Deloitte.

Internal Audit Insights
High-impact areas of focus – 2020

Contents

We see Internal Audit functions around the world continuing to expand their impact and influence within their organizations, building on the advances reported in our most recent global survey of chief audit executives[1]. Prominent among these advances are adoption of new methods of working with stakeholders, increased use of automation in assurance, and delivery of advisory services as well as assurance around the most important risks to the organization.

Assure, advise, and anticipate form the core value proposition of Internal Audit 3.0[2]. Initiatives in these areas are essential not only for Internal Audit to fulfill its assurance mandate but to advise management and help anticipate risks in our rapidly evolving technology and risk environment. To continue to increase its value, Internal Audit must approach risk assessment, audit planning, sampling, and testing in new ways. Data is now too comprehensive, available, and valuable to go to waste. Moreover, the technologies to enable access to and analysis of that data are readily at hand and more cost effective to utilize.

Therefore, we have identified Internal Audit initiatives related to digitalization, as well as to sustainability, crisis management, EERM, and the three lines of defense, for you to consider in crafting Internal Audit plans and identifying projects for 2020. In particular, we urge you to venture beyond traditional audit planning and focus on the most important risks, of which a number are covered within these pages. For example, Agile Internal Auditing and dynamic risk assessment can help allocate assurance resources to areas where they will do the most good. By the same token, Internal Audit can, by playing its part as effectively as possible and by helping the other lines of defense to do the same, assist the entire organization in raising its risk management game to the levels that executives, audit committees, and other stakeholders now expect.

---

[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

[2] Internal Audit 3.0: The future of Internal Audit is now, Deloitte, 2018
https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Audit/gx-internal-audit-3.0-the-future-of-internal-audit-is-now.pdf

The Three Lines of Defense

Internal Audit is well positioned to lead the coordination of the end-to-end risk management process across all three lines of defense

Digitalization, new technologies, new business models, and a rapidly evolving risk landscape signal the need for organizations to update their approaches to risk management. For this challenge, the three lines of defense (LOD) governance model of risk management provides an excellent frame of reference. Levels of maturity in the risk-related activities in each line differ across organizations, but most companies recognize that the first line (the business) manages risk, the second line (supporting functions) oversees risk, and the third line (Internal Audit) assesses the effectiveness of the first two lines, as part of their activity.

Financial institutions, given their business and regulatory environments, tend to have well-defined roles and responsibilities across the three lines, while companies in other industries vary more widely. However, in all companies, the proliferation of risks and the increasing severity of risk events demands a rigorous approach to defining roles and responsibilities in the end-to-end risk management process. Internal Audit is ideally positioned to lead this approach and to advise the first and second lines regarding roles, responsibilities, priorities, and methods.

Defining and rationalizing risk management across the three lines enhances efficiency and effectiveness while reducing assurance fatigue in the business. It also provides opportunities for Internal Audit to enhance its impact and influence within the organization by exercising its advisory role. While some internal audit groups may see providing advisory services in this area as potentially compromising their independence, we consider it a critical part of Internal Audit's role to assist the first and second lines in improving their capabilities for the benefit of the wider organization.

Steps to consider

As the first and second lines adopt automated assurance, continuous monitoring, advanced analytics, and similar technologies, they need a model that identifies priorities, defines responsibilities, and minimizes duplication of effort. The three LOD model provides flexibility as well as rigor, which makes it a practical guide for identifying risk-related roles and responsibilities.

One starting point would be to assist first- and second-line functions in adopting assurance by design – building assurance into processes – or automating core assurance. Also, assist

them in understanding tools and methods for monitoring populations of transactions, accounts, and other data in real time or close to real time. Another starting point would be to map the organization's assurance efforts in order to locate redundancies and gaps and then to help address them, thus alleviating assurance fatigue while improving risk management. Neither of these approaches starts with the three LOD; instead, the model would come up organically within an automated assurance or assurance mapping initiative. The three LOD also offer a starting point for identifying where and how risks are being managed, and for assessing the risk governance and risk management framework in a clear context. This provides relief for first and second lines experiencing audit fatigue and provides a clearer executive-level view of the risk landscape.

If the organization's framework is unclear or weak, the three LOD model can be used to strengthen it by clarifying risk-related roles and responsibilities and placing them within a sound risk governance and risk management infrastructure. Internal Audit can not only assist the organization in this area, but lead efforts to clarify, rationalize, and enhance risk governance and management along these lines.

Assurance by design

Reducing assurance fatigue by leveraging automation to satisfy second and third lines of defense efforts and to bring greater visibility to compliance

Assurance by design aims to meet the second-line functions' compliance and risk management needs and the third line's assurance needs with the same control at the same time. Ideally the system of controls generates risk and noncompliance reports that notify those responsible for addressing the risk or remediating the compliance breach so they can take the appropriate steps. In this scenario, Internal Audit might audit the response to a rising risk, a risk event, or a control breach rather than audit the integrity and performance of the control; of course, traditional audits of controls remain part of Internal Audit's responsibility. The overall goal is to design-in and build-in mechanisms that reduce the amount of effort human beings have to contribute and to enable real-time assurance as well as dynamic risk assessment (also covered in this document).

While on the leading edge, assurance by design has become a reality in a number of organizations. For example, a company created a bot that connected the IT ticketing system with the production system, so that when an application went into production the bot would run an analytic that tested whether the change was in compliance with expectations, such as user acceptance testing and separation of responsibilities. This provided assurance by a mechanism that evaluated 100 percent of the population while avoiding manual sampling and time-consuming extraction of data. Other companies have used assurance by design for evaluating Sarbanes-Oxley compliance and IT governance. Use cases exist across the business, and they should consider the requirements of assurance as well as the actual need for controls.

Steps to consider

Internal Audit can assist management in identifying opportunities to enhance second- or first-line capabilities for providing assurance on processes or controls. During planning of new systems or changes to existing ones, Internal Audit should discuss each line's assurance needs and potential mechanisms for meeting those needs. Likely processes include those subject to regulatory reporting, in which a bot can pull 100 percent of transactions or accounts, prepare the data, conduct the initial analysis, identify the exceptions, and route them to the appropriate second-line people. This enables Internal Audit to review the process, tool, and results.

To add significant value, Internal Audit will need to learn about the workings and applications of robotic process automation (RPA) and commit to collaborating with the first and especially the second line of defense – tasks that are far less daunting than they may initially seem. Seek opportunities to consult on control mechanisms that generate greater efficiency, rather than more work. Suggest ways to eliminate reviews and tests, especially of controls that monitor relatively high-volume, low-risk processes. Look for situations that are prone to human error where robotics can deliver more consistency, and suggest that bot developers consider Internal Audit's needs as well as those of the first and second line. Aim to rationalize assurance by leading the conversation about who needs what information and how often, and how it can be delivered more efficiently through intelligent automation.

Benefits to stakeholders include better control, more real-time risk and compliance data, greater visibility into systems and processes, and reduced assurance fatigue.

Dynamic risk assessment

Leveraging data and technology to continuously monitor risks and trends leads to more precise audits and enhanced management of valuable Internal Audit resources

Dynamic risk assessment (also known as continuous risk assessment or continuous business monitoring) allows Internal Audit to deploy its resources in more precise and useful ways. Using data and technology to continuously monitor risks and trends across operations, processes, and functions, this capability enables Internal Audit to review key performance indicators (KPIs), key risk indicators (KRIs), and risk topics (such as customer or public sentiment analytics) across the business. This positions internal auditors to pinpoint areas for further review, such as units where receivables are increasing, customer service levels are decreasing, or inventories are flowing more slowly through the supply chain. It also positions them to ask far more useful questions while using their time and resources, and those of auditees, more effectively.

Dynamic risk assessment can transform annual audit planning by replacing manual, fragmented, often unrepeatable or gut-instinct approaches to risk assessment with rigorous, repeatable, standardized methods and tools to continuously monitor risk and adjust the audit plan accordingly. Internal Audit groups interested in adopting agile (also covered

in this document) benefit because they can more effectively identify anomalies, use them to prioritize audit activities, and run an audit sprint to better understand the issues and identify areas for deeper inquiry. Dynamic risk assessment goes beyond technology; in fact, fixating on the technology guarantees failure. Developing this capability requires the right people, processes, and technologies, all directed toward a shared vision.

Steps to consider

Start by reviewing the process by which you collect and use data for the annual risk assessment and audit plan. Explore ways of improving data capture, access, and analysis. For example, could you retain and analyze past interview notes and audit reports as well as risk scans across the business in electronic formats? That would enable the use of topic modelling and natural language processing tools to extract risk topics and identify the most consequential concerns of the enterprise. Quantitatively, could you be capturing KRIs aligned to risk domains? The answers will help strengthen the quantitative aspects of the annual risk assessment.

If you have the basics in place, consider KRIs that would deepen Internal Audit's understanding of risks in specific domains, such as financial, operational, or regulatory, and ways of monitoring trends within domains. Consider data analytics and visualizations that will portray risks and trends more vividly and immediately for stakeholders. Develop a vision of the desired target state, which may include automated reporting cycles and migration from annual risk assessments and audit reports to something closer to real time. Create a roadmap for moving from the current state to the target state from both an enterprise and an audit-planning perspective.

Also consider methodologies and processes that will be needed – or that will need to change – for the organization and Internal Audit to use new data-related tools. Realize that moving from a relatively rudimentary stage to true dynamic risk assessment is a three- or four-year initiative, but that the benefits start to accrue from the earliest efforts to adopt this approach.

Agile Internal Audit

Agile Internal Audit is here to stay and is becoming increasingly popular as Internal Audit functions shift their mindset to execute audits better, faster, and with happier teams and stakeholders.

Because the world continues to change at high velocity, Agile Internal Audit ("Agile IA") has become a perennial high-impact area of focus. One of the boldest moves that Internal Audit is making to address the changing risk landscape is to adopt agile methods, and we are increasingly seeing companies moving in this direction. Moreover, these experiences are adding to our collective knowledge of what does and doesn't work.

Agile clearly isn't going away, based on the number of internal audit and business functions adopting it. Organizations are changing too rapidly, needs for assurance are too urgent, and Agile IA has succeeded too often for that to be so. Committing to agile works. Internal audit groups that undertake the right pilot projects with the right expectations and the right resources succeed and then go on to replicate that success. There will be challenges and they can be overcome

Chief among the challenges is the need for audit teams below the chief audit executive (CAE) level to shift their mindsets and adopt new roles and responsibilities. Command-and-control leadership and rigid planning are anti-agile and undercut benefits such as the speed

and insights achieved by empowered internal audit teams. Moving from success on individual Agile IA projects to the whole portfolio of internal auditing tasks is another challenge.

Internal audit groups that address these challenges are rewarded with results that are better (more engaged teams and stakeholders make for deeper insights), faster (progress to value, insights, and reporting – and the ability to make course corrections as the situation dictates – are all accelerated), and happier (teams love working in this way, and stakeholders appreciate the transparency and collaboration).

Steps to consider

If you have not learned about Agile IA and launched a pilot, you should consider doing so.[3] Find out if other departments at your company have gone agile, and meet with them to understand their journey. IT departments in many companies are agile and often their training and coaching can be leveraged. Connect with CAEs of other organizations who have adopted Agile IA to see what their successes and challenges have been and to learn how they have adapted it.

If you have adopted Agile IA, step back and reflect on the changes you have made. Have your adjustments been more form than substance, such as adding a daily stand-up or working in sprints but not really empowering your teams? Some companies have changed their organizational hierarchy without really changing the way they work together. Mindset shift is not easy, and culture change takes years. Examine how you have adjusted your leadership style. Do you cling to command-and-control modes of management or do you practice servant leadership?

Change is not something that happens to everyone else. When internal audit leaders commit to adopting agile and then empower their people, they enable their teams to achieve more than they ever thought possible. And remember that Agile IA, like all applications of agile, should evolve continually to address new situations and meet the organization's ever-changing needs.

---

[3] 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

Sustainability assurance

Focusing Internal Audit on the range of business issues linked to governance and social responsibility can provide assurance around brand and reputation risk

Companies around the world now see sustainability as an imperative; it is a key concern for all stakeholders, from current and prospective employees, shareholders, investors, and regulators to the larger community and society. Boards who once viewed sustainability as a side-issue now see it as central, and they are exercising closer oversight. This reflects increasing regulatory requirements as well as the risks posed by extreme weather events, shareholder activism, the #MeToo movement, intensified media coverage, and heightened reputational exposure. Sustainability encompasses a broad range of business issues linked to governance and social responsibility, including climate change, executive compensation, tax policy and payment, health and safety, diversity and inclusion, resource consumption and efficiency, ethical procurement, product responsibility, and responsible investment.

The trend clearly has been toward increased attention on a wider range of sustainability issues from a broader base of stakeholders. This trend has driven higher priority on leadership agendas. Regulators worldwide have continued to focus on climate change, executive pay, diversity and inclusion, working conditions, and product content issues (such as conflict minerals and child labor). Many

jurisdictions have mandated or encouraged greater disclosure of sustainability practices and risks, with major stock exchanges doing the same in various geographies. While shareholder resolutions have seen varying degrees of success, they have prompted at least two major oil and gas companies to align their business strategies and performance goals with the Paris Agreement. Pressure from consumers – and the associated risks to brand and reputation – should also be considered.

Steps to consider

Internal Audit's priorities with respect to sustainability will depend on the organization's industry, operations, locations, regulatory environment, and the maturity of its sustainability management and reporting processes. Mature organizations will have KPIs to review and controls to test; less mature organizations may lack both. In the latter cases, Internal Audit can advise management of key risks and opportunities and ways of assessing and tracking them effectively. For more mature organizations, Internal Audit can assess how management has identified the key issues for regulators, investors, stock exchanges, NGOs, and employees.

Internal Audit can access sources such as the Global Reporting Initiative and the Sustainability Accounting Standards Board for reporting guidelines and standards to reference. For information on combined financial and nonfinancial reporting, Internal Audit may consult the International Integrated Reporting Council.

While specific areas of focus will vary by sector, many of the issues noted above will be within the scope of Internal Audit's work. How risks related to sustainability (for example, the management of the physical and transition risks associated with climate change) have been considered within the organization's risk management processes should be a key focus, as should the role of the board in understanding these risks and overseeing their management.

Internal Audit can also review internal data collection and analysis processes, and support continuous improvement in the quality of sustainability data. There is also a role for Internal Audit in assisting the first or second line in enhancing this information through review of their data governance policies and procedures and advising them in developing formal programs and sustainability analytics to improve, measure, and report on performance.

Crisis management

Internal Audit plays a role in the life cycle of a crisis, from having an opportunity to provide assurance prior to a crisis, advising during a crisis event, to preparing board reporting post-crisis

Deloitte's 2018 survey of more than 500 crisis, continuity, and risk management executives found that 80 percent of organizations have had to mobilize their crisis management teams at least once in the past two years[4]. In addition, 86 percent of organizations feel they are very or fairly mature in crisis preparedness, but most have not tested that belief. We define a crisis as an emergent event that, if not addressed, could threaten organizational reputation, viability, or existence; however, many crises falling below that threshold require management intervention. Each organization must define what constitutes a crisis, and Internal Audit should provide assurance and advisory services regarding crisis preparedness, response, and recovery capabilities.

Given generally heightened reputation risk and the susceptibility of global supply chains to risk events, boards are seeking greater assurance that the organization is fully prepared to respond to and recover from crises. While many internal audit groups have been auditing business continuity and resiliency, actual crisis management has been relatively overlooked. For standards to audit against, Internal Audit can look to the organization's crisis management policies as well as any applicable regulatory requirements or expectations.

Internal Audit can enable the board, the senior executive team, and specific functions to understand the maturity level of the organization's crisis management capabilities. Those capabilities should include a well-defined crisis management structure, with clear accountabilities and governance for decision making.

Steps to consider

Internal Audit can act as the eyes and ears of the board (particularly for non-executive directors) before, during, and after a crisis event. Before a crisis, provide assurance on crisis management capabilities, auditing against the organization's internal crisis management policy or standard and/or international standards such as PD CEN/TS 17091: 2018 (Guidance for Developing a Strategic Capability in Crisis Management) and/or specific regulatory directions or expectations. Observe crisis management exercises for their scope, including the extent of participation by the board, the executive team, and operational and technical teams, and for the relevance, realism, and complexity of scenarios. Also evaluate the maturity of the exercise, for example a single-team table-top discussion versus a multiteam dynamic simulation, and the outcomes, such as lessons learned and needed improvements.

During a crisis event, provide (perhaps within a crisis management office) resources to support logging and recording, information management, and situational awareness. Consider taking a "red-teaming role" to advise on, challenge, and review key decisions in real time and, when appropriate, support or conduct investigations into what went wrong, how and why, and who is accountable. On a cautionary note, avoid becoming so involved that Internal Audit's ability to conduct an objective post-event review is compromised.

Post-crisis, conduct a review to identify root cause, event impacts, and response effectiveness, and to prepare appropriate reporting to the board. This review and report can, for a significant event, serve as input for an external, independent review commissioned by the board. Also, audit progress against any post-event report recommendations and public commitments made by the organization as a result of the crisis.

---

[4] Deloitte 2018 Global Crisis Management Survey – Stronger, fitter, better: Crisis management for the resilient enterprise, Deloitte 2018. https://www2.deloitte.com/content/dam/insights/us/articles/GLOB305_Crisis-management-survey/DI_Crisis-Management-Survey.pdf

AI and RPA assurance

Risks exist throughout the intelligent automation life cycle and, in particular, Internal Audit plays an important role in assessing how these types of models reach a decision

Many organizations are ramping up artificial intelligence (AI) and RPA initiatives. In May, 2019, a Deloitte global survey of more than 500 executives in a range of industries found that 58 percent of organizations have started to use RPA and AI at some level.[5] Among these, 38 percent are piloting (1-10 automations), 12 per cent implementing (11-50), and eight per cent are automating at scale (51+). The latter percentage figure is twice that of 2018. Respondents viewed process fragmentation – differences in process management methods – as the greatest barrier to adoption of intelligent automation (36 percent) and IT readiness as the second greatest barrier (17 percent).

While organizations tend to start their intelligent automation journeys with RPA, those that combine RPA and AI realize greater benefits in data collection, processing, analysis, and actual decision making. RPA and AI applications often originate in operations, where people face the need to automate repetitive manual tasks to increase efficiencies, reduce human error, and redeploy talent. However, this can cause lack of oversight of these innovations.

Many organizations lack a talent strategy

around intelligent automation, either for managing the cultural impact or upskilling and redeploying current workers. In addition, many lack a cogent framework for managing the risks that intelligent automation can introduce to processes.

Steps to consider

Start by identifying as many of the models in the organization as possible and mapping all automation assets: what is being used, who is using it and how, and with what results. Then assess the risks around each model. Chief among these is that models may be trained on data sets that create biases or can acquire biased ways of making decisions or communicating as they work on new or expanded data sets. These stand apart from the financial, operational, regulatory, and other existing risks of the process. AI models and chatbots also present reputational risks.

Management needs a sound framework for managing these risks across the intelligent automation life cycle, which includes identifying use cases, developing solutions, maintaining the models, and managing and governing automations. Use cases should be chosen

carefully and identify points when human involvement is essential. Be sure that solutions are well-understood and that black-box thinking – in which the model is expected to "know what it is doing" – is avoided. Feedback into AI models must be continuously monitored to avoid inaccuracies and biases in the model and its output.

Internal Audit functions in need of RPA and AI expertise and experience typically access them through co-sourcing or outsourcing arrangements. The auditability of a model can be challenging, but how the model reaches a decision must be clarified. This means identifying the way it was trained, the steps it conducts, and why it reaches the decisions it does. Finally, these models should be used only for their intended purpose and someone must be identified as accountable for the risks posed by each model.

Cloud assurance

For all industries, the rapid migration of applications to the cloud raises security concerns for Internal Audit to address

Conscious of both cyber risk and third-party risk, executive teams, audit committees, and boards are increasingly seeking assurance around cloud services. The proliferation of organizations migrating from on-premise data centers to private/public/hybrid cloud models has substantially altered the risk profile of IT and the enterprise. Understanding the changes in risks and evaluating management's response to those changes pose a new challenge for Internal Audit.

The rapid adoption of cloud-enabled models for both organizational IT needs and strategic delivery of services through software as a service, platform as a service, or infrastructure as a service models has been anything but uniform. Within the same organization, different business units may have taken different cloud migration approaches, on varying timetables and using various methods. In addition to the inherent complexity of cloud migration, lack of uniform control processes introduces an additional layer of risk that must be assessed.

When an organization migrates to a public or hybrid cloud model, it becomes dependent upon the cloud providers' security and control processes. In essence, a partnership forms between the organization and the cloud provider, and vulnerabilities will likely result without the appropriate configurations and security "handshake" between the organization and the provider. This dependence on the cloud provider has given rise to the AICPA SOC2 report, which provides assurance to the organization and its auditors over the security and control processes at the cloud provider. Even with an unqualified SOC2 Type 2 report in place, there is no complete assurance that security is maintained, due to the nature of the partnership and the fact that such an assessment is only made at a point in time.

Like other complex and technical areas such as cyber security, cloud adoption, and migration presents technical risks that Internal Audit is being called upon to assess.

Steps to consider

Migrating to a cloud model introduces new and incremental risks, which Internal Audit must evaluate. Develop an understanding of the alignment between the organization's cloud strategy with the overall business and IT strategy.

As in many situations, governance is a good starting point for Internal Audit. Determine whether a cloud governance framework is in place and whether it is being followed. Also, develop an understanding of the processes being used to conduct cloud migration in a secure manner, while ensuring data integrity. Understand the processes that management has in place to consistently evaluate cloud risks, which will typically change over time with new initiatives and deployments, and the risk mitigation processes and procedures implemented by management.

Internal Audit functions vary widely in their cloud assurance skills, and while lack of technical skills can be a barrier, it's one which can be addressed through co-sourcing arrangements, training, and certification programs.

Extended enterprise risk management (EERM) assurance

Management of third parties continues to be a heightened area of risk for organizations as the extended enterprises becomes even more extended through the use of subcontractors

Global regulators are re-focusing enforcement attention on organizations' responses to regulations that affect the supply chain, such as anti-corruption, labor rights, product content, and similar legislation. Many of these regulations were put in place some time ago and companies issued frameworks and plans accordingly. Now we are at the point where regulators aim to assess how those frameworks and plans are being implemented. In this environment, companies must be acutely aware of the extended enterprise, more specifically the role that subcontractors play in the extended enterprise.

While most organizations have identified their primary third parties and vendors, many have not focused on subcontractors to those parties. What risks do they pose? What has the organization – or the third party – done to address those risks? As the organization diversifies its network of third-party providers, it becomes more likely that, at some point, some of those providers are using the same subcontractor. For example, if your organization uses numerous third parties, it's likely that more than one will be using one of the major cloud providers. That presents concentration risk.

Given the ever-increasing reliance on third parties in most business models, Internal Audit needs to champion the establishment of and assurance over third-party risk management programs. However, many internal audit functions lack the experience and skills to go beyond the basics of providing EERM assurance and therefore the ability to challenge the organization properly and deliver the requisite assurance around EERM.

Steps to consider

If you haven't done so, assess your organization's or a business unit's approach to EERM across the third-party life cycle – needs identification, vendor selection, contracting, onboarding, monitoring, and renewal or termination. Most organizations, through procurement and onboarding processes, do reasonably well with the first three or four steps. Information security, anti-corruption, and business continuity also tend to be areas of relative strength, particularly at the onboarding stage but less so in monitoring. So, look to monitoring practices in those areas.

However, most organizations tend to be less adept at risk assessment and, at renewal time, amending contracts. Further considerations

include labor rights, health and safety, and financial liability risks, which are often not well managed. Look at what has been designed and whether it is operating effectively across the third-party life cycle. How comprehensive have assessments and monitoring been? Where are areas of overkill (often, information security) and where might more resources be useful (as in labor rights)? Internal Audit or the business units can identify subcontractors by directly asking primary contractors who they use in their work for the organization. There are also specialized tools available that can identify transactions between organizations, indicate subcontractor relationships, and enable Internal Audit to assess concentration risk.

As a value add, Internal Audit can identify opportunities for cost recovery emanating from contract and performance reviews of third parties. Finally, any identified skills gaps can be addressed through co-sourcing arrangements, training, and recruitment.
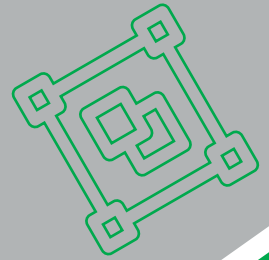
Payments technologies

Rapidly increasing risk for all industries due to new payment technologies requires a focus on third parties, cyber, and regulatory compliance

The trend towards new types of payments is acting as a catalyst for rapid change and disruption throughout financial services and fintech, with impacts increasingly felt in other industries. This is generating risks around cyber security, operational resilience, and regulatory matters, as well as significant opportunities. Getting to the right strategic choices and positioning in terms of payment methods, and selecting the right technologies and third-party providers can be challenging. For organizations that respond effectively, the opportunities include an enhanced customer experience based on the ability to transact instantly as well as richer payment data that enables value-added services. Many countries are also responding, upgrading their payment infrastructures with a focus on instant payments, open banking, and overlay services on top of payment systems. There is a concerted move toward a global common language for payments, using the ISO20022 messaging standard, which will enable transactions to carry richer data.

These developments are increasing pressure on banks to update legacy systems to adapt to and compete with new providers. Wider accessibility is being driven by open banking, which fosters a broader ecosystem of participants focused on tangential service offerings. These offerings range from increased customer convenience through spend-analysis dashboards to corporate-specific services to payments managed from treasury or ERP systems. These providers can initiate payments with customer consent and access data from bank accounts via application programming interfaces (APIs). Open banking benefits from developments in mobile, biometric, and wearable technology – all of which provide more access points to the payments infrastructure.

Steps to consider

Internal Audit functions in impacted organizations need to keep pace with the risks associated with this rapidly changing and more open, real-time, and data-rich payments ecosystem. Integral to this is an end-to-end understanding of the payment services deployed by your organization; this includes the use of any third-party providers, where gaining assurance over their operations can be a critical factor. Consider the level of change required for the organization and the associated technology, compliance, and security risks.

For payment service providers, cyber should be a focal point and include implementation of strong customer authentication in response to regulatory requirements and in compliance with the SWIFT Customer Security Programme (CSP), which mandates a formal independent assessment as of 2020 (which may be performed by Internal Audit). Review management of payment regulatory requirements, both in terms of horizon-scanning for requirements and the ways in which compliance is achieved. Payments-related APIs should be assessed for compliance with security, governance, and maintenance requirements. Identify and review payments-related projects to ensure they are being properly managed with respect to their goals, risks, governance, budget, and resources.

Organizations beyond the largest banks tend to have less mature payments technology, and Internal Audit may lack the resources to provide comprehensive assurance around payments. Therefore, consider briefing sessions and other sources of information (such as Deloitte's 2019 Payments trends report[6]) to learn more about this area and future developments, and to gauge your organization's maturity. Also, consider co-sourcing arrangements to access expertise and guidance related to assurance activities and effectively respond to developments in payments.

---

[6] InFocus Payments trends 2019, Deloitte, 2019.
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/usi-fsi-infocus-payments-trends-2019.pdf

The year ahead

The digitalization of business models, processes, and relationships presents challenges as well as opportunities, which often represent two sides of the same coin. For example, digitalized business models and processes, as well as the Internet and social media, cause risks to proliferate and increase in severity at a time when Internal Audit resources are remaining flat or close to flat. Yet digitalization and cognitive technologies enable new ways of identifying, monitoring, mitigating, and managing risks, including risks that go beyond those directly related to digitalization. Organizations will need the objective, independent perspectives, and assistance provided by Internal Audit to tap into those new ways of addressing risk as they pursue new opportunities.

This means that Internal Audit must act with courage to move beyond its traditional role, particularly if that role has confined the function mainly to providing assurance related to compliance. As the business pursues innovative ways to serve customers, enhance the supply chain, and achieve efficiency, Internal Audit, directly and in concert with the second-line functions, can and should provide guidance and guardrails around risks and opportunities. That occurs only when Internal Audit leaders take the initiative and work proactively with stakeholders to identify the risks and ways of managing the risks posed to the organization as it adopts new business models, technologies, processes, and methods of delivering on its mission.

Global Internal Audit Leadership

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

Sandy Pundmann
Global Internal Audit, Growth
spundmann@deloitte.com
+1 312 486 3790

Neil White
Global Internal Audit, Digital
nwhite@deloitte.com
+1 212 436 5822

Sarah Fedele
Global Internal Audit, Transformation
sarahfedele@deloitte.com
+1 713 982 3210

Deloitte.