Contents

Section 1: Planning Priorities for Internal Audit

Artificial Intelligence and Robotic Process Automation  01
Cyber  02
Data Privacy and GDPR  03
Cloud  04
Crisis Management  05
Auditing culture  06
Oversight of 3rd parties (Part A – General)  07
Oversight of 3rd parties (Part B – IT & Technology)  08
Risk Culture  09

Section 2: New Methodologies for Internal Audit

Agile Internal Audit  13
Talent  14
Quality Assurance (QA)  15
Web-Based Risk Sensing (WBRS)  16
Risk Assessments  17
It’s my pleasure to present Deloitte’s 2019 Internal Audit Planning Priorities.

It is clear from the breadth of topics covered in this publication that the role of internal audit (IA) continues to evolve. Recognising the increasingly complex assurance that IA is being challenged to provide, and a continued focus on functional transformation.

For the first time we have included a dedicated section focusing on some of the new tools and techniques available to IA to deliver against their evolving mandate. Agile auditing, the use of automation and the talent needs of the IA teams of tomorrow are all featured. Whilst readers may be familiar with some of these terms, the inclusion of topics such as risk sensing represent the cutting edge of internal auditing and demonstrate how technology is changing the way our professions works.

There are also a number of new focus areas to consider for inclusion in annual audit plans. We anticipate an increased emphasis on digital risks (including artificial intelligence and ‘cloud’ computing), a continuing focus on data privacy and GDPR and oversight of 3rd parties.

Our ‘Topics by Theme’ section provides further detail on each of these interesting topics including, where relevant, additional sector-specific insights. For each of the topics you will find a brief commentary providing some background, along with notes on how the topic can be audited and some of the potential challenges that you may face.

As always, we hope this edition contributes to your annual planning process, providing useful insights and generating meaningful debate with key stakeholders and with your teams. Should you wish to discuss any aspect in further detail, please do not hesitate to contact one of our team.

David Kinsella
Partner
Section 1
Planning Priorities for Internal Audit
Artificial Intelligence and Robotic Process Automation
Evolving process efficiency

Why is it important?

Artificial Intelligence (AI) makes use of machine learning, visual recognition and natural language processing techniques, with advanced algorithms offering the ability to analyse data in an “intelligent” way. This can in turn drive operational and cost efficiencies as well as strategic transformation programmes, resulting in better and more tailored customer engagement.

Robotic Process Automation (RPA) is an evolving form of business processing that relies on automated technologies such as software robots to perform repeatable processes in an efficient and cost effective manner.

The use of AI and RPA 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 should you be doing?

There are a range of potential activities that IA can perform, some of which are captured below:

- IA can map AI and automation assets against their audit universe, paying particular attention to over-reliance on third party providers. Challenging management on continuity arrangements in these cases will be key.
- IA should consider establishing a framework and methodology for auditing 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, more about existing risks that may be harder to identify, given the complexity and speed of solutions.

Potential Challenges?

There are a number of challenges to auditing AI & automation solutions, some of which are set out below:

- Auditability – AI solutions are developed to ‘learn’ and evolve their capabilities over time, making it inherently challenging to completely decode their decision processing layers, which in turn makes auditability and traceability of the decision-making rationale challenging.
- Skillset – It is recognised that the industry suffers from a lack of in-house skills to appropriately supervise or audit solutions that are being adopted. Lack of cultural integration of such resources may also pose a challenge for IA functions seeking to upskill their teams and complement their resource base.
- Full participation – A shift to using a “sandbox” environment across the organisation, and involving IA, as well as other risk and control functions may be required. Full participation will allow IA to help shape an appropriate and pragmatic governance, risk and audit approach.
Cyber Risk is a priority today more than ever, as technological advances such as Artificial Intelligence, IoT, Robotics, Virtual Reality and Cloud Computing are increasingly making our home and work-lives easier. All of these advances come with an associated level of risk and particularly Cyber risk, as compromise by malicious entities can cause untold damage and even lead to direct fatalities. Standardisation and quality assurance (including security) is critical in managing many of these risks. Some industries are ahead of others, as stakeholders in FS for example, are heavily regulated including as GDPR, the NIS Directive, PSD2, and EU-TIBER focus on cyber threat as a critical risk to FS today. Our recent report on Cyber Risk identified that in 2019 we expect FS regulators in European jurisdictions to pursue a combination of the following:

- Develop and communicate clearer standards and cyber resilience expectations;
- Formalise incident identification and breach reporting procedures;
- Place increased pressure on banks’ Boards to demonstrate ability to provide effective challenge, through access to independent expertise; and
- Focus on risk and control frameworks and quantification of cyber risk.

As cyber risk has remained a key focus area for several years, the majority of functions have put in place plans or actions to address the fundamentals of prevention and detection. IA should consider a shift in focus from assessing the adequacy of cyber defences to “recoverability” and the ability of an organisation to adequately respond and recover from an attack. This should include:

- Assessing whether the organisation has an understanding of the digital assets that are fundamental to survival and whether measures are in place to ensure these are available to enable recovery;
- Challenging 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; and
- Utilising new technologies, such as AI, which amplify the awareness of threats to the cyber resilience of the organisation.

IA should consider the following challenges:

- **Flexibility** – Executives need to anticipate and interpret regulatory developments and their impact on their organisation in order to make timely decisions, as well as their own threat analysis and cyber programmes. Equally, IA functions need to stay close to these developments and have a clear plan on what to do next.
- **Timeliness** – Many cyber initiatives have the objective of improving cyber maturity over a period of years. This makes determining the appropriate time to perform an audit challenging. IA should 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.
- **Resourcing** – IA may find resourcing cyber audits with staff who have had exposure to cyber specific risks difficult. This could impact IA’s ability to provide an appropriate level of assurance.
Data Privacy and GDPR
Ensuring ongoing compliance

Why is it important?

Data protection continues to be a topic of ongoing discussion, challenge and focus by management, Boards, and IA alike. While 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. As such, many have focused on what they deem as their “high risk” areas to establish what they hoped would be a defensible and pragmatic approach for when the new legislation became enforceable.

Now the legislation is fully enforceable, the focus for organisations is primarily two-fold:

- One, to undertake the remedial activities required to ensure they become fully compliant with GDPR; and
- Two, to transition their ongoing projects into BAU activities once firms have reached a position of full compliance.

What should you be doing?

Now that GDPR is fully in force, we suggest that IA consider the following activities:

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

Potential Challenges?

Continuous audit activity may be most appropriate in this area as the challenges surrounding GDPR will remain. This could amplify the following risks:

- **Scoping** – Many organisations have not yet fully scoped the projects or the resources needed to ensure compliance in a post 25th May world. Many are unsure how large the gaps between current state and full compliance are, challenging IA’s ability to scope their work.
- **BAU phase** – The transition from project to BAU is often complicated and this is expected in the case for GDPR. While initially some IA 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.
Cloud

Backing up data safely, securely and efficiently

Why is it important?

All industries have seen rapid growth of cloud services and “cloud first” strategies. As a result, IA’s ability to understand the impact of migrating data to, and use of, the cloud as part of the organisation’s operational risk profile is critical.

Use of the cloud exposes firms to a number of risks. There is typically less visibility of security and governance controls, differing cloud standards and guidelines to consider, and multiple implementation approaches. All of these can expose a firm to significant brand, reputational or privacy breach risk.

What should you be doing?

IA’s focus will vary depending on the level of cloud adoption by the business and the maturity of existing third party management processes. Three possible approaches are:

• For organisations with a limited cloud footprint, IA should challenge management on the appropriateness of their cloud strategy and the capability of existing risk management functions to address cloud specific risks. This will include engaging with business stakeholders to identify and discuss cloud specific risks.

• In more mature cloud environments, IA 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.

• Where firms have a fully embedded cloud solution, IA’s work can centre on risk mitigation activities, to ensure associated risks are minimised. This may include evaluation of the cloud provider to ensure stability and data storage and ownership are considered.

Potential Challenges?

IA may face challenges in the following areas:

• Resourcing – The limited availability of resources with exposure to cloud technologies and an understanding of cloud specific risks will make auditing this area challenging. 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.

• Cloud migration – One of the challenges for IA can be involvement in the initial cloud migration project setup. Lack of visibility of key controls in this crucial design stage may hamper IA’s ability to identify control weaknesses until these are being implemented by the business.
Crisis Management

Actively protecting brand value and reputation

Why is it important?

In a rapidly evolving world, organisations find themselves operating in a landscape of uncertainty with heightened risk and stakeholder scrutiny. These risks can come from geopolitical, economic, financial and societal events through to corporate misdeed and high impact operational or technological failures.

Crises present the biggest and growing threats to corporate value and executive reputation and 2018 has been characterised by a number of such events in the market.

Organisations that fail to effectively deal with the risk of crisis can see their reputation, strategic interests, bottom line, and even their existence, threatened or destroyed.

What should you be doing?

A range of approaches can be taken by IA, outlined below:

- A review of the process and controls set out in the firm’s crisis management policy and procedures manual;
- A review of lessons learned stemming from crisis management test scenarios; and
- A review of progress against remedial activity identified through initial gap analysis/test scenarios.

Alternatively, a framework evaluation tool can be used to audit the current crisis management capabilities across the entire crisis and risk lifecycle. This will allow IA to:

- Identify any vulnerabilities in the lifecycle;
- Benchmark against existing best practice; and
- Make recommendations with regards to focus areas moving forwards.

Potential Challenges?

IA may find challenges in the following areas:

- **Senior audit sponsor** – Lack of an obvious C-suite level audit sponsor, which could potentially impact business buy-in.
- **Organisational bias** – IA will face challenges in delivering difficult messages when findings are identified in conflict with organisational bias in the area.
- **Lack of transparency** – Often areas of weakness (business units, subsidiaries, etc.) do not want to share details of failings in operational discipline. IA will face challenge in auditing these areas.
Auditing culture
A Powerful Competitive Advantage

Why is it important?

An organisation’s culture is a complex, highly valuable asset, difficult to replicate and a powerful competitive advantage when aligned with corporate strategy. Culture is “the way we do things around here” and becomes visible in the choices people make, how they interact with one another and how they deliver against their objectives. Culture can be transformed through an understanding of the current and desired future state, and by activating various organisational levers, such as changes in management processes, learning, recruitment, and leader behaviors, to steer the culture in the desired direction.

Increasingly, culture is seen as a priority measure for Boards. Internal audit, through its work and focus on audit results and cultural themes, can provide the Board and Senior Management some assurance and a point of view on the state of organisational culture and the responsiveness of the organisation to acknowledge and address cultural issues. Also, auditing and assessing culture is critical for monitoring traction on culture initiatives designed to transition the organisation towards a desired organisational culture.

What should you be doing?

There are a variety of ways to audit culture in your business, this includes performing a cultural assessment for each and every audit on the plan, or a dedicated ‘big bang’ audit. The one-off approach is typically more challenging, however, we have seen success using this approach where IA consider the following factors:

- Align IA’s work to an existing culture framework or programme (preferably internal to the business in question);
- Building of a repository of evidence;
- Consideration of interviews with key stakeholders; and
- Delivery of findings aligned to the business’ strategic objective.

Potential Challenges?

Potential challenges for IA in assessing culture include:

- Culture indicators - One of the challenges for IA in auditing culture is that they can typically only move as fast as the business. Without a clear culture framework to audit against, IA will need to establish what indicators they should use.
- Audit approach - IA will need to develop a cost effective and efficient approach to audit an organisation’s culture profile. This will need to be supported by tangible evidence that provides the required level of assurance for reporting to the Audit Committee.
- Audit skills - Internal auditors need not only to be controls and business experts, but they also need to have heightened levels of self-awareness and be more sensitive to the emotional drivers of teams, management, and the organisations. They need to understand how poor behaviour can adversely impact day-to-day activities within an organisation and ultimately its strategic direction. A good balance between left brain thinking — logical, analytical, and technical— and right brain thinking — creative, feelings, holistic— is needed. That said, auditors do not need to be psychologists. Instead, more honed, soft skills combined with effective communication capabilities will help them engage in credible culture discussions and educate stakeholders on the importance of culture and behaviour.
- Benchmarking - IA will need to access an appropriate benchmark to compare culture and indicators of good culture in the organisation against industry expectations. Actions will need to be focused on removing discrepancies between the firm’s culture and that in the rest of the industry.
Oversight of 3rd parties (Part A – General)
Identifying and mitigating third party risk

Why is it important?
Recently, there have been several high profile cases where third party supplier failure, or the inappropriate actions of suppliers, have caused either monetary loss or reputational damage. The issue of oversight of 3rd parties has been an issue raised in previous iterations of this publication, however, given these high profile failures it is clear that the risk has crystallised and concern in the market continues to be well placed.

Additionally, Organisations continue to increasingly outsource activities which traditionally would have been undertaken internally, exposing them to additional third party risks (TPRs). This can be due to inadequate controls being in place at, or performance failure of, the third party, or inadequate oversight by the outsourcer.

Our experience has shown that there is sometimes a cultural misunderstanding in organisations, with organisations not having as much control or oversight of their third parties as companies have over their own operations. This makes this a key area for IA moving into 2019.

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

Design effectiveness
Assess if the following factors are designed adequately:
• Overarching governance framework
• TPR framework and associated policies
• Appropriate allocation of roles and responsibilities
• Processes and controls to manage TPRs throughout their lifecycle
• Tools and technologies supporting the TPRM process
• Appropriateness of metrics used to measure effectiveness of TPRM framework

Operating effectiveness
Assess control performance in the following areas:
• Risk identification and assessment
• Third party selection
• Contract execution
• Role and responsibility allocation
• Ongoing monitoring and reporting assessment appraisal
• Contract termination and exit or renewal management

Potential Challenges?
Organisations will have to decide on implementing either a centralised or de-centralised TPR operating model. Most organisation will not adopt a purely centralised model, meaning challenges for IA will lie in:

• Inconsistency – A decentralised model may result in inconsistent application of third party policies and procedures and a lack of a holistic view of risks. Hence IA should seek to challenge instances of inconsistency in application of policy/methodology.

• Complexity – Organisations may have partially or fully outsourced the management of TPM/TPRM to external providers. This will lead to additional complexity when undertaking an internal audit of the framework.
Oversight of 3rd parties (Part B – IT & Technology)
You can’t outsource risk

Why is it important?
The trend in outsourcing IT functionality is increasing, and will likely continue to do so given the availability and value of IT outsourced services.

There are various levels of IT outsourcing, with the risk increasing as the provider has greater levels of access to a firm’s data and/or systems configurations.

Services provided should fit the business need (for example continuous access by the provider versus access granted on an ad-hoc basis).

Whatever the level of outsourcing, firms should be clear that the risks will continue to reside within the business.

What should you be doing?
There are a number of activities that IA can perform specifically in the outsourcing of IT area, we have detailed a selection of these below:

- IA can undertake an assessment of the internal function (e.g. IT/ Risk) holding responsibility for governance and oversight over 3rd parties. The objective of this review is to ensure that there is a comprehensive 3rd party risk management framework embedded to ensure risks are sufficiently mitigated.

- IA can also undertake dedicated work over the 3rd party through exercising the contractual right to audit (where this exists). As part of this audit IA should consider reviewing the sufficiency and appropriateness of MI and other ad-hoc reporting provided by the 3rd party.

- IA can also undertake direct testing, or engage an independent 3rd party to review an IT providers control environment (e.g. through specific technology certifications such as ISO27001 /SSAE18 / or assurance reports).

Potential Challenges?
Due to the high number of potential risks in this area, IA may face any number of challenges when conducting their work. Examples include:

- Documentation – Insufficient documentation of required internal procedures that outline required oversight of the provider. This makes it difficult for IA to audit against an agreed set of principles.

- Certification – Insufficient clarity over required independent certification, and certification frequency from the IT Provider.

- Right to audit – The absence of a contractual ‘right to audit’ can prevent IA from fully discharging its remit where pervasive issues with the provider have been identified.

SSAE18 SOC2 Trust Principles

- Confidentiality
- Privacy
- Security
- Processing Integrity
- Availability
Risk Culture

You can’t outsource risk

Why is it important?

Risk Management, driven by regulatory pressures and the desire for competitive advantage, is at the heart of why risk culture is at the top of many Boards’ agendas.

Increasingly, risk culture is seen as a priority measure for IA. In particular, a risk intelligent culture is seen as the ‘invisible glue’ that makes organisations work. Also, auditing and assessing risk culture profiles across population demographics is critical for monitoring traction on transitioning towards a desired risk culture.

The risks of not getting risk culture right are:

• Not achieving the organisational purpose, strategy, philosophy, and longer term business objectives; and/or
• Breaches in risk appetite and/or regulatory compliance.

What should you be doing?

There are a variety of ways to audit risk culture in your business, this includes performing a cultural assessment for each and every audit on the plan, or a dedicated ‘big bang’ audit. The one-off approach is typically more challenging, however, we have seen success using this approach where IA consider the following factors:

• Align IA’s work to an existing risk culture framework (preferably internal to the business in question);
• Building of a repository of evidence;
• Consideration of interviews with key stakeholders; and
• Delivery of findings aligned to the business’ strategic objective.

Potential Challenges?

Potential challenges for IA in assessing risk culture include:

• Risk culture indicators – One of the challenges for IA in auditing risk culture is that they can typically only move as fast as the business. Without a clear risk culture framework to audit against, IA will need to establish what indicators they should use.

• Audit approach – IA will need to develop a cost effective and efficient approach to audit an organisation’s risk culture profile. This will need to be supported by tangible evidence that provides the required level of assurance for reporting to the Audit Committee.

• Benchmarking – IA will need to access an appropriate benchmark to compare risk culture in the organisation against industry expectations. Actions will need to be focused on removing discrepancies between the organisation’s risk culture and that in the rest of the industry.
Section 2
New Methodologies for Internal Audit
Agile Internal Audit
Better, faster, happier

Why is it important?
Throughout 2018 Agile has become more topical amongst the IA community. Since then, there has been a significant increase in the number of IA departments adopting Agile.

Agile IA is a mind-set supporting a collaborative environment for audit and the business to solve audit problems through taking an iterative, time-boxed approach. Agile may not be for everyone and careful consideration should be given to the potential benefits to each specific financial institution of adopting such an approach, comparing to the costs involved. Hence many IA functions have taken a workshop and pilot approach to assess these factors before deciding whether to undertake more significant investment. Once you have clarity on your vision and Agile IA blueprint, the next step is to pilot.

How can IA use it?
Agile is a proven framework that places focus on teams value and impact. Through the application of Agile techniques, audit teams can deliver better, faster, and happier audits by:

- Helping functions create more value and impact through better interactions with IA's stakeholders;
- Surfacing problems sooner, forcing teams to address and improve areas that could lead to quality issues and driving better quality audits;
- Focusing on team performance, increasing productivity, creating more sustainable working practices and building trust through empowering staff;
- Reducing the input effort required to deliver value and minimising the time between work and providing assurance;
- Allowing IA to adapt rapidly to the changing needs of the business through an iterative and collaborative approach; and
- Creating an ownership culture where teams are empowered to make decisions, learn from each other and feel valued.

Potential Challenges?
IA may find challenges in adopting Agile in the following ways:

- **Tone from the top** - Agile is not a methodology, it’s a mind-set and framework, supported by techniques and processes. Adopting Agile requires a transformation in leadership behaviour.
- **Coaching** - To deliver true mind-set shifts and transformations there needs to be an executive level mind-set shift, and an Agile Champion within the function. Those functions who have been most successful in their adoption of Agile have been supported by Agile IA coaches to help teams change their behaviours.
**Talent**

**Addressing the Internal Audit resourcing needs of the future**

As this document clearly demonstrates, there is an increased focus on the role and remit of IA, and audit committees are increasingly challenging functions to provide more complex assurance. With this, there is greater emphasis on hiring from non-traditional IA backgrounds (e.g. accountants) in favour of industry and subject-matter specialists (e.g. cyber specialists, data scientists, etc.).

Addressing IA’s talent needs through diversification of the team will allow IA to respond to both today’s and tomorrow’s challenges.

---

**Why is it important?**

As this document clearly demonstrates, there is an increased focus on the role and remit of IA, and audit committees are increasingly challenging functions to provide more complex assurance. With this, there is greater emphasis on hiring from non-traditional IA backgrounds (e.g. accountants) in favour of industry and subject-matter specialists (e.g. cyber specialists, data scientists, etc.).

---

**How can IA use it?**

Whilst it is increasingly common for larger IA functions to have in-house data analytics and cyber security and many functions will not be able to draw on these resources. For those functions with a more traditional resource base, consideration of the following will help to address this challenge:

- **Identify skill gaps** – IA functions should perform a preliminary assessment of potential skill gaps. Discussions with direct reporting lines and audit committee members will help to identify which gaps are deemed to be a priority.
- **Use of co-source partners** – many external providers can offer access to specialise skillsets on a ‘pay as you go’ basis. This option is attractive for IA functions with limited budgets and/ or one-off engagements requiring specialist support.
- **Leverage existing firm skillsets** – the use of business secondees is a popular option to plug skill gaps. Leveraging in-house skills from established IT, data analytics and other teams is a cost effective way of addressing gaps on a short term basis.

---

**Potential Challenges?**

With a number of topics in this document, we have identified talent as an area of concern. In an evolving market we expect this trend to continue, however, this highlights several key challenges:

- **Budgets** – Specialist resources often come with a high price tag. With IA budgets typically remaining static, recruitment of specialist resources may be considered a luxury.
- **Timing** – Identifying the right individuals at the right time may take time.
- **Training** – Identifying the right individuals at the right time may take time.

---

**Why is it important?**

As this document clearly demonstrates, there is an increased focus on the role and remit of IA, and audit committees are increasingly challenging functions to provide more complex assurance. With this, there is greater emphasis on hiring from non-traditional IA backgrounds (e.g. accountants) in favour of industry and subject-matter specialists (e.g. cyber specialists, data scientists, etc.).

Addressing IA’s talent needs through diversification of the team will allow IA to respond to both today’s and tomorrow’s challenges.

---

**How can IA use it?**

Whilst it is increasingly common for larger IA functions to have in-house data analytics and cyber security and many functions will not be able to draw on these resources. For those functions with a more traditional resource base, consideration of the following will help to address this challenge:

- **Identify skill gaps** – IA functions should perform a preliminary assessment of potential skill gaps. Discussions with direct reporting lines and audit committee members will help to identify which gaps are deemed to be a priority.
- **Use of co-source partners** – many external providers can offer access to specialise skillsets on a ‘pay as you go’ basis. This option is attractive for IA functions with limited budgets and/ or one-off engagements requiring specialist support.
- **Leverage existing firm skillsets** – the use of business secondees is a popular option to plug skill gaps. Leveraging in-house skills from established IT, data analytics and other teams is a cost effective way of addressing gaps on a short term basis.

---

**Potential Challenges?**

With a number of topics in this document, we have identified talent as an area of concern. In an evolving market we expect this trend to continue, however, this highlights several key challenges:

- **Budgets** – Specialist resources often come with a high price tag. With IA budgets typically remaining static, recruitment of specialist resources may be considered a luxury.
- **Timing** – Identifying the right individuals at the right time may take time.
- **Training** – Individuals transferring to their first role in IA may require a period of training to understand key working protocols and terminology.
Quality Assurance (QA)
Continuous improvement, value creation and culture

Why is it important?
The remit, scope and approach of audit functions is under increased focus, with stakeholders and regulators looking to assess the value, the reach and the impact of IA.

In response, IA functions (large and small) are refreshing their approaches to QA to focus on all aspects of audit quality. Correspondingly, the scope of audit QA now typically includes:
• Methodology compliance;
• Audit risk;
• Continuous improvement opportunities;
• IA value creation;
• Learning and development; and
• Culture.

Our experience suggests that some functions have embraced a supportive QA approach incorporating “quality coaching” that is supportive yet still maintains independence and objectivity.

Other firms continue to take more of a “policing” approach, focusing on methodology compliance and ensuring strict independence between IA staff.

How can IA use it?
Increasingly, IA teams are using different types of QA which, in combination, are designed to embed audit quality at all stages of the audit process. The goal of this activity is to also support ongoing development and continuous improvement of the audit team. Typical examples include:
• In flight reviews – Shadowing of reviews at key points of the audit cycle with active engagement and real time feedback to the team.
• Thematic reviews – Focused post-audit reviews of high risk/ high impact areas across a sample of reviews.
• Continuous monitoring – Tracking of QA KPIs, identification of emerging trends, and/ or material issues and visibility for the whole function.
• Analytics - Use of data analytics in some larger functions to provide real time sight of quality hot spots (e.g. timing of review, quantity of documents retained on file, timeliness to archive). Use of this continuous monitoring capability will help build a forward looking, proactive role to drive improved standards.
• Reporting – In larger functions, formalisation of regular meetings between Heads of QA and AC Chairs to support their stewardship of this role, environment (e.g. through specific technology certifications such as ISO27001 /SSAE18 / or assurance reports).

Potential Challenges?
IA may face challenges in adopting a revised QA approach in the following ways:
• Resourcing – The adoption of a new QA approach may require increased resources, technical skills or SME capability. In some cases, IA functions have looked to outsource this activity.
• Communication – A new approach may bring changing requirements. Any changes will need to be proactively managed with clear communication amongst all those involved.
• Approach – IA functions with a well developed and clearly articulated QA approach may benefit from a regulatory dividend where confidence in IA may lead to a less intrusive approach.
• Responsive – With the introduction of Agile IA, audit teams will need to consider development of a responsive QA approach reflecting the values and principles of this methodology.
Web-Based Risk Sensing (WBRS)

Using open-source data to identify emerging risks

The increase focus on data has prompted new, efficient and targeted ways of accessing and analysing information. Risk sensing, the practice of analysing open-source data, can help identify emerging risks.

It can also help an organisation address a number of challenges, including:

- Monitoring and tracking the relevant regulatory environment, including identifying changing regulatory regimes across the globe;
- Identifying risks specific to the business and "connecting the dots" across different risk areas;
- Generating insights by analysing the data to create actionable intelligence for key business decision-makers; and
- Understanding the extent of a firm's digital footprint.

Whilst WBRS is an emerging technology, it can produce actionable intelligence for IA and can be used throughout the annual planning and audit lifecycle as follows:

- Risk assessment and annual planning: IA can use WBRS as a tool to identify emerging risks. Additionally, it can be a useful tool to provide the audit committee with a view of potential hidden risks;
- Audit scoping: WBRS can also be used during the audit planning process to identify key priorities and potential scope areas; and
- Audit fieldwork and reporting: Additionally, WBRS can be used to supplement IA's fieldwork and reporting to analyse data and provide additional insights on the business addressing gaps on a short term basis.

IA may face challenges in the following areas:

- **Impact** – WBRS relies on these open-source data including results derived from scanning social media platforms such as Twitter and Facebook. A potential challenge with its use as a tool for IA can be that it relies on this information, perceived, often incorrectly, as less accurate than internally generated management information.
- **Knowledge gap** – WBRS is an emerging technology and one of the perceived barriers to its use by IA functions is ease of access. WBRS tools typically exist as a managed service and there are several providers in the market. Discussion with these providers can provide greater clarity on WBRS capabilities and potential uses for IA.
Increased transparency in the assessment and audit of risks

**Why is it important?**

Some IA functions have found that a traditional planning model can lead to a lack of transparency in the risk assessment process with audit plans based on risk-assessing auditable entities not necessarily translating later in the audit cycle into detailed focus on the key risks.

Other suboptimal impacts found in traditional planning processes include inconsistencies in the size of auditable entities, in part as a result of:
- Irregular structuring of the audit universe;
- A lack of focus on individual auditable entities; and
- Inconsistent interpretation of which risks should be assessed on an entity-by-entity basis.

Consequently, many functions are revising their planning approaches to increase transparency and consistency in the identification and initial assessment of risks, tracking these through to individual audits.

**How can IA use it?**

IA functions should take the opportunity to review their risk assessment process and audit universe, using this exercise to increase clarity surrounding how the plan has been formulated and how the key risks are communicated to audit committees and other stakeholders. When undertaking this exercise IA should consider alignment with other assurance providers in respect of both risk taxonomy and reporting.

A starting point would be to review and re-establish the principals behind the audit universe and the audit plan – what is IA trying to achieve? The principal goal should be to reinforce the link between initial risk assessment and the risks covered in the planning and execution of individual audits. Other benefits can include greater comfort over the completeness and composition of the audit universe, increased efficiency through greater focus on only key risks, and greater clarity of roles and responsibilities within the audit function for individual risks or auditable entities.

**Potential Challenges?**

IA may face challenges in the following areas:
- **Change** – Revising an established risk assessment and planning methodology can be time-consuming, especially for larger functions and those that have an deeply-embedded and technology-enabled risk assessment and planning process.
- **Materiality** – Establishing the level/ size of auditable entities within the audit universe is critical – each should be large enough to be meaningful and to contain material risks but should be sufficiently granular to focus attention on key risks and to facilitate detailed operational planning (and to cover specific areas of focus such as regulated subsidiaries).
- **Transition** – Changes to the audit plan may require a transitional “catch-up” period to adjust from previous the previous coverage model to the new audit model.

**Why is it important?**

**How can IA use it?**

**Potential Challenges?**
At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As the largest global professional services and consulting network, with approximately 263,900 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients. In Ireland, Deloitte has nearly 3,000 people providing audit, tax, consulting, and corporate finance services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience and insight to collaborate with clients so they can move forward with confidence. 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 Ireland 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 Ireland LLP is a limited liability partnership registered in Northern Ireland with registered number NC1499 and its registered office at 19 Bedford Street, Belfast BT2 7EJ, Northern Ireland.

Deloitte Ireland LLP is the Ireland 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 Ireland LLP. All rights reserved.