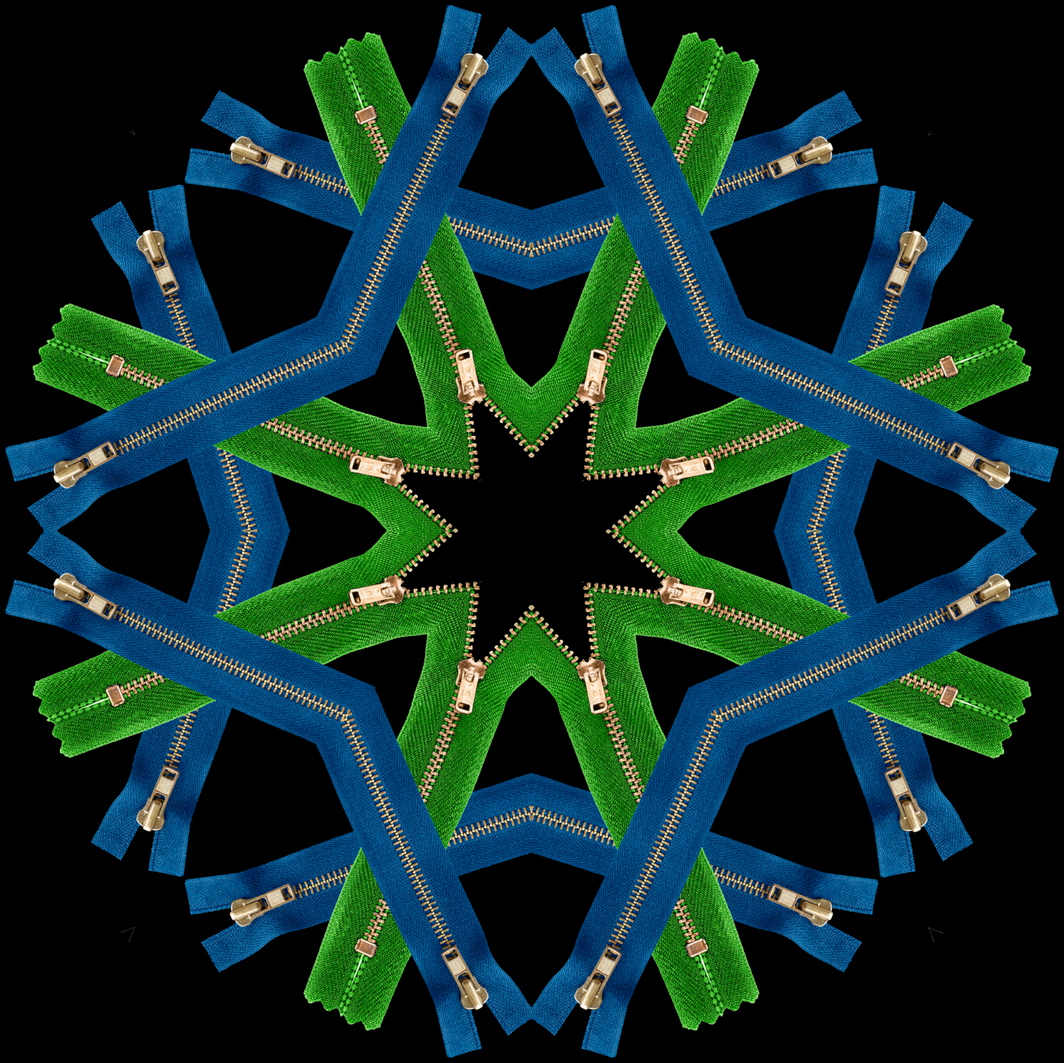
Deloitte.



Internal Audit Insights 2019

High-impact areas of focus

Operational Risk ●

Deloitte's 2018 Global Chief Audit Executive survey found that Internal Audit groups having the most impact and influence in their organizations also tend to be the most innovative.[1] Not content with doing the same things in the same ways, they learn how to deliver the assurance, advice, and risk anticipation that stakeholders need, when they need it, and they use whatever new methods and technologies they need to do that. If you think about it, this is the only way for Internal Audit to fulfill its mission and remain relevant as the organization evolves.

So, we've taken innovation as the theme of our 2019 edition of *Internal Audit Insights: High-impact areas of focus.* Look to these areas and suggested steps as you consider your internal audit activities for the year ahead. And bear in mind that Internal Audit groups around the world across all industries are already using these ways of increasing their organizational impact and influence, and the value they deliver to their stakeholders.

[1] *The innovation imperative: Forging Internal Audit's path to greater impact and influence—Deloitte's 2018 Global Chief Audit Executive survey report,* Deloitte, 2018 <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ra-cae-survey-2018.pdf>

Table of contents

Agile Internal Audit

Innovative Internal Audit groups have been actively adopting agile methods, with benefits that can be summed up in three words—better, faster, happier.[2] Better because audit results are more linked to business risks and relevant to stakeholder needs. Faster because internal auditors work with stakeholders in a collaborative, focused, iterative manner to quickly identify what they need—and don't need—to do. Happier because they are working as a team with autonomy to determine how to get the work done and are allowed to focus on the task at hand. Agile directs teams to higher risk areas and higher value work, and helps the function to attract, develop, and retain talent. Internal auditors use more of their capabilities and feel more engaged, because they are. As a result, Internal Audit teams who experience agile almost never want to revert to traditional methods. However, adapting agile methods to Internal Audit work presents predictable hurdles. In assisting Internal Audit groups on their agile journeys, we have learned that pilot projects are relatively easy, but achieving transformation is more challenging—yet clearly achievable.

Steps to consider: Agile calls for no special technology, only a willingness to work in a different way. This means not only learning new ways of working together but also *unlearning* what we have been practicing for years. This is not just a change within Internal Audit; you also need to bring your key stakeholders on the journey. Carefully planned pilots are almost always successful, particularly when they include experienced agile coaches. Then, you will need to consider transformation, moving fast enough to capitalize on the momentum but deliberately enough for the organization to absorb and sustain the change. Specific areas of organizational change management to consider will include the physical space for your teams (to create more collaborative work areas), performance measurement and rewards (to assess the performance of teams as well as individuals), and your target organizational structure (to define new roles versus titles, and a flatter structure).

[2] *Becoming agile: A guide to elevating internal audit's performance and value –Part 1: Understanding agile internal audit, Deloitte, 2017* <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-advisory-agile-internal-audit-planning-performance-value.pdf>

Integrated assurance

Organizations' responses to risk events and regulatory mandates have often resulted in assurance activities that can be characterized as narrowly focused, redundant, costly, intrusive to the business, and unrelated to drivers of value and performance. Integrated assurance aims not only to rationalize assurance activities and achieve efficiencies; it also aims to direct assurance activities to where they will create the most value for the organization.[3] Yet organizations often have difficulty adopting, or even properly framing, integrated assurance. It should not be confused with combined assurance, which typically either rolls up existing reports or bogs down in ultimately futile mapping exercises. Integrated assurance aims to align assurance activities around the drivers of value in the organization and to create visibility into risks and the effectiveness of risk management, while boosting efficiency. Despite its many benefits, integrated assurance often faces barriers to adoption. Chief among these are an organization's tendency to misunderstand it, overestimate its complexity, underestimate its value, or cling to existing methods. However, any Internal Audit group seeking to increase its impact and influence while decreasing stakeholders' assurance fatigue should seriously consider integrated assurance.

Steps to consider: The essential lead-off question is: Are each of our assurance activities focused on what matters most? The answers will reveal the extent to which they are linked to strategic value and business objectives. That, in turn, will shed light on whether assurance is actually supporting the creation and preservation of value. To the extent that it is not, those activities should be redirected or stopped. The next question is, Which of the three lines of defense is conducting which assurance activities—and how well? This will reveal instances of over-assurance, assurance fatigue, inefficiency, and lack of coordination. Work then moves on to establishing a new organizing principle for assurance—the drivers of value. These are not necessarily obvious and, when they have not been clearly defined, it's natural that assurance activities become inefficient. But under a set of defined drivers of value, you can identify key risks to value and develop risk themes that enable you to organize assurance activities across the three lines, and ultimately develop more relevant assurance reports. In general, we see five benefits that support integrated assurance: better value for the investment in assurance, reduced burden on the organization, more reliable business outcomes, improved coverage on enterprise risks, and greater insights into business strategy and operations. Any of these constitutes a valid reason to consider moving toward integrated assurance.

[3] *Integrated risk assurance - Get a clearer understanding of the risks affecting business value,* Deloitte, 2018 <https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-integrated-risk-management-report-aoda-pov-en.pdf>

Evaluating culture

Culture supports business strategy and must be actively understood and managed. Risks to culture occur when there's misalignment between the organization's values and leaders' actions, employees' behavior, or organizational systems. Deloitte's global research shows that 86 percent of executives rate culture as very important or important and 82 percent see it as a potential competitive advantage.[4] Yet only 12 percent of organizations believe they are creating the right culture. Culture has also become key to success and performance, as well as a source of legal and reputation risks. Internal Audit can help management and the board drive the right culture, which is essential amid today's ongoing digitalization, intense media and regulatory scrutiny, and heightened oversight expectations. As the third line of defense, Internal Audit has a traditional assurance role to play in evaluating management's program for evaluating culture. Internal Audit can also play a very important role in assessing culture which yields important insights for stakeholders and can be invaluable in the planning and scoping of internal audit activities. Internal Audit can also act as a valued business partner in providing advice to management regarding its culture risk framework.

Steps to consider: Many companies have some processes for monitoring culture, such as employee engagement by HR, insider threat monitoring by security, and other second-line initiatives. But they also need an overall program for managing culture, based on a practical framework. Deloitte's framework encompasses employee engagement, behavior, and insider threats as well as management's efforts to build a positive culture and manage culture risk—and monitoring of market signals that reflect reputation. Internal Audit's advisory role can be crucial in the absence of, or in development of, a formal program for managing and evaluating culture. Internal Audit can provide guidance on steps that management and the board can take to develop a program or elements of one, including setting the tone at the top, sending the right cultural messages, and aligning incentives with values. Internal Audit can also provide assurance services by embedding an assessment of culture into all audit segments with the goal of assessing whether the culture is enabling the area to achieve organizational goals as well as the risks of a local culture breakdown. Many auditors find culture to be a theoretical concept as it is by its nature subjective. Yet the risks are real and can be quantified, and efforts to do so work particularly well over time.

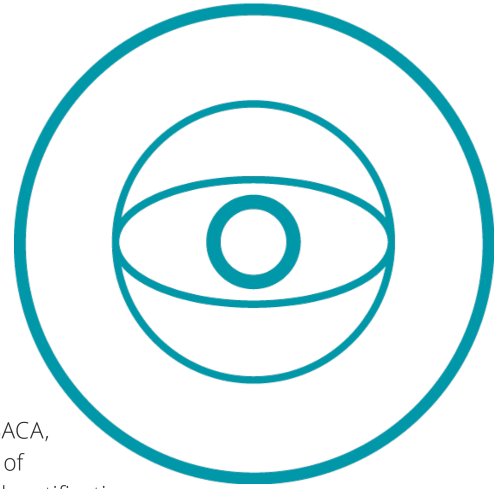
[4] *Auditing Culture: Assessing risk and providing internal audit assurance on the tangibles and intangibles of culture;* IIA presentation by Cary Oven, Partner, Deloitte US and Michael Schor, Partner, Deloitte US, May 15, 2018.

GDPR assurance and advice

The European Union's (EU) General Data Protection Regulation (GDPR) raises the bar for data privacy for any EU organization collecting or processing data on individuals, or non-EU organization doing business in the geography. GDPR is a risk-based regulation that does not prescribe how to protect customer data; rather, it sets expectations in terms of the data, based on its sensitivity and the potential risks. Instead of a uniform response, the regulator seeks customized approaches that protect the types of data the organization processes, geared to the risks posed to the data. So, the GDPR program must be geared to the sensitivity of the data and the potential impact of risks on the individual and the organization. The organization determines how to design and run the GDPR compliance program, and how to evidence that it has done so. Most of the work of readying the organization to comply with GDPR, which went into effect on May 25, 2018, has been driven by the data privacy function, working with other stakeholders to define how best to manage compliance. However, GDPR requirements make it impossible to build and manage compliance only in the privacy function and then hold it accountable. Internal Audit may have supported the organization's GDPR initiative by taking a risk-based approach to addressing requests and requirements and emphasizing key systems, as well as proving assurance and advice while developing Data Privacy Impact Assessment or third party data hand-off processes. The regulation involves the business in managing compliance.

Steps to consider: The compliance date has passed, however the GDPR journey has only begun. Similar to any other system of compliance, the GDPR compliance program is a continuous process not an end state in itself. GDPR-related audits should be incorporated into the annual risk assessment and internal audit planning processes, as undertaken for other regulatory compliance assurance activities. Internal Audit holds the responsibility to become educated on the privacy by design and mandated responses to data subjects of the regulation, or to leverage a third party with the required subject matter expertise in order to complete these audits. Internal Audit should perform activities to identify gaps in the program, recommend improvements, and provide updates to key stakeholders. Perform tests to determine the extent to which privacy by design has been achieved, and suggest ways it can be achieved more efficiently and effectively. All areas of the business must be accountable for protecting data, managing the risks, and evidencing that they are doing so—real opportunities to provide advisory services. Also, if a business intends to change its collection or handling of data, GDPR must be considered. Internal Audit can assist the organization with gauging the data needs, risks, and processes and procedures required for compliance, noting that this is as much a business and cultural matter as it is a technology and compliance matter. In addition, companies and internal auditors currently not affected by GDPR should consider it a wakeup call as we expect other jurisdictions around the world to consider and adopt similar legislation.

Cyber Internal Audit



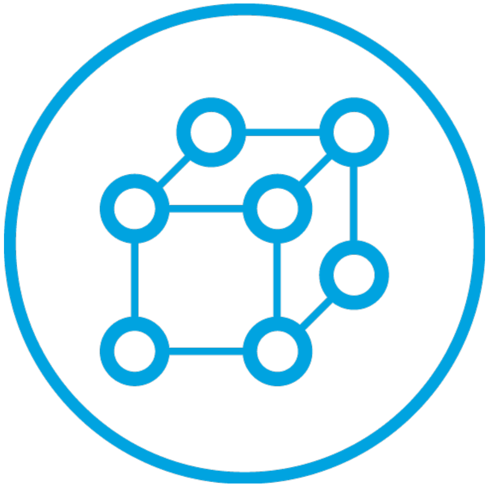
As the strategic importance, risks, and opportunities of cyber increases, Internal Audit needs to adapt if it is to continue to provide value to the organization. This entails a shift from IT and compliance-based approaches to a more risk-based approach to cyber. In making this shift, most Internal Audit groups find covering all cyber issues challenging, mainly due to lack of resources and depth of skills. As the gap between organizational needs and Internal Audit resources grows, the function can feel overwhelmed and unsure how to proceed. Despite this, Internal Audit cannot ignore cyber risk due to its criticality. It can also be challenging to communicate cyber risks in the language of the audience—the audit committee, the board, and senior executives. Yet decision makers need to understand the business risks and potential negative impacts of cyber. Responsibility for cyber security permeates all business units and functions, which means the related governance must span the organization and all three lines of defense must be involved—and their roles and responsibilities clarified.

Steps to consider: Start with a cyber security governance assessment because governance sets the entire framework and tone for the cyber security program and for operationalizing cyber security. Then drill down into specific areas of concern to the organization, while considering tools and measures already in place to address specific risks. These areas might include data protection, identity and access management, cloud security, and risk monitoring. A cyber risk assessment can then target those specific domains. Also, assess the maturity of the cyber risk program, risks associated with each domain, and audit relevance. Realize that while Internal Audit priorities may differ from those of the CIO or CISO, these groups must work together to ensure a holistic approach to addressing cyber risk. Develop an audit plan for the coming quarters and years based on the assessment and risk ranking of the domains, and specify the scope of each audit—for data protection, identity and access management, and so on. Assess the audit plan and scoping at least annually for continued relevance amid emerging issues. Each Internal Audit group must make the “buy, build, or rent” decision regarding capabilities. Organizations, such as ISACA, can be excellent sources of information, training, and certification. In addition, co-sourcing arrangements with external experts can enable Internal Audit to assess threats, prepare and execute audit plans, and acquire skills through knowledge transfer.

Workforce of the future

Two powerful trends are shaping the future of work: rapid adoption of automation and cognitive technologies, and the increasing use of alternative staffing models. These trends are raising questions as to who is doing the work (on or off balance sheet talent) and where the work is being performed (on-site or remotely). Both trends present new risks for organizations to address and new opportunities for Internal Audit. For their part, Internal Audit functions have been embracing alternative sourcing models for years, such as guest auditors, co-sourcing, rotational programs, and more recently crowdsourcing; indeed, about three-quarters of Internal Audit groups use some form of alternative sourcing model.[5] As the larger organization changes the ways in which it sources, engages, and compensates talent and as historical uses of talent evolve into automation opportunities, management must establish an appropriate governance model geared to addressing the risks inherent in these talent models and technologies. The days when most workers were full-time, on-site employees are past.

Steps to consider: Internal Audit must understand and review how the organization is engaging with all talent sources, from the policy, procedural, and physical workplace perspectives. Be prepared to alert management to the risks of mobile workers using their own or the organization's devices as well as regulatory and tax issues—and to provide assurance and advice accordingly. Maintaining a strong culture becomes more challenging with a dispersed workforce, so emphasize the need to define and manage culture; for example, culture assessments should perhaps include part-time employees and independent contractors. When developing the internal audit plan and specific audit programs, keep in mind areas with heightened risk in an extended workforce. These might include ways in which the company manages off-balance sheet workers' performance, intellectual property exposures, and compliance with company policies and procedures. Lastly, Internal Audit should periodically update its own automation methods and alternative talent models to keep pace with organizational change.



[5] *The innovation imperative: Forging Internal Audit's path to greater impact and influence, Deloitte's 2018 Global Chief Audit Executive research survey,* Deloitte, 2018 < https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ra-cae-survey-2018.pdf>

Continuous risk assessment

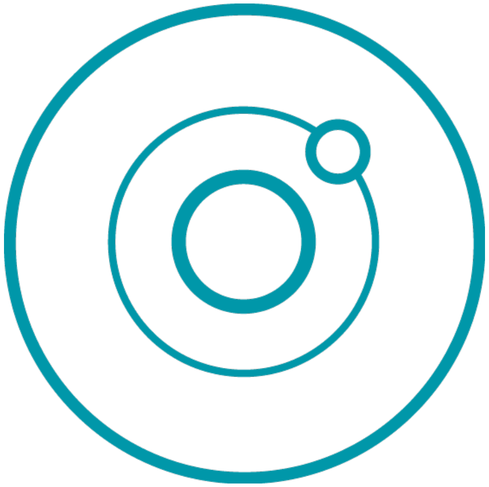
The traditional audit planning process is of limited value in assessing risks in today's disruptive environment. Continuous risk monitoring, assessment, and tracking can help Internal Audit to direct its resources to where they're most needed—a valuable departure from rotational audit plans. This approach can change the dynamic with stakeholders, enabling Internal Audit to more effectively anticipate risks and advise management. Leading functions are moving toward real-time risk monitoring via technology-enabled risk sensing, analytics, and visualization tools. Continuous risk assessment can leverage, but is not limited to, continuous monitoring of controls. It can begin with using automated mechanisms in an ERP system to ensure that controls are effective; however, continuous risk assessment ideally extends to ongoing monitoring and assessment of a broad range of risks across the enterprise, from external and internal factors. While continuous risk assessment usually sits in second-line functions, the output should definitely be considered by Internal Audit, which can also conduct its own continuous risk assessment. While Internal Audit should not absorb management's risk identification responsibilities, the function should have the tools needed to form a view and alert the organization to emerging risks.

Steps to consider: Use output from second-line risk assessments to develop more dynamic audit plans and work with second-line functions on what is, and should be, monitored and why, as well as on forms of monitoring and how output is used. Identify areas where you can develop or access KPIs, controls, and risk indicators critical to a business or function. Use output to maintain ongoing conversations with stakeholders. Recommend ongoing risk assessment around variables such as employee engagement and customer sentiment. Use continuous risk assessment to answer questions related both to assurance (Has management identified and addressed all risks?) and advisory work (How could management enhance the organization's approach to risk management and governance?). Aim for more frequent audits of higher risk areas and revisit the annual audit plan at least quarterly, based on the changing risk landscape and output from continuous risk assessment. Internal Audit can itself use risk sensing or output from second-line sensing and publicly available data to develop an outside-in view of risk. For example, a retailer's reviews of social media data found negative sentiment, much of which pointed to the logistics provider, indicating the need to enhance third-party controls and assurance. Such data can also pinpoint competitors' problems. All of this positions Internal Audit to advise the business on risks that may otherwise not even be known.

Automating assurance

Leading Internal Audit groups are aiming to automate core assurance to the greatest extent possible. This is primarily because automation leads to higher levels of assurance as larger populations of transactions can be tested and controls can be continuously audited. Automated assurance also enables movement of assurance-related activities to the second line—to compliance, cyber security, risk management, and similar functions—or to the first line, where the risks should be managed and where people can act on the results. Internal Audit would then adjust its procedures to provide the necessary independent assurance in these areas. There is a secondary benefit of automating assurance activities—reallocation of limited resources and potential cost savings. Many leading Internal Audit organizations are shifting focus from mainly assurance work to providing more advisory and anticipatory services to their organizations. Automating core assurance functions can free up time and capacity to support this shift.

Steps to consider: Consider creating cross-functional teams that can use pre-determined strategies to identify automation opportunities across the lines of defense. The quick wins are typically in core business processes (for both SOX controls and operational controls), such as accounts payable, travel and entertainment, payroll, and general ledger, and in IT. Automating these "low-hanging fruit" activities can build confidence in key stakeholders who are instrumental in the broader deployment of automated solutions. As key assurance activities are automated, an infrastructure must be established to ensure that these functions are operating as expected. A key component of this infrastructure is an operating model that addresses issue monitoring, escalation, and remediation. Management should implement strong governance over these activities, including testing automated solutions and instituting effective change management controls.



Applying robotic process automation and cognitive intelligence

Having already established analytics programs encompassing data science, visualization, and predictive analytics, many Internal Audit groups have started to advance toward robotic process automation (RPA) and cognitive intelligence (CI) tools (collectively RPA&CI) to drive efficiency, expand capacity, boost quality, and extend audit coverage. While fewer groups have applied machine learning and artificial intelligence (AI), all of these disruptive technologies are winning acceptance as innovators and early adopters continue to prove their value throughout the internal audit lifecycle. For example, some Internal Audit groups have piloted AI to identify emerging threats for risk assessments, utilized natural language generation for automated report writing, or leveraged automation to drive efficiencies in SOX testing.[6] Those finding the greatest success adopt a systematic approach that considers the operating model, infrastructure, and use cases across the audit lifecycle, and then develop and launch pilot projects. This approach enables Internal Audit to plan phases of adoption and to realize improved resource allocation, reduced costs, higher quality, and enhanced value.

Steps to consider: First, develop a well-defined vision and strategy for automation. This begins with identifying where and how automation technologies can be embedded into Internal Audit activities and reasons for doing so. This vision and strategy can span a single application or an entire transformation. Likely areas to automate include test steps within a single audit or process, a data extraction process to supply standardized information for use within multiple processes or audits, or operational activities such as hours tracking, board reporting, or managing certifications and CPE credits. Whatever the goal, a strategy should be articulated and communicated up front. Second, build an infrastructure to support deployment of automation capabilities. This will facilitate effective implementation, ongoing maintenance, and risk mitigation. Ensure that the operating and governance framework aligns to enterprise standards and leading practices within the organization. Some key infrastructure components include enhanced governance, change management processes, continuous testing and monitoring, exception handling, and proper training. Third, develop a target-state operating model to support and sustain automation. This model should be a natural extension of the existing operating model, but also consider ways in which automation will affect the interplay of people, processes, and technology and call for changes in each of those components.

[6] *Adopting automation in internal audit: Using robotic process automation and cognitive intelligence to fortify the third line of defense,* Deloitte, 2018 <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/adopting-robotic-process-automation-in-internal-audit.pdf>

Auditing the risks of disruptive technologies

Driven by the need to create value and drive efficiencies, organizations continue their rapid adoption of disruptive technologies, such as robotic process automation and cognitive intelligence. While adoption, both in the business and in Internal Audit, is spreading fastest in financial services,[7] innovative organizations across all industries are using these technologies, or at least considering them. Yet neither the organization nor Internal Audit is always prepared for the new risks, which can be easily overlooked or misinterpreted when enthusiasm drives rapid adoption. Internal Audit must understand the risks of these technologies in the organization, advise management on those risks, and provide assurance that they are being adequately addressed. For example, while bots—automated technology applications driven by rules-based algorithms—can do repetitive tasks at much faster rates than humans, they can also proliferate errors at much faster rates. In addition, as machines "learn" a process they may also learn to discriminate against certain classes or ethnicities of people, for example in loan approval or customer service processes, generating unexpected effects, unanticipated consequences, and unusual risks.

Steps to consider: Internal Audit should balance their assure, advise, and anticipate responsibilities in this area. In providing assurance, get involved early as the organization adopts disruptive technologies and the second line of defense modernizes its approach to controls testing. This will help Internal Audit to provide assurance that isn't duplicative. Practical considerations for Internal Audit to add valuable assurance include having access to testing procedures and independently reviewing sampling test cases, results generated, and issues logged. Also, review the exception monitoring and handling process and provide assurance on the design and operating effectiveness of applications of the technologies. Encourage stakeholders to perform an annual recertification of the design and implementation of automation technologies. In advising management and other stakeholders, get involved in pre-implementation and provide input on the risks and the organization's ability to address them and on leading practices for driving performance and value. As an advisor, Internal Audit should also weigh in on documentation and the risk assessment process, and consider adopting the Agile Internal Audit framework. Internal Audit should focus on anticipating risks associated with these technologies by using data analytics and risk sensing tools to proactively identify emerging risks and by running crisis simulations to reveal potential lapses in the organization's ability to respond.

[7] *Auditing the risks of disruptive technologies: Keep the tempo, A forward look at Internal Audit in banking and securities,* Deloitte, 2017 <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-digitization-banking.pdf>

Take courage

At this point, the main impediments to Internal Audit making more rapid progress through innovation are limitations born of legacy mindsets. Chief Audit Executives, other Internal Audit leaders, senior management and audit committees must work to change mindsets in their functions and organizations—and, often, within themselves. The evolving nature of Internal Audit work lends itself to new methods enabled by new technologies and new ways of working with stakeholders. Yet too many Internal Audit groups and leaders are mired in traditional roles and relationships. That can create resistance to new terms, tools, and approaches. It takes commitment and courage to pursue innovation. That commitment must originate with Internal Audit leaders, who must then develop the courage to initiate innovative changes, within themselves and within their Internal Audit groups.

Global Internal Audit Leadership

Peter Astley
Global Internal Audit Leader
Internal Audit Leader, EMEA
pastley@deloitte.co.uk
+44 20 7303 5264

Kristopher Wentzel
Internal Audit Leader, Americas
kwentzel@deloitte.ca
+1 416 643 8796

Porus Doctor
Internal Audit Leader,
APAC
podoctor@deloitte.com
+91 22 6185 5030

Neil White
Internal Audit Analytics
Global Leader
nwhite@deloitte.com
+1 646 436 5822

Sandy Pundmann
US Internal Audit Leader
spundmann@deloitte.com
+1 312 486 3790

Sarah Adams
IT Internal Audit
Global Leader
saradams@deloitte.com
+1 713 982 3416

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500®companies. Learn how Deloitte's approximately 264,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.