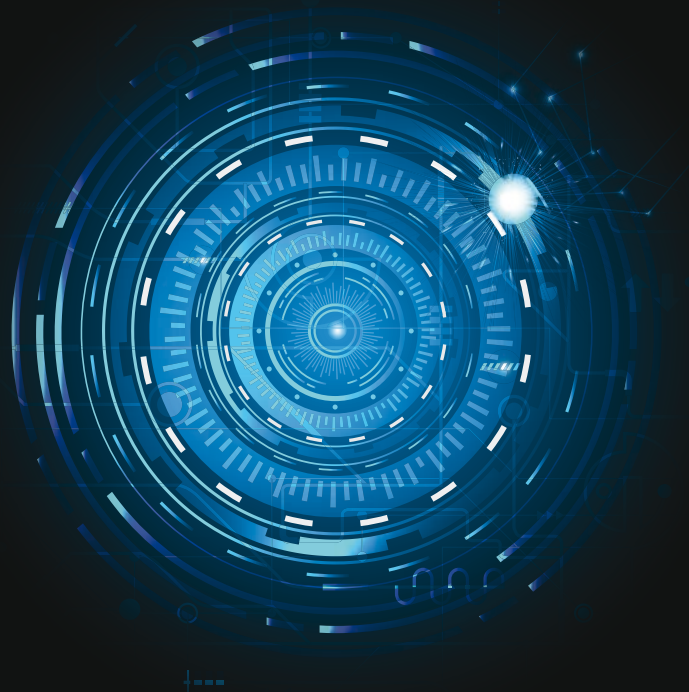




An eye on the future

2019 Hot Topics for IT Internal Audit
in Financial Services

An internal audit viewpoint

Contents

	Introduction	01
	1. Challenges for IT Internal Audit Functions	02
	2. Effective IT Internal Audit in Financial Services	04
	3. IT Internal Audit Hot Topics through the years: 2012-2019	09
	4. Internal Audit viewpoints by topic	12
	Contacts	27



Introduction

We are pleased to issue our latest review of the information technology hot topics for Internal Audit functions in financial services.

The paper is informed by a survey across UK financial service organisations and our discussions over the past 12 months with Chief Internal Auditors, Heads of IT Audit and IT Audit professionals, who have openly discussed their areas of focus and the organisational challenges in relation to their firms' technology control environment.

We interviewed over 20 key organisations across the financial services sector in the UK to obtain perspectives on the 'hot topics' or areas of focus in IT internal audit plans for 2019. Whilst "cyber security" claimed, once again, the top spot of our list, it is interesting to see a shift of focus to cyber 'recoverability', incident response and resilience, as well as security considerations over new digital assets. In fact, in this year's survey, functions seem to have "an eye to the future", quoting for the first time topics such as artificial intelligence (AI), robotics, DevOps and specifically highlighting the audit challenges they will need to overcome; whilst we still refer to them as 'emerging risks', it is not difficult to foresee a time in the near future where these become core risks impacting business as usual activities.

This paper also includes a commentary on the challenges that IT Internal Audit functions are facing ([section 1](#)) based on the results of our survey, our viewpoint on the effective IT internal audit of the future ([section 2](#)) and our perspective on its role in the continuous evolution of Internal Audit functions.

As usual, the detailed viewpoints by topic ([sections 3-4](#)) reflect our analysis on how internal audit should address these top-10 areas

It is always a pleasure receiving positive feedback on the publication, as well as constructive feedback for its continuous improvement. We would like to thank all organisations that participated or had open conversations with us over the year, that have informed this publication. We genuinely hope it offers insights while planting the seeds for further debate on how to improve the role of IT internal audit as an innovative and value-generating function.



Mike Sobers
Partner

1. Challenges for IT Internal Audit Functions



Challenges for IT Internal Audit Functions

The word cloud in Figure 1 shows the words/phrases that our respondents used most frequently when asked about challenges for their IT Internal Audit function. 40% of organisations that responded to our survey expect **budgets** to be stable or decrease. These functions are still being asked to deliver “more with less”, while seeking to address a wider range of IT risks and deliver on expectations regarding ‘innovation’ and increased use of analytics.



Figure 1. Challenges for IT Internal Audit Functions
“Word cloud” of responses.

Resource challenges, which featured heavily in previous years, continue to be a key area of focus. The right skills are not always easy to find (or retain), particularly ‘polymaths’ with strong and deep IT expertise coupled with good business awareness. As one respondent highlighted, “...it is increasingly difficult to find and retain people that combine optimally technology and business audit skillsets, with the right interpersonal and softer skills to continue to drive together business and IT audit for truly integrated approaches that add value”.

As we also mention [later in the report](#), the industry suffers from a lack of in-house **specialist skills** around emerging technologies such as cloud, robotics and AI solutions. Functions looking to augment their core team with technology specialists may find that cultural differences between technologists and auditors around risk and control may result in the need to invest in upskilling specialists to operate as effective auditors.

The use of technology and **innovation** to transform the function and deliver ‘predictive’ insight, is an increasingly common demand by audit committees and stakeholders alike, however many functions still struggle to deliver on this objective. Reasons for this lack of progress include; inadequate dedicated investment budget for such pursuits; insufficient specialist resource to lead such initiatives; or cultural constraints in teams dominated by a traditional audit mind-set.

Other challenges include the **effective risk coverage** as part of the annual risk assessment and audit universe, **collaboration with three lines of defence, delivering ‘agile’ auditing** in an integrated manner (and/or across global teams) and striking the right balance between providing assurance on risk and control and providing ‘advice’ to the business. Crossing the red line of **independence** is still a concern, particularly in an environment where Internal Audit is seeking to establish better ways to continue as a value-add function.

It is not uncommon for IT Internal Audit functions to ask, or be asked, “what does effective IT internal audit look like?” and, importantly, how they can futureproof its position as a function fully able to meet evolving stakeholder needs and well-equipped to deal with emerging technology risks.

The [following section](#) aims to shed some light on this question.

2. Effective IT Internal Audit in Financial Services



2. Effective IT Internal Audit in Financial Services

As financial services sector organisations seek new methods of creating value, and actively leverage digital, disruptive technologies and operating models, they embrace innovation and immerse themselves in new approaches to deliver such value. We have started seeing the more mature Internal Audit functions in the industry develop new tools and innovative capabilities – in many cases with dedicated Innovation or Research and Development teams – in order to

effectively respond or align themselves to such organisational developments and challenges.

Our report on [Internal Audit 3.0¹](#), presents a framework for the next generation of effective Internal Audit, as a function well attuned to the challenges of emerging risks, technologies and disruption. The analysis in this section leverages this framework, and focuses specifically on the role of Heads of IT

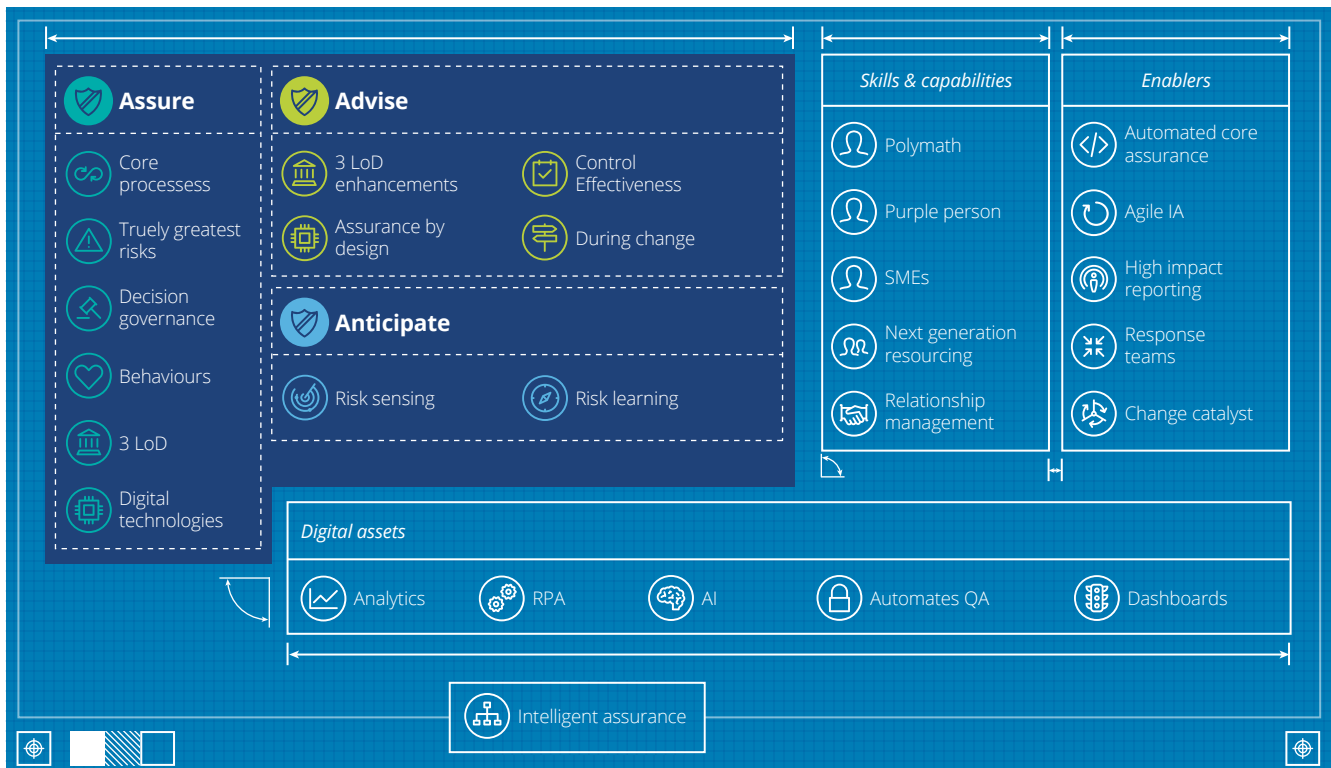


Figure 2. Deloitte Internal Audit 3.0. Assure, Advise, Anticipate framework.

Audit. In our view, an effective IT Internal Audit team 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 core dimensions of value that stakeholders now want and need can be classified as one of the following, (in line with our Internal Audit 3.0 framework in Figure 2): **Assure, Advise, Anticipate**. The delivery of these components is facilitated through an optimal mix of enablers such as **digital assets, skills & capabilities** and **processes**.

This isn't a 'one-size-fits-all' approach, and many of the above won't apply to the same degree for some functions. In our view, however, the key principles and success criteria of the effective IT Internal Audit function are pertinent across all functions including: the adoption of a coherent vision in line with the wider Internal Audit function; a vision that prioritises change across the variables of value/services, stakeholder engagement, and enablers (people, process, and technology); a focus on responding credibly to the challenges of the CIO functions, and safeguarding the organisation for now and the future.



Assure

The provision of timely assurance is core to the internal audit mission statement. An effective, well-equipped for the future IT audit function, needs to be able to balance an audit plan that delivers assurance over core processes and controls, such as core applications and IT infrastructure, IT operations, identity and access management, while ensuring appropriate coverage over primary or high profile risks (including emerging) such as cyber, digitisation, change, risks from new technologies.

Many functions have already implemented a number of tools and approaches to enable continuous auditing; use of technologies such as AI, robotics and advanced analytics can, on the one hand, facilitate ongoing, fully-automated controls monitoring in real-time, while on the other hand enable automated (e.g. real-time dashboard) reporting. When IT Audit enables such assurance capabilities, the function is benefited by optimal allocation of skilled resources to less 'commoditised' areas or topics of higher risk, freeing assurance time for root-cause analysis, advisory or future insights driven interactions with management.



Advise

Whilst continuous auditing or control monitoring approaches are often designed and developed by the third-line, these often fit better within the remit of first or second-lines of defence; we regularly see IT audit functions sharing knowledge and analytical tools they have developed. The Advise component of our framework, suggests that IT internal audit should advise first and second-lines on their assurance capabilities and help with digital/technology assets that can facilitate this. Of course this should be done within their sphere of independence and objectivity, i.e. being cautious not to design controls or take management decisions.

More broadly, effective IT Internal Audit functions should add value through sharing insights, industry risk frameworks, peer practices and 'best-in-class' approaches. A case in point is AI and new technologies: these present risks that may not yet be well understood with management so focused on functionality and proof-of-concept execution, that may have side-lined consideration of the risks. IT audit can advise on risk frameworks and promote the concept of "control by design"; this will help IT management embed mechanisms and automated controls that support the goals of real-time assurance or exception reporting.

Finally, a seat at the table of IT transformational programmes will allow IT audit to move away from simply offering 'assurance' activities when it comes to change and act as a agent of challenge and real-time risk support.



Anticipate

The truly innovative, and future-looking IT Internal Audit functions focus on generating and offering management preventative insights on emerging risks or issues/events before they materialise. This, in a way, is the reverse of the traditional 'backward-looking' audit approach of focusing on what went wrong or where controls did not operate.

The focus is on looking to the future by applying advanced data-driven analytics or machine learning and AI capabilities to assess key control indicators to predict areas of higher risk of control failure that management may be unaware of.

Examples in industry, include analysis of customer complaints (assisted by either behavioural analytics and/or AI), risk event registers, regulatory issues, that can help generate causal relationships, get to the root cause or produce predictive insights that could drive preventative action. Although still the minority, we increasingly see functions thinking in this way and investing in developing solutions that can offer predictive analytics capabilities and use cases that can demonstrate value.



Enablers

“Enablers” consist of skills and capabilities (people), **digital assets** and solutions (technology) and key processes – agile IA for example. We mentioned some of the tools and solutions in use by functions (delivered either by IT Audit or Innovation teams), adding value to audit delivery or enhancing the operational effectiveness of the function itself (refer also to the Digital Assets section).

In terms of talent and skills, functions should be looking for the optimal blend of all-rounder IT auditors that can easily understand risks exposures by a new IT solution and assumptions made by them, and specialists that can delve deep into risks of AI and new algorithms (for example) or best practice cyber approaches.

In all cases, an understanding of the business context is paramount. A focus on internal talent development programmes, again, is a distinguishing characteristic of the truly effective functions.



Digital Assets | Examples

Some of these technologies may include advanced text or voice analytics, in some cases with **behavioural and emotional analytics capabilities**. The latter can act as fully integrated voice and interaction surveillance platforms that monitor interactions across a variety of risk factors (customers, employees etc.).

We have also seen functions innovating with the use of **unsupervised machine learning applications** to supplement risk and controls based analytics, using a number of different algorithms, including cutting edge techniques such as topological data analysis, to tease out relationships and outliers in the dataset. This is done in a completely data driven manner, thereby reducing the risk of analyst bias inadvertently limiting the scope of investigation.

Conversely, traditional **analytics** are typically driven by a standard set of controls, or the knowledge of a subject matter expert who understands the area under investigation and analysis of results can be quicker/simpler. While their use and value should not be underestimated, they do not take into account the possibility for “unknown unknowns” due to analyst biases or preconceptions.

Although these tools are developed by very technical data scientists, once they are deployed they usually require minimal specialist skills and can be used by auditors to identify anomalous behaviour across business functions which generate a data footprint. They allow a more sophisticated selection of exceptions and outliers, including those which might not be normally spotted by conventional means.

3. IT Internal Audit Hot Topics through the years: 2012-2019





3. IT Internal Audit Hot Topics through the years: 2012-2019

Table 1 presents a comparison of the top 10 IT internal audit hot topics over the past eight years as identified through our annual survey of Heads of IT Internal Audit in the financial services sector. It highlights some interesting trends over time, including the continued presence of cyber security and strategic change and transformation at the top of our list, as well as the recent emergence the data management/protection

and digital risk themes (cloud, AI, application development). Topics which appear in more than two years have been colour-coded to help illustrate their movement in the top 10 over time.

Rank	2019	2018	2017	2016	2015	2014	2013	2012
1	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Large scale change	Third-party management	Cyber threat
2	Technology Transformation and Change	Strategic change	Strategic change	Strategic change	Disaster Recovery & Resilience	IT Governance and IT Risk Management	Identity & Access Management	Complex Financial Models
3	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 & Quality	Data Leakage
4	Technology Resilience	IT Disaster Recovery & Resilience	Third-party management	IT Disaster Recovery & Resilience	Enterprise Technology Architecture	Data Governance & Quality	Large scale change	Data Governance & Quality
5	Extended Enterprise Risk Management	Information Security/Identity & Access Man.	IT Disaster Recovery & Resilience	Data management and Data Governance	Third-party management	Third-party management	Cyber Security	Rogue Trader and Access Segregation
6	Cognitive Automation and Artificial Intelligence	Third-party management	IT Governance and IT Risk Management	Information Security	Information Security	Cyber Security	Resilience	Regulatory Programmes
7	Cloud Computing	IT Governance and IT Risk Management	Information Security/Identity & Access Man.	Digital and Mobile Risk	Digital and Mobile Risk	Digital and Mobile Risk	Cloud Computing	Financial Crime
8	Legacy architecture	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	Digital and Mobile Risk	Cloud Computing	Enterprise Technology Architecture	IT Governance and IT Risk Management	Disaster Recovery & Resilience	Complex Financial Modelling	Social Media
10	Payment Technologies	Enterprise Technology Architecture	Digital and Mobile Risk	Payment Systems	Service Management	Cloud Computing	Social Media	Mobile Devices

Table 1. IT Internal Audit Hot Topics through the years: 2012-2019

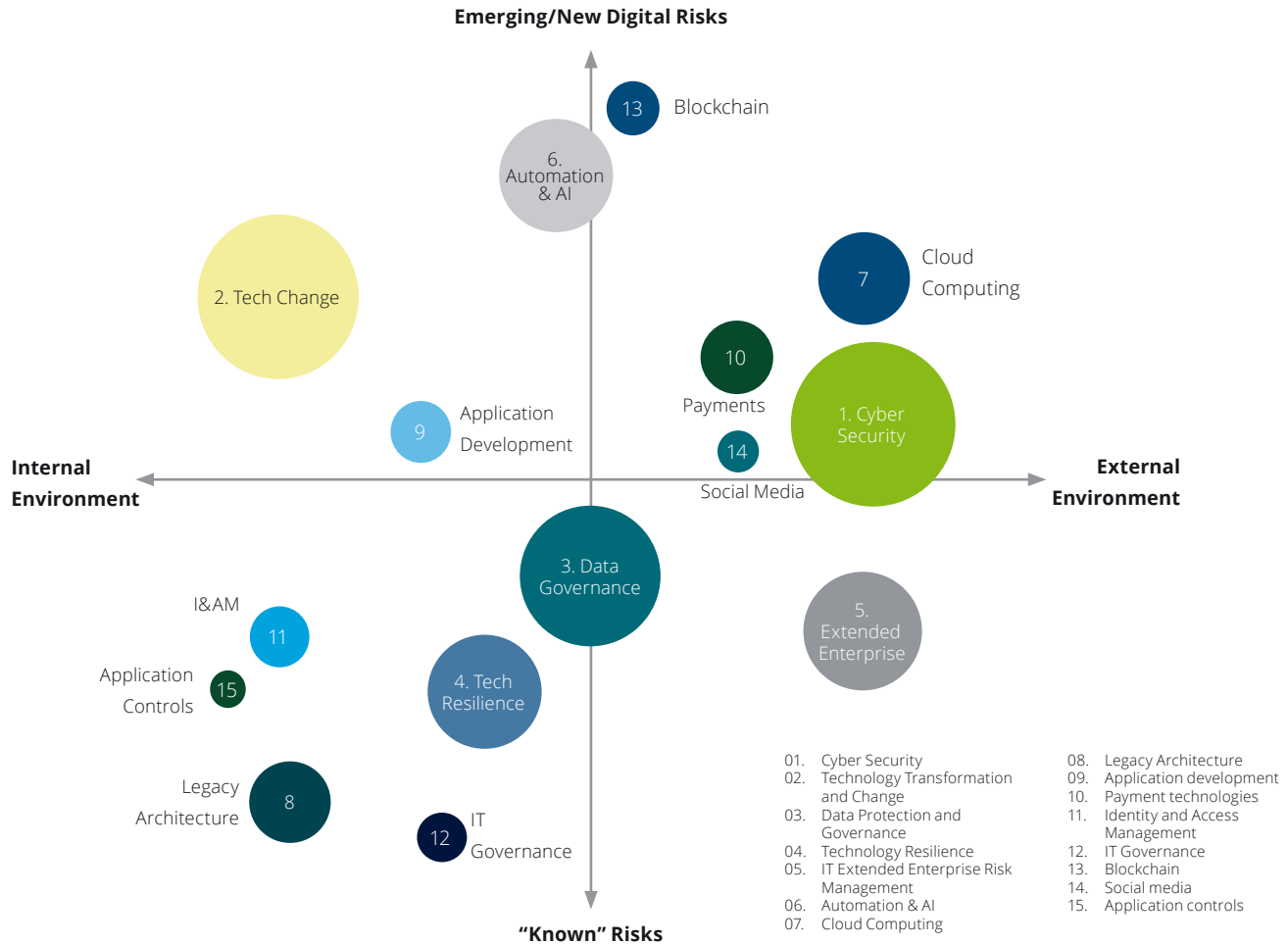


Figure 3. Classification of the top IT internal audit hot topics. The size of the bubble reflects the ranking in this year's list, while the horizontal axis shows the threat environment (internal or external to the organisation). The vertical axis classifies the topics across the spectrum of existing/known, new and emerging risks".

4. Internal Audit viewpoints by topic





4. Internal Audit viewpoints by topic



1. Cyber Security (=1)

Why is it important?

Predictably, Cyber risk remains a key priority for all stakeholders in financial services organisations and the sector overall. Jerome Powell, the new Chairman of the US Federal Reserve identified cyber threat as “maybe the single-most important risk that our financial institutions, our economy, our government institutions face”. Not surprisingly, our recent report on [Cyber Risk](#)² highlights that in 2019 we should expect FS regulators in European jurisdictions to pursue a combination of the following:

- Increased pressure on Boards to demonstrate ability to provide effective challenge, through access to independent expertise.
- Incident identification and breach reporting procedures; GDPR brought this area to the fore, focusing on timeliness and effectiveness of firms’ procedures.
- Risk and control frameworks and quantification of cyber risk; development of sophisticated approaches and metrics to measure, report and then improve.
- Collaboration on real-time threat intelligence; explore barriers to this and encourage this approach between firms (and potentially countries).

What is Internal Audit’s response?

IT internal audit teams should challenge management on their ability to understand and map exposure to cyber risks through risk management frameworks, and their efficiency in detecting and reporting data breaches rapidly. Furthermore, the use of new and emerging technologies such as AI, blockchain, cloud solutions and their increased use could amplify a range of threats to the cyber resilience of the organisation, so Internal

Audit should ensure appropriate cyber coverage across these areas, commensurate to the risk and in coordination with the wider internal audit team.

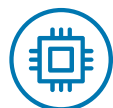
What are the challenges?

Executives need to anticipate what the supervisory developments mean for their organisation and make decisions based on these as well as their own threat analysis and cyber programmes; equally, IT Internal Audit functions need to stay close to these developments and have a clear plan on what to do next. This, in turn, will inform the requisite skills and resource mix needed for the internal audit teams.

Many cyber initiatives and programmes have an objective of improving cyber maturity over a period of years. This makes determining the appropriate time to perform an audit challenging. Internal audit should not lose sight of their mandate and remit, and focus on their responsibility to provide the Board with timely insight into the appropriateness of the organisation’s approach to, and execution of, their cyber strategy on a regular (we suggest at least annual) basis.



Note: The number in brackets indicate the ranking of the topics in our 2018 survey and the relative movement this year.



2. Technology Transformation and Change (= 2)

Why is it important?

After years of under-investment, many financial sector organisations have a complex and challenging technology environment and still grapple with large, strategic transformational programmes designed to respond to such challenges and help them move away from a legacy environment. In addition, the impact of regulatory change remains significant, as is the maturing threat from challengers, particularly in the FinTech, InsurTech and RegTech arenas.

Customer expectations, as well as the customer experience/ customer journey, have become increasingly important, and innovation forms a key differentiator for organisations in a competitive market. This is particularly significant when there is an appetite for the customer journey to become more 'digitalised'. The aforementioned challenger organisations are able to adopt 'digitisation' programmes and emerging technology rapidly without legacy constraints – something many establish players in FS have recognised and are responding by setting up large Digital Transformation initiatives.



What is Internal Audit's response?

Whilst the benefits of these initiatives, and those of strategic change more broadly, to the business can be considerable, the cost of getting it wrong cannot be overstated. The long term impact on reputation, customers, shareholders and regulators can be harder to predict. Some areas that internal audit should focus on in our view are:

- Delivering Digital Transformation and adopting new technologies may require considerable shift to ways of working by the business and technology functions alike; Internal Audit should seek to understand the risks of new 'digital' technologies, in the context of the transformation initiatives, and provide assurance over the risks to the achievement of project objectives and realisation of benefits, but also to the achievement of the wider organisational strategy.
- Providing timely (real time) assurance is invaluable for strategic change, with coverage achieved by securing a seat at the programme/project table. Many effective internal audit teams provide continuous assurance without compromising independence, are being engaged early and are challenging the traditional view of 'post implementation' assurance value.
- We have noted a recent focus on 'sequential auditing', with functions moving away from large scale reviews. More rapid, bite size audits are being planned, with very focused scopes and timeframes, audits are completed in weeks, aiming to deliver more timely assurance.

What are the challenges?

Even in certain mature functions and organisations, there is still an - arguably out-dated - perception that internal audit intervention will delay or adversely impact on strategic change delivery.

The organisational culture is of critical importance to that end Internal Audit should reinforce the benefits and position 'auditing change' as pivotal for successful project delivery or programme management, offering healthy challenge that is far from acting as an inhibitor. Programme teams should be encouraged to embrace the challenge of strategic change, and engage with all three lines of defence throughout the delivery journey.



3. Data Protection and Governance (GDPR) (= 3)

Why is it important?

Data protection and data governance will continue be topics of ongoing discussion, challenge and focus by management, boards, and Internal Audit alike. Whilst at the time of writing the investigation into the British Airways data breach in September 2018 and whether it could have been reasonably prevented was ongoing, there is a sense that the organisation may become the first high-profile case to face the impact of the new General Data Protection Regulation (GDPR) rules.

While the GDPR came into force on the 25 May 2018, many organisations had “risk-accepted” long before that date that they would not be fully compliant with the legislation. The fact that many organisations did not start their readiness activities soon enough or did not fully comprehend the scale of the task to ensure full compliance, meant many had to adopt a ‘risk based’ approach to their readiness programmes. As such, they focused on what they deemed as their “high risk” areas and the most sensitive personal information, to establish what they hoped would be a defensible and pragmatic approach for when the new legislation became enforceable.

What is Internal Audit’s response?

Now the legislation is fully enforceable, the challenge for organisations is primarily two-fold. One, to undertake the remedial activities required to ensure they become fully compliant with the GDPR, and, two, to transition their ongoing projects into ‘business as usual’ activities once they have reached a position of full compliance. This stable position will ensure that the organisation can continue to demonstrate a defensible position and thereby compliance with the legislation.

Internal Audit professionals need to consider the following:

- Understand the “next steps” in an organisation’s GDPR journey; consider the gaps between current state and full compliance and the risks associated with the programme to achieve full compliance.
- Challenge how management aims to ensure ongoing compliance, covering also the people perspective – What training is in place? How are they managing the expected – and necessary – cultural shifts?
- Internal Audit will have a role to play in ongoing monitoring, for example through audits of data processes; Internal Audit Heads should be part of the early conversations in establishing that ongoing role.





What are the challenges?

Internal Audit should be at the forefront of the aforementioned activities, challenging management and structuring an audit plan that focuses appropriately on the above, commensurate to the risks. Continuous audit activity may be most appropriate as the challenges will continue and the risks can be amplified:

- Firstly, the journey to full compliance will not be straightforward; many organisations have not yet fully scoped the projects or the resources needed for this second stage of the journey. Many are also unsure just how large the gaps between their current state and full compliance may be. For the majority, significant work is still required and this will entail investment of resources and time. While the Information Commission Office ultimately adopted a pragmatic approach in relation to compliance by the May 2018 legislative deadline, there is no guarantee this will continue.

- Secondly, the transition from project to business as usual is often fraught with challenges, which is also expected in the case of GDPR. While initially some organisations and internal audit teams may have seen May 2018 as the end of their GDPR related activities, in reality it is only the beginning of an ongoing journey.



4. Technology Resilience (= 4)

Why is it important?

Technology resilience capability remains a key priority for all stakeholders in financial services organisations and the sector overall, with IT Internal Audit focusing in particular on resilience from cyber attacks (refer also to the [Cyber Security topic #1](#)). The topic remains pertinent, and our [report on the cyber regulatory environment](#)³, recognised – amongst others – that regulators in Europe are expected to:

- Develop and communicate clearer standards and resilience expectations for critical firms, while focusing in areas such as application platform security, offline storage of critical backup systems.
- Focus on resilience testing by expanding and embedding mature frameworks and establishing programmes running more frequently and across sector/firms.

What is Internal Audit's response?

As technology and cyber resilience risk has remained a key focus area for several years, the majority of organisations have put in place plans or actions to address the fundamentals of ensuring their business remains resilient in an ever more technology enabled environment. Internal Audit's focus should shift from exclusively assessing the adequacy of cyber defences to also include "recoverability" and the ability of an organisation to adequately respond and recover from an attack.

This should include assessing whether the organisation has a clear understanding of the digital assets that are fundamental to survival of the organisation, and has put in place sufficient resilience measures to ensure they can enable recovery when needed.

What are the challenges?

The rapid pace of technological change and the mass digitisation of FS institutions, coupled with the need to respond to the ever evolving regulatory expectations in this area, bring a challenge for internal auditors in formulating their plan and focusing on the high risk areas.

Following a series of high-profile outages at Visa and TSB Bank earlier in 2018 with significant customer impacts, there is pressure on organisations to improve their resilience and continuity of critical (customer-facing) systems and outage response procedures.

There is an ongoing exercise by organisations to respond to the FCA and Bank of England joint discussion paper on outage response procedures and the maximum, acceptable amount of time for critical systems downtime. We are seeing many institutions with complex legacy infrastructure and application environments, experiencing difficulty meeting these requirements.

The appetite of supervisors for quick recovery seems higher than that of organisations and is driven by focus on preventing systemic issues; although this will be an ongoing discussion, it becomes imperative that organisations should be able to demonstrate (and that internal audit can provide reasonable assurance) that continuity and recovery arrangements have been robustly developed and tested against various scenarios to aid a "prompt" recovery.



5. IT Extended Enterprise Risk Management (▲6)

Why is it important?

Third-party (and fourth-party) risk management is a topic that has consistently featured in our survey for a number of years now, reflecting on the one hand the underlying challenges of organisations in dealing with risks across a complex ecosystem of external IT parties (that still remain) and on the other the regulatory attention in that area. Our recent report and survey on [Extended Enterprise Risk Management](#)⁴, acknowledges that for many organizations, “their third-party ecosystem, or ‘extended enterprise,’ is an important source of business value and strategic advantage. As the reliance on third-parties continues to grow, so do the associated risks, bringing potential reputational damage and regulatory action”.

Extended enterprise risk management in Financial Services has continued to benefit from greater executive awareness allowing organisations to tackle the topic with appropriate focus and investment. This is even more important given the threats of high profile business failure, illegal third-party actions, or regulatory action with punitive fines. For financial sector organisations, in particular, the key focus points are identifying the most strategic third-parties to ensure proportionate risk management effort, and addressing operational risks in relation to the extended enterprise. However, it is pleasing to see that FS organisations seem to be taking a more strategic view of risk drivers to create value and identify new opportunities.

What is Internal Audit’s response?

- Internal Audit should seek to challenge management on the ability of their extended enterprise framework maturity to identify and manage all forms of such risks, looking at both process and technology solutions to deliver value and meet contractual obligations. Organisational self-assessment of overall third-party risk maturity continues to improve but at a slower pace, despite a perceived increase in the inherent risks in third-party dependence.
- There is a trend by organisations to centralise many elements of third-party roles, structures, and technologies, with operating models based on Centers of Excellence (COEs) and Shared Service Centers (SSCs) arising as dominant; the suitability of these models, as well as the centralisation programmes themselves, are additional areas for Internal Audit to consider incorporating into their reviews.
- Some of the key challenges for organisations in relation to extended enterprise risk relate to internal coordination, talent and processes. Indicative areas for Internal Audit to probe on are: *Is there sufficient clarity on who does what across the three-lines of defence model? Are there overlaps or gaps? Have resources with adequate capacity and skills been placed optimally to address the most significant areas of concern and opportunity across the business?*
- Refer also to the Cognitive Automation and Artificial Intelligence hot topic (#6), where we make reference to the risks of reliance on smaller start-ups for AI and emerging technologies, and the need to ensure an appropriate and mature extended enterprise governance framework (including risk assessment) is applied consistently.

What are the challenges?

Our survey⁵ showed that organisations are lacking appropriate visibility and monitoring of sub-contractors engaged by third-parties, and it is area that continues to be challenging to appropriately audit. Recent regulation such as the Modern Slavery Act in the UK and GDPR in Europe which include requirements to manage fourth and fifth parties (where applicable) is likely to increase the level of challenge in managing risks, and constitute an area that Internal Audit would need to incorporate into their scoping accordingly.





6. Cognitive Automation and Artificial Intelligence (NEW)

Why is it important?

Financial sector organisations are operating in a 'digital' environment, which presents exciting opportunities but also many challenges, as new game-changer technologies and emerging digital competitors present a threat to existing business models. Artificial Intelligence makes use of machine learning, visual recognition and natural language processing techniques, with advance algorithms offering the ability to analyse data in an "intelligent" way; this in turn can drive operational and cost efficiencies as well as strategic transformation programmes, resulting to better and more tailored customer engagement.

Our paper on [AI and Risk Management](#)⁶, highlights that EU and international regulators have taken an active interest, and while they recognise the benefits AI can bring to markets and customers, they are increasingly mindful of the risks and unintended consequences for regulated firms. In the financial services industry in particular, processes are becoming more automated, the use of robotics⁷ and AI is increasing, therefore the need for a robust and reliable control environment, and the ability to effectively report on the status of that environment, is ever more critical.

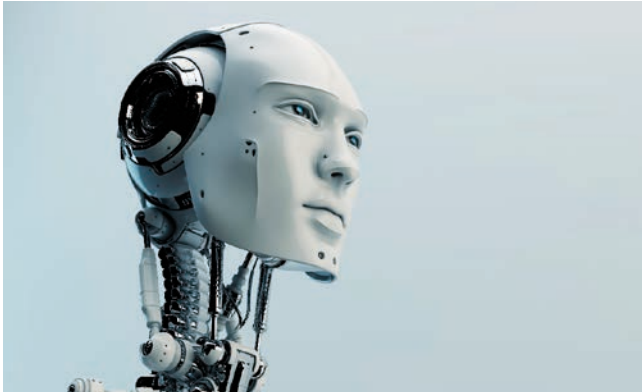
What is Internal Audit's response?

Boards and senior management need to develop a meaningful understanding of these new technologies and their implications, in order to reap the full benefits and avoid pitfalls in the future. In this context, we see Internal Audit as a useful ally in the successful adoption and implementation of such

technologies. There is clear opportunity for Audit to lead the way in terms of understanding of risks around AI, as well as the broader regulatory context, and spearhead education of the organisation.

Some suggestions for Internal Audit to consider:

- Functions should have a clear view of the AI and automation/robotics assets across the organisation, including all relevant technologies and third-party firm involvement. They should assess and map these against their audit universe, paying particular attention to over-reliance on third party providers and the associated risks. Especially in the case of new smaller AI start-ups, which may not have sufficient risk maturity and internal controls in place. Challenging management on continuity arrangements in those cases will be key. Refer also to IT Extended Enterprise Risk Management hot topic (#5).
- Internal Audit should establish a framework and methodology for auditing such technologies; this should be based on a multi-disciplinary approach to risk, and not rely purely on technology risk domains. AI is less about completely new risks, but about a multitude of existing ones that may be harder to identify, given the complexity and speed of solutions. Risks may manifest in unfamiliar ways and with unprecedented velocity and impact.
- Functions should stay close to the global regulatory developments, as this may influence the approach to adopt. In anticipation of clear supervisory guidance, the [CIIA Global Perspectives paper](#) on AI⁸ offers some insights, but we also recommend that Audit leverage the principles of existing supervisory statements relating to use of algorithmic trading, supervision of models, operational, cyber and technology resilience, the Senior Managers and Certification Regime and general requirements on IT controls.



- As our AI and Risk Management [paper](#) suggests, a mental-shift to a scientific mind-set may be required, using “sandbox” environment across the organisation and involving Internal Audit, as well as other risk and control functions. Full participation would allow all parties to understand some of the critical technical aspects, and help shape an appropriate and pragmatic governance, risk and audit approach.

What are the challenges?

- AI solutions are developed to ‘learn’ and evolve their capabilities over time, making it inherently difficult to completely decode their decision processing layers, which in turn makes auditability and traceability of the decision making rationale challenging.
- It is recognised that the industry suffers from a lack of sufficient in-house skills to use, appropriately supervise or audit AI solutions that are being adopted. Internal Audit functions looking to augment their core team with technology specialists may find that cultural differences between technologists and auditors around risk and control result in the need to invest in upskilling technology specialists to operate as effective auditors.



7. Cloud Computing (Δ8)

Why is it important?

The adoption of cloud services and “cloud first” strategies is characterised by a rapid growth particularly in the financial services sector, and define not just IT strategy but corporate strategy. As a result, understanding the impact of ‘consuming’ cloud services and migrating data to the cloud on the organisation’s operational risk profile is critical.

Although organisations see a large part of their IT functions being handed over to a cloud service provider, they should not lose sight of the fact that they are still accountable and they must “stay in control” by proactively assessing and adequately managing the associated risks.

What is Internal Audit’s response?

Internal audit’s focus will vary depending on the level of cloud adoption by the business and the maturity of existing third party management processes. For organisations with a limited cloud footprint, Internal audit should focus on the appropriateness of cloud strategy and the capability of existing risk management functions to address cloud specific risks. In more mature cloud environments, Internal Audit functions should perform reviews that assess the effectiveness of controls to protect services delivered from/assets managed in the cloud and consider reviews that assess the degree to which the stated benefits of cloud migrations have been realised.

We recommend that Internal Audit functions assess risks vs benefits in these four areas: creating a strategy for cloud adoption; managing people and change; integrating digital and legacy technology; and managing operational risk and

compliance. Our recent [Deloitte paper](#) on cloud⁹, shows that successful use depends on getting it right in these four domains.

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

What are the challenges?

The limited availability of resources with relevant skillset, experience and exposure to cloud technologies and an understanding of cloud-specific risks is a key challenge.

While guidance from organisations such as the Cloud Security Alliance (CSA) can assist technology auditors in scoping cloud audits, an understanding of cloud business models, the shared responsibility model of controls and the technology that supports cloud environments is required to perform robust reviews of cloud controls.





8. Legacy applications (▲10)

Why is it important?

Many financial services organisations are still burdened with a complex legacy technology estate that is the product of historical growth strategies. A tangled web of systems creating significant overhead to “keep the lights on”, both in terms of cost and resources required.

In an environment where emerging FinTech competitors unencumbered with this history are able to rapidly deploy new products in a locally hosted or cloud environment, this legacy technology baggage acts as a limiting factor for organisations trying to keep up with the pace of change. 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.

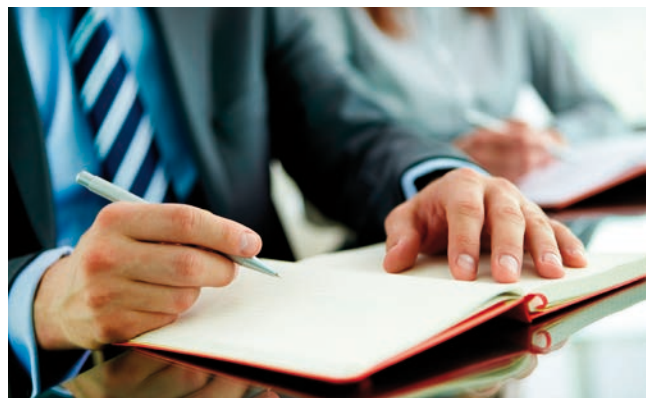
What is Internal Audit's response?

This topic remains a key challenge for Internal Audit departments, aiming to ensure adequate cover across such areas of the estate. They need to assess whether reliance on legacy applications results in an aggregate risk exposure that is outside of risk appetite due to the impact on the ability to adapt to the changing environment, comply with new regulation and provide the business with the resilient systems they require to meet the expectations of both customers and the regulators.

This requires an understanding of the overall risk presented by the legacy estate and management's process for assessing, understanding and defining an appropriate 'risk treatment' for these risks – accept, mitigate, avoid. Refer also to the Technology Transformation and Change hot topic (#2).

What are the challenges?

Internal Audit functions are often confronted with a view from the business that changing legacy systems or migrating to new systems is too difficult or too costly. It is crucial to be able to articulate the ongoing impact of not addressing the underlying issues of managing a complex legacy estate and the potential for this to limit the ability of the organisation to manage risk within appetite and evolve over the medium and long term. This may mean challenging the business investment decisions and approach to risk prioritisation.





9. Application Development | Agile and DevOps (NEW)

Why is it important?

As financial services organisations recognise the need to respond to rapid technology and business change, they are adopting working practices that provide the necessary responsiveness to meet business and customer demands. Adoption of Agile and DevOps (development and IT operations) methodologies represent a significant cultural and organisational change from the traditional software development lifecycle. Adopting Agile principles can accelerate the delivery of solutions while combining the disciplines of Development and Operations reduces the overhead of siloed teams and inefficient release management.

Well implemented Agile and DevOps delivery methods can result in a higher degree of automation of controls and provide an enhanced audit trail. Getting the implementation of these methodologies right, would lead to a series of benefits, such as reduction in production incidents, releasing frequently in small chunks rather than through a 'big-bang' approach, resolution that take less time given automated/repeatable process with enhanced traceability.

Conversely, poorly implemented Agile and DevOps approaches, particularly without the appropriate focus on controls, can lead to a lack of accountability on risk, lack of documentation, failure to implement built-in controls and, importantly, unrealised benefits.

What is Internal Audit's response?

While Agile and DevOps may present a significant change in the way that software is produced, the key principles of applying well-designed and implemented controls to mitigate risk, are still pertinent. As ever, organisations must have an understanding of their risk appetite and the extent to which any changes impact their risk exposure. Controls implemented in a DevOps process may look substantially different to traditional controls, but should still focus on addressing the same underlying risks.

Internal Audit must educate themselves on the use of automated approaches to software testing and release management, and provide assurance that controls implemented as part of new ways of working continue to adequately mitigate the underlying risk. They need to have a robust understanding of the transition from monolithic to 'micro-services application architecture, as well as keeping an eye out for the impact of emerging technologies which are continuously introduced thus multiplying the potential risk scenarios and exposure.

There is also an opportunity for teams to leverage new data points and sources that become available through DevOps automation. This will enable continuous assessments of key automated controls in addition to the periodic review cycles



In addition, Internal Audit should be aware that technology functions that adopt Agile and DevOps practices are continuously aiming to evolve their ways of working, with this being one of the principles of agile “retrospectives”, thus adding another layer of complexity and challenge for internal auditors.

What are the challenges?

Skills in auditing Agile and DevOps models are in high demand, but functions need to ensure they have the capability to understand the true risks, speak the ‘language’ of the auditees, and respond to the assurance needs. While Agile and DevOps can drive value with accelerated speed-to-market, the enterprise wide adoption of these methodologies is complex and often built on outdated processes, burdened with legacy thinking and systems.



10. Payments systems (NEW)

Why is it important?

Payments is a key source of revenue and relationship anchor with customers. The payments market is undergoing significant disruption and the current dominance of traditional financial institutions has come under threat due to changing consumer preferences, regulatory and industry interventions and technology-enabled innovation.

The introduction of the second [Payment Services Directive \(PSD2\)](#) and [Open Banking](#)¹⁰ are opening up the payments market and are enabling non-bank participants and FinTech firms to offer new payment services. Legacy payment technology environments are being modernised and the use of open API platforms is enabling connectivity with service providers while also driving collaboration between major financial institutions and FinTech firms. Regulatory scrutiny remains high, as firms develop new payment strategies and respond to increasing compliance requirements. Recent instances of significant payment system-related outages have also attracted a lot of attention.

What is Internal Audit's response?

Internal audit has a role to play in providing assurance that organisations adapt and develop their payment offerings and comply with the evolving regulatory requirements. There is a need to challenge first and second line of defence functions to ensure that payments transformation activities are appropriately managed and that they are able to demonstrate ongoing compliance with new regulatory requirements.

Creating and launching APIs typically involves the use of Agile delivery methods; internal audit should ensure that they consider the implications of adopting new ways of working as described in the Application Development section of this publication ([#9](#)).

What are the challenges?

Internal audit will be expected to perform a variety of assurance activities covering regulatory risk assessments, technology security assessments, project assurance reviews as well as assessments of the resilience and reliability of existing payment systems services. In order to cover all of these aspects there may be a need to fully comprehend the regulatory requirements and implications, and upskill or supplement staff accordingly.





Endnotes

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

² Cyber risk and regulation in Europe: A new paradigm; 2018; Deloitte LLP

³ Cyber risk and regulation in Europe: A new paradigm; 2018 Deloitte LLP

⁴ Focusing on the climb ahead, Extended enterprise risk management survey 2018, Deloitte LLP

⁵ Focusing on the climb ahead, Extended enterprise risk management survey 2018, Deloitte LLP

⁶ AI and Risk Management: Innovating with confidence; Centre for Regulatory Strategy EMEA; 2018 Deloitte LLP

⁷ IT Risk Automation Pulse Survey: Driving value through automation; 2018 Deloitte LLP

⁸ CIIA Global Perspectives and Insights: Issue 9/Special Three-part Series: Artificial Intelligence, Internal Audit's Role, and Introducing a New Framework; 2018 CIIA <https://na.theiia.org/periodicals/Pages/Global-Perspectives-and-Insights-Archives.aspx>

⁹ Maintaining control in the cloud; Developing and managing an effective cloud strategy; Deloitte LLP; 2018

¹⁰ Opening up the opportunities within Commercial Banking, PSD2 and Open Banking; Deloitte LLP; 2018

Contacts



Mike Sobers

Partner

020 7007 0483

msobers@deloitte.co.uk



Yannis Petras

Director

020 7303 8848

ypetras@deloitte.co.uk



Jonathan Roffey

Director

020 7007 8755

jroffey@deloitte.co.uk



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

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

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

© 2018 Deloitte LLP. All rights reserved.