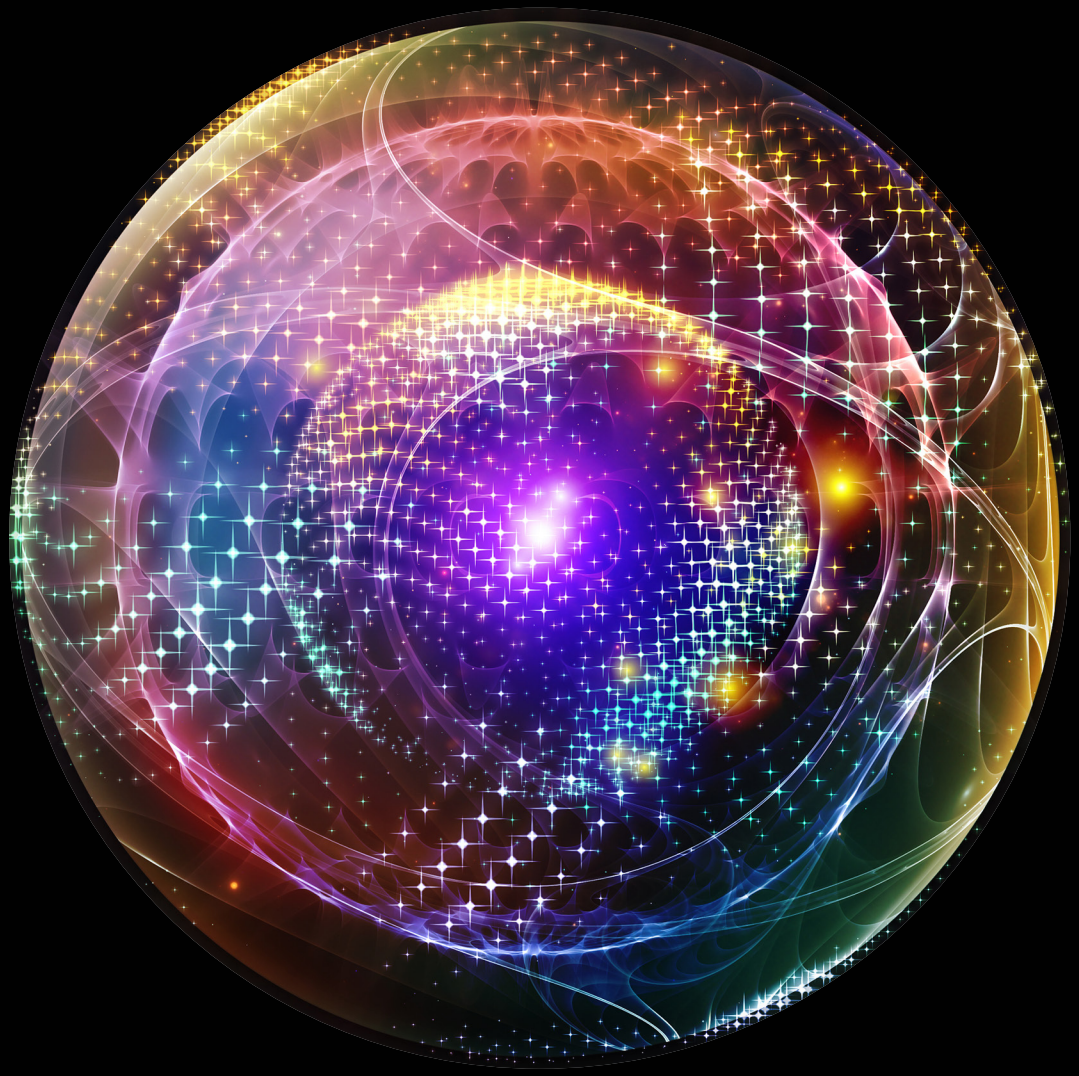
Deloitte.



Internal Audit Insights 2018

High-impact areas of focus

Deloitte research[1] and experience strongly indicates that stakeholders expect Internal Audit to be far more focused on the risks and issues of the future than on those of the past. This means shifting from auditing the past to advising on the future and to focusing on activities that present new and unfamiliar risks. Some of this will require new skills and talent models. Some demand new frameworks and interaction with new stakeholders. Failing to keep pace with the evolving organization and environment, however, puts at risk Internal Audit's role as a relevant, engaged, and strategic player within the organization.

For that reason, our 13 high-impact areas of focus for 2018 identify activities and risks that present opportunities for Internal Audit to make a positive impact. Whether by adopting new methods, such as automating core assurance and taking an Agile approach to internal auditing, or auditing new threats, such as digital risk, a focus on these areas as they relate to your organization will heighten Internal Audit's impact and influence. Moreover, these areas of focus will satisfy stakeholders who desperately need Internal Audit's objectivity, skills, and advice as they tackle new challenges.

1 *Evolution or irrelevance? Internal Audit at a crossroads, Deloitte's Global Chief Audit Executive Survey*, Deloitte, 2016 <http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Audit/gx-deloitte-audit-executive-survey-2016-print.pdf>

Table of contents

Robotic process automation and cognitive intelligence

Robotic process automation (RPA) is the use of software to perform rules-based tasks in a virtual environment by mimicking user actions to obtain the same or enhanced results. RPA also often taps multiple systems. In general, it makes repetitive manual activities more efficient and effective.

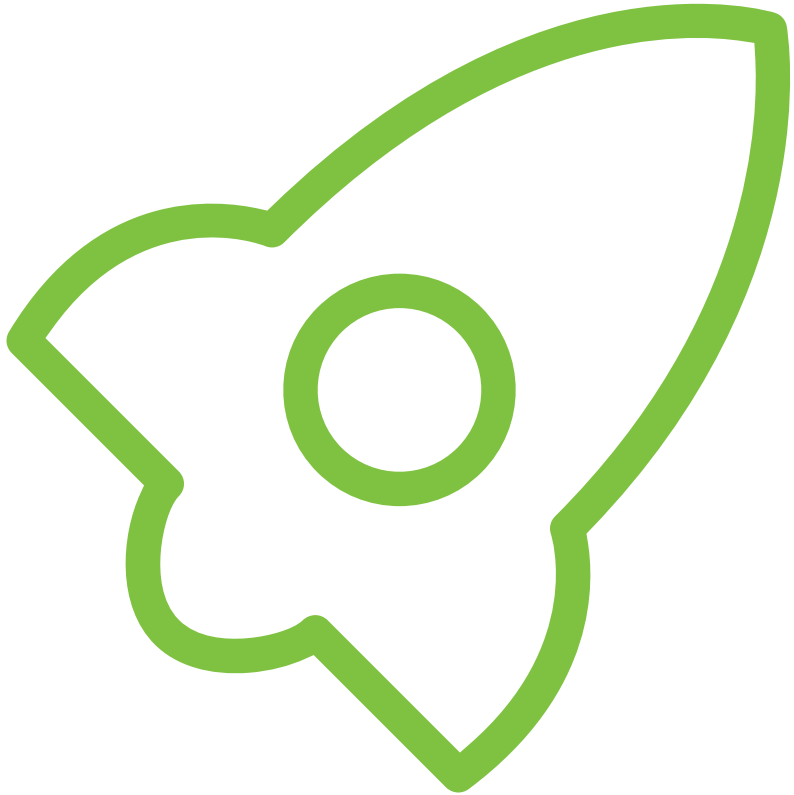
Cognitive intelligence (CI)—a step beyond RPA—includes natural language processing and generation, artificial intelligence, and machine learning. CI can extract concepts and relationships from data, "understand" their meaning, and learn from data patterns and prior experience.

Both RPA and CI are seeing adoption in the business and second-line functions, particularly in financial services and other data-intensive industries. In addition to many benefits, RPA and CI pose operational, financial, regulatory, organizational, and technology risk. Fortunately, the associated risks can generally be addressed by extending existing approaches.

Consider: As functions adopt RPA, CI, and similar technologies, Internal Audit should support them in identifying, assessing, and monitoring the risks that come along with these technologies. Doing so calls for an understanding of the new risks and the need for well-designed and properly implemented controls. It is also necessary to govern the use of these technologies in areas like integrity, data access, change protocols, and security.

Internal Audit plans should address the effects of RPA and CI on processes, management, and the organization. To provide sound assurance, Internal Audit should become involved early. Review documentation of testing procedures and any prior testing by sampling test cases documented, results generated, and issues logged. Ascertain that a framework and process exist to monitor "bots" in testing and production environments and to triage issues. Specifics include issue identification and resolution, bot change management, third-party risk management, and supervision and compliance. Opportunities also include advising on risk mitigation, leading practices, and automation strategies.

Finally, Internal Audit should consider using RPA to automate repetitive controls testing and internal reporting tasks.



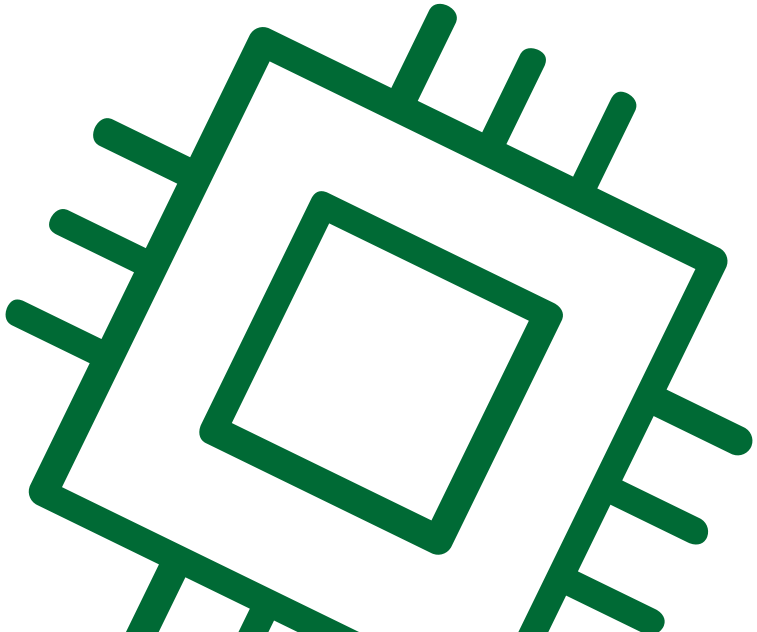
Back to contents

Auditing digital risk

Many companies have established digital transformation strategies; created siloed teams to develop apps, websites, and other digital channels; and embedded first- and second-line teams in these efforts. Yet Internal Audit generally lags in understanding the technologies, methods, and tools of digital initiatives. These include application-development methods, dev-ops teams (which combine development and operational professionals), and tools that automate controls. Many Internal Audit groups retain traditional mind-sets and methods, whereas digital innovators employ more agile and automated techniques. Apps and websites used in customer acquisition and interactions can raise a range of identity, privacy, and security risks. Meanwhile, many organizations lack risk frameworks and risk management capabilities equal to the complexities and challenges of those risks and those posed by external partners who provide these new technologies, channels, and services.

Consider: In audit planning, use key risk themes to assess risks of digital programs, processes, and products. Review the digital strategy and road map and decide where to focus, given the risk themes. Digital poses the usual cyber risks, plus new strategic, reputational, and third-party risks—in a fast-paced environment. Internal Audit should aim to understand the tools used to automate processes and controls, and then assess the integrity of the tools. Track digital project pipelines and get involved in early stages and selected iterations.

Focus on how related risk functions are involved, since they are closer to the delivery teams. Promulgate fit-for-purpose digital risk frameworks, methods, and oversight in the first and second lines. This includes providing the appropriate level of assurance over frameworks for managing external parties in digital initiatives. Integration of platforms blurs the boundary between organizations and third parties, so clarify the processes, data flows, and regulatory implications. Internal Audit groups are increasingly using cosourcing, upskilling, and dedicated teams to develop the focus and resources needed in this area.



Cyber security

In recent years, cyber security audits have often focused on regulatory compliance - areas such as data privacy, IT security, and business continuity. These audits have generally ascertained compliance with regulations and standards (such as ISO 27000). Compliance will continue to be high on most companies' radar, especially for US-listed organizations with the Securities and Exchange Commission making cyber security a priority in its National Exam Program, and with its recent creation of a Cyber Unit within its Enforcement Division. Also, new regulations are being developed daily in parallel with the new AICPA cybersecurity risk management examination. Companies should continue to focus on assurance while understanding that compliance with existing regulations hardly guarantees high, or even adequate, cyber risk management.

Organizations involved in several recent high-profile cyber incidents were likely in compliance with applicable cyber regulations. Indeed, while most cyber security activities focus on the IT department, corporate email, and the like, the highest risks now emanate from business teams using cloud-based systems, working with external developers, and using applications outside of IT proper. Much of this activity escapes the attention of the CIO, CISO, and Internal Audit, and presents serious risks. The challenge now is to identify a broader range of cyber risks before they occur.

Consider: Internal auditors accustomed to providing compliance-related assurance need new mind-sets and methods. Start by thinking broadly. For example, in a pharmaceutical company, Internal Audit may audit cyber risks related to privacy regulations and drug trials, but overlook those related to a small nuclear reactor used in radioisotopes (an actual situation). In Internal Audit planning, be proactive and cast a wide net. Look beyond rotational audit plans to seek out new initiatives, products, markets, contracts, and external parties. Then challenge management on risk identification, monitoring, and management in those areas.

Management should instill a culture of awareness of how decisions and behaviors magnify or minimize cyber risk. Encourage the use of war gaming to test the impact of cyber incidents on operations, infrastructure, data, finances, reputation, and recovery and to gauge responses and resilience—both of which should be regularly assessed.

Back to contents

Data privacy

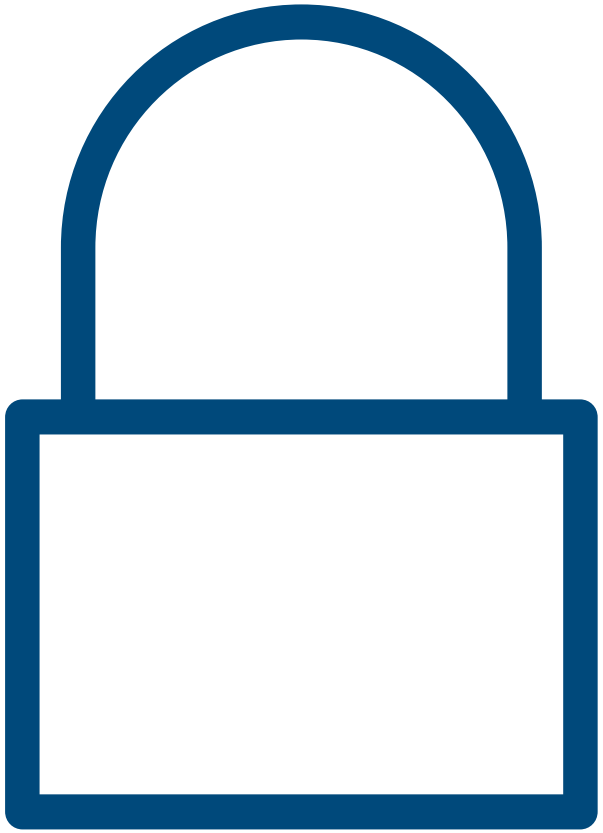
The EU General Data Protection Regulation (GDPR), effective May 25, 2018, affects all EU organizations that collect or process data on individuals, and non-EU organizations with EU operations. The GDPR greatly expands individuals' ability to determine which personal data is collected on them and how it is treated. For example, individuals will have to opt in to allow certain uses of their data. The GDPR establishes strong penalties for noncompliance, and calls for appointment of a data protection officer (DPO) and detailed documentation of roles, responsibilities, and processes related to the collection, use, and retention of data on individuals, including employees and independent contractors.

While most affected organizations have been working to fulfill these requirements, many are lagging in certain areas. Moreover, GDPR presents real opportunities for the organization given the marketing and analytical possibilities provided by enhanced data mapping and management. Internal Audit can help the organization to manage the increased risk posed by the new regulations and to realize the potential of an enhanced understanding of data that this work can create.

Consider: Organizations must establish clear accountabilities around data. Apart from appointing a DPO, this means clarifying who is responsible for addressing specific requirements, such as data requests, breach response, and data retention. Accountabilities and related processes must be documented in a framework that explains the execution of information requests, retention of data, and other procedures. Given the mandate to retain data only as long as it is needed, focus on the data life cycle and on retention and deletion policies.

The organization must also document what data is collected by which systems, where data is transferred and stored, and for what purposes. Help stakeholders to identify data repositories, data flows, and who uses and who can alter data. This data mapping positions the organization to respond to information inquires and manage individual consent.

In Internal Audit planning, take a risk-based approach to addressing requests and requirements and emphasize key systems, as defined by data volume, importance, and sensitivity. Ensure that a Data Privacy Impact Assessment (DPIA) is conducted for any new initiative involving individual data and pay close attention to hand-offs of data to any third parties.



Back to contents

Internal Audit analytics

Analytics is a perennial high-impact area for several reasons. First, beyond-the-basics analytics is the single most powerful booster of Internal Audit efficiency and effectiveness available. Second, the continuing digitalization of business generates huge quantities of data, which analytics can transform into valuable information and business insights. Third, the tools for analyzing and visualizing data are now simpler, cheaper, more available, and easier to use than ever. Finally, stakeholders' needs for higher-level assurance, insights, and risk anticipation have never been greater.

Yet Internal Audit's adoption of analytics has been relatively uneven and slow. Internal Audit is, admittedly, a function that can find changing the status quo and adapting to a new way of life difficult. An often-undiagnosed barrier to progress can be methodology: traditional audit approaches can choke innovation, restrict data gathering, and treat analytics as a bolt-on capability rather than an imperative.

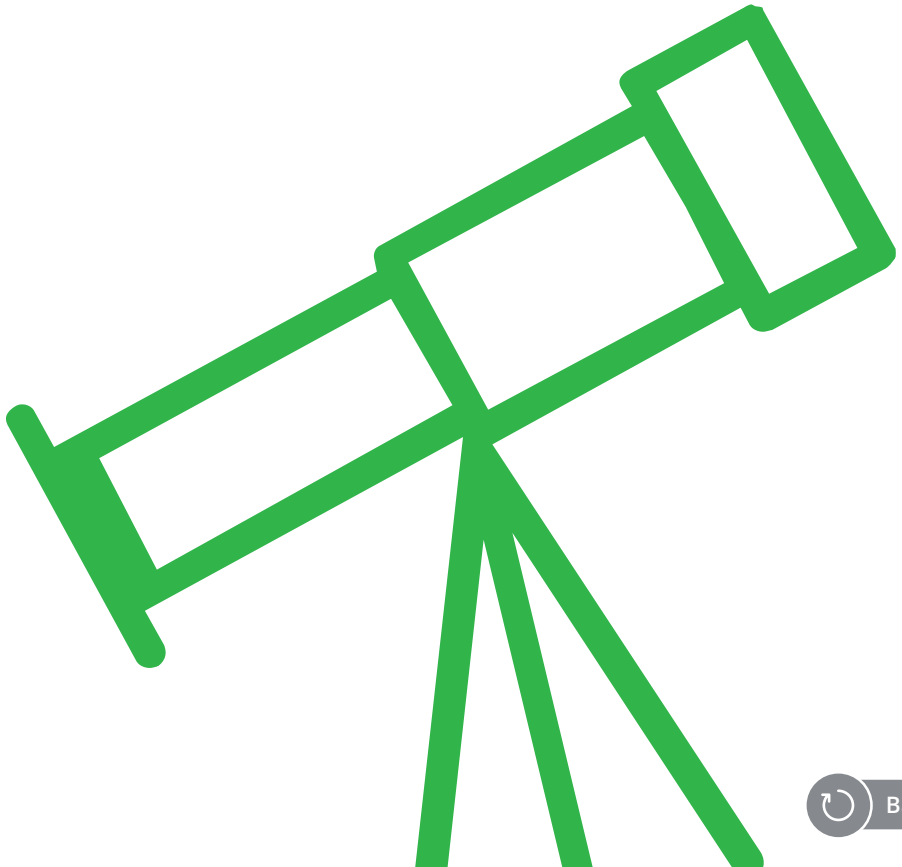
Consider: Analytics should be seen as integral to all of Internal Audit's planning, execution, and reporting, and should be reflected in methods and skills accordingly.

Rather than setting uninformed and fixed audit objectives, use data in the audit scoping stage to highlight unusual patterns, unexpected relationships, and changes in business conditions.

To prove the value of analytics, initiate pilot projects in areas where data is readily available, success is fairly certain, and results will drive value (such as reducing fraud, waste, or other policy breaches).

Start with a hypothesis and gather relevant data; for example, we expect a certain behavior or outcome here; is that supported by the data? Then iterate through the data to drive sampling and generate relevant insights (rather than lists of exceptions), and communicate using data visualization tools.

Also, consider using RPA and CI (as noted above) to automate repetitive tasks and accelerate reporting. Set your sights on "Digital IA,"[1] an integrated set of analytical capabilities geared to using and auditing advanced technologies.



[1] The untapped power of "Digital IA," Deloitte, 2017.

Back to contents

Automated core assurance

Leaders realize that risks associated with business as usual need to be managed even as they pursue new initiatives, and they are coming to expect ongoing assurance on these core activities. Internal Audit groups should be moving to provide this continuous comfort—ongoing assurance—on those core processes, controls, and activities to management and the board.

Automated assurance implies real-time reporting that flags actionable items. Such reporting enables rapid remediation, with the option of continued monitoring pending further notification. At this point, using a sampling approach when entire populations could be monitored, and reporting irrelevant details, is becoming a hallmark of a backward-looking Internal Audit function that cannot keep up with developments or provide assurance efficiently.

Technologies to facilitate automated assurance and real-time reporting include off-the-shelf tools, which hold some benefits, and custom solutions that can deliver automated assurance over most critical processes and controls.

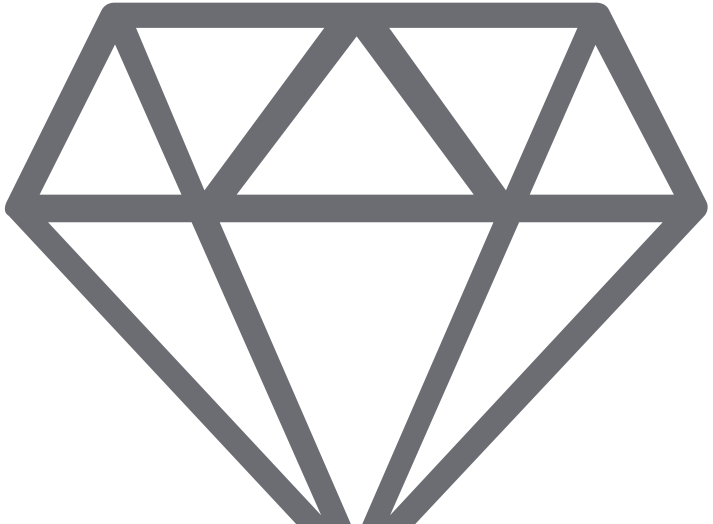
Consider: Automated assurance should gear comfort levels to the drivers of value and risks to those drivers. Begin by assessing core processes in the first line, their criticality, and the risks, and then prioritize accordingly.

Technology tools in existing systems provide many capabilities for automating core assurance, although the first and second lines rarely fully employ them. So promulgate use of these capabilities and the embedding of them into processes and systems. First- and second-line functions are often unaware of these capabilities, which vendors rarely emphasize.

Conversations with stakeholders can identify key risks and controls to monitor. Not everything should be automated, which raises scoping issues—whether to emphasize, for example, financial or operational risks and controls.

Become familiar with the possibilities of automation tools, and locate early and easy wins, typically found around key financial controls and reconciliations.

Overall, automation provides ample opportunities for easily-achieved cost savings and enhanced assurance simultaneously. Automating core assurance also enables Internal Audit to allocate resources to higher value areas and activities.



Cloud migration

Using cloud services can significantly alter an organization's risk profile, depending on the data involved, cloud service and model type, and strength of user and third-party controls. The term cloud includes software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). SaaS and PaaS provide cloud-based software and platforms, while IaaS provides infrastructure services. Cloud service models include private, public, or hybrid models (a mix of on-premise, private cloud, and public cloud services).

The risks for these service types depend mainly on access and data criticality. Given the varying levels of user control, security requirements will differ for each service and model type. The appropriate security controls will also depend on the data and processes involved.

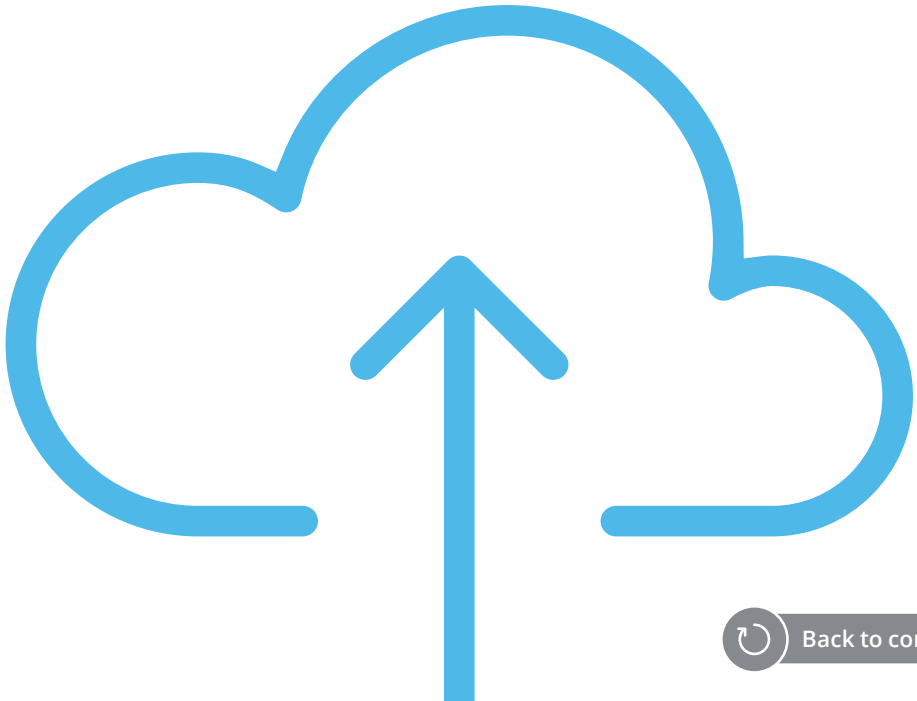
Regardless of service type, in a public cloud, you are entrusting data to a third party, and you can audit controls design and execution only up to a point, after which you rely on that party's assurance. Whatever assurance is obtained from the cloud provider or through procurement, you have limited visibility into the provider's environment.

Consider: Traditional audits of areas such as network configuration, asset protection, access control, logging and monitoring, and vulnerability assessment are still relevant for the cloud, but can differ. Cloud standards and guidelines from the SANS Institute, NIST, ISO, and the Cloud Security Alliance are useful, but each has its own focus, so you must tailor an approach that fits your organization's strategy, risk profile, cloud use-case(s), and cloud service. Assess the cloud environment holistically, and evaluate governance elements and shared responsibilities.

Often-misunderstood areas include inherited controls, incident response responsibilities, and disaster recovery capabilities. Consider obtaining cloud certification and tapping external expertise.

While cloud services are often positioned as cost savings, ensuring optimum value calls for choosing services carefully, monitoring and managing resources tightly, and deactivating unnecessary components promptly—all items to review.

Additional assurance can be gained by evaluating providers' locations, business model, customer base, history, and financial soundness. Ascertain that management understands which contractual responsibilities are the cloud service provider's, the organization's, or shared.



Back to contents

Third-party risk

Organizational leaders have long expected assurance around processes for vendor screening, selection, contracting, evaluation, payments, and termination. They have also expected audits geared to identifying potential cost savings and recovery.

Developments in technology and automation have introduced more advanced analytics capabilities and real-time assurance. Beyond this, however, leaders want—and need—a more holistic picture of third-party risks and their management.

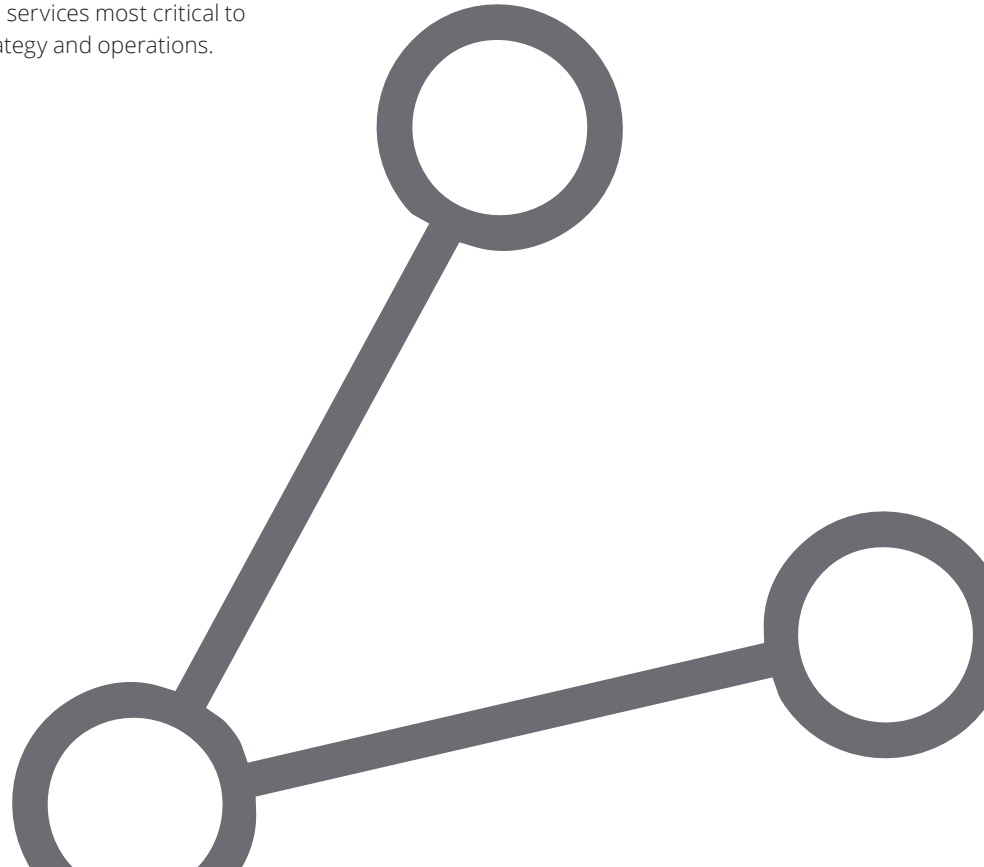
This calls for Internal Audit to understand the organization's entire approach to third-party relationships. As noted in a 2016 Deloitte global survey[2], the third-party risk universe includes the third-party ecosystem, third-party risk management and governance, and technology and methods for monitoring and managing relationships.

While cost savings and recovery remain key, excellence in extended enterprise risk management (EERM) is also a must. Why? Because third parties have become critical to most organizations while presenting myriad risks.

Consider: When planning your internal audits, start with an assessment of third-party contracts on the basis of spend and risk. Large, complex contracts will generally present more potential exposures and risks than contracts for goods purchased within the usual procurement process.

For vendor spend assurance, promote adoption of automated tools for analyzing spend and vendor performance, if they are not in place; if they are in place, provide assurance on their integrity and effectiveness. Some of these tools can apply RPA to data on deliveries, service levels, billings, and other metrics, making real-time third-party assurance a reality—and, soon, an expectation. These tools also free resources to work on other third-party, or extended enterprise, risks.

An overall EERM framework can be utilized to surface key areas of risk specifically embedded within the third-party ecosystem. Effective audit programs that assess the health of the ecosystem and its components will help to reduce risk over the sourcing of goods and services most critical to business strategy and operations.



[2] The threats are real: Third party governance and risk management, Deloitte global survey, 2016 < https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA_Third_Party_Governance_and_Risk_Management_Survey_RA_Dec16.pdf >

Back to contents

Culture risk

An organization's culture plays a major role in business performance and marketplace reputation. Culture can also create risk for the organization when there is misalignment between an organization's values and leaders' actions that shape culture, employee conduct and behaviors that sustain culture, or organizational systems that reinforce culture.

The spotlight often shines on culture risk issues only after an organizational crisis or incident, but a growing number of leaders are shifting to a proactive approach turning culture into a value enabler and driver of organizational performance. Such an approach requires gaining greater data-driven insight into the organization's culture, better understanding of employee engagement and employee behaviors, and looking for external market signals to get ahead of risk issues and drive necessary management actions.

As the third line of defense, internal audit plays a vital role in culture risk management—providing assurance and advising on culture as appropriate and validating mitigation activities. Auditing culture is not a matter of reviewing risk-related policies and procedures; it is a matter of developing an understanding of people's approach to managing risk as they do their jobs. In a strong culture, there is clear awareness and alignment of values, organizational processes, behavioral norms, internal and external statements, and reward systems to promote the right decisions, the right risk management behaviors, the right conduct—and, thus, the right culture.

Consider: Internal Audit should engage in broader organizational-level culture risk management efforts—providing assurance and advice on culture as appropriate and validating risk management activities. To do this, consider aspects of culture throughout the life cycle of an internal audit; for example, coordinate with culture stakeholders (e.g., human resources, risk, compliance, customer experience, security, technology) to understand potential areas of risk to optimize audit coverage, link cultural and employee engagement assessments into internal audit risk assessments, and incorporate culture metrics and control aspects into audit programs, including aspects of culture risk in audit reports.

Internal Audit can also perform assessments of the organization's culture risk management activities against leading practices to provide recommendations to management and perform additional procedures to assess culture risk management programs' effectiveness. A culture risk assessment can provide insight into intangible drivers of risk, controls effectiveness, compliance failures, and potential misconduct; it can also direct audit fieldwork and analysis to where it most matters. Such an assessment can include a range of activities, such as confidential interviews, focus groups, and data analytics geared to discovering where controls are working well, causing frustration, or failing to deliver intended results.

Assess how culture differs across locations and ascertain whether the risk management framework can identify and address outlier behavior.

Work to ensure that the second line of defense has visibility into culture at the first line, and ensure management and the Board understand that culture will always remain a work in progress.

Back to contents

Operational risk assurance

While functions such as cybersecurity and employee health and safety already provide assurance around operations, Internal Audit should conduct deeper assessments of operational efficiency, effectiveness, and risk management.

Operational audits focus mainly on nonfinancial assets and processes. They aim to determine how performance aligns with management's expectations, identify areas to be investigated, and propose enhancements. Meanwhile, many internal auditors are oriented more toward financial processes and performance.

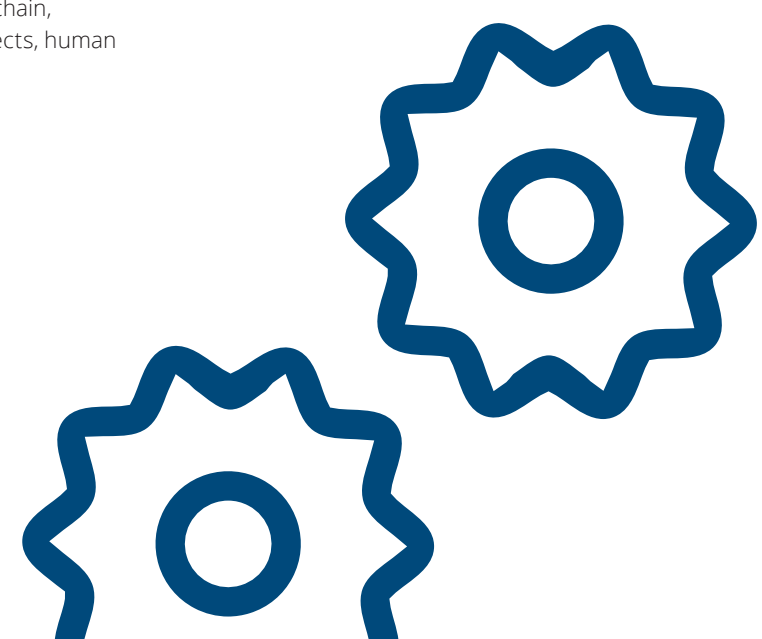
Even in capital-intensive industries like manufacturing and oil and gas, traditional audits may overlook basic operations. Internal Audit groups in such industries typically conduct useful company-level audits around the supply chain, cybersecurity, contract compliance, capital projects, human capital, and sustainability. However, field-level audits—of productivity, asset performance management, maintenance activities, operations technology and systems, regulatory compliance and safety, and asset integrity—may present more opportunity to add value.

Consider: Excellence in company-level operational internal audits should be table stakes. A clear focus on core operations demands an understanding of field-level operations as well as company-level operational risks. Start by ascertaining that second-line activities are providing proper assurance and, if they are not, help them to do so or provide the needed additional assurance.

When developing the Internal Audit plan, tie operational audit activities to organizational goals and strategies and to key operational risks posed to them. Using an operational risk lens, identify upcoming capital projects, significant maintenance, and similar initiatives. Look to the organization's risk assessment and the Enterprise Risk Management system, but also conduct robust conversations with key operating executives.

Apply analytics to process data to isolate trends, patterns, anomalies, and root causes, and enhance reports through visualization tools, added insights, and risk anticipation.

Consider whether external subject matter specialist resources may be needed, or whether knowledge can be accessed internally through guest auditor or rotation programs.



Back to contents

Crisis management

Crisis management provides the structure, leadership, decision-making, and communications to support the organization in managing a crisis situation. It encompasses business continuity, disaster recovery, cyber incident response, and financial market crisis response planning and execution. Most major organizations have basic business continuity plans and disaster recovery plans in place, particularly for IT, supply chains, and facilities.

Usually Internal Audit will, on a rotational basis, review those plans, provide assurance on related compliance, and conduct post-event reviews. However, the focus on continuity management has widened to include any event that could irreparably damage finances, operations, cyber capabilities, reputation, or other essential assets.

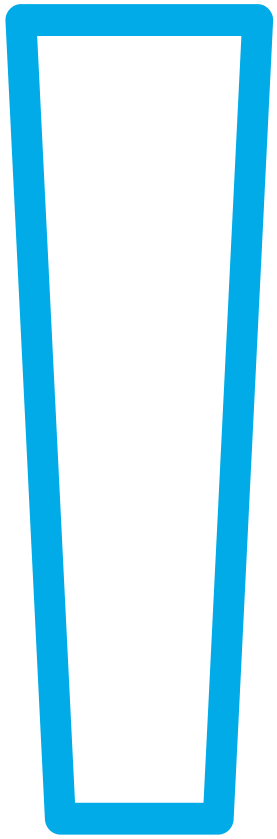
A crisis management plan provides a framework and contingency plans for senior executives should the need arise. Responsibility for crisis management sits with senior leaders, which means that Internal Audit is the logical—and perhaps only—source of assurance and advice.

Consider: An organization needs a crisis management program encompassing governance, processes, and risks. Governance organizes program ownership and the roles and responsibilities of security, legal, IT, Internal Audit, and other functions. Processes are needed to address crisis response, decision-making, recovery, communications, and contingency plans. Risks must be identified to enable scenario planning and response capability development through training and simulations. Aim to provide assurance and advice in each of those areas, and to anticipate events and promulgate best practices.

Consider whether leaders can answer the questions: What are you prepared for? How prepared are you? Ensure that simulations are regularly conducted and used to develop and test overall plans as well as playbooks for specific events.

Go beyond regulatory guidance and checklists and audit not just the existence of plans, but their likely effectiveness.

Also, consider industry-specific issues and evolving regulations, such as the EU's GDPR reporting requirements for breaches. Internal Audit may need to upskill or tap external sources to add value in this area, but doing so can save the entire enterprise.



Back to contents

Auditing agile

Organizations are increasingly adopting Agile methods of managing projects and processes. Companies and functions in technology and financial services lead the way, but others seeking increased speed, efficiency, and innovation are also coming on board. (These include Internal Audit functions—see below.) Desired outcomes include faster results, greater focus on user needs, more nimble decision-making, and reduced documentation.

Agile empowers people to make decisions and take calculated risks based on more targeted objectives delivered in shorter time frames, but these attributes can stress some control environments. A fast pace can introduce more frequent impacts or errors, but that can be offset by increased direct business ownership.

An intense focus on user needs can overlook other considerations, such as security or regulatory concerns, which can be mitigated by ensuring that standards are known and applied across Agile teams. Reduced documentation can make it hard to know what was done, by whom, when, and why, which calls for changes to governance and controls.

Internal Audit must be aware of Agile processes and projects in the organization, and of their potential issues and impacts.

Consider: Internal auditors should understand Agile methods and clarify responsibilities, schedules, resources, deliverables, and risks and controls—in discussion with Agile team leaders. A flatter structure may mean greater variability in the way outcomes are achieved, while less documentation may reduce visibility into risks. Controls may be given short shrift as the pace of work picks up. Therefore, assurance functions, including Internal Audit, should assess risks and controls during all phases, from ideation to pre-implementation.

Traditional audit plans may be less useful than early involvement and parallel visibility into the work. Internal Audit may best approach Agile by understanding what is to be delivered—what the Agile project or process aims to achieve, delivery risks, and proposed controls—and by understanding how it is being delivered, including management of risks and use of controls.

Proactive engagement by Internal Audit is key to establishing how Agile can be managed while maintaining balanced and sustainable levels of control.

Back to contents

Agile internal auditing

Principles and practices of Agile development are being applied to audits and projects by forward-thinking Internal Audit groups. Agile methods foster rapid response to emerging issues, closer collaboration with stakeholders, faster delivery cycles, and streamlined reporting[3]. Agile also changes the approach that internal auditors take to their work. For example, instead of auditing to a periodic schedule, internal audits are conducted when needed, particularly when the need is urgent. Rather than waiting until an internal audit is complete, auditors deliver weekly or even daily updates as findings or issues emerge. Rather than presenting unnecessary details, reports deliver insights on what matters most.

Agile has the power to revolutionize Internal Audit by making audits and reviews more relevant, risk-based, and real time.

Consider: First, be clear about what Agile is and what it is not. While it is a flexible methodology, simply calling a process Agile (or using terms such as Sprint, Scrum, and Backlog) does not make it so. Agile Internal Audit adapts Agile to Internal Audit needs. It is up to you to decide whether and where Agile might work in your function. Good candidates are areas with a need for more responsive and relevant reporting, high-stakes projects like IT installations or merger integrations, and where Internal Audit groups need to do more with less.

Learn about Agile from internal practitioners in software or systems development, or enlist external support. Understand that adopting Agile demands a change of mind-set as well as methods, and not every internal auditor can adapt. However, those who do usually find that they relish the pace of work, engagement with stakeholders, and enhanced effectiveness that result from Agile Internal Auditing.

[3] Becoming agile: A guide to elevating internal audit's performance and value, Deloitte, 2017 < https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-advisory-agile-internal-audit-part1-introduction-to-elevating-performance.pdf >

Back to contents

The year ahead

Clearly, the year ahead calls for a strong focus on all things digital. Of our 13 hot topics, more than half are aligned directly or closely with information technology and capabilities. Most Internal Audit groups should prioritize assurance and advisory work around uses of these technologies in the organization and ways of using them to enhance their own work. Just as customers are tending to outpace organizations in their uses of digital technologies, many stakeholders now outpace Internal Audit in similar ways.

Forward-thinking Internal Audit functions seek not only to provide assurance and advice, and to apply digital technologies to their own work, but also to anticipate issues and risks associated with those technologies. They anticipate stakeholders' potential moves to new technologies, strategies, and business models so they can ready themselves and the organization for those moves. In this way, they assist stakeholders in some of the most challenging areas they face—new areas where risks are emerging and where new value can be created—thus increasing their impact and influence in visible and valuable ways.

Global Internal Audit Leadership

Terry Hatherell
Global Internal Audit Leader
thatherell@deloitte.ca
+1 416 643 8434

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

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

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

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

Deloitte.