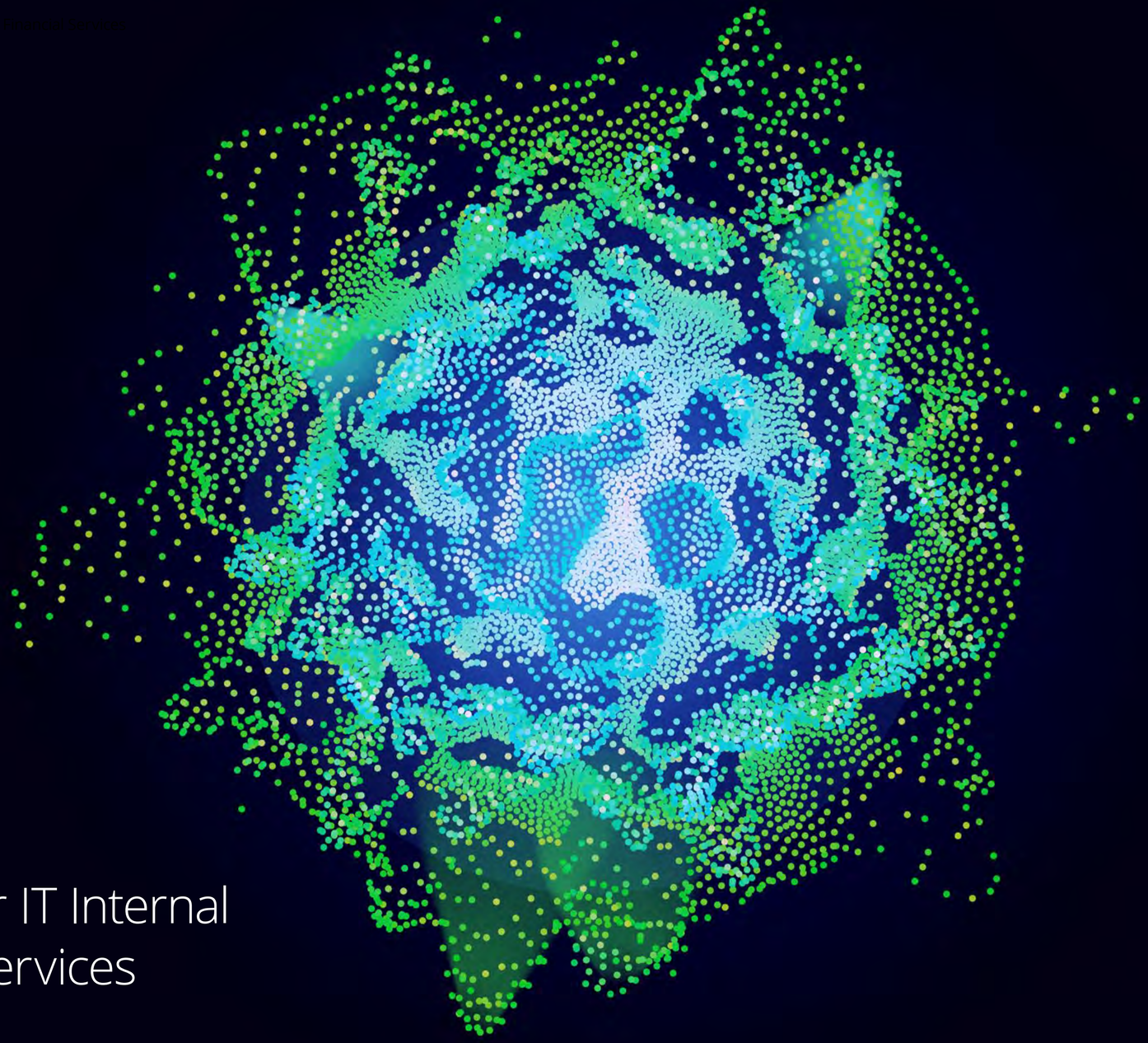
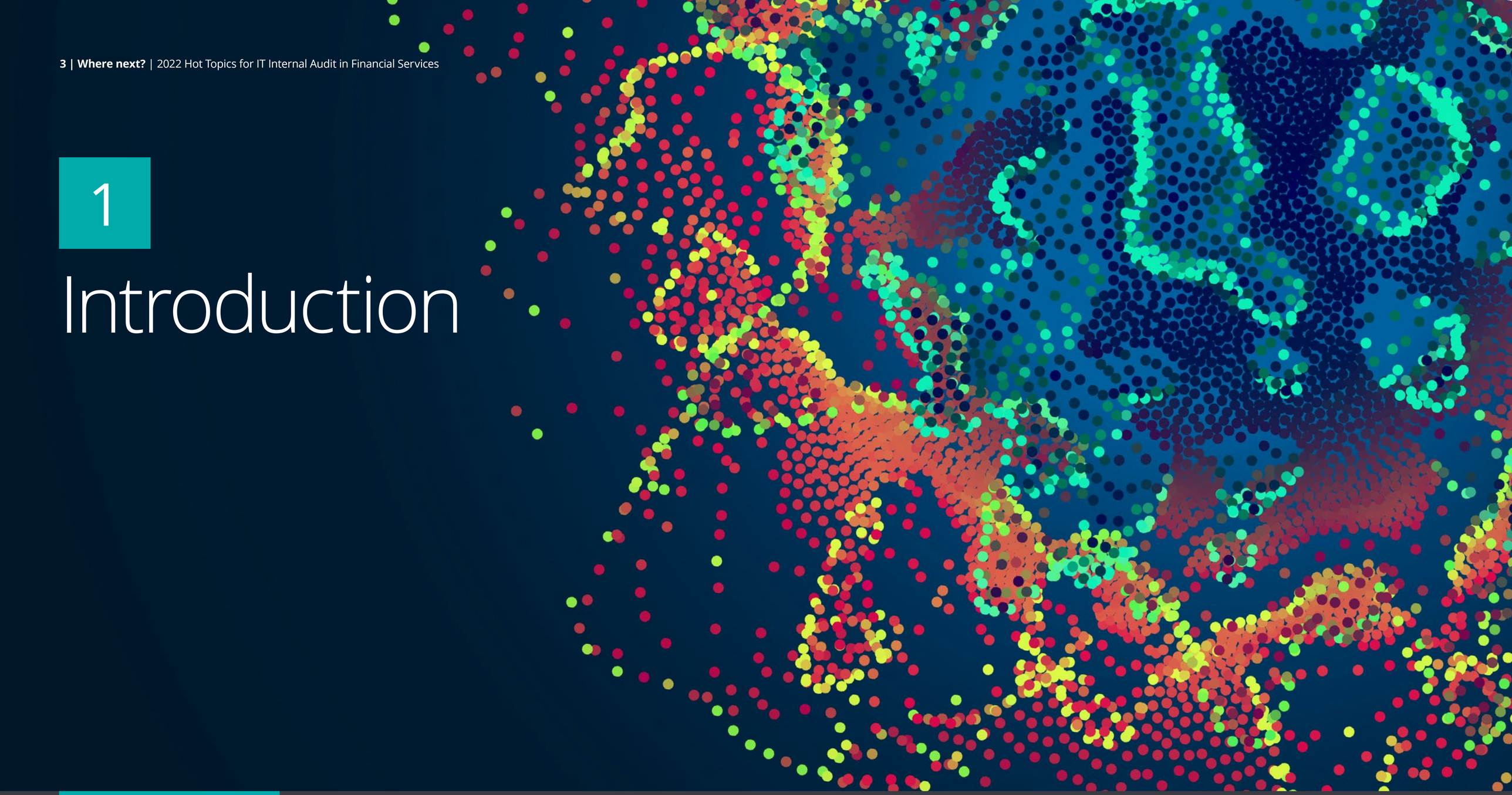
Deloitte.



Where next?
2022 Hot Topics for IT Internal Audit in Financial Services

An internal audit viewpoint

Contents



1

Introduction

Welcome to our annual viewpoint on the information technology hot topics for Internal Audit functions in Financial Services. The format of the paper should be familiar to many now. It is based upon our specific survey across the sector, combined with our qualitative insights and viewpoints from a number of conversations we have had with IT Internal Audit practitioners and leaders, as well as CIOs, CISOs and business leaders across the sector. Thank you to all the organisations that participated and contributed to this survey.

Last year's survey was completed in a period defined by what was arguably the most significant global event in decades, in the form of the COVID-19 pandemic. This year's survey has come to fruition as we hopefully head towards brighter times; current business sentiment and economic forecasts indicate growing confidence. As with all periods of significant change, business leaders have been required to act quickly to respond, and Internal Audit 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.

The repercussions from these events continue to play out, resulting in continued uncertainty over the future direction of the economy. Regardless of these factors, it appears clear that technology, digitisation, and resilience are central themes seen by the financial services sector as underpinning future business success. IT internal audit must 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.

Cyber remains the number one 'hot topic', continuing the trend for the best part of a decade now we have been running this survey. Certain underlying trends we have noted this year, revolve around topics like cloud, operational resilience and data governance which were much more prominent in the overall mix of responses.

It is also noticeable that topics such as operational Resilience and cloud, are areas where multiple IT risk disciplines such as cyber, technological resilience, and third party risk management (all of which are captured in the survey as items in their own right), coalesce, and we believe this reflects the importance of also considering such IT risk areas in aggregate. This requires IT Internal Auditors staying close to the changing regulatory environment around these areas, and Internal Audit leaders ensuring the combination of skills in the team are keeping pace with emerging risk themes.

Finally, I would point to the impact increased digitisation is having on change delivery, strategy and planning, where greater collaboration and integration between business and IT strategy will be paramount, more than ever before.

We hope this paper offers useful insights for your ongoing conversation with technology and business leaders, and supports your risk assessment and planning process for 2022.

Mike Sobers, Partner

2

IT Internal Audit Hot Topics through the years: 2012-2022

IT Internal Audit Hot Topics through the years: 2012-2022

The table 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 in Financial Services. Cyber remains the number one 'hot topic', continuing the trend for the best part of a decade now we have been running this survey.

Certain underlying trends we have noted this year, revolve around topics like Cloud, Operational Resilience and Data Governance which were much more prominent in the overall mix of responses. It is also noticeable that topics such as Operational Resilience and Cloud, are areas where multiple IT risk disciplines such as Cyber, technology resilience, and third party risk coalesce.

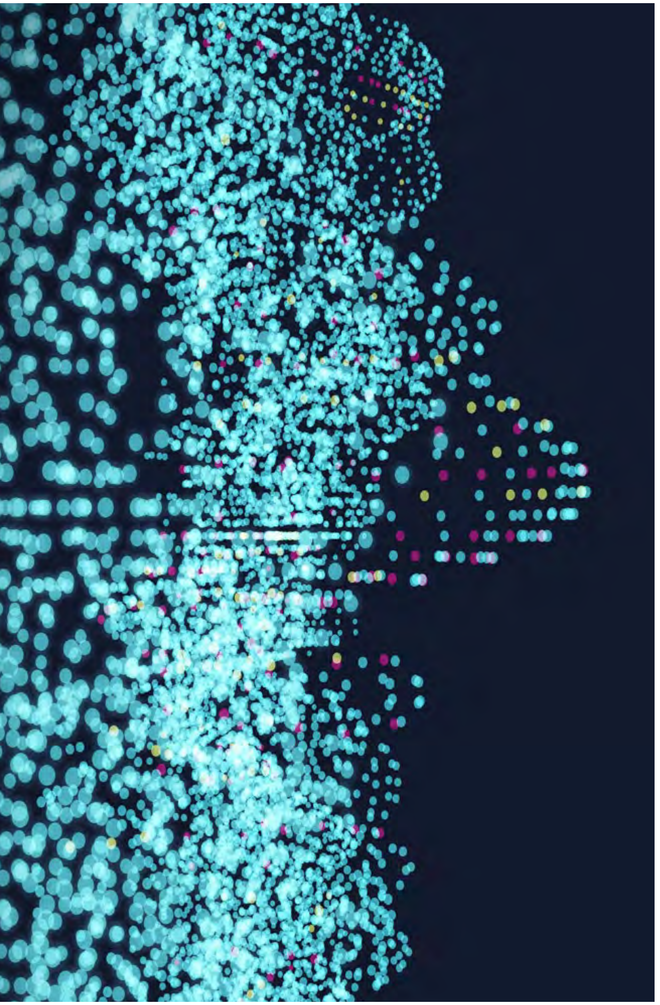
Topics which appear in more than two years have been colour-coded to help illustrate their movement in the top 10 over time.

Table 1. IT Internal Audit Hot Topics through the years: 2012-2022

Rank	2022	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	Cyber Security	Large Scale Change	Third-party management	Cyber Threat
2	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	Operational and IT Resilience	Cloud Governance	Operational Resilience	Data Protection and Governance	Data Management and Data Governance	Data Management and Data Governance	Third-Party Management	Large Scale Change	Identity & Access Management and Data Security	Data Governance and Quality	Data Leakage
4	Data Governance	Extended Enterprise Risk Management	Extended Enterprise Risk Management	Technology Resilience	IT Disaster Recovery and Resilience	Third-Party Management	IT Disaster Recovery and Resilience	Enterprise Technology Architecture	Data Governance & Quality	Large Scale Change	Data Governance and Quality
5	Transformation and Change	Transformation and Change	Digital Technologies	Extended Enterprise Risk Management	Information Security / Identity & Access Management	IT Disaster Recovery and Resilience	Data Management and Data Governance	Third-party management	Third-party management	Cyber Security	Rogue Trader and Access Segregation
6	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	Extended Enterprise Risk Management	Data Governance	Cloud Governance and Security	Cognitive Automation and Artificial Intelligence	IT Governance and IT Risk Management	Information Security / Identity & Access Management	Digital and Mobile Risk	Digital and Mobile Risk	Digital and Mobile Risk	Cloud Computing	Financial Crime
8	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	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	Application Controls and Integrated Auditing	System Development	Legacy Environments	Payment Technologies	Enterprise Technology Architecture	Digital and Mobile Risk	Payment Systems	Service Management	Cloud Computing	Social Media	Mobile Devices

1 CYBER SECURITY | 2 CLOUD GOVERNANCE AND SECURITY | 3 OPERATIONAL AND IT RESILIENCE | 4 DATA GOVERNANCE | 5 TRANSFORMATION AND CHANGE | 6 DIGITAL RISK | 7 EXTENDED ENTERPRISE RISK MANAGEMENT | 8 IT STRATEGY AND IT GOVERNANCE | 9 PAYMENTS | 10 APPLICATION CONTROLS AND INTEGRATED AUDITING

1 (1) Cyber Security



Why is it important?

Cyber security remains a critical risk and a key concern for organisations, with threats increasing and diversifying as a result of recent changes in social norms, working habits, and lack of "cyber-safe" technology environments which are more vulnerable to attacks.

Cyber leaders and Chief Information Security Officers (CISO) have risen to the challenges brought on by the pandemic, balancing the ongoing security of their technology estates against resilience and vigilance considerations. With most employees unexpectedly working from home for an indefinite period, CISOs secured networks for remote work by enabling or expanding multifactor authentication, enhancing system monitoring to receive early detection and alerts, and reviewing readiness plans to address the possibility of unexpected cybersecurity incidents. We have seen cyber-attacks increase significantly in the wake of the pandemic, with fraud, social engineering attacks, blackmail and email compromise particularly heightened. While the pandemic highlighted cyber leaders' resilience, it has also called attention to long-standing cyber security – as well as information security more broadly - challenges that many organisations are facing.

What's new?

- As we've commented elsewhere in our paper, the pandemic has amplified the longstanding need for digitisation, and has accelerated such programmes. Digitisation challenges have also emphasised the essential role that cybersecurity needs to play in the discussion. Cyber leaders should be at the forefront of these initiatives.
- Changes in risk management brought on by these shifts in the risk landscape and digital / technological advances have forced cyber leaders to consider how they are addressing these changes in relation to information security across business and how they can best promote its strategic goals.
- They are responsible for managing and increasing the efficiency of the cybersecurity program and cyber risk management. The organisation's information security risk needs to be managed in alignment with broader enterprise risk by working closely with Chief Risk Officers.
- This includes focus on recruitment and engagement of talent by creating a risk-aware culture. Cyber leaders are also expected to keep track of the shifting cyber regulatory environment to ensure the legacy processes are in compliance, which needs investment in time, effort, and money.
- CISOs should determine how to balance priorities and challenges across the "four faces" of the CISO: technologist, guardian, advisor, and strategist. CISOs serve the vital functions of managing security technologies (technologist) and protecting enterprise assets (guardian). At the same time, they are increasingly expected to focus more on setting security strategy (strategist) and advising business leaders on security's importance (advisor).

1 (1) Cyber Security (continued)

What should Internal Audit be doing?

Internal Audit's role over the past few years has been critical in terms of applying a risk lens to the organisations' cyber agenda, driven by regulatory, senior management and board demands on assurance and challenge.

We recommend Internal Audit functions map their cyber audit universe and use this as part of their risk assessment, adopting a cyclical approach across planning periods. This will ensure completeness of coverage, a more thorough understanding of cyber risks across the ever-changing business and technology estate, and alignment with regulatory guidance or industry good practice (such as NIST, ECB cyber framework etc). In our view, some critical areas of focus for Internal Audit functions this year should include:

- **Cyber risk management:** assessing the ability of the organisation to identify, manage and report on the cyber risk profile of the organisation against risk appetite, and in alignment with the broader enterprise risk framework. This may involve a focus of Key Indicators (KI), reporting to committees and regulators; timeliness, quality and diligence.
- **Cyber resilience:** refer also to our Operational Resilience topic. The recent supervisory statements around resilience call for enhanced, reliable, data-based metrics to monitor vulnerabilities, performance against KI and tolerances by system/component/third-party (mapped to important business services) that in turn can drive enhanced executive and board level visibility and decision making.
- **Strategy and governance:** review of the current cyber security strategy in the context of operations, environment and current organisational model. This will include checking alignment to future business, people and organisational plans.
- **Remote working practices:** review their business's remote working policy and security architecture, focusing on aspects such as: Bring Your Own Device (BYOD) schemes; and other associated controls, such as the use of multi-factor authentication; organisational controls around automated monitoring and alerting; the capability of the Cyber operations teams being able to appropriately support and mitigate threats whilst working remotely.
- **Review the management and oversight of third-party services in relation to cyber risk and control:** this should include initial take-on procedures, contract management, relationship management and ongoing reviews. Refer also to the Third Party Risk Management topic.

Find out more:

Deloitte Global Risk Management Survey – Cyber Risk

2 ▲ (3) Cloud Governance and Security

Why is it important?

Cloud services have continued to be rapidly adopted across all sub-sectors of the FS industry in 2021 and are increasingly ubiquitous with IT service delivery across the sector enabling organisations to adapt business models, products and channels and pervasiveness of use.

Risk, Control and Assurance functions, including Internal Audit, are often struggling to keep up with rapid transition at many organisations to cloud technologies. There are significant regulatory obligations around moving to the cloud, and these are ever increasing, and many organisations have significant cloud migration programmes coming to fruition which require suitable related assurance regimes.

What's new?

- Other emerging areas of regulation are relevant to cloud, and so it is increasingly important to ensure strong linkage between an organisation's cloud team and the regulatory and compliance specialists. For example, Operational Resilience Supervisory Statements released in 2021 by the PRA and FCA require organisations to consider their cloud usage and understand the implications of these services for their operational resilience. This has led to regulators requesting Internal Audit functions to review cloud related submissions, such as the cloud for outsourcing register completeness and accuracy.

- As cloud usage grows across the industry, the modification and "adaptation" of existing IT risk and control frameworks to address cloud risks is increasingly important. False 'baseline' assurance is often placed over fresh migrations to the cloud, where it is assumed that complete assessment of the controls and risks in the cloud environment has already been undertaken, but as organisations have moved gradually to the cloud, the risk profile or exposure may have changed since the cloud environment assessment. Ongoing risk assessments and assurance work over the operation of the controls is, therefore, key.

- Cloud transformation programmes have continued to be front and centre of many organisation's change agendas but are being delivered in unfamiliar circumstances during the COVID-19 global pandemic in the last 12-18 months. For large scale migrations (e.g. those which involve a complete exit of the onsite data centre), a strong level of assurance over the business case, cost savings, and performance metrics of the delivered cloud estate are paramount, as is the mapping of the organisation's control framework to the cloud solution controls to assess continuity of coverage.

- Software as a Service (SaaS) offerings, where a third party hosts and administers all aspects of the platform, including the actual application itself, continue to proliferate, and therefore third party risk management concerns become of increasing importance as part of the delivery of services. Cloud service providers are expected to have responsibility for a greater range of IT controls compared to models such as Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

2 ▲ (3) Cloud Governance and Security (continued)

What should Internal Audit be doing?

- Internal audit teams considering auditing cloud deployments or stable environments, should consider audits of (a) cloud governance, (b) cloud migration programmes, and (c) targeted reviews over one or more technical areas across a stable environment/deployment. These focus areas will enable an increased understanding of how effectively the organisation is identifying and managing the risks associated with cloud.

- Functions will need to reflect on the increasing adoption of cloud and consider the audit approach they will need to adopt. A cyclical approach of looking at elements of cloud deployment or application/ infrastructure components over a period of time may be appropriate for more complex or mature estates.

- Now may also be a sensible time to reflect on the assurance that is provided over cloud service providers, and whether piecemeal adoption of cloud solutions, has resulted in an overarching control framework which lags behind the prevalence of cloud usage. Focussing on management's understanding of cloud usage across the enterprise and the controls which prevent procurement of cloud capabilities outside of central IT knowledge and established procurement processes can be a useful area of focus here.

- Given the ever-increasing regulatory focus and overlap with other areas of emerging regulatory attention (such as Operational Resilience), functions should consider using multi-disciplinary teams and involve regulatory compliance audit expertise, for a broader and more comprehensive coverage of the associated cloud risks.

- Internal Audit functions need to evaluate and truly understand the risks in the context of cloud and how they should be controlled, ideally using automated and tech-enabled controls; for example development access to production environments could be controlled through configuration of cloud pipelines and controls over changes to code, rather than traditional controls such as manual reviews of user access lists.

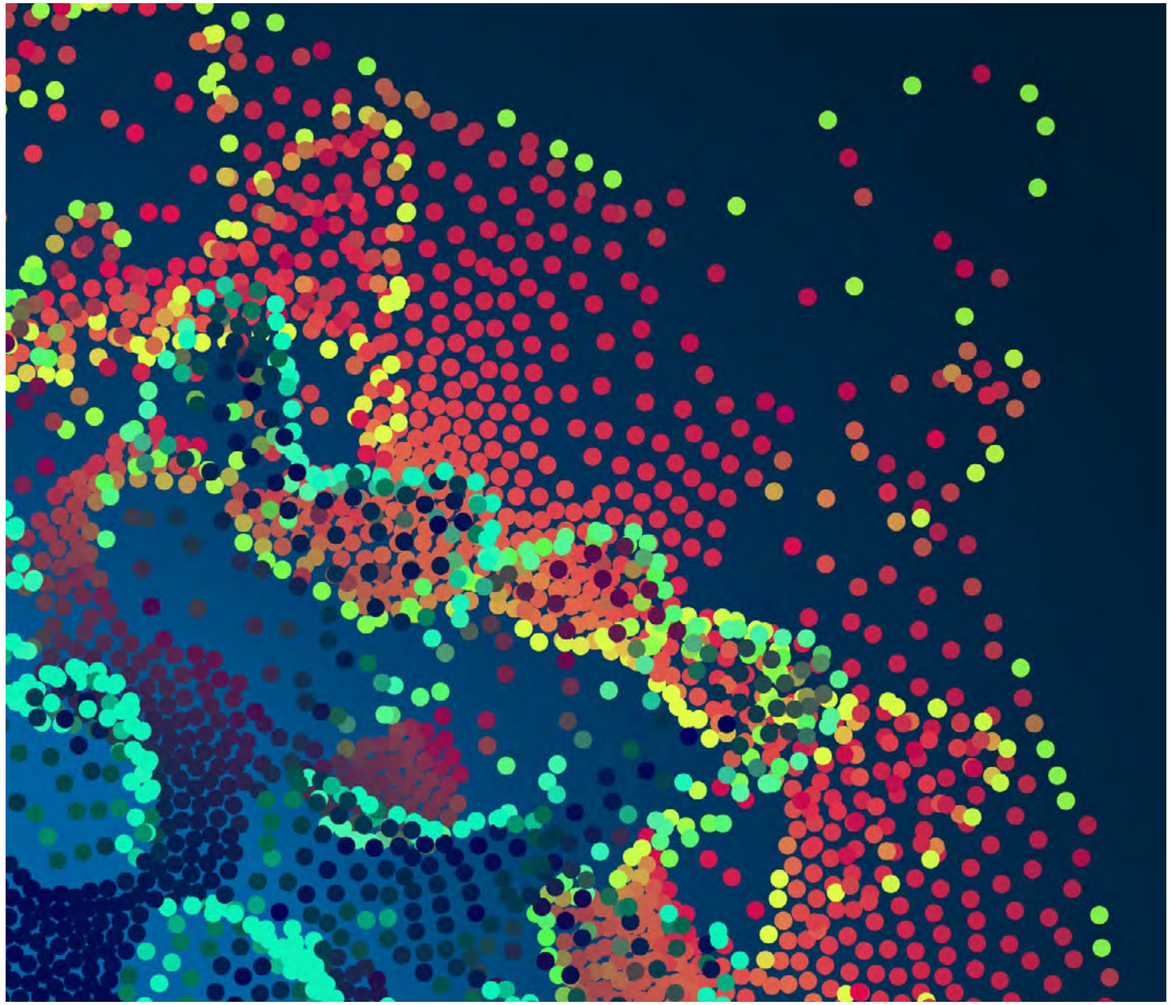
Find out more:

Cloud and regulation: overcoming the barriers

Cloud risk and compliance: Understand the landscape and meet requirements

Internal audit teams considering auditing cloud deployments or stable environments, should consider audits of (a) cloud governance, (b) cloud migration programmes, and (c) targeted reviews over one or more technical areas across a stable environment/ deployment.

3 ▼ (2) Operational and IT Resilience



Why is it important?

Businesses' ability to react to crises and major changes in working conditions continue to grow in necessity and successful enaction of Operational Resilience plans played a key part in enabling the Financial Services industry to adjust to a remote working environment where many have remained over the course of 2021.

The pandemic is a timely reminder of the changing world in which we live, and the need for organisations to be able to manage challenging circumstances and events successfully and effectively. The previous 18 months have tested firm's resilience to the limit, and this can be leveraged to enable a stronger and more successful response to the next disruptive event.

Operational Resilience remains a key regulatory hot topic, both now and into the future, and firms' need to demonstrate that a full assessment of their operational resilience has been completed and vulnerabilities have been identified with a view of being rectified as the highest priority.

Whilst Operational Resilience outcomes are currently being driven by regulatory requirements in the Financial Services industry (particularly in the UK), the principles and concepts around holistic consideration of resilience are very important to all businesses regardless of sector, and adoption of Operational Resilience approaches across broader geographies and industries will surely follow.

The previous 18 months have tested firms' resilience to the limit, and this can be leveraged to enable a stronger and more successful response to the next disruptive event.

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

Firms are likely to be running their Operational Resilience programmes over this entire period, to ensure they have sound, effective and comprehensive strategies, processes and systems in place to address the risk of operational disruptions.

What's new?

In March 2021, the UK's financial services supervisory authorities, the Prudential Regulation Authority (PRA), the Financial Conduct Authority (FCA) and the Bank of England, issued supervisory and policy statements setting out the final rules and expectations for Operational Resilience for firms and financial market infrastructures (FMIs).

Policy requirements will take effect on 31 March 2022, by which point businesses will be expected to have designed and implemented their framework. This is followed by a three-year timeline ending on 31 March 2025 during which firms are expected to have carried out the necessary remediations to their systems and processes, so that there are no instances where they are likely to fall outside of impact tolerance when stress testing their important business services under 'severe yet plausible' scenarios.

Firms are likely to be running their Operational Resilience programmes over this entire period, to ensure they have sound, effective and comprehensive strategies, processes and systems in place to address the risk of operational disruptions.

Ultimately the regulator expects that firms should as soon as reasonably practicable after 31 March 2022 and no later than 31 March 2025, have:

- performed mapping and testing to enable them to remain within impact tolerances for each important business service; and
- made the necessary investments to remediate where required and ensure operating consistently within impact tolerances.

What should Internal Audit be doing?

Internal Audit functions need to support firms in both the short term to enable the deadline of 31 March 2022 to be achieved and, also, over the longer term to support the build out and maturity of the Operational Resilience Framework.

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

Short Term: Readiness Assessments
Internal Audit's primary focus in advance of 31 March 2022 should be to assess the firm's operational readiness to meet the Operational Resilience requirements set out by the regulators. This may include gap analysis against the policy statements and should consider the documentation and evidence supervisory authorities expect to be in place by this date:

- Review how the firm has **interpreted the regulation** and taken actions in response to this, leveraging industry response and lessons learned from COVID-19.
- Assess the adequacy of firms' Operational Resilience **project and programme governance** in place to be able to develop and implement an Operational Resilience framework within the regulatory deadline of 31 March 2022.
- Review the **roles and responsibilities** which relate to Operational Resilience, and their adequacy for achieving the related goals of the business in relation to the regulation. This should include the **board's understanding of its own responsibilities** and where their sign off for the approach under the regulations is required.
- Challenge management's process for identifying the most **important business services** in order to prioritise work and investment in Operational Resilience, and whether the associated rationale for inclusion or rejection of business services as important demonstrate sufficient merit, and is built upon the 3 criteria on which this assessment should be made (levels of customer harm, financial impact on the business should something go wrong, systemic harm to the wider financial system).
- Assess the robustness of management's **process mapping**, including documentation of the people, processes, technology, facilities, information and third parties that support important business services in order to identify vulnerabilities and substitutions and to run meaningful scenario stress-tests.
- When considering the above process mappings, paying particular attention **to third party risk management**, as a key area of resiliency risk which has both i) typically not been well understood within organisations, and ii) is subject to parallel and related regulatory attention.
- Ensure that management has set appropriate **impact tolerances** that articulate the maximum tolerable disruption to important business services.
- Review the **severe but plausible scenarios** and stress-testing approach developed by management. Whilst substantial testing may not have been completed before 31 March 2022, management should have considered how they will assess the firm's resilience and demonstrate that this falls within the impact tolerances that have been set. Careful consideration should be given by Internal Audit as to whether the scenarios being used to really fit into the parameters of 'severe but plausible' and whether there is an adequate feedback loop of the results back to the selection of important business services and their related impact tolerances.
- Validate whether the firm has an adequate **internal governance** framework in place for managing Operational Resilience.

Review how the firm has **interpreted the regulation** and taken actions in response to this, leveraging industry response and lessons learned from COVID-19.

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

Longer Term: Building Maturity
Moving forward, the role of Internal Audit should move to more holistic, thematic based formats, challenging stakeholders over the validity and accuracy of outputs in line with changes in the external environment and maturing of the Operational Resilience Framework:

- Challenge and benchmark management's **scenario stress-testing programme and assumptions** regarding the nature, extent and duration of the included scenarios, as well as the plan to deliver important business services during prolonged uncertainty in a way that is safe, flexible and resilient.

- Audit should **consider carefully the timing and involvement of any procedures around scenarios stress testing** – as an important and challenging area within the overall Operational Resilience methodology, innovative audit approaches such as real-time reviews of the scenario modelling could help provide valuable assurance that the Operational Resilience Self-Assessment responses are based on well defined and executed models.

- Assess and monitor actions arising from scenario stress-tests to **address identified vulnerabilities** and enhance resilience, enabling the firm to demonstrate its ability to remain within impact tolerances in the event of disruption.

- Tracking of **costs and investment required to fix vulnerabilities**, and budgeting and resource planning around these areas is also key.

- Understanding the organisation's **'resilience toolkit'**; what else does the firm have available to it to respond to resiliency challenges? How strong and understood are recovery plans? Where can substitutions be made in the delivery of services, and how well is this already understood? Are crisis management processes and communication plans well understood?

- Evaluate the dedicated Operational Resilience management information provided to the Board and management committees, considering whether this is adequately robust.

- Review management's plans to roll out the firm's approach to Operational Resilience and consider progress made in **embedding** the framework across the business. Operational Resilience outcomes need to be delivered in a sustainable manner which ensures long term compliance with the regulation. Internal Audit should therefore be mindful of the **sustainability of Operational Resilience** delivery, after any related project or programme draws to a conclusion. Culture towards resilience and entrenchment of Operational Resilience within the delivery of the organisation's change agenda are both key areas to consider.

- Further on culture, assessing whether the organisation has **embraced resilience not just as a cost, but a means of obtaining competitive advantage**; if Operational Resilience is truly entrenched in the mindset of an organisation then the enhanced resilience outcomes which will be achieved over time, should result in better strategy achievement.

- For multinational organisations, Internal Audit teams will need to play their role in horizon scanning and understanding the international regulatory requirements around Operational Resilience, with increasing requirements around Operational Resilience in other legal jurisdictions (e.g. DORA and BASEL).

- Ultimately **operating within an acceptable tolerance** (i.e. within a tolerable level of impact) will be the focus for firms – whether that is through effective recovery, substitution of service, alternative procedures or a combination of all three.

Find out more

Deloitte Operational Resilience microsite

Operational resilience policy (FCA)

Operational resilience Supervisory Statement (PRA)

Time to Thrive

4 ▲ (7) Data Governance

Why is it important?

Data is arguably the most important asset an organisation holds. If used properly, it can change how the organisation operates, giving it the ability to make faster and better decisions as well as identifying areas of improvement. For Internal Audit functions, data can be used to support strategic activities and identify emerging risks. On an operational level, data-driven audits can be executed more efficiently, can deliver deeper insights, and provide management with a higher level of assurance.

While the benefits are clear, these opportunities come with risks that must be addressed. Increased regulatory scrutiny and unclear data governance requirements, uncertainty over data ownership and usage, issues with data privacy and data security as well as data quality issues which could lead to poor decision-making and lost revenue.

The last 18 months of upheaval across the global economy have clearly demonstrated the value of high-quality data to the corporate infrastructure, where the accelerated shift to the digital economy has meant high quality and secure data continues to provide a competitive advantage.

The last 18 months of upheaval across the global economy have clearly demonstrated the value of high-quality data to the corporate infrastructure.

4 ▲ (7) Data Governance (continued)

What's new?

Increased focus on data security

With the increased frequency and sophistication of cyber-attacks, the move to hybrid working and the continued shift towards cloud storage and computing, data security is becoming more and more important. Security teams rely on data governance to ensure that the appropriate metadata is captured to allow the data to be classified appropriately.

Enterprise data risk management and control

Many organisations have yet to define a central and dedicated data governance framework instead opting for a fragmented approach across multiple departments which leads to:

- undocumented and undefined ownership of data;
- lack of appropriate levels of data management responsibilities resulting in issues that are not identified, investigated, or resolved; and
- poor controls and no policies in place regarding accessing, handling, and processing data.

Firms should carefully review their regulatory reporting processes to ensure that their infrastructure, controls, and governance meet regulatory expectations. If there are gaps, plans should be put in place to address any shortcomings with a view to prioritise the control of data for regulatory reporting, and to demonstrate the reliability and provenance of data used for external and regulatory reporting.

Working across all verticals and functions, the Head of Data Governance is accountable for driving enterprise-wide utilisation and governance of the data assets. By being the bridge between the business, IT and data owners, they have helped improve financial performance, supercharge operations and support data privacy and compliance management. They are also responsible for establishing a data-driven culture to support the achievement of strategic objectives.

Increasing pressure on Regulatory Reporting

The Prudential Regulation Authority (PRA) has issued a further 'Dear CEO' letter in relation to Regulatory Reporting on 10th September 2021 reflecting on the findings of the S166 reviews conducted earlier. The previous letter was issued in October 2019. This clearly indicates the regulator's concern over the lack of progress in areas outlined in its original letter and how firms have not been able to sufficiently demonstrate their adherence to standards expected by the regulator.

Some of the challenges faced by financial institutions around core regulatory reporting include:

- Ever-increasing complexity in the reporting systems;
- Difficulty in interpreting regulatory requirements;
- Shrinking reporting timeframes to ensure a timelier view of financial risks; and
- Reliance on manual processes with multiple siloed systems to meet complex requirements.

In addition to this, tech giants and other large multi-nationals are coming under increased scrutiny around how they manage and process personal data. Organisations are expected to move beyond compliance to a point that they are considering the ethics of processing data.

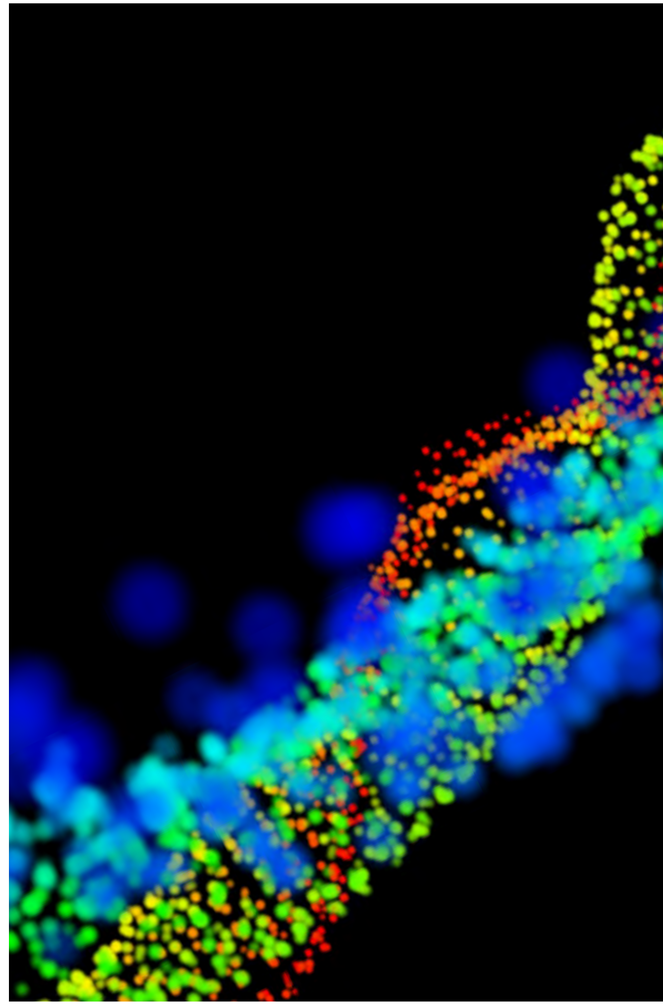
4 ▲ (7) Data Governance (continued)

What should Internal Audit be doing?
Internal Audit can play a pivotal role in promoting the strategic value of data governance. Its unique reach within the organisation coupled with its risk management and problem-solving skills make the function a critical contributor in defining and promoting the organisation's data governance framework. Internal Audit is also able to bring many industry perspectives by benchmarking against peers and similar sized organisations.

In turn this will also strengthen Internal Audit's data and analytics driven activities as the function will be exposed to data sources across the organisation. The function can discover new data sources and document key information such as data availability and access, stakeholders, and data quality. This information can be used to support future audits throughout the entire lifecycle.

To support the design and implementation of a data governance framework, Internal Audit should consider the current state of data governance and help reinforce the capabilities by:

- **Actively participating in data governance groups:** Internal audit can support data governance communities by inputting from a risk and control perspective whilst gaining first-hand exposure to developing areas;
- **Assessing data governance controls:** Assess and evaluate the controls surrounding various data sources, critical backups, and data migration plans whilst evaluating how prepared the function is to deal with a data crisis;
- **Reviewing data policies:** Internal Audit should also ensure that all policies around data collection and retention policies are well documented;
- Maintaining an independent data catalogue: Any data sources identified as part of an audit should be documented and classified for future reference;
- Review risk model considering whether data is processed, obfuscated, analysed and presented in a way which is ethically and socially responsible;
- Test effectiveness of controls that are in place to protect data; and
- Consider the implications of offshoring data where cloud infrastructure is in place e.g. are teams cognisant of where data is being processed and stored and the legislative requirements that apply in these jurisdictions.



5 (5) Transformation and Change Assurance

Why is it important?

The requirements for organisations to deliver rapid and successful change across a broad range of initiatives, to support the digitisation agenda and remodelling of business structures to reflect the ever-changing corporate environment have been increasing. As a result we continue to see significant demands for assurance across programmes and projects with wide ranging remits, in order to identify risk to execution and maximise the probability of programme success.

With the macro-economic environment subject to significant and ongoing wholesale change due to COVID, climate change, continued geo-political changes such as Brexit, and any number of regulatory requirements across sectors, the trend for increased and faster paced transformation initiatives will continue to accelerate. As the uncertain economic environment in the last year caused many organisations to reduce or halt their strategic initiatives, we see significant pressure to deliver this delayed pipeline of activity as economic activity bounces back globally. Against a background of high rates of failure in relation to programme delivery, and light touch portfolio management and prioritisation governance, successful transformation and change delivery, and assurance continues to be very important.

What's new?

Whilst many of the concerns around programme delivery and assurance are not new, some of the ones we regularly see are as follows:

i) No methodology/third party methodology being followed in programme delivery.
ii) Failure to define programme benefits and requirements adequately.
iii) Inadequate assurance time dedicated to large scale programmes.

Additional risk factors as a result of recent changes in the business environment:

Remote delivery of programmes – Remote and hybrid delivery is placing additional challenges on programme delivery, particularly when collaborative working techniques aligned with Agile principles are being adopted.

Real world challenges accelerating demand for solutions via strategic change – Pace of change, capacity within change delivery teams, and the ability to maintain sufficient emphasis on quality during programme delivery are increasingly competing factors in successful change delivery.

Dev ops, agile and other modern delivery methods – Challenges around methodology, control, and Internal Audit expertise to provide effective assurance over these newer areas of programme delivery continue to grow.

Collaboration tools – Collaboration tool adoption such as Azure Dev Ops, Jira, and Confluence has become a pivotal area of focus for successful delivery of change and are now mainstream in their usage across industries.

Constraints around access to experienced change practitioners – The prevalent skills shortage, changes to IR35 rules, as well as personnel changes in response to the changing economic environment, have resulted in a challenging environment for programmes to gain access to the skills and experience they need to deliver successfully.

5 ◀▶ (5) Transformation and Change Assurance (continued)

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 organisational strategic objectives, including regulatory requirements, 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, and 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'. Analytics, especially visualisation tools, are invaluable in change portfolio management. Deploying data visualisation can increase the visibility and accountability by profiling the portfolio's delivery timelines and identifying potential bypassing of change controls.
- **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.
- **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.
- **Third Party Assurance:** With the move away from individual contractors, there are increased levels of third party relationships and corporate alliances to deliver change, including via cloud providers, and Internal Audit functions need to support in the assurance of these changes, and appropriate oversight of strategic supplier delivery.

Find out more

Assuring Agile Programmes and Projects

6 (6) Digital Risk

Why is it important?

The pandemic has accelerated the trend for increased use of digital services by both corporate and personal customers, across the UK and global economy, and the Financial Services sector has been no exception to this. Businesses across all sub-sectors of the FS marketplace are considering their digital strategies to stay competitive. More than ever seen before, in response to customer expectations, businesses are offering new innovative digital services.

Whilst the transformation of digital services, as a result of the pandemic, has not been as pronounced in the FS sector as in some others (retail for example), those organisations which have embraced digital services to a greater degree have generally been better placed to adapt and respond to their changing consumer demands.

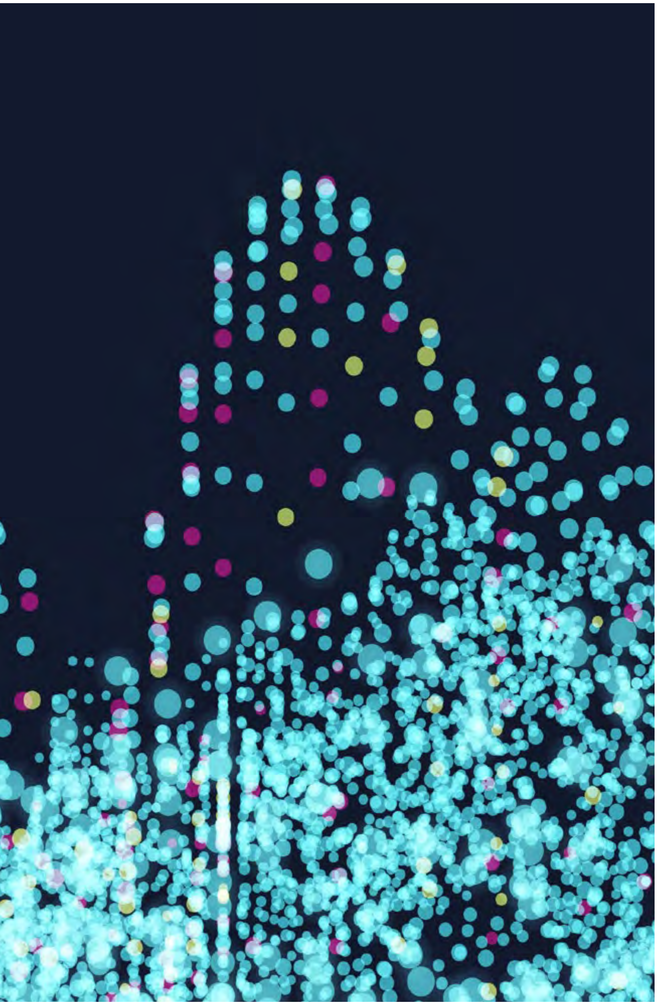
Fast paced change and adoption of digital services does, however, bring with it a plethora of risks to be managed, and many businesses are challenged to evolve as required, whilst also managing these risks effectively.

What's new?

- The last 18 months has seen the wholesale interruption of established supply chains for Financial Services products, alongside changing product requirements from customers.
- The velocity required by FS organisations to successfully change their digital presence, across new products, new digital challenges, whilst managing increased demand on existing web and mobile digital channels has been unparalleled.
- The regulatory framework around digital services continues to evolve, with areas such as cloud, operational resilience, and third-party risk management, all being subjected to increasing levels of regulation.
- As digital becomes increasingly central to organisations' business strategies, it is becoming more challenging for businesses to ensure they have the right skillsets on hand, from a technical standpoint as well as the associated transformation skills for digital delivery (agile, Dev Ops etc).
- Further the requisite skills and methodologies to provide risk and compliance assurance from all three lines of defence over digital areas remain in short supply.
- The convergence of domains and associated risks such as conduct and digital (for example where artificial intelligence is making customer decisions), continues to evolve and drive the continuing regulatory agenda in relation to digital domain.

Businesses across all sub-sectors of the FS marketplace are considering their digital strategies to stay competitive.

6 (6) Digital Risk (continued)



What should Internal Audit be doing?

- Internal Audit functions need to remain sufficiently close to the organisation's Digital strategy, as well as the business strategy to be able to register when the two might be diverging. In the wake of the pandemic, this may be a good time to reassess the business fit of the technology strategy (including digital).

- Review whether the 2nd line framework-driven approach to risk management meets all the needs of the business in managing risk day to day. If not, what is the gap and how can Internal Audit functions support the business in closing the gap.

- Coordinate with other lines of defence at scoping and planning assurance activity on digital (given scarcity of skills) aiming for a combined view across the lines of defence how to best focus risk and audit resources on areas of highest risk.

- Functions need to stay close to regulatory developments in this space, being mindful that the definition of 'digital' should embrace: (a) products and services, (b) ways of working and channels but also (c) infrastructure / technology. In terms of the latter, we expect regulatory focus on the disruptive technologies, with the European Commission releasing its highly anticipated Artificial Intelligence (AI) Act earlier in 2021. It represents their attempt to regulate AI technologies to date, encourage investment and innovation in AI, and build public trust that AI systems are robust, controlled, safe and used in ways that respect fundamental rights. The Act considers the introduction of a four-tiered risk framework, which recognises the varying levels of risk posed by AI systems and sets out proportionate requirements and obligations per risk level.

- Review of critical themes and key risks which reflect the interplay between technology digital, regulatory requirements, and business processes, can also inform the digital risk landscape, such as:

  - Product design governance.
  - Web and mobile development processes.
  - Data governance and security.
  - Digital customer journey design and implementation.

Find out more:

Digital Risk Turn Digital Risk to Digital Advantage

7 ▼ (4) Extended Enterprise Risk Management

Why is it important?

Whilst not every organisation is necessarily increasing the volume of engagement with third parties in its ecosystem, we are observing a trend of organisations becoming increasingly reliant on third party relationships. Reasons for this include the nature of the relationships, how bespoke the services are being tailored (making substitutability challenging), or even how 'close to core' the services are. The financial impact of a failure in this ecosystem is costly (through fines, loss of custom or reputational damage).

In addition, the COVID-19 pandemic has rapidly increased focus on third party risk as firms have seen accelerating digitisation across entire operations, with traditional services and operating models requiring unprecedented changes to new ways of working in such a short space of time.

Furthermore, regulators are providing more clarity and greater harmonisation of third party risk regulations in 2021, providing increased direction for firms operating across multiple jurisdictions, greater linkages to third party management and operational resilience across group level entity structures and heightened data security requirements, including use of the cloud.

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

What's new?

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 on third party risk that have broadened requirements for firms.

The Prudential Regulation Authority's (PRA's) Supervisory Statement (SS) 2/21, that was published in March 2021, 'Outsourcing and third party risk management', makes it more explicit that firms are now 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.

In addition, the PRA's SS2/21 and SS5/21 on 'International Banks: The PRA's approach to branch and subsidiary supervision', have started to increasingly focus on the risks that may arise from intra-group outsourcing. The Regulators do not necessarily consider intra-group outsourcing as carrying less risk compared to external outsourcing services, but they acknowledge that firms may adjust due diligence requirements and adapt contractual clauses depending on the level of 'control and influence' they have over the intragroup entity.

7 ▼ (4) Extended Enterprise Risk Management (continued)

What should Internal Audit be doing?
Internal Audit should consider if the firm has an adequate Third Party Risk Management (TPRM) framework embedded across the business and should examine this from both a design and an operating effectiveness perspective:

Design effectiveness:
Assess if the following factors are designed adequately:

- Overarching governance model;
- TPRM framework and associated policies;
- Appropriate allocation of roles and responsibilities;
- Processes and controls to manage third party risks throughout their lifecycle;
- Tools and technologies supporting the TPRM process; and
- Appropriateness of metrics used to measure risk appetite and tolerance within the organisation.

Operating effectiveness:
Assess control performance in the following areas:

- Risk identification and assessment;
- Third party selection;
- Contract execution;
- Role and responsibility allocation;
- Ongoing monitoring and reporting assessment appraisal; and
- Contract termination and exit or renewal management.

Hot topics:
Given the uncertainty brought about by the COVID-19 pandemic, particular focus should be given to understanding how the TPRM framework assesses and monitors financial insolvency, operational resilience, subcontracting risk and digital risk. For example, Internal Audit should be understanding how the business is utilising tools that enable access to real-time information to supplement the more traditional 'point-in-time' data that is collected, which we are seeing has become a key funding priority as firms continue to respond to the pandemic.

Regulatory compliance:
Assess adherence to key regulatory requirements, including the:

- Financial Conduct Authority's (FCA's) SYSC 8.1 general outsourcing requirements;
- FCA's Senior Managers and Certification Regime, particularly SMF24 responsibilities;
- PRA's SS2/21 Outsourcing and third party risk management, and relevant sections of SS1/21 and SS5/21; and
- Outsourcing guidelines published by European Banking Authority, European Securities and Markets Authority, European Insurance and Occupational Pensions Authority and others.

Find out more:

Deloitte Global third party risk management survey 2021

8 (8) IT Strategy and Governance

Why is it important?

IT Strategy continues to remain a significant area of focus, particularly as the economic and social shifts of the last 18 months, have upended operating models, with IT responses often being tactical rather than strategic in nature, and consideration of IT strategy (and very often business strategy) playing catch up.

With the likelihood of a continued trend for digitisation and accelerated change delivery, IT strategy and governance needs to be both streamlined, and also in some cases, enhanced.

What's new?

Key developments have been a trend to shift from project focused to product or value chain focused operating models for the delivery of change, with corresponding impacts on approaches to IT strategy. IT strategies continue to flex from having a basis in large scale strategic change programmes, to incremental change and improvement, and a product centred architecture and approach to change delivery supports this increased dynamism.

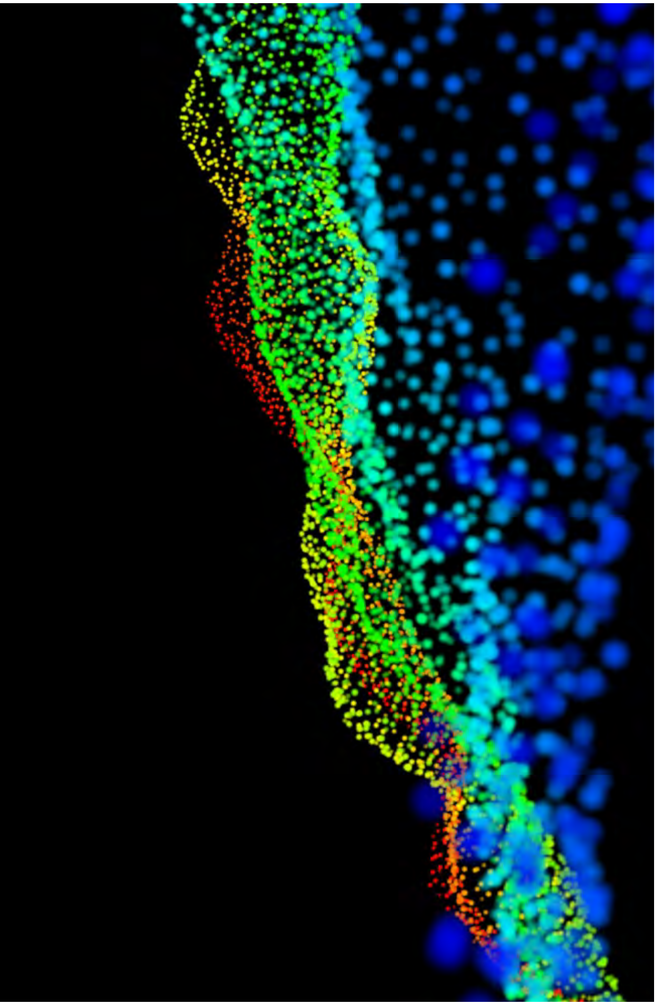
However only in the most mature organisations has this refactoring to product centric delivery models, reached the upper echelons of change delivery mechanisms (e.g. budget and strategy), although a number of organisations have achieved changes within Business Analyst and Operations Teams. Other key areas to support the transition are within service management where skills in Agile/Dev Ops and cloud, further enhance the ability to support a product centric operating model.

Ultimately businesses may soon have to evolve from the concept of having separate strategies for technology and business aims and produce corporate strategies which include digital and technology components as a core integrated element of the main strategic outputs.

The pandemic has demonstrated to businesses globally they can make fundamental changes to their business model (remote working) overnight, and yet survive and in many instances thrive as a result, so an increased thirst to be able to adjust strategic direction in response to external stimuli is likely.

From a governance point of view, challenges remain around management of IT risk holistically, including KRIs, reporting, and ownership of controls, to name a selection, but in the face of accelerated strategic change, the pressure to digitise and 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?

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

Harmonisation of Business and IT Strategies

- In an increasingly digital world, have 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.

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.

Digital Strategy and Architecture

- Internal Audit should determine whether digital strategy is being adequately catered for during business and IT strategy setting processes, and also whether the architecture strategy for the business is being adequately considered as well.

Find out more:

Global Tech Trends – Strategy Reengineered

9 ◀▶ (9) Payments

Why is it important?

New technologies and changing customer expectations are driving significant growth and innovation in Payments. A large number of new players have entered the space and existing players are expanding into new markets. As this happens, major new regulatory requirements are coming to the fore and require significant investment and attention, particularly from banks and payment providers.

What's new?

There are some major changes being enforced by key regulation that are impacting payment firms. SWIFT payment messages are moving to the globally common ISO 20022 standard and this is gathering momentum, requiring major programmes to implement as well as a strategic transformation focus from banks to unlock its full potential, and consideration from other payment providers. ISO 20022 allows an enhanced data set to be included within financial messages, providing a number of key benefits.

Another key area seeing notable development amongst banks, Financial Market Infrastructures (FMIs) and payment providers is operational resilience which is becoming an urgent priority for Financial Services regulators, driven by increased technology proliferation and rising cases of technology failures and cyber attacks. Firms are having to respond to detailed regulatory requirements to put in place major programmes to address operational resilience throughout their businesses.

The digital assets ecosystem is also in a state of major evolution with further institutional interest from major banks and asset managers. The issuance of CBDCs and stablecoins is on the agenda of all major central banks including the Bank of England. As regulations evolve and further licensing requirements come into force, firms will need to assess their business models and strategy to align with their local regulatory perimeter, for example, registration requirements under AMLD5 and upcoming Markets in Crypto Assets (MiCA) in the EU.

They will need to carry out a product review of their entire digital assets product inventory to identify 'product classification' which will ultimately inform financial and non-financial risk reporting requirements. They will also need to enhance their risk management frameworks related to their Foreign Exchange (FX) and payments business lines to mitigate additional risks specific to digital assets.

9 ◀▶ (9) Payments (continued)

What should Internal Audit be doing?

ISO 20022:

Internal Audit should perform a detailed review of ISO 20022 programme activities to validate that regulatory deadlines will be met, and that 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.

SWIFT will enable ISO 20022 messages for cross-border payments and cash reporting businesses starting from the end of 2022. Existing messages used for cross-border and cash reporting payments will be decommissioned in November 2025. Impacted firms have the option to use message translation services to convert messages into the new format.

Direct participants in CHAPS will need 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 currently assessing CHAPS participants' readiness for these key dates. 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/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.

ISO 20022 migration is inherently complex, posing serious challenges for impacted firms, in particular:

- Impact on banks across business, operations and technology requires careful and comprehensive consideration, including significant impacts to bank technology stacks.
- Competing priorities may place a strain on successful migration with banks dealing with COVID-19, mandated infrastructure initiatives such as Open Banking, and large-scale transformation programs.
- The scale of the migration can put intense pressure on business and technical resources.

Digital Assets:

As firms offer new products and services relating to digital assets, Internal Audit will have a key role to play in providing assurance that the firm meets it regulatory requirements and maintains a robust risk management framework while offering innovative digital products and services to satisfy customer needs and expectations. In particular:

- **New Product Approvals:** Assurance should be carried out to ascertain that product approval requirements and new business initiatives were reviewed and approved through a bank's existing Product Approval Committees before any external announcements were made or contractually binding commitments entered into. Given the regulatory scrutiny and sensitivity around digital assets it is imperative that firms follow established processes and standards to protect themselves and their clients.
- **Risk and Control Enhancements:** Internal audits conducted for a bank's risk function should concentrate on the steps carried out by 2LOD to mitigate additional risks arising in key risk domains (i.e. operational risk, compliance and regulatory risk, market risk, credit and liquidity etc.) when offering digital assets, including controls enhancements carried out. Many payments digital assets, e.g. crypto currencies, are highly volatile and require enhanced statistical modelling to mitigate financial risks related to them. Additionally, when working with clients with digital assets exposure (e.g. Virtual Asset Service Providers), banks will need to carry out enhanced due diligence during on-boarding to meet AML/CTF requirements related to digital assets. Internal Audit should comment on the enhancement carried out to the firm's AML/CFT framework to mitigate new risks posed by digital assets and service providers related to these assets who the bank may on-board as clients.

Find out more:

Global payments remade by COVID-19: Scenarios for the global payments ecosystem

10 ★ (–) Application Controls and Integrated Auditing (NEW)

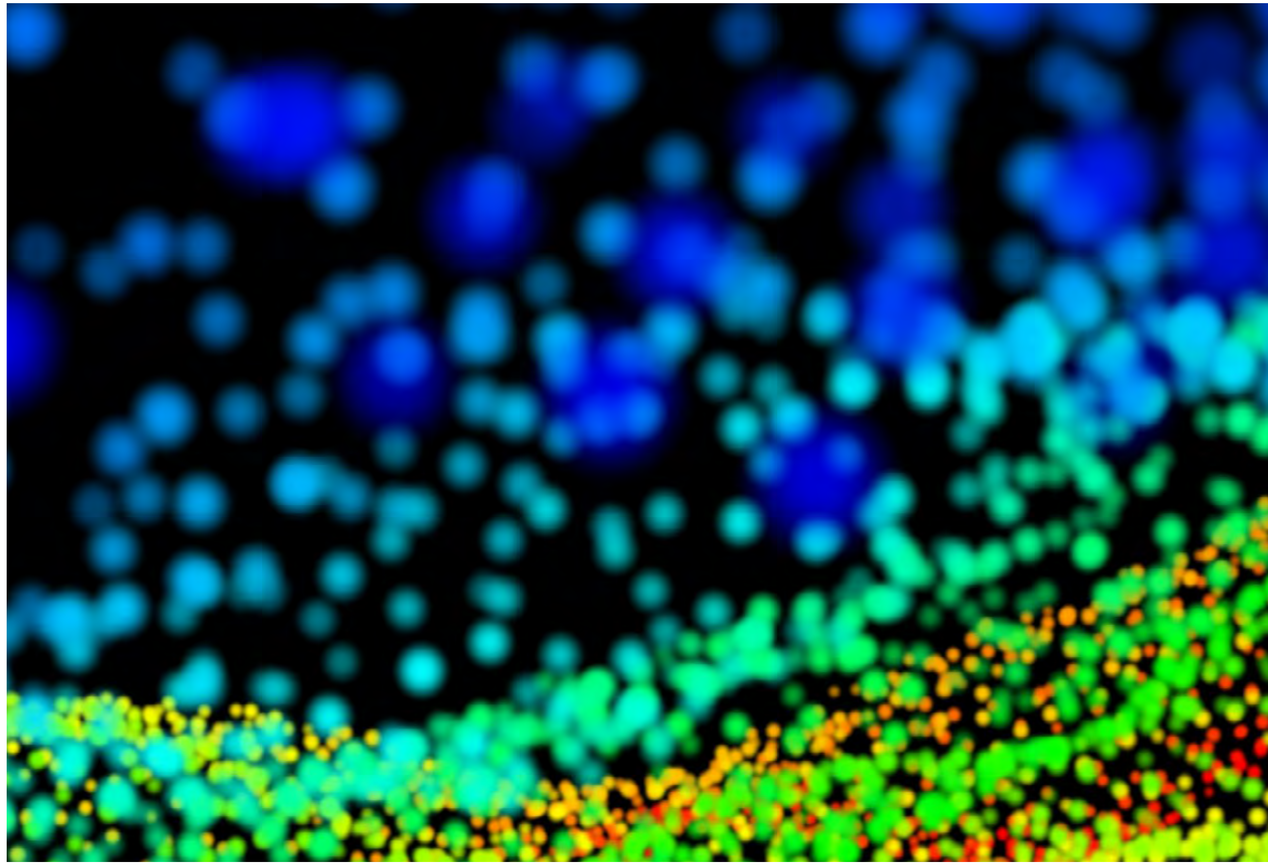
Why is it important?

A core component of any organisation's IT Audit Universe should be the application systems that support the processing of business transactions as part of the customer journey. 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. At the same time, adequate audit attention should be placed on the 'technology enabled' or automated application controls in support of system processing, providing assurance that, in conjunction with relevant manual controls, business process risks should be appropriated managed.

What's new?

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 financial 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.

Many organisations have started considering their roadmap to that end, 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 financial reporting will be of increased importance.



10 ★ (–) Application Controls and Integrated Auditing (NEW) (continued)

What should Internal Audit be doing?

- Whilst Internal Audit functions will be a key stakeholder for the new proposed controls regulation, nicknamed 'UK SOX' 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 have a role to place in the following:

  - Challenging management's financial risk assessment, to show the breadth of areas likely to be in-scope and

  - 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 controls that need to be identified and tested, include the core General IT controls (e.g. access controls) but also entity-level, and process-level controls. Given the dependency on applications systems to run such processes many of these controls are automated and embedded within the systems (e.g. configurations, tolerances and limits, segregation of duties, enabled/disabled functionality etc). The experience of US SOX showed how important it is for the latter to be audited using a joint multi-disciplinary team that includes technology and application expertise.

- To provide such assurance, Internal Audit would need to work effectively in an 'integrated' manner, supported by auditors combining technology, application knowledge, business process understanding, as well as regulatory expertise, where this is required. This is not always easy or straightforward, due to resourcing constraints, scheduling, and capacity conflicts, or simply because of the notion by some that omitting automated controls or not involving technology auditors may be an easier and faster way to execution.

- Effective application audits are resourced by multi-disciplinary teams, working closely together in a collaborative and agile manner. Planning and scoping should demonstrate a clear mapping and alignment of the higher-level, business process risks all the way to associated manual and application automated controls that help mitigate these in a multi-layered manner, as well as the core general IT controls, which act as the foundational blocks that bring stability and security.

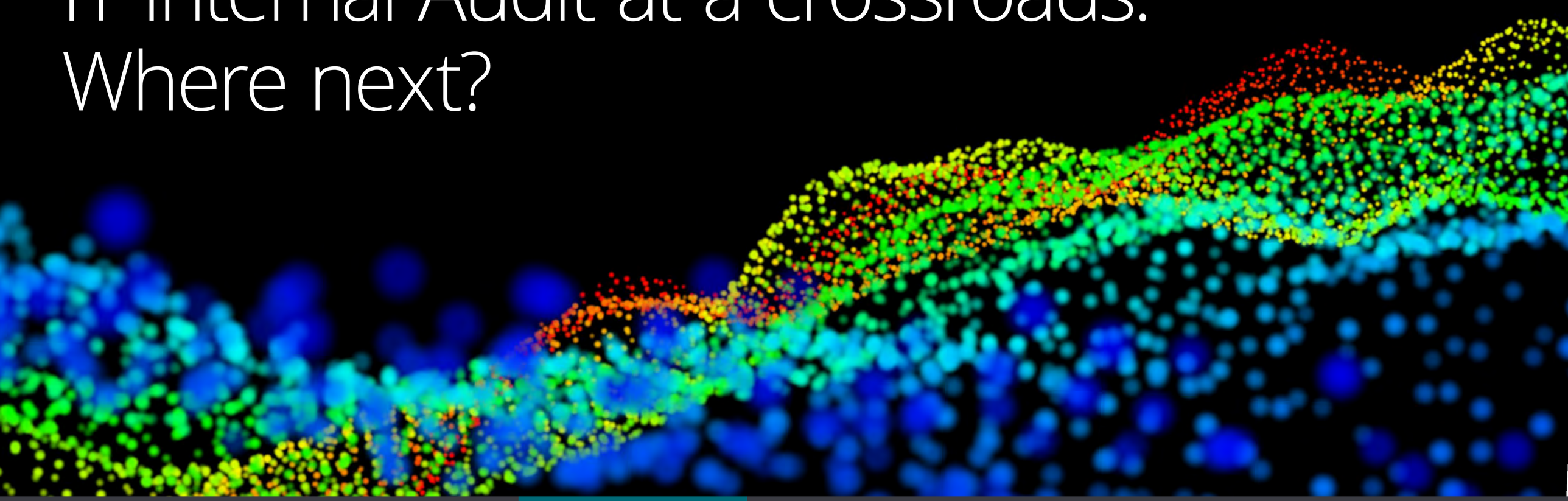
- Audit reporting in those cases present findings and controls issues in a manner that reflects the lineage between the IT issue all the way to business process risk, allowing the auditor to credibly opine on risk exposures after having considered the effectiveness of the broader internal control environment. This naturally leads to increased assurance, a more pragmatic ways of looking into the risks and helps strengthen the organisation's control environment.

Find out more:

Considerations for Internal Audit in light of UK SOX

3

IT Internal Audit at a crossroads: Where next?



IT Internal Audit at a crossroads: where next?

Some recent reflections

The role, position and influence of IT Internal Audit remains critically important, and reflects the wider trend around a growing focus by boards, executives and regulators, on technology risk, cyber, and risks associated with the rise of disruptive digital technologies.

The consistency in the ranking of many of the themes across the years, may be interpreted by some as signs that improvements in the standard of control are not being achieved, or that organisations continue to struggle with long-term deficiencies. While there may be some truth to this notion, given the complexity of a technology estate and architecture that constantly changes, we also believe that:

- The regulatory expectations regarding the standards of control to effectively mitigate risks that are mutating and evolving continuously, such as cyber, cloud or data, add an additional layer of challenge to management's remediation efforts, but also Audit's focus in terms of breadth and depth of coverage.
- Certain remediation or control improvement initiatives (such as privileged access management, or legacy platform replacement) are long-term, inherently complex programmes which require time to embed and deliver the requisite control improvement benefits.

What should IT Internal Audit do?

With a new world now appearing following the global pandemic, functions should take the opportunity to consider what these socio-economic changes mean in terms of their role and position for the future. They need to assess how they can adjust and adapt in order to continue to achieve their core remit of supporting the function to assure, advise and anticipate technology risks – current and emerging – in an effective manner.

On that basis, what strategies could Internal Audit functions consider and adopt to best support their effort to keep pace with technological change, create value in an innovative way and enhance its impact and influence?

Firstly, let's explore some of the most common issues with technology control environments:

1. **Immature culture within IT departments towards operation of IT controls** – the focus on 'getting things done', 'fast time to market', 'break things to move fast' historically has led Technology and Engineering team on a path where risk awareness and strong risk and control culture weren't necessarily the priorities. In many organisations IT risk and control responsibility has been devolved into specific teams within first line, rather than being built into the job accountabilities and core capabilities of delivery teams.

2. **Missed opportunities to embed a robust system of internal controls as part of strategic projects such as system implementations, cloud migrations** – often we observe large strategic initiatives have insufficient emphasis placed on the associated control environment. Governance and control are often sacrificed when programme budgets or deadlines are at risk, resulting in missed opportunities to strategically improve the IT control environment .

3. **Inadequate investment in IT risk and controls across first and second line of defence management teams** – it remains very common for dedicated IT risk personnel to be relatively few in number compared to the requirements of the organisation, and investment in skills and training around IT risk management is not always commensurate to the IT risks the organisation is facing or has to manage.

4. **Failure to adequately leverage the potential for automation** – In most organisations the opportunity for digital automation of the control environment has not yet been explored fully. Given the plethora of relevant skills, but also opportunities for automating simple tasks, processes, reporting across IT, this is a significant strategic opportunity for the future of the functions.

IT Internal Audit at a crossroads: where next? (continued)

So, what is next for Internal Audit? What should functions do to take a step back, modify their approach and adequately respond to these challenges?

- **Broaden recommendations in relation to individual control failures** – Question why the failure was not detected by existing controls or identified by the oversight and governance (e.g. 2LOD) mechanisms. IT control improvement recommendations often focus on improvement of the direct preventative control which has failed leading to an audit finding, and not always on the genuine root causes, the broader requirements for appropriate detective monitoring controls, and the wider risk and governance failure that have contributed to the weakness.
- **Automation of IT Controls** – IT controls tend to be data rich in nature, lending themselves well in many cases to the use of analytics or automation. Audit has a role to play in terms of providing advice and support along this journey of automation.
- **Deployment of analytics over the IT control environment by Internal Audit** – considering where and when analytics can be developed and then 'left behind' with the second or first lines, has historically been an effective way for Internal Audit to improve risk management practices across the organisation, whilst discharging their advisory roles.
- **Adequate consideration of risk awareness and risk culture** – many functions already include risk and control culture as a key consideration as part of standard audit delivery, or via a separate assessment, however this is not yet sufficiently adopted as a practice across the industry and there is certainly opportunity for improvement.
- **Risk and control considerations as part of strategic project delivery** - very often organisation's fail to take full advantage of large strategic projects to fundamentally challenge and improve the existing control environment. Internal audit should make this a key focus as part of their real-time project assurance reviews, with adequate focus on how control redesign is baked into requirements setting, and indeed the benefits and business case for the entire programme. Early identification of the need to introduce and embed controls to new systems architecture is crucial, and can contribute to an enhanced control environment.

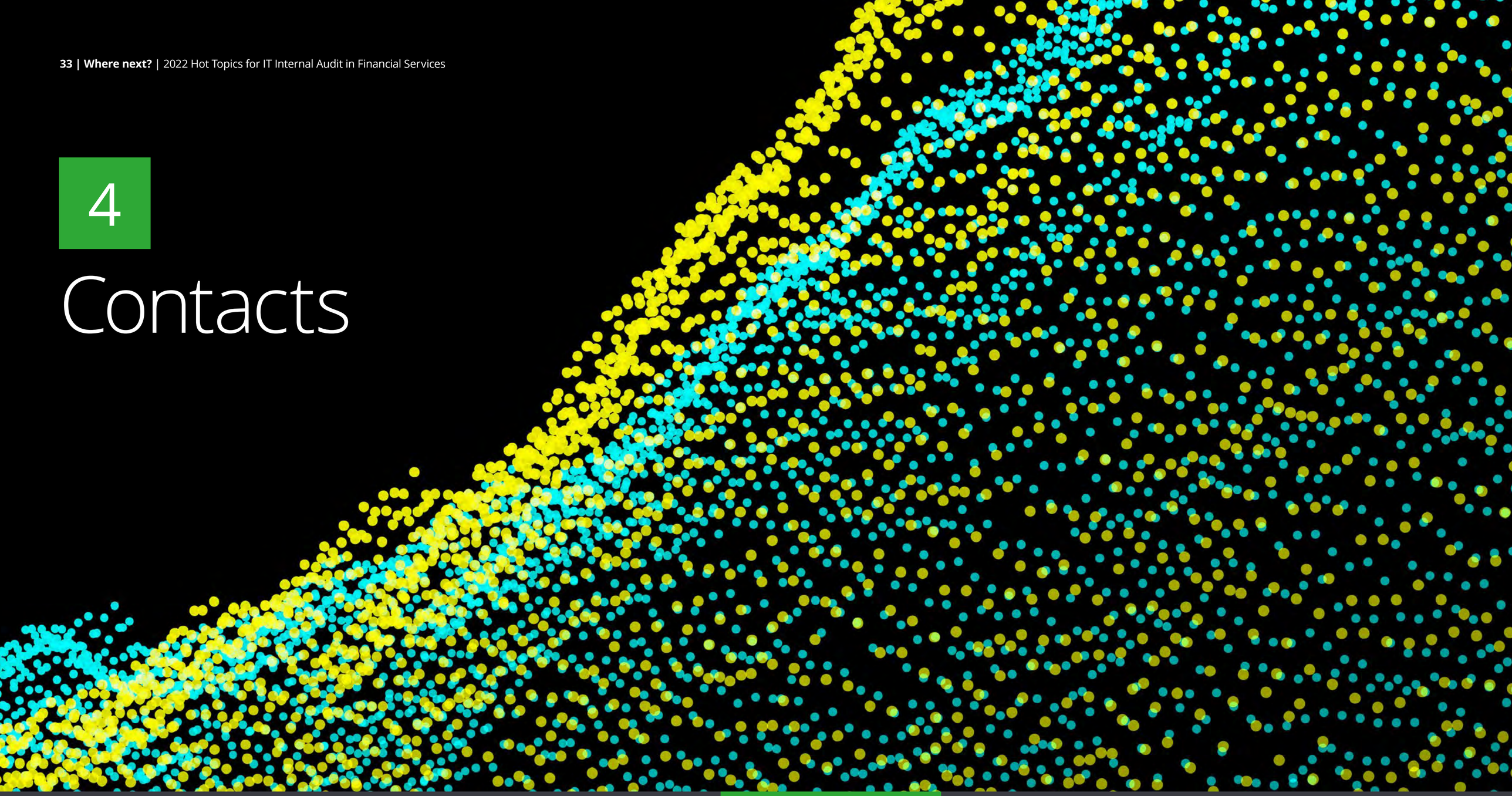
An effective IT Internal Audit function actively contributes to setting and delivering a vision, as part of the strategic direction of the Internal Audit function overall as well as the organisation.

Conclusion

In our view, an effective IT Internal Audit function actively contributes to setting and delivering a vision, as part of the strategic direction of the Internal Audit function overall as well as the organisation. It seeks to keep pace with technological change, create value and enhance impact and influence not only across the CIO organisation but also more broadly.

What this vision means, will differ from organisation to organisation, and will be governed by the need to get attuned to the strategic organisational direction and overall business change. The strategies discussed in this section should help functions provide assurance in an innovative way, advise in an insightful manner, create value and enhance impact and influence across the organisation.

4 Contacts



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.