Deloitte.

Staying Relevant

2020 Hot Topics for IT Internal Audit in Financial Services

An internal audit viewpoint

Contents

1. Introduction

1 Introduction

I am pleased to present our latest viewpoint on the information technology hot topics for Internal Audit functions in financial services.

As in previous years, this is based on our survey across UK financial services organisations and our discussions over the past 12 months with Chief Internal Auditors and Heads of IT Audit, who have openly shared their areas of focus and the organisational challenges in relation to their firms' technology control environment.

In this publication we provide a view of their planning priorities, covering both why each topic is relevant and of particular focus to the organisations we surveyed, and also what Internal Audit functions may consider, or seek to do differently, in order to address the associated risks.

We anticipate an increased internal audit focus in 2020 on digital, disruptive technologies – elements of which have been added to many internal audit plans – as well as continued emphasis on cyber, strategic change assurance and third party risk. You will also notice, Operational resilience has emerged as a key area, following recent regulatory and business focus. This is a topic which, of course, encompasses other high-impact domains, such as cyber and technology resilience, crisis management, incident response and recovery.

Section 4 of this publication focuses on the areas of focus for IT audit plans (the hot topics) and, hopefully, will help provide insights on "what and how to audit"; section 2 details our view on some of the aspects that will influence the future shape of Internal Audit functions. We have captured these thoughts under the strap-line staying relevant, where we explore this challenge in an ever changing social, corporate and technology environment. Specifically, it offers our views on the benefits and challenges of "automation", the use of data-driven auditing and digital technologies to deliver efficiencies and boost the influence and value they offer the business.

We hope this paper helps inform your 2020 planning, and continues the healthy debate on how to improve the role of IT internal audit, as a relevant, influential and insights-driven function.

Mike Sobers,

Partner

2. IT Internal Audit of the Future: Adopting Automation

2 IT Internal Audit of the Future: Adopting Automation

Staying relevant

Organisations have recognised that barriers to entry are falling in every sector, with new entrants and digital start-ups taking advantage of cloud computing and open source software. In response, we are seeing business leaders embracing innovation and emerging technologies to transform their businesses and gain competitive edge.

In this environment, we see Internal Audit functions asking how they can stay relevant, how they can enhance the value and impact of service they provide while at the same time nurturing and retaining strong talent. Our survey showed that in the past few years leading functions have been focusing on integrating 'innovation' based roles and changing the way they operate from traditional to more agile models. They are embracing the use of data-driven auditing and enabling digital technologies to boost the value they offer the business and, to an extent, futureproof the function in an ever-changing social and corporate environment and culture.

Our survey showed that some of the key challenges functions are facing this year (as the word-cloud of responses shows below) are around harnessing the pace of change, innovating to stay relevant, adopting new data or tools-driven approach to transform the way they operate or provide their services. Resourcing remains a challenging area, as the desirable skills (or, better, combination of skills) is hard to find and retain. This section will provide some of our viewpoints on the above.

2 IT Internal Audit of the Future: Adopting Automation (cont.)

Digital enablers

The Deloitte Internal Audit 3.0[1] framework provides a structure aiming to help organisations build the next generation of Internal Audit as a function well attuned to the challenges of emerging risks, technologies and 'disruption'. It seeks to bring a culture of innovation, help functions keep pace with technological change, and enhance their impact and influence across the organisation. The vision that emerges 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.

In order to successfully lead that transformation, Internal Audit will need to focus on domains such as: *skills and capabilities* (people), *ways of working* (processes – agile models are quite popular options recently) and *digital assets and solutions* (technology). Many leading Internal Audit functions have already begun their journey into the world of automation by extending their use of traditional analytics to include predictive models, robotic process automation (RPA), and artificial intelligence (AI). These initiatives have started realising benefits such as audit quality enhancements, risk reduction, as well as increased risk intelligence.

With automation technologies advancing quickly and early adopters demonstrating their effectiveness, we believe now is an opportune time for Internal Audit to understand and prioritise use cases for automation, and take important steps to prepare for thoughtful, progressive deployment.

The spectrum of automation

Internal Audit functions, we observe, are familiar with the initial stages of the spectrum (see figure 1), many having deployed basic data analytics tools, practices and technologies to increase the level of assurance as part of audit fieldwork or having run more quantitative risk assessment processes as part of annual planning. Although very few functions are operating at the advanced end of the spectrum, there are interesting and highly promising instances of experimentation with predictive models, advanced technologies with cognitive elements and (foundational) artificial intelligence or machine learning capabilities.

Some examples relate to the use of unsupervised machine learning to extract hidden relationships and outliers from the dataset (thereby preventing analyst bias), as well algorithms to identify emerging risks. These can help auditors generate causal relationships, get to the root cause or produce predictive insights that could drive preventative action.

[1] Internal Audit 3.0; The future of Internal Audit is now; Deloitte LLP; 2018

2 IT Internal Audit of the Future: Adopting Automation (cont.)

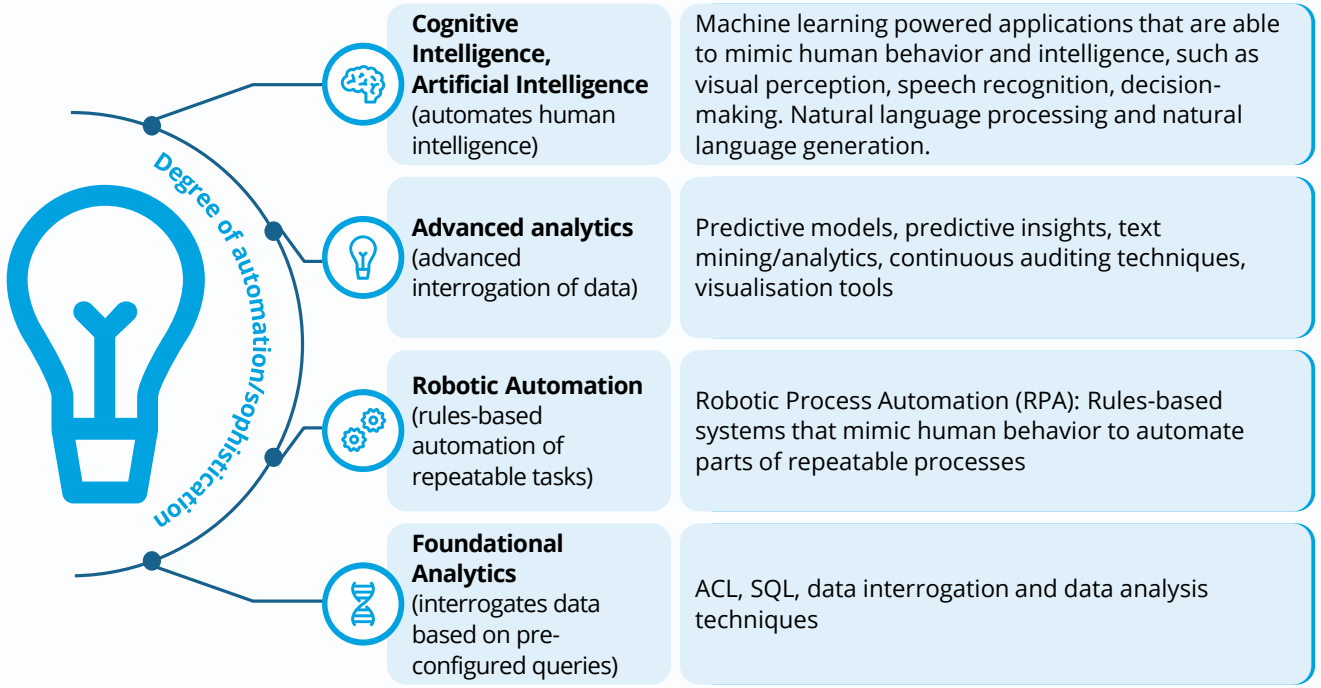
The spectrum of automation (Cont.)

Regardless of the current maturity levels, our view is that the landscape is changing fast. The technologies are becoming cheaper, the skills proliferate, and, importantly, Internal Audit ambitions are expected to become more prevalent as early adopters continue to demonstrate tangible results on the impact and value imbued in the function.

We consider the use of robotics automation within Internal Audit is more embryonic than analytics, but we expect the development to follow a similar usage path, as part of Internal Audit strategies. Currently, we're seeing the more advanced functions exploring the implementation of rules-based systems to automate parts of repeatable processes, such as reporting for instance or quality assurance activities. Some proof of concepts aim to drive efficiency/effectiveness, expand capacity or reduce costs and boost quality.

Figure 1

The Spectrum of Automation for Internal Audit



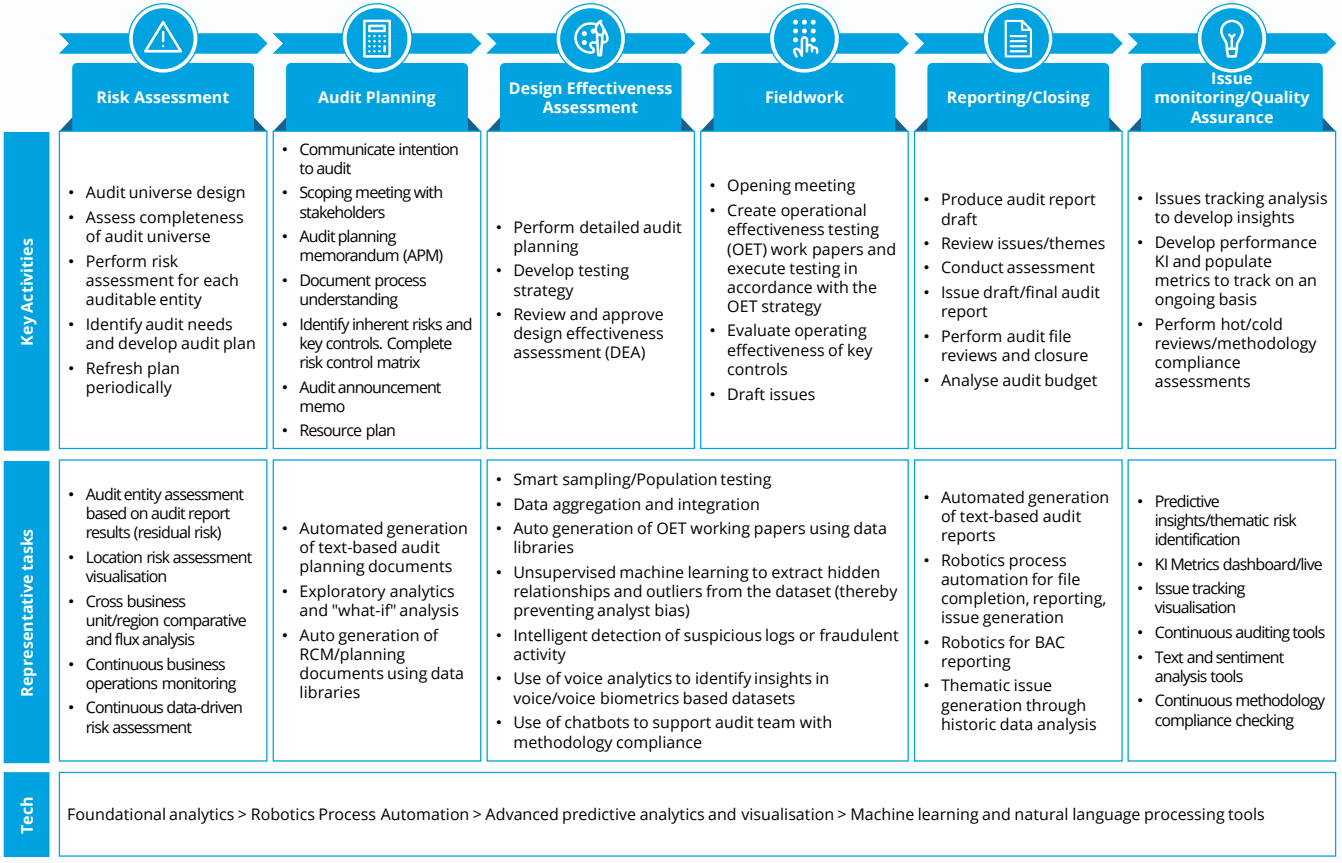
2 IT Internal Audit of the Future: Adopting Automation (cont.)

Audit lifecycle and automation opportunities[2]

The opportunity for automation with the use of robotics or cognitive intelligence tools, does not rest in planning or audit fieldwork activities. There are numerous use cases or opportunities to leverage automation to improve quality, reduce costs or enhance efficiency of audit processes. The diagram below presents some of these opportunities.

Figure 2

Automation opportunities across the audit lifecycle



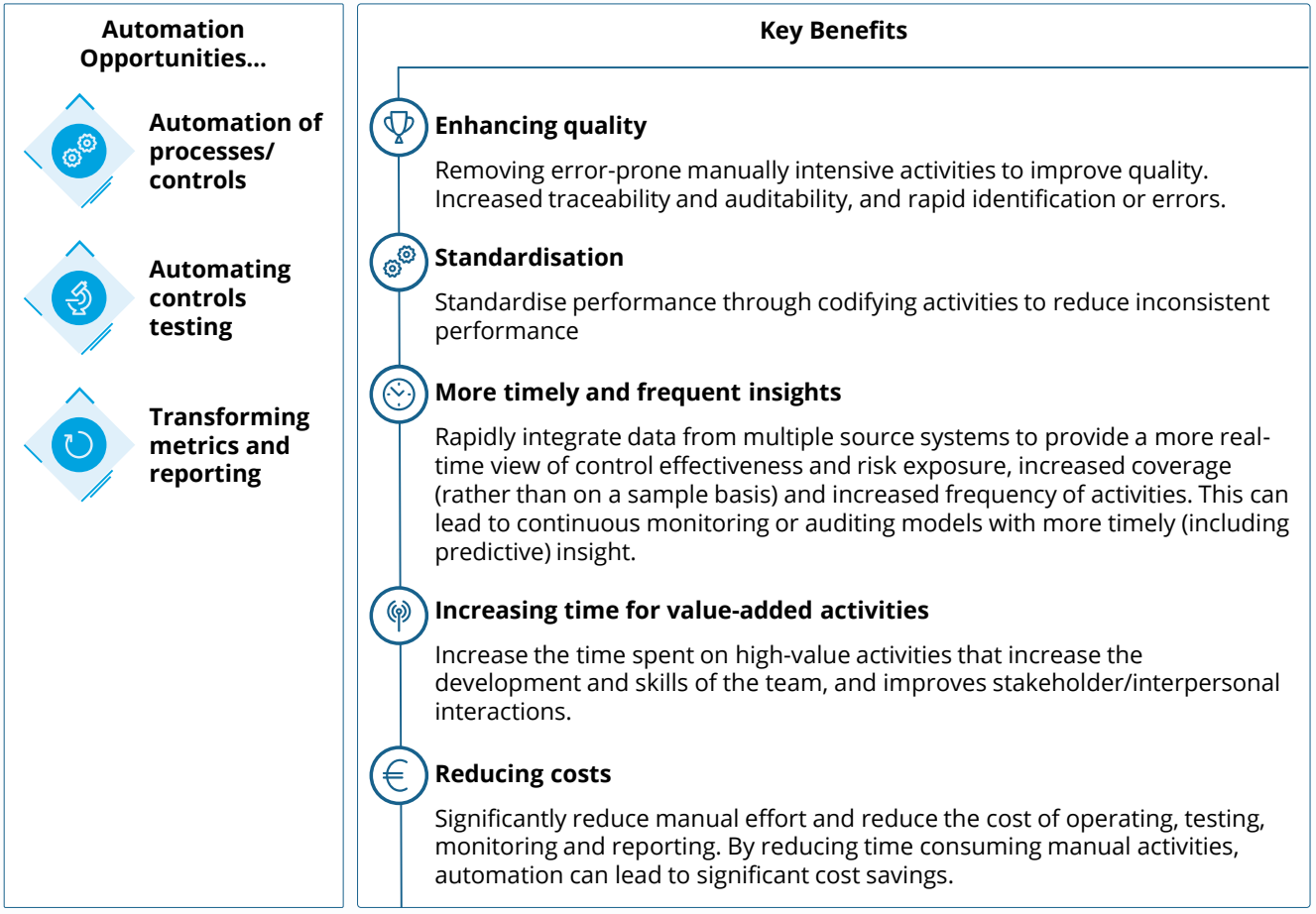
[2] Based on the Deloitte paper: Adopting automation in internal audit. Using robotic process automation and cognitive intelligence to fortify the third line of defence; Deloitte Development LLC; 2019

2 IT Internal Audit of the Future: Adopting Automation (cont.)

Audit lifecycle and automation opportunities (Cont.)

Figure 3

Realising benefits



2 IT Internal Audit of the Future: Adopting Automation (cont.)

Use Case: Innovation and intelligent automation for Quality Assurance (QA)

QA processes within an internal audit context are characterised by some repetitive activities, quality checks and in some cases large workload, which will lend themselves to opportunity for automation and standardisation, freeing up valuable staff time for more value-add tasks. The objective of those responsible for QA would be to integrate solutions that ensure enhanced quality and minimisation of errors, increased coverage of audits and potentially reduction of costs.

Some of the opportunities to apply automation or analytics in QA include the following:

- Methodology compliance (as part of hot and cold file review process)
- Reporting and KPI tracking (automating metrics generation and dashboard reporting)
- Operational efficiency (population vs sample coverage)

Suggested tool or approaches to deliver could be:

- Traditional analytics,;
- Visualisation tools – Tableau, Qlikview;
- AI-powered analytics/tools such as text analytics.

Functions that have successfully deployed automation in this area have focused on the implementation of solutions such as: performance metrics and key indicator dashboards for Heads of Audit, text sentiment analysis tools using text analytics/mining and scanning (to validate audit report ratings for instance). Some more advanced use cases include use of robotics (e.g. for report generation), continuous methodology compliance tracking, intelligence and insights generation.

What Internal Audit functions need to consider

As functions embark upon this automation journey and seek investment, there are a few areas we believe they should pause to consider in order to increase the opportunity for success:

Strategy for automation: Chief Internal Auditors need to ensure the automation initiatives are aligned to the broader strategy for the function, and are driven by a strong vision on what are meant to achieve. For example the digital transformation of the whole function needs to be managed very differently in comparison to an implementation of a single application for advanced analytics. Considerations such as: integration of the technologies, impact on existing processes, defining benefits, are pertinent at this stage.

Risk management and assessment: When introducing these RPA and CI technologies into the ecosystem of the function, functions are exposing themselves to potential risks that need to be addressed. They should perform risks assessment and ensure appropriate controls are in place. Some of the risks to consider include algorithmic, model risk (code reviews for example), technology risks (change management), operational risks (implementation and delivery capability), people risks (the impact on team morale), regulatory risks or financial risks.

2 IT Internal Audit of the Future: Adopting Automation (cont.)

What Internal Audit functions need to consider (Cont.)

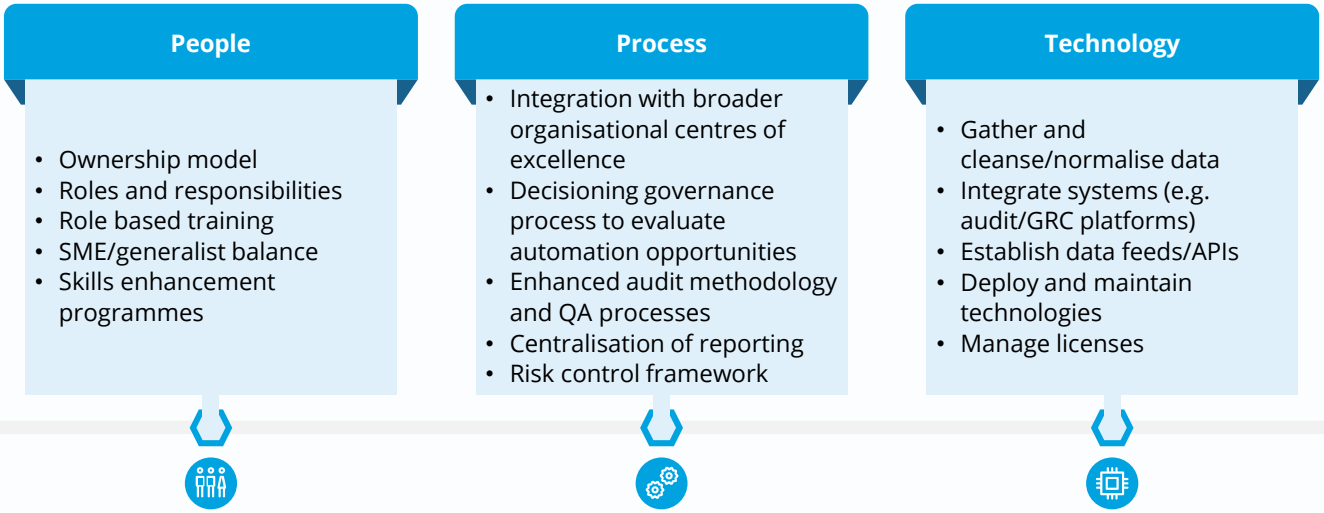
Infrastructure to support deployment of capabilities: The operational capability and infrastructure to design, deploy and maintain should not be underestimated. A robust governance framework, change and testing processes will safeguard the ongoing support, management of risk and ultimately success of the automation initiatives. Some of the areas of focus:

- Governance
- Change management
- Testing and monitoring
- Skills and resource training

Design and implementation of the target-state operating model: The deployment of digital technologies can help the function reshape their operating model in line with Internal Audit 3.0 or similar frameworks. Functions should consider the impact of this transformation to the people, process and technology pillars of the 'as-is' function, while also considering the integration with firm-wide initiatives or governance structures, such as shared services centres, centre of excellence for automation of digital transformation. They should also make use of risk management and control frameworks to sustain the model and ensure its continuous effectiveness and relevance.

Figure 4

Target State Operating Model: People, process and technology considerations



3. IT Internal Audit Hot Topics through the years: 2012-2020

3 IT Internal Audit Hot Topics through the years: 2012-2020

Below is a comparison of the top 10 IT internal audit hot topics over the past nine years as identified through our annual survey of Heads of IT Internal Audit in the financial services sector. The continued presence of cyber security and transformation/change at the top of our list, particularly in the past 4-5 years cannot be ignored as well as the recent emergence of the new technologies enabling digital business models and transformation initiatives across FS organisations.

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

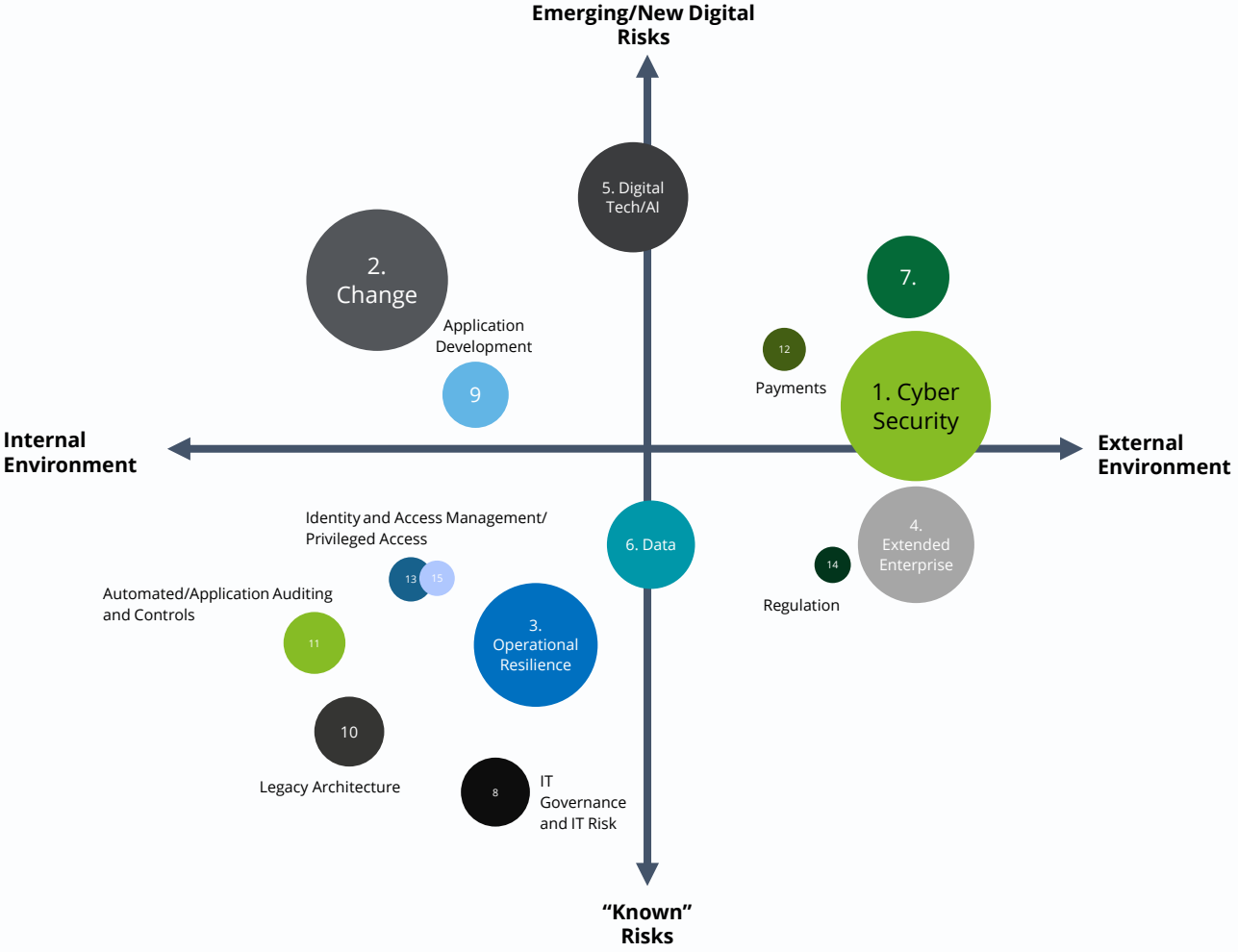
Table 1. IT Internal Audit Hot Topics through the years: 2012-2020

Rank	2020	2019	2018	2017	2016	2015	2014	2013	2012
1	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Large Scale Change	Third-party management	Cyber Threat
2	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 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 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	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	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	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 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	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	Legacy Environments	Payment Technologies	Enterprise Technology Architecture	Digital and Mobile Risk	Payment Systems	Service Management	Cloud Computing	Social Media	Mobile Devices

3 IT Internal Audit Hot Topics through the years: 2012-2020

Figure 5. Classification of the Top-15 IT Internal Audit Hot Topics for 2020.

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.



4. IT Internal Audit viewpoints 2020 by topic

4 IT Internal Audit viewpoints 2020 by topic

1 Cyber Security (=1)

Overview

Given the high profile cyber incidents across financial services in recent years, coupled with the continuing regulatory interest in this area – from the 'Dear Chairman Exercises (DCE) focusing on firms' technology resilience (DCE I and DCE II), to the Financial Policy Committee's (FPC) cyber stress testing pilot – we anticipate that demands and requirements for organisations around cyber security and resilience will only increase.

The focus is shifting from cyber prevention to incident identification and breach reporting, focusing on timeliness and effectiveness of firms' procedures to respond to a cyber-risk event. In addition, organisations are expected to strengthen their risk and control frameworks in terms of quantification of cyber risk, and develop approaches and metrics to measure, report and then improve.

The Bank of England, PRA and FCA issued a joint Discussion Paper, '*Building the UK financial sector's operational resilience*' in 2018, returning the spotlight to operational and cyber resilience (refer also to topic 3).

This time the focus of the regulators is on the development of a broader framework for firms, enhancing resilience stress testing and establishing strong impact tolerances and performance metrics. Financial services organisations will be expected to set own resilience tolerances (max downtime for instance) in line with a resilience baseline and taking into account inter-connectedness with other financial services firms.

Internal Audit's role

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.

So, whilst this is not a new topic, functions cannot be complacent and should strive to raise the bar in line with broader developments. In our view, some critical areas of focus for Internal Audit functions this year should include:

- Governance; senior manager accountability on cyber security;
- Incident identification and response capability;
- Cyber threat intelligence;
- A holistic, enterprise-wide approach when it comes to cyber and operational resilience, that can instill a 'resilience' culture in the organisation and drive resilience-by-design, particularly when it comes to the technology environment;
- Enhanced, reliable, data-based metrics to monitor disruption, performance against KI and tolerances by system/component, that can drive enhanced executive and board level visibility and decision making.

4 IT Internal Audit viewpoints 2020 by topic

2 Transformation and Change (=2)

Overview

As digital maturity is increasing globally, and with external pressures on organisations to improve customer service, responsiveness, resilience, and technology capabilities, we are seeing large, transformational programmes being initiated to respond to such challenges and help organisations differentiate themselves from the competition – primarily the FinTech and Digital entrants.

The project assurance scope in the digital transformation domain is expanding from assuring simply governance or specific technology 'build', to encompass the alignment of transformation programme objectives to the customer journey and organisation's strategic objectives when it comes to technology and digital.

Auditors continue to challenge IT management's perception that oversight is "not needed" in Agile change and that intervention will delay or adversely impact on strategic change delivery. We note from some respondents that there continue to be barriers related to the fact that Internal Audit is not being seen as a true risk 'partner' through the delivery journey and a positive enabler to successful delivery. We believe some of this is driven by the skills gap but also by lack of stakeholder management to establish the value of close and continuous assurance.

Internal Audit's role

Internal Audit should reinforce the benefits and position 'change assurance' as pivotal for successful change delivery, offering healthy challenge that is far from acting as an inhibitor. Equally, programme teams should be encouraged to embrace the challenge of change risk and change assurance, and engage with all three lines of defence throughout the delivery journey.

Some areas that Internal Audit should focus on, in our view, are:

- Where organisations are delivering Digital Transformation and adopting new technologies and methods, auditors may require considerable shift to ways of working to mirror those by the business and technology functions alike.
- Internal Audit should look beyond the risks of individual transformation activity, and also focus on the overall portfolio management. Effective change audit teams challenge management in terms of top-down portfolio management, the realisation of benefits across the whole portfolio and whether individual programmes add value against the overall portfolio. They should also seek to express an opinion over the board and executive's oversight and challenge over change and execution risk across the organisation.
- Internal Audit should seek to understand the risks of disruptive digital and cloud technologies, in the context of transformation initiatives and beyond, and provide assurance over the risks to the realisation of benefits in a competitive landscape, but also the impact on customers, stakeholders and employees.
- Lack of the relevant technical and change management skills in internal audit functions can lead to misinterpretation and underestimation of the change impact to business as usual operations as well as strategic implications. Successful learning programmes and targeted training needs to be adapted to co-opt the relevant technical expertise including agile, DevOps and cloud based solutions.

4 IT Internal Audit viewpoints 2020 by topic

3 Operational Resilience (▲ 4)

Overview

As mentioned earlier in this paper, the Bank of England, PRA and FCA issued a joint Discussion Paper, '*Building the UK financial sector's operational resilience*' in July 2018 (DP 1/18), returning the spotlight to operational resilience. Significant regulatory attention is focusing on how firms and financial market infrastructures (FMI) can improve their operational resilience to high-impact events.

This follows a series of initiatives [for example the Recovery and Resolution Planning (RRP), Operational Continuity in Resolution (OCIR), the Dear Chairman Exercises (DCE)] by the regulatory authorities over the past few years which reflect their desire to build a financial services sector that can absorb the impacts of unexpected events without further contributing to them.

This marks the beginning of a clear direction of intent for operational resilience by the regulatory authorities. We are seeing operational resilience emerge as a hot topic in the context of internal audit and risk management, encompassing other high-impact domains and initiatives, such as cyber and technology resilience, crisis management, incident response and recovery.

The recent Deloitte paper on Operational Resilience[3] provide some clarity over the opportunity to enhance operational resilience, suggesting the following three ways:

- Making senior leadership accountable and creating a mind-set that considers more severe disruptions as inevitable;
- Aligning operational resilience with the operational risk framework; these are two sides of the same coin, as risks need to be managed effectively but if they materialise they must be mitigated;
- Using severe but plausible scenarios, alongside impact tolerance statements, to assess and test resilience measures, identify gaps and invest appropriately.

Internal Audit's role

Financial institutions operate in a complex and challenging environment, where the protection of customers and other market participants is paramount. Some of the challenges include: technical innovation, system complexity, changing consumer behaviours and expectations. This helps widen the discussion of what operational resilience covers; it needs to be considered as a holistic, enterprise-wide domain, straddling a broader range of strategic, technology, regulatory and operational risks.

To that effect, a change in mindset may also be required and Internal Audit's approach in assuring this area will help. Improved alignment of risk management systems promotes better sharing of good practices and helps establish common understanding of what is important to the business, the impact of a disruption and the priorities during response and recovery.

Internal Audit functions auditing the effectiveness of operational resilience frameworks or capabilities should focus on whether firms can practically align what are often seen as separate risk management systems, such as business continuity, cyber and information security, operational risk and third-party risk. They need to better understand how they can collectively contribute to the overall resilience of business services. A robust operational resilience framework should also cover:

- Governance (including risk committees, interlocked policies and procedures across a range of relevant principal risk domains);
- Business Impact Analysis;
- Threat Risk Assessments;
- Business Continuity Planning;
- Technology and Data Disaster Recovery;
- Crisis Management Planning (including communication and pandemic scenarios)
- Plan Exercising and Testing (including table-top exercises, simulation and war games for instance);
- Training and awareness;
- Management information and board reporting.

[3] Time to flourish: A practical guide to enhancing operational resilience in the UK financial services sector; Deloitte LLP; 2019; https://www2.deloitte.com/uk/en/pages/risk/articles/operational-resilience-in-financial-services.html

4 IT Internal Audit viewpoints 2020 by topic

4 Extended Enterprise Risk Management (▲ 5)

Overview

Financial services organisations are increasingly relying on a globally interconnected third party ecosystem to stay competitive. This rapidly evolving ecosystem is exposing them to a growing portfolio of risks, costs, regulatory pressure and heightened board expectations.

We anticipate that Financial Services sector regulators will encourage innovation in this area, but at the same time they will become more powerful with a broadened area of responsibility to address emerging risks as highlighted in recent laws and regulations, such as the Modern Slavery Act and GDPR.

Third-party risk management has been a topic of focus for Internal Audit functions for many years, and has consistently featured in our annual 'Hot Topics' survey, reflecting the challenges of tackling as well as the regulatory attention in this area. Our 2019 global survey on Extended Enterprise Risk Management (EERM)[4], recognised an increasingly high interest and leadership focus on third-party risk management. Some of the key findings and areas of challenge in this area as reported in our survey were:

- Boards and executive management continue to take a deep interest in third-party risk management and want to provide more coordinated and responsive input. This is reflected in their investment in actionable intelligence and desire to pool and analyse information on all risks and across the whole organisation.
- The desire to reduce costs has become the biggest driver for investing in EERM maturity, followed by reduction in third-party incidents, regulatory, and internal scrutiny.
- The pursuit of efficiency, standardisation and simplification is driving organisations to embrace a number of solutions. These include emerging technologies/new tools that enable *more mature processes; federated structures; shared utilities; and managed services delivery models*.
- Chronic underinvestment is making it hard for organisations to achieve their desired maturity levels, and more fundamentally, has hindered many organisations from doing basic core tasks well (e.g. ongoing third party risk profile monitoring, risk assessments etc.); this means the full benefits from cutting-edge initiatives and solutions can't be realised.
- Federated structures are becoming the most dominant operating model for EERM. The majority of respondents said their organisation has now adopted this model, where strong central oversight is combined with accountability held by organisational units or leaders in different countries, reinforced by a combination of central policies, standards, services, and technologies.

Internal Audit's role

Financial Services organisations are still facing challenges in the management of the extended enterprise, with a staggering 83 percent of organisations experiencing a third-party incident in the past three years, and many still struggling with the basic risk management practices and control in this area.

These challenges against a backdrop of programmes to improve the management of third party risk by bringing efficiencies, investing in talent, cutting-edge technologies, and robust operating models, mean that Internal Audit should maintain their well-warranted focus on this area. Our 2019 survey reveals that boards are championing an approach to EERM that includes better engagement, coordination, and smarter use of data (including greater innovation, and real-time actionable intelligence facilitating boardroom reporting on third-party risks).

All of these are areas that Internal Audit should review as part of their third-party audit portfolio. We suggest that they also consider the following:

- The emergence, design and implementation of new operating models (federated versus centralised, for instance).
- The risks of automation and new technologies in this area. These could be Enterprise Resource planning tools, risk intelligence tools, automated dashboards, use of emerging technologies such as the cloud, robotics process automation, and artificial intelligence.
- A key aspects of third-party risk management that until recently hasn't always been adequately addressed: subcontractor risk (also known as fourth/fifth party risk). This becomes increasingly important, not least given the regulator focus on concentration risk. Organisations often do not have visibility or do not know enough about the subcontractors engaged by their third parties, which in turn makes it difficult for organisations to determine how to manage subcontractor risk, and to apply this strategy with discipline and rigor.

[4] Third party governance and risk management: Extended enterprise risk management survey 2019; Deloitte LLP; 2019; https://www2.deloitte.com/be/en/pages/risk/articles/third-party-risk1.html

4 IT Internal Audit viewpoints 2020 by topic

5 Digital Technologies (▲ 7)

Overview

Disruptive technologies and digitalisation are a key part of today's business lexicon. Technological advances and trends in advanced analytics, robotic process automation (RPA), and cognitive intelligence, including Artificial Intelligence, are rapidly transforming organisations. They reshape business models and enable innovation in terms of productivity and operational efficiency and also, critically, in the way they connect with, and offer products and services to, their customers.

These technologies are rapidly advancing, with more interconnected and powerful networks, high-performance computing, and the advent of digital tools, including data analytics, RPA, and machine learning-based software.

Although the regulation in this area is still catching up, there have been some recent developments. The EU Commission published the steps it is taking for "building trust in Artificial Intelligence (AI)", which includes the publication of the final Ethics Guidelines for Trustworthy AI[5], aiming to encourage public and private investment in AI and related technologies whilst managing the risks.

The Guidelines indicate that to be "trustworthy", an AI application should comply with the law, fulfil ethical principles and be robust.

They highlight a list of seven key requirements that AI applications should respect to be considered trustworthy and presents an assessment list to help check whether these requirements are fulfilled:

1. Human agency and oversight;
2. Technical robustness and safety;
3. Privacy and data governance;
4. Transparency;
5. Diversity, non-discrimination and fairness;
6. Societal and environmental well-being; and
7. Accountability.

Internal Audit's role

The EU Commission's announcements highlight that the ethical dimension when it comes to disrupting new technologies is increasingly becoming a priority and, as such, it will need to become an integral part of firms' digital journey. In this regard, it makes sense from a regulatory and business perspective for Internal Audit functions to start challenging how these seven key requirements for trustworthy AI are integrated in both the solutions their firms are deploying, as well as those that are already in use.

Naturally, the rate of adoption of disruptive technologies may be different for each company, and the approach and maturity levels of each Internal Audit department to respond to the risks posed will vary. The challenge remains however: auditors need to accept that the business will be 'disrupted' and need to stay ahead of how to deliver quality reporting, insightful assurance, and impactful advice.

While some may be more mature with their approach than others, most departments are in the early phases of this journey. In all cases, assessing the impact of such technologies on the existing controls environment is imperative to the successful adoption of digital technologies. These risks can be addressed by extending existing approaches to managing enterprise risk. Internal Audit should assess whether appropriate controls are being implemented to prevent and detect new and emerging risks, and they should find a balance among their responsibilities to: Assure, Advise and Anticipate, preparing for new risks on the horizon. Refer also to topics around Cloud Governance and Security (7) and Application Development (9).

[5] Ethics guidelines for trustworthy AI; European Commission; Report/Study; 2019; https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

4 IT Internal Audit viewpoints 2020 by topic

6 Data Protection & Data Privacy (▼ 3)

Overview

Data protection, data privacy and data governance remain topics of continuous attention and focus by senior management and Internal Audit teams alike. In a year dominated by data breaches and regulatory fines, it comes as no surprise that for another year this is amongst the hot topics in our survey.

The General Data Protection Regulation (GDPR) rules came into force in May 2018, and for some time organisations were waiting to see how the regulators across European jurisdictions will deal with the breaches; how tough they were going to be defending the new regulations and safeguard citizen's personal data. Significant fines have been levied to date by the Information Commissioner's Office (the UK supervisory authority), most notably £183m for British Airways and £99m for Marriot International, while the issues of eroded customer trust and reputation remain major concerns.

GDPR remains very topical for boards and IA functions for two main reasons: Firstly, organisations are still undertaking remedial activities to ensure they become fully compliant with the regulatory requirements, or transition their ongoing projects into 'business as usual' activities once they have reached a position of full compliance. The objective is to ensure the organisation can continue to demonstrate a defensible position and thereby compliance with the legislation.

Secondly, they realise the strong connection of the data programmes with the broader resilience, data breach and incident response activities across the organisation (refer also to topics 1 and 3). Businesses are seeking to develop effective data breach response programmes, to enable them to effectively weather such crises when they occur. These will encompass processes to ensure they engage effectively with customers, the public and media, while battling the breach crisis environment – characterised by lack of information, complexity, uncertainty, huge risks and significant time pressures[6].

Internal Audit's role

Internal Audit should challenge management on their customer data breach readiness procedures. Breaches will continue to occur. It is actually a case of "when rather than if", as the saying goes. 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 timely respond in order to contain the issue while providing high-levels of customer service to safeguard reputation. Some of the areas that can be covered, include:

- Technical and cyber response playbooks and forensic investigation strategies
- Customer and stakeholder notification, support strategies and implementation plans
- Insurance awareness, strategy and reality
- Legal support and access to privacy expertise
- Regulatory strategy and response
- Incident response capabilities
- Training, awareness and exercising
- Media monitoring, management and social media response

In addition, Internal Audit should consider the following in their data governance scope:

- Assess the implemented data protection policies, procedures and controls to comply with GDPR;
- Consider the gaps between current state and full compliance and the risks associated with the Data Privacy programmes to achieve full compliance.
- Evaluate the effectiveness of the implemented framework and controls in response to the regulatory requirements;
- Focus on technical data protection controls, including Data Leakage Prevention solutions and other security controls to prevent data breaches;
- Evaluate effectiveness of high risk functions (e.g. incident management, marketing and any other functions handling large amount of personal data); and
- Assess the accountability framework and data processing taking place abroad.

[6] Customer Breach Support; Deloitte LLP; 2019 https://www2.deloitte.com/uk/en/pages/risk/solutions/customer-breach-support.html

4 IT Internal Audit viewpoints 2020 by topic

7 Cloud Governance and Security (▲ 8)

Overview

Cloud adoption has, as anticipated, seen a significant upward trajectory over the past few years, with the worldwide public cloud services market for Cloud Service Providers (CSP) growing by 21% to $186 billion total revenues in 2018[7].

Its transformational benefits, such as flexibility (pay-as-you-go), technological sophistication, cost and tax efficiency, customer empowerment, are undeniable, and have fuelled the exponential rise in its popularity and successful adoption. It is projected to grow another 63% over the next three years.

The risks, however, if not managed carefully can be significant. There have been some significant issues and failures that have hit the news. A glitch at a major cloud service provider (CSP) in 2017 caused hundreds of thousands of websites using its services to function badly or not at all for a few hours. Lloyd's, the specialist insurer, estimated in a report published in January 2018 that if an extreme cyber incident took a top cloud provider offline for three to six days it would cost US businesses around $15 billion.

Despite its recent expansion, level of adoption and technology maturity, using the cloud is not straightforward. Even though a large part of the IT function is handed over to a cloud service provider – and with it, much of the operational hassle – clearly the users of these services still bear the ultimate risks and responsibilities if things go wrong.

Refer also to the hot topics of Cyber Security (1), Digital Technologies (5) and IT Extended Enterprise Risk Management (4).

Internal Audit's role

Further to the above, it is imperative that risk, assurance and control functions ensure that businesses remain on top of the risks. While security at CSP level has noticeably matured in recent years, the greater risk remains within the user organisations' controls, as they are still responsible for operating controls such as the provisioning of access rights and requesting/authorising configuration changes, for instance.

It is also important to recognise that the cloud user organisation always remains accountable for the governing and safeguarding of its data (including data discovery, classification, assessing and mitigating risks of data exposure) while the cloud provider is responsible to address operational, security and privacy concerns.

Naturally, the focus of Internal Audit functions will vary depending on the level of cloud adoption by the business, but some of the areas functions can consider for their 2020 reviews are:

- **Cloud governance and strategy**: Benefits realisation; business alignment; appropriateness of cloud service model and deployment type (given the type of service, data and risk appetite of the organisation); selection of the right CSP and appropriate ongoing oversight. This can also include a review of the shared responsibility and accountability model. Although, individual responsibilities can be transferred (e.g. infrastructure and platform security with use of a SaaS-application), the cloud consumer always remains accountable for the governing and safeguarding of its data.
- **People and culture**: Cloud insider risk; communications and people retention post cloud deployment.
- **Technology integration**: Complexity of integration with legacy platforms; deployment impact across technology estate; project assurance over transformational or integration initiatives; security controls.
- **Compliance, legal and risk management**: Data privacy considerations including physical location of data; broader operational and compliance risks; implications of GDPR and complying with other national laws.

[7] Maintaining control in the cloud: Developing and managing an effective cloud strategy; Deloitte LLP; 2019; https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-maintaining-control-in-the-cloud.pdf

4 IT Internal Audit viewpoints 2020 by topic

8 IT Governance and IT Risk (NEW)

Overview

The topics of IT governance and IT risk re-emerged in the top-10 of this year's survey on the back of increased regulatory focus on the topic and CIO challenges on the pace of technological change. The robustness of an organisation's IT governance practices and the transparency of decision making processes underpin performance across a number of other priorities or IT risk domains. Inadequate IT governance arrangements could lead to an unfocused strategic direction for IT, or decisions being made without a full appreciation of the impact on the organisation's broader strategy as well as risk profile and appetite.

Boards continue to challenge CIOs to demonstrate that effective governance structures are in place to ensure that the service and performance of the CIO/CISO functions are proactively and effectively managed, that they deliver value for money to the business and help protect the organisation from the – ubiquitous – technology, digital and cyber risks.

Internal Audit's role

When auditing governance in IT or performing assessments of CIO or CISO functions of an organisation, internal audit teams should challenge whether their objectives are achieved, ascertain whether risks are managed appropriately and verify that the enterprise's resources are used responsibly. They should provide an opinion as to whether the IT is effectively and efficiently managed to deliver value to the business, whilst ensuring that associated risks are managed effectively.

The ISO/IEC 38500:2015 standard as well as Control Objectives for Information and Related Technology (COBIT) continue to be leveraged by audit departments in their assessments of organisational compliance against established IT governance frameworks. We recommend that the IA approach in auditing this area be aligned to key enterprise governance standards, and centred around these four pillars:

- Strategic Alignment (strategic IT planning and organisational structure)
- IT Risk Management (risk management structures, policies and processes are in place to ensure that risks have been adequately managed including the assessment of the risk aspects of IT operations, projects or investments)
- Resource Management (resource planning including capacity and capability; IT third party management) and
- Value Delivery and Performance Measurement (service performance and value measurement, including MI/KPI reporting mechanisms).

IT Internal Audit has also a key role to play in evaluating the effectiveness and maturity of first or second line of defence IT risk functions. The role of such functions is elevated in recent years, with the emergence of cyber and technology risks as some of most complex and critical challenges organisations are (and will be) facing. Indicative areas that can be covered in such an assessment include:

- Governance and Organisation (including accountability structure, resource, skills and capability)
- Risk Identification and Assessment practices (threat intelligence and risk identification and assessment process)
- Compliance, Assurance and Monitoring (controls self-assessment; ongoing controls effectiveness monitoring; risk and issue remediation tracking)
- Reporting processes and mechanisms.

4 IT Internal Audit viewpoints 2020 by topic

9 Application Development (=9)

Overview

Agile and DevOps are becoming widely adopted by financial service organisations bringing substantial benefits in terms of speeding up the development and delivery of software changes. Organisations are realising faster time to market for new product and services brought by these delivery methodologies, which allows them to adapt to changing requirements at a faster pace.

The use of DevOps for application development is gaining traction this year, albeit at a much slower speed than the adoption of Agile. DevOps is effectively a software development practice that combines software development (Dev) and IT operations (Ops) domains. Automation, the main component of DevOps, requires compiling and sequencing of internal and external software tools to create automated Continuous Integration/Continuous Deployment (CI/CD) pipelines. It is important that the controls embedded within the tools adopt appropriate minimum standards to ensure the overall integrity of the CI/CD pipeline.

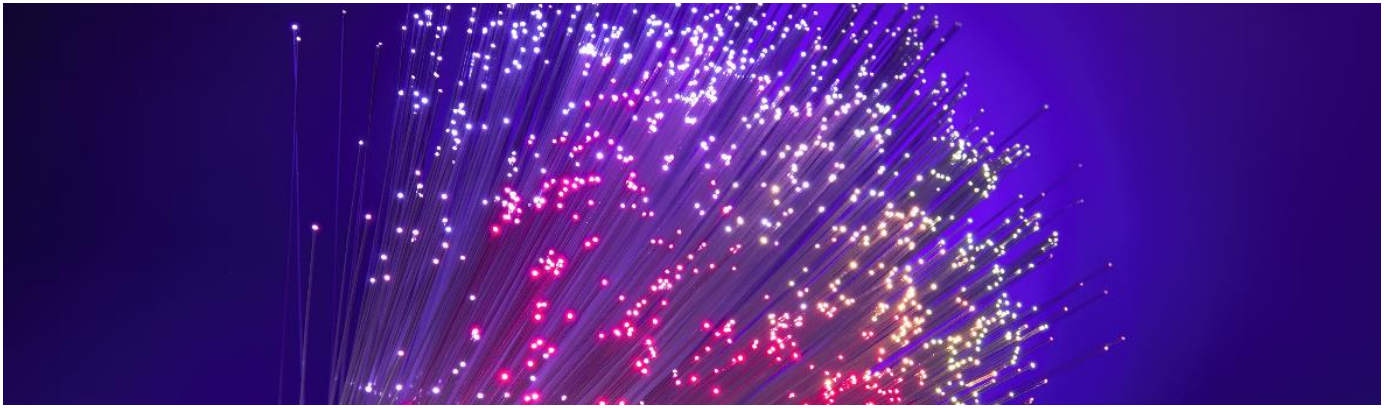
Lack of effective controls around DevOps tools could lead to unauthorised application releases into production resulting in turn to live service disruptions. Getting the balance right between the speed of onboarding and adequately risk-assessing these can be a challenge. Automated provisioning of pre-approved software tools using centralised governance has helped some organisations overcome this problem.

Internal Audit's role

Knowledge is increasing across Internal Audit teams around the principles of Agile and DevOps practices and how these are applied in IT application development. Their approach towards assuring these has also needed to be adapted to accommodate these deliver methods. Agile is now being used outside of IT functions, including within Internal Audit, where we are seeing Internal Audit teams applying Scrum practices and principles to transform their functions and ways of working. In such cases, reviews are carried out iteratively and in increments in accordance with more streamlined and shorter audit cycles. Initiatives such as these are bringing better alignment and understanding between IT and other parts of the business.

Internal audit teams are required to challenge the consistency and diligence in which Agile and DevOps methods are applied across the end to end IT Application Development lifecycle. Often during transition of operating procedures, parts of the processes meet the newly implemented Agile and DevOps controls while others are still operating Waterfall-style manual controls. Naturally, during this period hybrid-model inconsistencies may surface in the way controls are applied to mitigate prevailing risks.

In addition, while understanding such methodologies is key for Internal Audit teams to assure software delivery processes, being able to provide assurance in an automated fashion through usage of key risk or control indicators still remains a challenge. Data points made available through DevOps automation are not always generated in a way that provides meaningful insights to Internal Audit and Risk teams; it is important that these teams provide input and feedback into the data requirements as early as possible so that adequate metrics can be derived later in the process.



4 IT Internal Audit viewpoints 2020 by topic

10 Legacy Technology Environment (▼8)

Overview

The complexity of the technology estates of organisations continues to increase, resulting in environments which are ever more difficult to manage and maintain. In many instances this is the legacy of not upgrading or decommissioning systems in the past, which now remain in production but are unsupported or prohibitively expensive to maintain. In other cases a lack of effective systems integration during past merger and acquisition activities has resulted in a myriad environment of applications and platforms.

As well as increasing operational costs and operational risks, this also impacts the ability to change systems, which in turn affects ability to remain competitive with new market entrants, such as FinTechs and digital banks. In addition, as regulatory requirements change, many firms have come to the realisation that legacy systems are either hindering them from meeting new requirements, or are negatively impacting the organisation's risk profile.

Internal Audit's role

Legacy systems can pose a number of risks, such as security vulnerabilities, shortage of skills to manage and externally support the systems effectively, increased complexity caused by add-on interfaces to core systems and limited interoperability. Given these risks, there are clear linkages and cross-overs with the cyber and operational resilience hot topics (1 and 3 respectively) which has increased the level of focus internal audit functions are placing on technology architecture. It is imperative that internal audit works closely with stakeholders in CIO and CTO areas to understand the technology architecture and ensure they can achieve sufficient audit coverage of legacy platforms, interfaces and information flows.

Internal Audit functions also have a challenge in how to address this risk in their audit plans in a way that adds value to management, rather than simply echoing a known problem. Some of these ways could include: planning audit activity to assess the large-scale programmes in place to replace legacy systems; focusing on upgrading and consolidation change activity with respect to the impact this may have on the stability of the existing environment; and placing such considerations front and centre of routine continuity and resilience audit activity.

5. Contacts

5 Contacts

Mike Sobers

Partner

Tel: 020 7007 0483

Email: msobers@Deloitte.co.uk

Yannis Petras

Director

Tel: 020 7303 8848

Email: ypetras@Deloitte.co.uk

Notes

Notes

Notes

Deloitte.

Designed by CoRe Creative Services. RITM0315756