email: pbalmforth@deloitte.co.uk

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

Deloitte.

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

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

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

© 2022 Deloitte LLP. All rights reserved.

Designed and produced by 368 at Deloitte. J30182