Deloitte.

Confronting Uncertainty

2021 Hot Topics for IT Internal Audit in Financial Services

An internal audit viewpoint

Contents

Introduction

Welcome to our latest annual viewpoint on the information technology hot topics for Internal Audit functions in financial services. As in previous years, this is based on our survey and discussions over the past six months with Chief Internal Auditors and Heads of IT Audit across UK financial services organisations, who have openly shared their areas of focus and the organisational challenges in relation to their firms' technology control environment.

In early 2020 markets were climbing, innovation and technology disruption were at the forefront of CIO agendas, along with a drive for transformational, rather than just incremental, change. The arrival of the pandemic a few weeks later had significant implications for organisations and their technology agendas. Business disruption is not new, but this proved to be the toughest test of technology and operational resilience many organisations have ever faced. Thankfully technology functions were mostly able to move quickly to invoke contingency plans, upgrade infrastructure and, most importantly, adapt and 'enable' businesses to continue to service clients in innovative ways.

CIOs played significant roles, leading crisis plans, acting as 'change' agents, proving that there is a unique opportunity for technology leaders to step beyond a functional leadership role, and drive technology deep into the fabric of the business. COVID-19 will continue to have implications for businesses, driving them to accelerate the move from physical to virtual ways of operating. Technology leaders are expected to architect significant enterprise changes as part of the digitalisation programmes that touch on customer channels, products, and ways of working. These priorities are reflected in our paper, with this year's top-10 topics presented under a lens of "lessons learned" thus far.

The impact of digitalisation programmes is reflected by an elevated focus on cloud, digital risk and digital transformation topics. That said, Cyber continues to be the at the top of the list, not surprisingly perhaps, as organisations struggle to deal with a notable increase of attacks, at a time when the organisational set up has completely changed with the prevalence of remote and mobile working.

Operational resilience, now more than ever, is a key area of regulatory and business focus. Heads of IT Internal Audit need to look how management is planning to ride the uncertain times ahead and rebuild confidence for the future by ensuring their response is resilient, safeguards the welfare and well-being of people, and is able to adapt to demand and supply challenges.

"Operational resilience, now more than ever, is a key area of regulatory and business focus."

We hope this paper helps inform your risk assessment and planning process for 2021, while at the same time offering useful insights for your ongoing conversation with technology and business leaders in an era of unfamiliar challenges and emerging technology risks.

Mike Sobers,
Partner

IT Internal Audit Hot Topics through the years: 2020–2021

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

The continued presence of cyber security at the top of our list, particularly in the past 4-5 years cannot be ignored as well as the emergence of risks around the new, disruptive technologies enabling digital business models and transformation initiatives across FS organisations. Focus for IT IA functions in 2021 is expected to be on Operational and IT Resilience, Cloud, Digital Risk and Extended Enterprise / Supplier Risk. Cyber remains the key technology risk areas for organisations, with relevant threats increasing particularly during the COVID19 pandemic.

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

"Focus for IT IA functions in 2021 is expected to be on Cyber Operational and IT Resilience, Cloud, Digital Risk and Extended Enterprise / Supplier Risk."

Table 1. IT Internal Audit Hot Topics through the years: 2012-2021

	2021	2020	2019	2018	2017	2016	2015	2014	2013	2012
1	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Large Scale Change	Third-party management	Cyber Threat
2	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	Cloud Governance	Operational Resilience	Data Protection and Governance	Data Management and Data Governance	Data Management and Data Governance	Third-Party Management	Large Scale Change	Identity & Access Management and Data Security	Data Governance and Quality	Data Leakage
4	Extended Enterprise	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	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	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	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	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	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	System Development	Legacy Environments	Payment Technologies	Enterprise Technology Architecture	Digital and Mobile Risk	Payment Systems	Service Management	Cloud Computing	Social Media	Mobile Devices

IT Internal Audit Hot Topics 2021: A viewpoint[1]

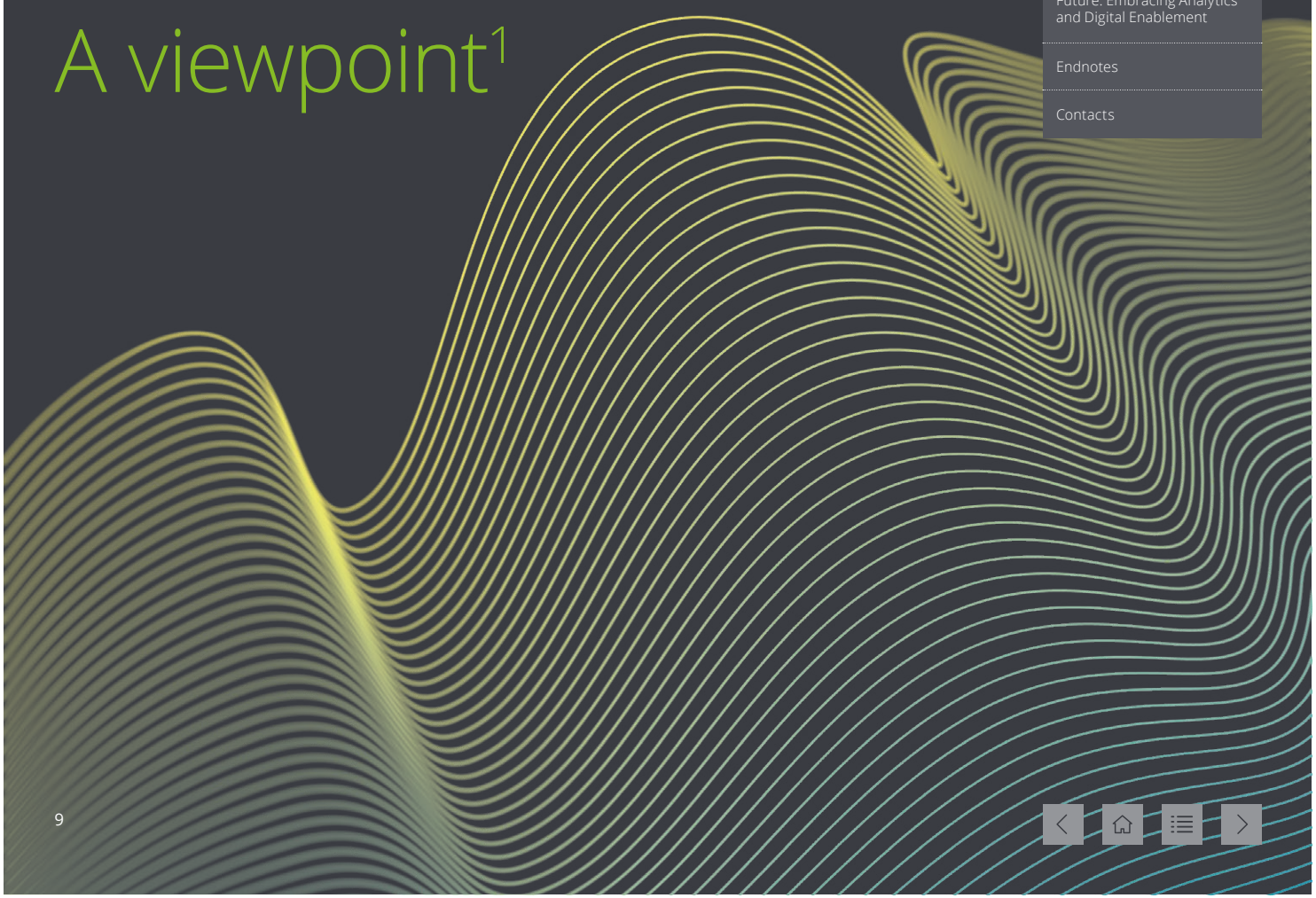
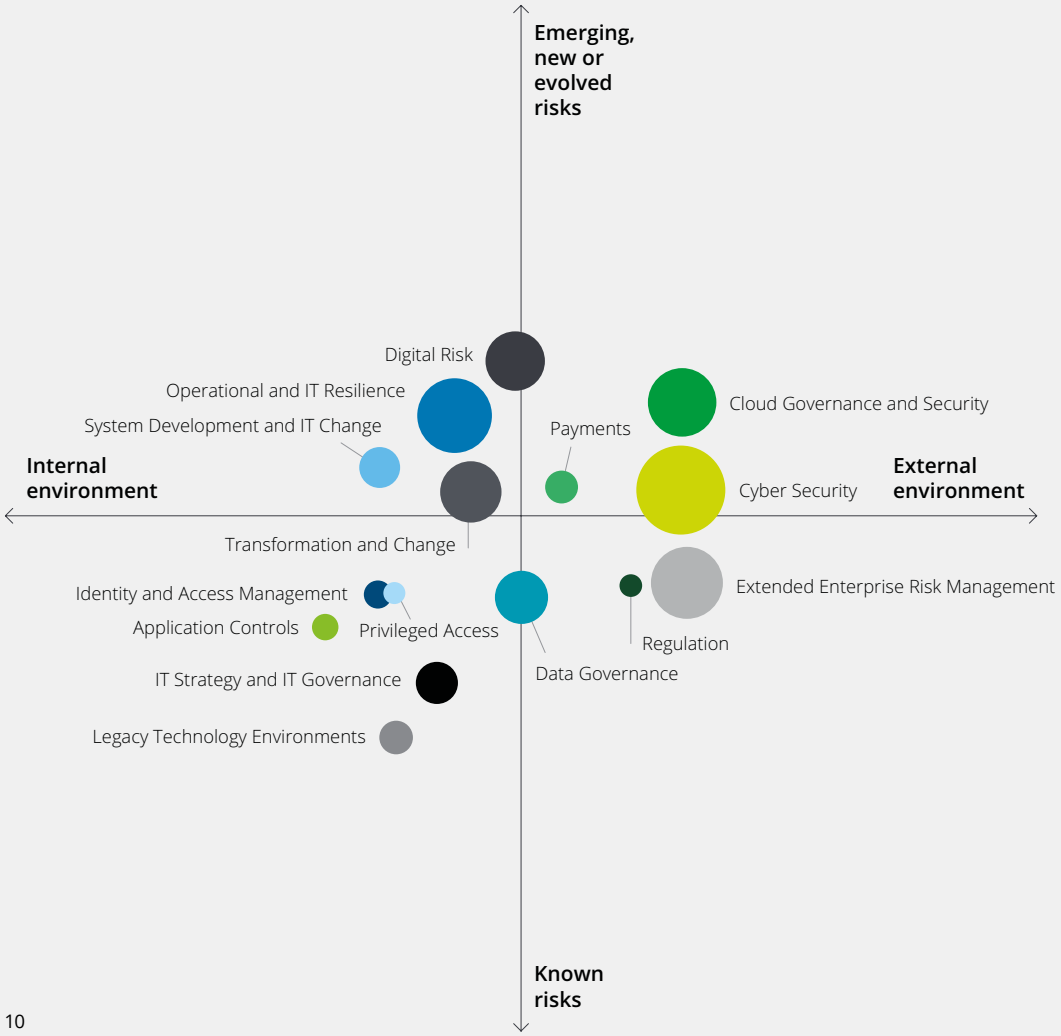


Figure 1. A Viewpoint – Classification of the Top-15 IT Internal Audit Hot Topics for 2021.
The size of the bubble reflects the ranking in this year's list, while the horizontal axis the threat environment (internal or external to the organisation). The vertical axis shows the range of emerging, new or existing risks.



1. Cyber Security (▶◀1)

Why is it important?

Cyber threats will likely remain one of the most frequent and potentially most damaging risks to organisations, and will continue to be one of the top agenda points for boards and Risk Committees in the financial services sector. We have seen cyber-attacks have increased significantly in the wake of the pandemic, with "phishing" emails connected to COVID-19 reported to have increased 600%. Security vendors are reporting significant spikes in attacks including scams, breaches, blackmail and email compromise.

What's new?

The COVID-19 crisis has also been characterised by a significant increase in fraudulent activity, including instances of social engineering fraud leading to identity theft. Cyber fraud flourishes when people are most vulnerable, or their personal, family or work circumstances are under significant change. The risk of unauthorised system access is also compounded as employees are forced to work remotely.

In addition, organisations have been facing a multitude of threats to their survival. Tough decisions have had to made, usually at pace and with limited information for staff regarding how they can continue to operate or service customers. For example how they provision IT resources to remote working staff, and how they continue to deliver core services (e.g. online and via digital channels). This has required existing control processes, on occasion, out of necessity, to be flexed or changed.

What should Internal Audit be doing?

The need for Internal Audit to continue to challenge management and provide advice on the optimal balance between adequacy of control, risk exposure and cyber risk appetite against business needs, will be paramount in 2021 and beyond. Functions should assess the maturity of their function and skills to cover cyber risk, whilst continuing to refresh the cyber audit plan in line with the threat environment and broader organisation risk assessment. We expect that some of the areas of focus for 2021 will be:

Remote working:

- Remote working heightens existing cyber risks while introducing new ones to organisations. It is an area that will continue to be a major focus as we move into the post-COVID-19, recovery phase. For example, in a household, multiple family members could be logging in on the same network, potentially exposing devices to malware that could then enter the firm's network if the right endpoint controls are not in place. In addition, we have seen a significant rise in the use of video conferencing facilities, some of which may have sub-optimal security standards, increasing threats to confidentiality and privacy.
- IA functions should review their businesses' remote working policy and security architecture, focusing on aspects such as: the need for work screens to be locked and laptops secured when not in use; Bring Your Own Device (BYOD) schemes; and other associated controls, such as the use of multi-factor authentication; etc. Additional areas of focus should be security requirements for wi-fi networks and device security measures such as personal routers and Virtual Private Networks (VPNs). Organisational controls around automated monitoring and alerting should be enabled - with alerts when corporate VPN is switched off for instance. There should be focus around capability of the Cyber operations teams being able to appropriately support and mitigate threats whilst working remotely.

Vigilance and Cyber risk awareness:

- IA functions should investigate approaches taken to increase the levels of cyber awareness across the organisation and look into the programmes to re-educate staff on cyber threats, or re-enforce key messages via CEO or CISO communication, for example. In an environment where malicious threat actors prey on emotions and uncertainty in an attempt to bypass training and rational thinking, the need for all employees to be alert to cyber issues and hyper-vigilant to phishing attacks is clearly high priority.

Resilience:

- Functions will need to be able to support the increased reliance on digital technology and IT transformation programmes, including the need to factor in cyber resilience-by-design, and adopting the principles of the regulators around operational resilience. As covered in our Operational Resilience topic, cyber risks will likely remain the most frequent threat to operational resilience, and should continue to be factored into any assurance work.

Cyber risk governance and monitoring:

- The immediate need to facilitate and support remote working for almost all staff, has led some organisations to loosen certain controls in the short term such as need for VPN, dual authentication, or monitoring. With levels of remote working likely to remain higher than they were pre-COVID-19, organisations may need to find ways to reset the balance and increase flexibility without compromising security or "flexing" control beyond risk appetite. Internal Audit leaders should challenge management where the control environment goes beyond risk appetite, and explore with them alternative arrangements, such as strengthening of controls, restricting access to high risk staff and access to sensitive data. The effectiveness of monitoring or alerting controls designed to spot unusual patterns of activity and flag it for further investigation should be considered in those cases.

Find out more
COVID-19 cyber risk preparedness and response: Securing your environment against elevated threats.
https://www2.deloitte.com/us/en/pages/advisory/articles/covid-19-cyber-risk-preparedness-response.html

2. Operational Resilience (▲3)

Why is it important?

Internal Audit, as the third line of defence, was uniquely placed to play a key role in the response to the crisis, from a position of good organisational knowledge and often with a highly relevant skill-set. We've seen many functions providing assurance on resilience programmes and the associated controls adopted by organisations, on a real-time basis as the crisis unfolds, however they will need to continue to do so going forward with the benefit of looking back and leveraging lessons learned.

Building the operational resilience of firms and Financial Market Infrastructures (FMIs) remains a key shared priority for the Bank of England (BoE), the Prudential Regulatory Authority (PRA) and the Financial Conduct Authority (FCA). UK Regulators have been monitoring the operational resilience of financial services firms during the pandemic, looking particularly closely at how firms refine their resilience plans, how they approach the governance of their operational resilience (including the role of the board and SMF24[2]) and the quality of their crisis communications.

What's new?

The three UK supervisory authorities published a shared policy summary and coordinated consultation papers (CP 19/32 and CP 29/19[3]) on new requirements to strengthen operational resilience in the financial services sector. The CP principles establish the draft rules that firms will be required to follow, placing particular focus on identifying important business services, setting impact tolerances and the need for regular self-assessments. It builds on the concepts set out in the operational resilience Discussion Paper published in 2018, and addresses many of the proposed policy changes based on the responses received.

What should Internal Audit be doing?

As part of the next phase, organisations must recognise that they will have to face a period of uncertainty and disruption over many months. Throughout this period, they will need to rebuild confidence for the future by ensuring their response is resilient, safeguards the welfare and well-being of people, and is able to adapt to demand and supply challenges. Internal Audit will need to focus on:

- Challenging and benchmarking management's *scenario-planning and assumptions* regarding the nature, extent and duration of the situation, as well as the plan to deliver services during prolonged uncertainty in a way that is safe, flexible and resilient based on a clear action plan.
- Understanding whether the resilience achieved to date was by design. If not, then what lessons should be drawn for the future? What are management's 'crunch points' in the *ability to deliver services* against planning assumptions?
- What is management's *strategy* to return to "business as usual" after the crisis, and move from "respond" to "recover" and then to "thrive"? How can it turn the crisis into an opportunity to emerge stronger?

The PRA has asked IA functions across a number of firms to undertake an operational resilience audit against the principles in the consultation paper or broader governance and approach. IA will need to:

- Review how the organisation has interpreted the regulation and taken actions in response to this whilst also leveraging industry response and lessons learned from COVID-19.
- Challenge management's process to identify their most important business services in order to prioritise their work and investment in operational resilience.
- Ensure that operational resilience is established across end-to end business services, looks at business outcomes from a customer perspective and takes into account third parties and the ecosystem of the firm as a whole.
- Validate whether the organisation has an adequate internal governance and a supporting control framework in place for managing operational resilience. Ensure management has plans to embed operational resilience across the organisation.
- Ensure that it has set appropriate impact tolerances for their important business services, and has documented the people, processes, technology, facilities and information that support their important business services.

Find out more
COVID-19 and operational resilience in the financial sector.
https://ukfinancialservicesinsights.deloitte.com/post/102g7ak/covid-19-and-operational-resilience-in-the-financial-sector

Preparing for the "next normal" – Build modified resilient operations.
https://www2.deloitte.com/uk/en/pages/risk/articles/preparing-for-the-next-normal.html

Operational Resilience and COVID-19: Internal Audit Planning Considerations
https://www2.deloitte.com/uk/en/blog/auditandassurance/2020/internal-audit-planning-considerations-for-internal-audit-functions.html

3. Cloud Governance and Security (▲7)

Why is it important?

A survey by the Bank of England earlier in the year identified the presence of thousands of cloud-based applications in use across the financial services sector, noting that cloud outsourcing, *"where companies store information and use software via shared virtual data and processing services, rather than relying on local servers"*, is becoming increasingly popular[4], as well as highly concentrated. The survey indicates that banks use cloud outsourcing more widely than insurers. They mainly use cloud outsourcing to run software and access additional processing capacity (Software-as-a-Service or SaaS) or to support IT infrastructure (Infrastructure-as-a-Service or IaaS). The use of SaaS outweighs the use of IaaS, and with digital transformations powered by cloud technologies being accelerated throughout the pandemic[5], the prevalence of cloud as the preferred technology architecture model will undoubtedly continue to grow.

What's new?

Reliance on the use of third-party outsourcing, including Cloud Service Providers, has resulted in an array of recent regulatory interest. With the EBA[6], EIOPA[7] and ESMA[8] all publishing guidance on the management of cloud outsourcing, the PRA has also published Consultation Papers seeking to enable more consistent oversight of arrangements. The *Outsourcing and third party risk management* Consultation Paper CP30/19[9] gives pragmatic guidance to firms for outsourcing (including cloud) with the CP 29/19 (see above in topic 2) also requiring firms to determine the cloud service's materiality to the outsourcing firm.

As part of transitioning or "migrating " to the cloud, the responsibility for the operation of many controls shifts away from the outsourcer to the service provider. This is commonly referred to as "the shared responsibility model" with the balance of responsibility being dialled up or down depending upon the service and the deployment model adopted.

The accountability over the operation of effective controls as part of this broader control environment resides with the outsourcer, however, who is also accountable in the regulators' eyes for the broader safeguarding of data and IT assets. As such, robust oversight and assurance mechanisms from the outsourcer perspective become obligatory in this environment.

The outsourcing organisations should also periodically assess and manage their associated concentration risks – particularly in the case of over-reliance on one of the top-three cloud service providers to support critical services. The regulators are particularly concerned as this can present operational risks for the organisation itself, but also financial stability risks for the system as a whole.

What should Internal Audit be doing?

Internal audit teams considering auditing the adoption of cloud within their organisation should consider audits of cloud governance, cloud migration programmes, and targeted reviews over one or more technical areas across a stable environment / deployment. These focus areas which will enable functions to understand how effectively the organisation is identifying and managing the risks associated with cloud.

The nature of the deployment, the complexity of the environment and the level of maturity will in turn determine the overall audit need and specific scoping for IT audit teams.

- ***Cloud governance:*** Internal audit teams should look to provide assurance over the governance around cloud deployments to determine the extent to which risks are proactively managed and risk metrics are defined and monitored, reducing the risks of "rogue" or non-compliant deployments for instance. This should also consider compliance with regulatory requirements with regard to the location of the cloud services. We increasingly see functions develop a Risk and Control Matrix and audit framework for cloud that, on the one hand helps bringing consistency in the delivery of cloud audit work across the function, and on the other ensures alignment to the organisation's key risks, applicable regulatory requirements as well as industry good-practice. The framework should leverage risk and control areas across other IT risk domains.

- ***Cloud programmes:*** These reviews should focus on: programme governance and migration approach; business case and benefits realisation; business alignment; plan for technology integration with existing infrastructure and legacy platforms; dependencies and deployment impact assessment across technology estate.

- ***Targeted reviews:*** In order to audit specific cloud deployed instances, internal audit teams should define an approach to prioritise the key risk areas for consideration and assessment as part of the audit. A review and challenge of cloud outsourcing register completeness will enable firms to understand their own level of concentration risk to an outsourced provider, including an overview of sub-outsourcing. Additional areas to consider include: access management across the firm and outsourcing organisation(s); potential reliance on service auditor reports or vendor external certifications; integration with legacy systems and impact assessment; governance and internal controls to identify, manage and report risks resulting from all third-party arrangements, including when they leverage embedded capabilities.

Find out more
Cloud outsourcing in financial services and COVID-19
https://ukfinancialservicesinsights.deloitte.com/post/102g6od/cloud-outsourcing-in-financial-services-and-covid-19

Cloud outsourcing – regulators clarify expectations
https://ukfinancialservicesinsights.deloitte.com/post/102g14b/cloud-outsourcing-regulators-clarify-expectations

Cloud and regulation – overcoming the barriers
https://www2.deloitte.com/uk/en/pages/financial-services/articles/cloud-and-regulation-overcoming-the-barriers.html?nc=1

4. Extended Enterprise Risk Management (◀▶4)

Why is it important?

For many organisations, their third-party ecosystem, or "extended enterprise", is an important source of business value and strategic advantage. However, as the reliance on third parties continues to grow, so do the associated risks, bringing potential reputational damage and regulatory action.

What's new?

Our 2020 global survey on Extended Enterprise Risk Management (EERM), highlighted an increasingly high interest and leadership focus on third-party risk management. Likewise, this area remains a key focus for Internal Audit.

Some of the key findings as reported in our survey were:

- A rise in regulatory activity related to EERM has put pressure on organisations, raising benchmarks and expectations as to the definition of good-practice and maturity in this area.
- The financial impact of a failure of a third party or sub-contractor has increased significantly in the last 5 years (at least doubled).
- Organisations are more aware of the need to act as a responsible business, and this forms a top driver for investment in EERM.
- Many organisations are developing their strategy and vision to transform EERM over the next two to three years.
- Early indications show that those firms that have made appropriate investments in EERM programmes were faring better in their response to the crisis than those that did not.
- We anticipate that organisations will re-evaluate how they position third party management to cope better with high impact events, and expect rapid acceleration of the TPRM maturity curve in the next 12 months.

What should Internal Audit be doing?

We have seen that senior executives have now been extending their focus beyond risk to encompass a broader view of third party management: equally, Internal Audit functions should be looking to encompass in their third party management audits areas and sub-disciplines such as contract management, performance management, financial management, and sourcing activities. They should be auditing the design and implementation of the firm's EERM framework; seek to understand how management assesses the nature and criticality of third party relationships and related contractual terms; and how they manage the associated supplier concentration risks, including those related to critical third parties.

Third party audits should seek to explore lessons learned from the crisis and how management have taken action to revise frameworks, controls and resilience measures to take these into account. Our research suggested that most organisations were unprepared to manage third party risk in the event of such large scale disruption, such as the COVID-19 pandemic. The crisis highlighted the strategic impact of third-party failures, particularly when the operational resilience programmes haven't taken into account third party dependencies and associated risks.

Furthermore, controls around the monitoring of subcontractor risk (fourth or fifth party) were still quite immature or non-existent – with organisations believing that it is the responsibility solely of the third parties that engaged them in the first place.

Conversely, proactive engagement and management of third parties, and alignment with operational resilience plans, significantly reduced the risk exposure. Some indicative actions include:

- Identifying critical business activities, products and services, and instances with high degree of dependency on third parties.
- Including intra-group arrangements, subsidiaries and affiliates in this analysis.
- Leveraging available data sources (internal and external) with regard to critical third parties to identify areas of potential risk – for instance delivery location, financial health, market sector etc.
- Developing or revalidating contingency plans for the "higher risk" third parties.

Find out more
Extended Enterprise Risk Management Survey 2020.
https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-third-party-risk-management-global-survey-2020.pdf

5. Transformation and Change Assurance (▼2)

Why is it important?

The crisis has elevated the need for strategic change and transformation up the board agenda to enable organisations adapt, survive and thrive in a changed environment. It has also dramatically disrupted how change is delivered within organisations and the way change teams now operate. With remote delivery having been forced on change teams, they have had to adapt and transform their approach to ensure they were still able to effectively deliver change whilst minimising its impact on the delivery plan.

What's new?

In this new landscape there is an increased need to deliver change at pace in order to adapt and keep up with the realities of a rapidly evolving macro environment. This, in turn, has driven (or accelerated) the adoption of new delivery methodologies and techniques e.g. Agile, in order to deliver at speed whilst adapting to frequent changes to requirements due to unforeseeable external factors.

In many cases, this has compounded the burden on the change teams as they adapt their ability to deliver programmes remotely, in an environment of frequent flux and often moving requirements. They are having to transition to new alternative methods of delivery, are training individuals and recruiting SMEs, whilst grappling with the challenge of how to maximise the full potential of these delivery approaches when having to deliver change using remote teams.

What should Internal Audit be doing?

With this fundamental shift in the approach to delivering change, it is important for Internal Audit to focus on the organisation's portfolio of change to ensure that the ability for organisations to meet their regulatory requirements or organisational strategic objectives has not been materially impacted. There are some key areas that we recommend Internal Audit should focus on:

- ***Continuous assurance:*** Establishing a continuous oversight and assurance approach that follows the change portfolio's lifecycle and helps to ensure, for example that programmes are appropriately resourced, have the right controls in place to achieve time, cost and quality objectives. As the assurance plan develops, the overall portfolio governance arrangements should be continually monitored for changes and potential delivery 'fatigue'.

- ***Leverage other assurance functions:*** Leveraging the relevant governance and assurance functions to review specific aspects of the project or programme at the right time can provide early visibility of risks and drive timely action before issues materialise.
  This can be achieved through the use of second line for ongoing oversight, challenge and support, especially in regard to risk around the change methodology and factoring its impact on the wider portfolio of change.
  Close collaboration between all lines of defence around the delivery of change assurance is critical to provide the optimal levels of assurance most efficiently across the change portfolio.

- ***Portfolio level assessments:*** The function should also look beyond individual transformation activity and ensure their work also covers the overall portfolio management practices; the role of the board and executives in terms of portfolio oversight against strategic transformation objectives; the realisation of benefits across the wider portfolio; and whether individual programmes add value against the overall portfolio.

- ***Agile reporting:*** The ability to provide near real time visibility of risks and flag concerns before issues materialise will be key to help drive successful delivery and added-value assurance, meaning a traditional "after the fact" audit will no longer suffice.

- ***Skills and training:*** Internal Audit teams need to be alert to any changes to delivery approaches by change teams, for example a shift away from waterfall delivery to Agile or DevOps delivery approaches, and plan to have the necessary skills and capabilities in place to be able to adequately provide oversight and assurance on these programmes.

Find out more
Project Assurance; bridging the gap between your boardroom and projects. https://www2.deloitte.com/lb/en/pages/finance/solutions/capital-projects/project-assurance.html

6. Digital Risk (▼5)

Why is it important?

Measures introduced in response to COVID-19 have driven many financial services organisations to accelerate their digital transformation initiatives. During the past few months we have noted elevated levels of adoption of digital technologies, with increased reliance placed upon new digital platforms, collaboration tools and distribution channels. At the same time, we are seeing organisations implementing new norms in the way they run their operations, including the way they manage a large remote workforce. In this climate, the need to adapt or transform can be fundamental to the success and survival of many organisations, and this is seen by many as an opportunity and catalyst to embrace digital transformation.

At the same time, the nature and pace of those digital initiatives introduce new "digital" risks, as well as changes to how existing, known risks manifest, at a time when getting it wrong can quickly create the next social media storm or front-page news story. Existing control processes have needed to be flexed at short notice, and often without fully understanding the potential knock-on impacts. Much like reckless spending can result in financial debt, rapid changes made in the heat of the moment can lead to accumulation of "control debt".

What's new?

Disruptive technologies, such as Artificial Intelligence ("AI"), robotic process automation and advanced analytics continue to be a core area of focus for organisations, as part of this digital transformation drive. The response to the pandemic has again highlighted to businesses the benefits of using these technologies to promote workforce productivity and operational efficiency, as well allowing digital connections and improved, faster interactions with their customers. At the same time, recent headlines in the UK about unfair and biased outcomes of algorithm-based decision-making highlight some of the potential ethical and practical challenges businesses are currently facing.

Technologies continue to advance rapidly, and assurance functions and regulators are attempting to strike a balance between innovation and control, whilst also providing firm guidance on digital ethics. Increasingly organisations may be seeking to operate an integrated assurance model to provide assurance over digital risks, promoting collaboration across lines of defence, as organisations look to build their skills and knowledge in these areas.

What should Internal Audit be doing?

Internal Audit should continue to play a key role in challenging management's approach to adopting these technologies and ensuring that the risks to the wider business are suitably understood, assessed and managed. As a result, auditors need to adapt their way of thinking to anticipate these risks as they arise (new / evolved, or existing risks manifesting in different ways).

Digital ethics is of increasing relevance to regulators and customers alike, which means organisations and developers will also have to take notice. As well as providing assurance and guidance to management in this area, Internal Audit should ensure that ownership of digital ethics is clearly defined. The EU regulators have provided relevant guidance in the area of "trustworthy" AI[10], and these principles should be duly considered by auditors, as well as factored into their digital reviews. As AI and data analytics will progressively play an important role in detecting patterns of vulnerable customer behaviour for example, this will allow organisations to provide timely support and improve customer interactions from a conduct standpoint.

However, ethics can also inform difficult judgement decisions and trade-offs when using AI enabled solutions, so appropriate consideration and assessment against key (interconnected) risk domains such as data protection, conduct requirements, ethical considerations and an overarching robust governance framework will be essential.

Where Internal Audit functions are introducing these technologies themselves, a number of factors require careful consideration; Chief Internal Auditors should be clear on the overall digital transformation strategy relating to the use of increased automation within the function, the risks being introduced and how these are to be managed.

Find out more
Managing the digital risks of a remote workforce.
https://www2.deloitte.com/uk/en/pages/risk/articles/managing-the-digital-risks-of-a-remote-workforce.html?id=uk:2sm:3li:4dcom_share:5awa:6dcom:risk

Digital dependence: How to balance speed with control?
https://www2.deloitte.com/uk/en/pages/risk/articles/digital-dependence-how-to-balance-speed-with-control.html?id=uk:2sm:3li:4dcom_share:5awa:6dcom:risk

7. Data Governance (▼6)

Why is it important?

Data should be seen by organisations as a key differentiator in maintaining competitive advantage, providing distinctive, customer-centric services and increasing the efficiency of their operations. Many organisations, however, continue to struggle, not only to effectively capitalise on their data, but to protect it.

Data protection, data privacy and data governance remain topics of continuous attention and focus by senior management and Internal Audit teams alike. In another year dominated by data breaches and regulatory fines, it comes as no surprise that for this is again amongst the hot topics and a planning priority for 2021. Data management failures or breaches have drawn significant regulator and public scrutiny and have resulted in increased regulations and pressure by boards for management to improve their data governance procedures, policies and related data protection safeguards.

What's new?

The significant increase in remote working amongst employees during the pandemic has heightened the information security risks that organisations are facing. More specifically, data loss and data protection risks are particularly elevated, compounded by the increase in fraudulent activity by malicious actors over the past few months. This is an area that will continue to be a major focus as we move into the next phase, post-crisis. Organisations realise the strong connection between protecting and safeguarding data and the broader resilience, data breach and incident response capabilities across the organisation. Businesses are seeking to develop effective data breach response programmes, to enable them to effectively weather a potential breach/crisis when/if it occurs. Such initiatives will encompass processes to ensure the business engages effectively with customers, the public and media, while trying to resolve the crisis.

What should Internal Audit be doing?

Some of the areas of focus for internal audit are:

- ***Data governance:*** Despite the strategic importance of data, many firms 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 for 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.

- ***Data privacy and regulation:*** Internal Audit should assess the implemented data privacy policies, framework and controls to comply with General Data Protection Regulation (GDPR), and broader data privacy objectives. From complying with existing regulations, to preparing for new requirements on a global or multi-region scale, organisations should have established processes to deal with the complex matrix of relevant regulatory requirements.

- ***Data security:*** Data auditors should coordinate with information security / cyber audit SMEs and focus on technical data protection controls, including Data Leakage Prevention solutions and other security controls to prevent data breaches. The level of manual processing or legacy functionality within key business applications should form a key component of any Internal Audit opinion on key application systems, as these are often the trigger points for data leakage within many financial services organisations.

- ***Data breach response:*** Internal Audit should challenge management on their customer data breach readiness procedures. Breaches will continue to occur, and it is actually a case of "when rather than if". Organisations that have experienced such events, recognise these are hugely complex events on many levels, technically, strategically and operationally. Internal Audit should review these areas, focusing on clear accountabilities, cross-functional collaboration, and readiness to respond on a timely basis in order to contain the issue while providing high-levels of customer service to help safeguard reputation.

8. IT Strategy and Governance (▶◀8)

Why is it important?

With the increasing prevalence of technology and, importantly, the digitisation of business operations, the requirement for a strong link between information technology and business strategy has never been more important. And yet, many organisations still struggle to combine the two effectively. IT should be seen as a catalyst for business enablement contributing to a competitive edge and innovative customer offerings. Often there are organisational and cultural barriers hindering the effective engagement between IT and business functions, driven in part by a traditional (and frankly outdated) mindset that sees IT purely as a back office support function with limited added value to the customer.

What's new?

CIOs and IT departments were at the forefront of COVID-19 crisis response activities supporting the continuity of operations and customer service, via infrastructure upscaling or the provision of new digital services. Robust IT governance arrangements that included efficient resource and vendor management, contingency plans, robust policies and operating procedures, proved to be the defining aspects of an effective, agile response during the crisis.

What should Internal Audit be doing?

Internal Audit have a continued role to play in challenging the strategic direction of IT as well its alignment with business objectives, and this role has been elevated by recent global events. Functions need to have a strong understanding of both the IT and business strategy as well a perspective on the complexities of the existing IT environment, in order to be well placed to assess risks and challenges in this area. Areas of focus should include:

IT Strategy Refresh Processes

- A review of current plans for refresh of the IT strategy should be timely, particularly in view of the economic outlook, changes to the broader market and operating environment. Of particular focus should be how clearly the IT strategy links to the business strategy, and the governance structures to ensure it is properly discussed, agreed and approved. Innovation and transformative ways to disrupt traditional IT operating models, such as migrating to the cloud, and adoption of DevOps operating models may be considered during strategic refresh to demonstrate diversity of thought and genuine challenge to the status quo.

Digital Strategy and Architecture Enablement

- Digital tools and a move to "digitalisation" is gaining sufficient traction in the sector. Many enterprises are considering their "digital strategy" and the architecture which enables the business to realise its digital goals. Internal Audit can play a role in highlighting the robustness of the approach and the strength of capability around digital strategy delivery. The suitability of the strategy itself as well as the maturity of the associated control framework and governance practices also form important areas for Internal Audit to provide a viewpoint on.

- The current market, economic, and social conditions indicate "this is the time for transformational, not incremental, change" – something that in many cases puts pressure on CIOs to move quickly and lead digital transformation initiatives. There is a risk here that these programmes may be reactive to the market without having considered the integration with the existing, legacy technology estate. Getting the basics right, such as remediating existing technology weaknesses, before embarking into such initiatives would be key for success preventing unnecessary complexity that would raise the risk exposure of the organisation.

Shadow IT

- "Shadow IT" indicates IT systems deployed and supported by departments outside central IT and by definition not aligned to the central IT strategy and direction. A review of such areas in combination with broader governance practices, can provide useful insight into the strategic provision of IT within the business and its true alignment to business strategy. Business departments operating their own IT platform indicate of areas of the business which may not being fully served by the existing IT department and strategy. A high propensity for shadow IT can also be indicative of a poor culture, or engagement between IT and business.

Find out more
Findings from the Deloitte 2020 Global Technology Leadership Study. https://www2.deloitte.com/us/en/insights/topics/leadership/global-technology-leadership-study.html[11]

9. Payments (NEW)

Why is it important?

The payments market has been undergoing significant disruption in the last few years. Regulatory scrutiny remains high, as firms develop new payment strategies and respond to increasing compliance requirements. Recent instances of payment system-related outages and cyber-attacks have also attracted a lot of attention. The Revised Payment Services Directive (PSD2) has been in force in the UK since 2018, and firms are continuing on their journey to fully adapt their customer propositions and technology operating models. Two of the most impactful areas of PSD2 were governed by the requirements set out within the Regulatory Technical Standard (RTS) and are as follows:

- The requirement to use *Strong Customer Authentication (SCA)* for electronic payments;
- The *Open Banking* requirements, namely allowing Third Party Providers (TPPs) access account information and initiate payments on behalf of customers through dedicated interfaces powered by Application Programming Interfaces (APIs) or through Modified Customer Interfaces (MCIs).

What's new?

Organisations are required to ensure that their implementation of the above PSD2 requirements is well governed, documented, periodically tested, evaluated and audited by operationally independent auditors with expertise in IT security and payments processes. Firms are in the process of preparing their review for their first full fiscal accounting year which, for the majority, will be December 2020 or March 2021 year ends.

Furthermore, to counter cyber-attacks on the SWIFT network, SWIFT introduced the Customer Security Programme (CSP) as a mandatory compliance initiative for the global SWIFT community, consisting of core security standards and an assurance framework applicable to all members – not limited to financial service organisations.

What should Internal Audit be doing?

Internal Audit will have a key role to play in providing assurance that organisations adapt and develop their payment offerings and comply with the evolving regulatory requirements. Specifically:

Payment Services Directive (PSD2)

- We see many reviews against the Regulatory Technical Standard being performed by Internal Audit functions that meet the independence and expertise requirements. Functions should be aware of these requirements, and build such reviews into their audit plan for 2021.

- A risk assessment and prioritisation of coverage may be needed, as the review requirements may generate a significant volume of work, depending on the number and complexity of firms' operations and channels. This is driven by the broad applicability of PSD2 across any channel offering access to "payment accounts" (including cards) across any customer segment (i.e. Retail, Business, Corporate, Private Banking etc.), and across all electronic customer channels, such as internet banking, mobile apps, firm provided software, enterprise software integrations, other software integrations embedded through APIs or other interfaces, and "Open Banking" channels.

SWIFT Customer Security Programme

- Under the CSP, SWIFT users have to submit an annual self-attestation to SWIFT on the result of their independent assessment against a list of mandatory controls upon an organisation's SWIFT-related infrastructure. Results of compliance are recorded centrally at SWIFT and non-compliance would therefore be visible to any SWIFT counterparties an organisation deals with. The attestations can be facilitated by Internal Audit or by an external provider, but we see increasingly Internal Audit functions driving these, in many cases using external specialist co-source support.

- SWIFT released an Independent Assessment Framework for 2020, which is designed to support users in verifying that their self-attestations correspond with their actual level of security control implementation, however due to COVID-19 pandemic, these new self-attestations will apply from mid-2021.

Find out more
Payments trends 2020 InFocus: Strategies to prepare for the future of payments https://www2.deloitte.com/us/en/pages/financial-services/articles/infocus-payments-trends.html

SWIFT customer security program https://www2.deloitte.com/global/en/pages/finance/solutions/gx-swift-customer-security-program.html

10. Systems Development (▼9)

Why is it important?

Organisations are continuously seeking efficiencies across their IT operations and application development is no exception. The adoption of DevOps methodologies (combining IT development and IT operations) is still maturing, aiming to drive efficiencies through automation and collaboration in application development.

What's new?

Organisations have also been utilising other means to gain efficiencies and meet business demand. For example, low-code, no-code ("LCNC") development platforms allow users with little or no programming experience to build and publish new applications, without writing any lines of code. Even though LCNC platforms have been around for years, they are recently enjoying increased popularity among developers and non-developers who are seeking to reduce "time to market". Such platforms are usually provisioned by third parties and they increase the risk profile of systems development. When configuring such platforms, striking the right balance between appropriate and sufficient controls whilst allowing for innovation to happen is key. Experimentation through the usage of "sandboxes" is a mechanism which some organisations have used to identify where this balance lies.

What should Internal Audit be doing?

Awareness is increasing across Internal Audit teams around the adoption of DevOps and LCNC platforms, and the role they play in version control, collaborative development, build validation, testing, and quality assurance. Controls implemented following the adoption of DevOps may look substantially different to traditional ones, but should still focus on addressing the same underlying risks. Organisations must have an understanding of their risk appetite and the extent to which such approaches affect their risk exposure, and they should be challenged on this.

Internal Audit's approach towards assuring LCNC needs to be adapted depending on the maturity of such platforms and their supporting processes, the users who operate them, and the solutions which they help develop. Certain key areas to look out for are:

- Third party controls around onboarding, ongoing management and exit of such vendors and platforms need to be assessed so that the right foundations are in place in line with the criticality of their use within the organisation.
- Internal Audit teams will need to challenge the consistency and diligence in which the controls within such platforms have been configured and are operated.
- Organisations are expected to apply proportional levels of security testing to code developed using LCNC platforms to that which they would develop using traditional means. Access controls that safeguards the appropriate segregation of access to data remain fundamental.
- With the necessary guardrails, operating within predefined boundaries, users can build solutions which are governed appropriately and therefore could contribute positively in limiting shadow IT. To realise such benefits it is important that the right governance measures are in place ahead of an organisational-wide adoption.
- It is key that third and second line of defence teams are engaged at the right time to provide input and feedback to ensure the organisation evolves with their digital transformation journey in a controlled manner.

IT Internal Audit of the Future: Embracing Analytics and Digital Enablement

Confronting uncertainty

Despite being an area of focus for Internal Audit teams for a number of years, many functions have yet to make significant progress in effectively and sustainably embedding the use of data-driven auditing and analytics. With COVID-19 impacting every aspect of the work environment, many Internal Audit functions have reflected on the impact of the pandemic on their businesses and have concluded that the manner in which they deliver services to the organisation will naturally need to adapt as well.

During a time of change, IA should continue to provide assurance over the most consequential risks, while simultaneously increasing its role in advising management and the board on the shifting risk and control landscape, including anticipating new emerging risks. Now, more than ever before, IA should consider deploying enabling digital technologies, beyond analytics and automation, with the objective of becoming more resilient, cost-conscious, and smarter about providing services that make an impact. Some of the reasons for this include:

- The increase of remote working arrangements themselves have highlighted the **need for data-based auditing**, particularly where web-based conversations are not as easy or productive as sitting next to the auditee. Deployment of analytics is a key assurance mechanism when direct face to face auditing proves challenging and IA needs to shift to low-to-no contact auditing.

- Increased **digitisation of business processes** across the business, as we have covered previously in this survey, is also driving analytics adoption and enablement during audit delivery.

- Similarly, the **evolving technology environment**, with the increased cloud adoption and digitalisation, means that accessing enterprise data warehouses and other key data sources is easier than ever and the quality of data itself has generally improved.

- The **frequent changes** to the external environment, associated threats and, in consequence, the risk profile in the current environment, increase the need for IA functions to have data driven metrics at their fingertips and to run continuous assessment.

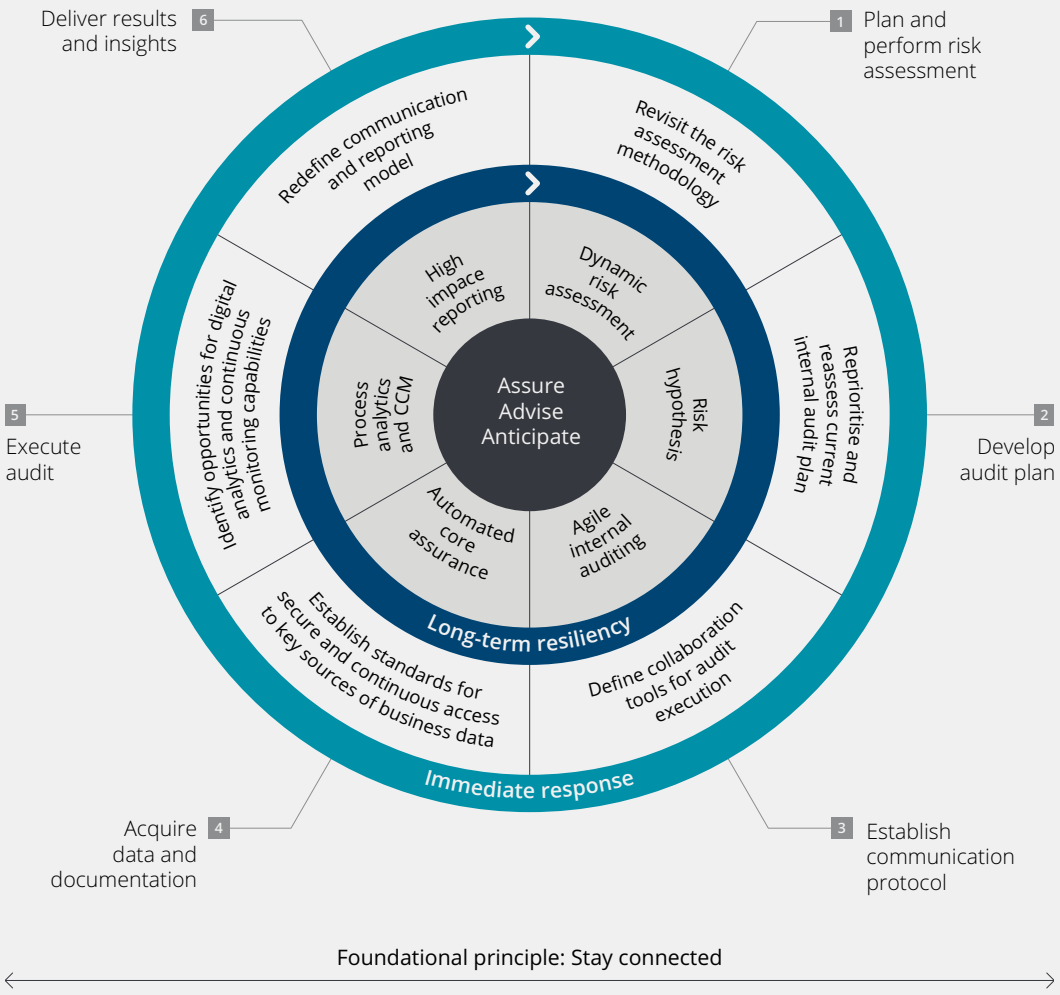
Guiding principles for building a resilient function

Deloitte has compiled a set of guiding principles across a standard audit lifecycle as an immediate response, enabling internal auditors to adjust to the "next normal" of remote internal auditing[12]. These principles highlight where the use of digital technologies, tooling and analytics methodologies can be utilised to drive change and increase long-term organisational resilience. Taking the time to institute a set of guiding principles for remote internal auditing is instrumental in preserving IA's ability to perform well, be present for stakeholders, and remain relevant in the long term.

While we make frequent references to tools and technologies, in our view success is achievable when the principles and business objectives lead the way, rather than the technology itself. Effective digital enablement for IA requires robust strategy, people, process, and technology – in that order.

"While we make frequent references to tools and technologies, in our view success is achievable when the principles and business objectives lead the way, rather than the technology itself."

Figure 2. Foundational principles for building resilience in Internal Audit[12]



Stage 1:

Risk assessment

Principles

- Performing risk assessment as part of annual or 6+6 planning is not sufficient.
- Functions need to collaborate with key stakeholders to identify emerging, shifting or new risks.

Data analytics and Digital-enablement opportunities

- Function need to be agile and respond in a dynamic way in recognising and evaluating shifting risk patterns.
- Use of external or internal data to facilitate continuous risk assessment or risk monitoring.
- Example of tools, include Continuous Business Monitoring, Dynamic Risk Assessment or Risk Sensing. These are powered by automation and machine learning capabilities, moving the function from manual, fragmented, often unrepeatable processes to repeatable, standardised tools and methods.

Stage 2:

Audit planning

Principles

- Functions should reprioritise the audit plan regularly to provide assurance over the most consequential risks.
- In addition, functions should consider which audits cannot be performed remotely, if data analytics can be applied, as well as align the plan to internal resource capacity and capability.

Data analytics and Digital-enablement opportunities

- Automation tools, enabling the generation of planning documents, files and RCMs using exiting control libraries can significantly speed up the planning process and reduce errors.
- Agile auditing techniques coupled with smart data interrogation (KPIs, incident reports, or performance dashboards) can help auditors focus their planning on areas that matter most.
- Data-driven auditing improve data access and reveal key insights before fieldwork commences.
- Making connections and comparing performance and key benchmarks between products, processes, and business units means auditors can focus on what is of utmost importance and avoid merely confirming the obvious.

Stage 3:

Collaboration and Communication

Principles

- By establishing communication and auditing protocols early on, and utilising tools that enable collaboration, auditors have a unique opportunity to use remote working to their advantage, minimising stakeholder disruption and getting the most out of virtual meetings.

Data analytics and Digital-enablement opportunities

- Auditors explore the use of tools with capabilities such as making and distributing request lists, uploading documentation, and tracking status.

- Many collaboration tools offer capabilities such as whiteboard, Kanban boards, thereby facilitating agile IA audit environments.

- One of the benefits of the use of video conferencing facilities is that it enables auditors leverage screen-sharing and screen recording to assess processes, such as configuration or code testing, which would typically be reviewed in-person with the process owner.

- Instead of requesting static screenshots, a live review conducted online can be more effective since it gives internal auditors the ability to ask questions in real time and drill down into modules that they otherwise wouldn't be able to access directly.

Stage 4: **Stage 5:**

Data | Audit execution

Principles

- The principles of running audits in the least invasive and quickest way possible are more important than ever.
- Auditors should take the opportunity and 'negotiate' with the business owners easy access to data, through data warehouses or pipelines to gain continued access to real-time data.
- Audit scope should be evaluated against manual testing procedures, and availability of complex but good quality data to determine where/how analytics can be utilised as part of audit execution.

Data analytics and Digital-enablement opportunities

- Target analytics toward audit areas that require standardised and repeatable tests, such as those required for meeting regulatory reporting standards. Rather than having to deploy new technologies, this can often be done by using existing automation, analytics, and data visualisation technologies that are readily available within the company's portfolio. These tools are frequently enough to start building a book of automated controls that can be assessed through exception review.
- Reflect on the current use of digital tools and assess the potential for reducing risk management costs, without impairing effectiveness. Take Continuous Controls Monitoring (CCM) for example. CCM would enable the first line of defence to take ownership of its risk profile and the second and third lines of defence to become strategic advisors.
- Other opportunities for analytics, including:
  - Smarter or risk-based sampling;
  - Full population testing over a large dataset, to increase level of assurance provided;
  - Statistical interrogation of data to test hypotheses;
  - Data quality assessment, data aggregation and integration;
  - Use unsupervised machine learning tools to extract hidden relationships and outliers from the dataset (thereby preventing analyst bias);
  - Use of voice analytics to identify insights in voice data and voice biometrics based datasets.

Stage 6:

Reporting and insights

Principles

- The reporting and communication strategies of the IA function should be adapted to the changing environment.
- This would mean adjusting the frequency of communication per stakeholder, as well as the nature and method of reporting.

Data analytics and Digital-enablement opportunities

- Use of interactive dashboards and visualisation techniques to report on audit findings is an innovative way of reporting that is adopted by many functions lately.
- Dashboards can convey insights quicker, and assist IA in creating impactful reporting as images and graphs based on data represent quantitative evidence of a hypothesis, which builds trust with the audience and positions IA well as an advisor and thought leader.
- Other reporting solutions and digital-enabled innovation include:
  - Automated generation of text-based audit reports
  - Robotics process automation supporting file completion, and auto-generation of audit report draft
  - Robotics supporting Audit Committee reporting, particularly where data and information is hosted across various / disparate platforms and systems
  - Predictive insights/thematic risk identification
  - Text and sentiment analysis tools

Lessons for the future

One of the principal lessons we have seen arising from the crisis, is that the more analytics-savvy and digitally mature functions performed better. They continued to provide assurance in a non-intrusive manner, analysing available data (e.g. business performance, incidents, customer complaints, cyber-attacks) in a manner that provided a level of visibility over the nature of risks faced by the organisation as well as the effectiveness status of key controls that was imperative at the time. In an environment where some functions had to pause all auditing activity, or were told to defer meetings with key staff during the initial phase of the crisis, the use of analytics and digital tools helped separate the truly 'resilient' functions.

We believe, for the long term, IA should embrace digital-enabled transformation, continuous risk assessment, automated testing, exploratory analytics, and more broadly, agile methods as a way of decreasing costs 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.

"A deeper digital transformation and the use of data-driven auditing will not be merely required by Audit Committees as a nice-to-have."

Endnotes

1. The number in brackets indicate the ranking of the topics in our 2020 survey and the relative movement this year.
2. Chief Operations Senior Management Function (SMF24) as introduced in 2017, by the UK Financial Services regulators (FCA and PRA), in line with the Senior Managers and Certification Regime (SM&CR)
3. https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper
4. https://www.bankofengland.co.uk/bank-overground/2020/how-reliant-are-banks-and-insurers-on-cloud-outsourcing
5. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-realizing-the-digital-promise-covid-19-catalyzes-and-accelerates-transformation.pdf
6. https://eba.europa.eu/eba-publishes-revised-guidelines-on-outsourcing-arrangements
7. https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en
8. https://www.esma.europa.eu/press-news/esma-news/esma-consults-cloud-outsourcing-guidelines
9. https://www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management
10. Building Trustworthy AI. A comprehensive approach to conduct, data protection, and ethics. https://www2.deloitte.com/uk/en/pages/financial-services/articles/building-trustworthy-ai.html
11. Findings from the Deloitte 2020 Global Technology Leadership Study https://www2.deloitte.com/us/en/insights/topics/leadership/global-technology-leadership-study.html
12. Source: *Building Resilience in Internal Audit. Guiding principles for thriving in a time of remote internal auditing and beyond;* Deloitte, 2020

Contacts

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

Deloitte.

Designed and produced by 368 at Deloitte, London. J20128