Internal audit insights
High-impact areas of focus
2017
In any organisation, there are numerous areas where Internal Audit’s objectivity, perspective, and skills can assist stakeholders and provide valuable insight. Yet Deloitte’s 2016 Global Chief Audit Executive (CAE) survey\(^1\) revealed that only 28 percent of CAEs believe their functions have strong impact and influence within their organisations. This raises a question: Where can Internal Audit have the most positive impact and influence? Though the answers differ for each Internal Audit group, generally impact and influence increase when Internal Audit attends to areas of greatest risk, importance, and concern to key stakeholders. For Irish organisations, 2016 has seen many new and emerging risks which will be high on the agenda for stakeholders arising from political, governance and compliance developments which have arisen globally, domestically and from within the EU.

This year’s edition of our Internal Audit Insights series identifies twelve areas of high impact for Internal Audit in the year ahead. It also explains why these areas are important to stakeholders and how Internal Audit might approach the area in upcoming audit plans.

\(^1\) Evolution or irrelevance? Internal Audit at a crossroads, Deloitte’s Global Chief Audit Executive Survey, Deloitte, 2016
Strategic planning

In strategic planning, management lays the foundation for the success or failure of the organisation going forward. In the above-mentioned survey, 53 percent of CAEs said their Internal Audit functions plan to review their organisations’ strategic planning process in the next three years (up from 35 percent in the past three years). Such a review is critical in these times of disruption, if only to ensure that the process is keeping pace with marketplace changes, which will be of particular importance in the aftermath of Brexit and the outcome from the recent US elections and emerging risks. Also the board, which must approve the strategic plan, wants independent assurance that the designated planning process was undertaken and, if not, why departures from that process occurred. Note that Internal Audit’s task is not to challenge the strategy itself, but to review the integrity of the process and the models that generated the strategy, as well as the alternative scenarios, strategic options, and underlying assumptions.

Steps to consider: Internal Audit should review all key components of the strategic planning process: parties involved, data and intelligence, models, assumptions, scenarios, approvals, and communication and use of the plan. Potentially high impact components would include management’s key assumptions and sources of data, such as those related to market share and growth, sales forecasts, interest rates, input costs, product pricing, funding sources, and regulatory and compliance activities. Internal Audit should also review the governance over the related models, including model access, formula integrity, and data governance. In addition, Internal Audit can provide recommendations to strengthen the strategic planning process. These might include involving more parties, using additional data sources, enhancing model integrity, developing broader strategic options, communicating the plan more effectively, and monitoring performance more rigorously against objectives.
The governance landscape has changed and continues to evolve. Those charged with governance are now required to be more transparent and demonstrate ownership for an increasing number of compliance requirements. For Irish companies, the introduction of the Companies Act 2014, and the Directors’ Compliance Statement requirement, has given rise to additional responsibilities for directors of in-scope companies. Directors of such companies are now required to explicitly state their responsibility for securing material compliance with “relevant obligations” and for conducting a review of those requirements during the year.

The UK Corporate Governance Code, which Irish-listed organisations are required to comply with and which many other large corporates seek to comply with, has introduced updates. There is now increased reporting requirements in relation to the viability statement requirement. This statement is unavoidably linked to risk management within the organisation.

For the Irish public sector, the new Code of Practice for the Governance of State Bodies, was released in August 2016, coming into force 1 September 2017. This is proving to be significantly taxing on public sector stakeholders due to the depth of transparency required around a range of financial disclosures and the limited window in which to facilitate compliance.

**Steps to consider:** In many organisations, Internal Audit is well placed to support the delivery of the compliance and reporting requirements. To support the Directors’ Compliance Statement, Internal Audit needs to understand the extent of the “relevant obligations”. Internal Audit can then work to review existing arrangements in place to secure material compliance. Areas to consider when completing such a review include: the people and skills engaged in those compliance requirements; governance of arrangements of related processes; and the sophistication of technology and data supporting compliance. Areas for improvement in the formalisation of arrangements and structures may be identified and Internal Audit can provide best-practice guidance on those improvements.

To support the viability statement required by the UK Corporate Governance Code, Internal Audit, are well-placed to provide support to the board on the risks and uncertainties impacting the period of assessment. Internal Audit may also offer support in assessing how robust underlying management’s assumptions are.

As public sector organisations continue to meet the challenges of the new Code, many organisations are seeing a role for Internal Audit to help understand the challenges within existing systems for data capture and to provide assurance on the completeness and accuracy of data generated.
The term cyber goes beyond cyber security, recognising that the board’s cyber concerns extend well beyond cyber incidents and security risks. As the extent and impact of cyber threats has become clear over the past year or so, many boards have decided that incident and security reports from the chief information officer (CIO) or chief information security officer (CISO) are not enough. They want Internal Audit’s independent, objective, comprehensive review of cyber risks. Legislative, regulatory, and other entities are also driving this trend, with developments across the US and the EU adding more to Internal Audit agenda. In Europe, the Network Information Security (NIS) Directive and the General Data Protection Regulations (GDPR) are placing increasing pressure on management, introducing significant fines and penalties where organisations found to be non-compliant. Organisations impacted by SOX are facing the potential Cyber-security Systems and Risks Reporting Act which could expand requirements to additional risks. In addition to this, any organisation considering listing on the Irish or London Stock Exchange are required to consider and address elements of cyber risks as they impact the Financial Position and Prospects of the organisation. This reflects the recognition that cyber is critical to organisations and must be periodically and rigorously reviewed.

**Steps to consider:** Forward-thinking Internal Audit groups are firming up their plans and capabilities accordingly. They are monitoring the requirements that will apply to them, understanding the types of reviews and assurance stakeholders will seek, and developing the needed capabilities. Given the market scarcity of cyber auditing skills, many groups will look to co-sourcing to help them develop capabilities, or simply outsource cyber audits. Whatever the near-term resourcing plan, Internal Audit should prepare to conduct independent, objective reviews (rather than continuing to wait for things to gel) because the risks are too high and varied—extending to brand, relationship, and reputational risks—and stakeholders and those charged with governance want greater assurance now. Internal audit needs to define a cyber auditing approach that meets the needs of the organisation, industry, and stakeholders, including regulators, third-party partners, and external auditors. The audit plan should prioritise the processes and capabilities to be audited, and define methods and frequencies of related audits. With that done, the function can line up the resources—the people, skills, and tools—that will enable Internal Audit to execute those plans.
Internal audit insights | Third party management

Third party management

Management must address all risks associated with the third-party ecosystem, which includes vendors, sales channels, affiliates, research and development partners, licensees, and cloud and other IT services. Deloitte research\(^2\) shows that 87 percent of companies have faced a disruptive incident with third parties in the past two to three years, of which 28 percent faced major disruption and 11 percent a complete third-party failure. Meanwhile, 94 percent of respondents have low to moderate confidence in the tools and technology used to manage third-party risk, and 87 percent have similar confidence in the quality of the underlying risk management processes. Boards are asking CAEs about third-party risks, and regulators, customers, investors, and the media are expressing concerns as well, with potential changes to legislation underpinning contracts with UK third-parties, whether vendors, distributors or others, arising from Brexit.

**Steps to consider:** Internal Audit should begin with an assessment of management’s process for managing third-party relationships and risks across the relationship lifecycle. That lifecycle extends from screening and selection, to contracting and onboarding, to monitoring performance and contract compliance, to extending or ending the contract. Review the process at each of these points for elements such as selection and contracting procedures, due diligence and onboarding checklists, and performance and contract compliance metrics. A third-party risk management maturity framework can assist in helping management to decide what level of rigor to target in specific areas. In 2017, we expect Irish corporates which are engaged with UK third-parties to consider an analysis of their third-party ecosystem. Internal Audit is well placed to support this and to provide an independent view of this to boards.

Reviews of third-parties offer potentially high returns in cost savings and cash recovery, which go directly to the bottom line. However, Internal Audit may need specialised skills to assess certain relationships, such as those in advertising, cyber, or capital projects or software asset management (SAM).

---

Regulators and boards are focusing on risk culture because it largely determines decisions, conduct, and risk taking within an organisation. Risk culture affects not only day-to-day operational and financial areas but also decisions involving research and development (R&D), development of products and services, and market entry and exit. Excessive risk taking is not always the problem. Often, organisations take too little risk, for example in innovation and technology adoption. A risk culture of informed risk taking can enable performance. Therefore, gauging risk culture within organisations on a periodic basis is becoming more critical across all industries. For example, public sector organisations tend to be sensitive to reputational risk. In life sciences organisations, risks related to R&D, acquisitions, business models and regulatory compliance are of high concern. At senior levels as well as in day-to-day operations, motivations and behaviours around value creation and risk must be clarified and properly directed.

**Steps to consider:** First, the organisation must define risk culture so all parties have the same view. For example, Deloitte defines risk culture as a system of values and behaviours present throughout an organisation that shape day-to-day risk decisions. Deloitte identifies a framework with indicators of risk culture. Whatever the framework, indicators should be used to assess the existing risk culture and monitor desirable and undesirable changes. Internal Audit can review risk culture within standard operational and financial audits by adding interview questions, gathering data, and developing an informal review. Alternatively, Internal Audit can conduct a formal review of the risk culture management process, metrics, and outcomes. Since risk culture can vary across organisational areas, the results of risk culture reviews should be considered individually and in aggregate. Internal Audit can also make recommendations to strengthen an organisation’s risk culture through training, incentives, controls, and other mechanisms. Quarterly “pulse checks” (of four to five questions) can assess the ongoing risk culture. While less technically complex than some auditable areas, risk culture demands knowledge of how to measure culture, frame questions, and seek insights.

---

3 See Cultivating a Risk Intelligent Culture: Understand, measure, strengthen, and report, Deloitte, 2012

Strategic and emerging risks

With its enterprise-wide view and responsibility for providing risk assurance, Internal Audit has much to offer in the areas of strategic and emerging risks. Strategic risks relate mostly, but not exclusively, to external disruptions or factors that affect key strategic assumptions or that can impact the ability of the organisation to achieve strategic objectives. Emerging risks are early-stage developments that could impact an organisation’s ability to achieve strategic and business objectives. Audit Committees want assurance that the businesses and risk management are able to detect strategic and emerging threats posed by competitors’ moves, nascent technology, changing marketplace trends, and regulatory, political and economic developments. Yet strategic risk identification is often done only to support the annual strategic planning process, and formal risk sensing capabilities tend to be underdeveloped. In general, organisations tend to focus on near-term, well-known, less strategic risks that are more controllable. Also, risk management may lack enough of a forward-looking, outward-looking focus to identify emerging risks. Without an integrated view of strategic and emerging risks, the organisation is exposed.

Steps to consider: Internal Audit’s involvement can range from informal conversations to formal reviews. Questions might include: How are these risks being proactively and comprehensively identified? How are they being assessed and monitored? Are these risks being considered when setting strategy and monitoring performance? Who “owns” various strategic risks? How confident are we in our risk sensing capability? Who is responsible for tracking emerging risks and how is it being done? Are strategic risks being benchmarked externally? Most organisations need a formal, technologically enabled mechanism for detecting and monitoring emerging risks. Existing efforts to monitor competitors, social media, and customer sentiment are often siloed, limited, or both. Instead, the organisation needs a framework and a formal, integrated, well-supported process. Internal Audit should review the framework, processes, and mechanisms for identifying, assessing, and managing strategic and emerging risks. However, this area may be new to Internal Audit. A good start would be to conduct exploratory interviews to understand the strategic and emerging risks the organisation faces and then incorporate reviews of them into audit plans.
Analytics can boost efficiency and effectiveness in a range of Internal Audit activities. Dynamic audit planning enables Internal Audit to plan based on evolving risks rather than on those of the past. Analytics also enables Internal Audit to provide insight and foresight regarding risks and issues of interest to stakeholders, as well as the insight driven dynamic reporting. To increase stakeholder engagement, Internal Audit groups are using visualisation tools like heat maps, bubble charts, and interactive graphics to report audit results as well as insights gleaned from analytics. Predictive analytics enable Internal Audit to provide forward-looking analysis of likely control breakdowns and to play an advisory role before and during an initiative rather than only a post-mortem after cost overruns, missed deadlines, or poor outcomes occur.

**Steps to consider:** Embrace analytics and accept the related challenges that every Internal Audit group faces. Perfect data does not exist. Analytics has been embraced and embedded even in situations where Internal Audit departments view their organisation’s data as suboptimal. Try to home-grow talent, but co-sourcing can help you get beyond basic analysis to more advanced analytic techniques and data visualisation. Train technically-inclined internal auditors in analytics tools, then hire data specialists only as needed. Use database applications and data aggregation tools to develop useful data sets and ways of identifying relationships and risks. For example, based on three years of data, a consumer bank predicted potential specific control weaknesses and noncompliance events at specific branches. Finally, analytics can be applied to a whole range of issues. Key examples include employee absenteeism, procurement fraud, culture change, conduct risk, and IT cost management, as well as execution risks related to capital projects, IT installations, organisational transformations, and product development initiatives.
Integrated risk assurance/
Combined assurance

Combined assurance has been gaining traction, but slowly, and the term integrated risk assurance may be preferable. Pursuing combined assurance can direct attention toward the goal of aggregating assurance reports from various sources, rather than that of generating an integrated picture of risk. While the desired result may be similar, integrated risk assurance may be the more useful approach from the planning, execution, and reporting perspectives. In audit planning, integrated risk assurance can generate more meaningful information and insights for stakeholders. In audit execution, it can improve co-ordination among the first and second lines of defense, and allocation of audit and risk management resources. In reporting, it can improve the quality of information, risk anticipation, and insights delivered to stakeholders. Integrated risk assurance enhances coordination of assurance activities and reports, across your three lines of defence (management, oversight functions and Internal Audit) thus serving the goals of combined assurance while generating an integrated view of risk and greater impact and influence for Internal Audit.

Steps to consider: Internal Audit’s position as third line of defence positions the function to develop and deliver integrated risk assurance. This means that audit plans should start with the business strategy, goals, and means of achieving them and the associated risks. Then, Internal Audit can—in collaboration with the business—develop several key hypotheses regarding risks and incorporate them into the audit plan. From a combined assurance standpoint, Internal Audit should ascertain where the first and second lines are already providing sufficient assurance, for example on health and safety, credit, or other risks. This can help in reallocating Internal Audit resources. At the reporting level, integrated risk assurance stems naturally from this approach because Internal Audit is focused on key risks rather than on aggregating assurance reports that may or may not achieve risk assurance goals. In this way, integrated risk assurance enables Internal Audit to generate more useful reports with the same or fewer resources.
Regulators, institutional investors, non-governmental organisations, and the media increasingly seek disclosure on sustainability risks that could materially affect the organisation and its performance. Those disclosures should be supported by sound processes, strong controls, and accurate data. In turn, Internal Audit should provide assurance to the board and management regarding the accuracy and integrity of public disclosures related to sustainability. Internal Audit should also provide assurance on the management of operational and regulatory risks as this will influence stakeholders’ evaluation of sustainability performance. Regulators and investors are increasingly focusing on nonfinancial data, which includes sustainability data, making this an area of high importance. Incomplete or inaccurate data may lead to fines, penalties, and reduced investor interest, among other consequences.

**Steps to consider:** Internal Audit should cover at least one area of sustainability per year, such as employee or contractor health and safety, carbon emissions, operations management systems, or community engagement, selected in light of the materiality of the issue. Mature sustainability environments have formal processes and reports to review. In less mature environments, Internal Audit should advise management on enhancements. Internal Audit can also go beyond compliance to ask: What strategic risks might sustainability present? How can sustainability drive efficiencies? If Internal Audit lacks requisite skills, then co-sourcing, outsourcing, hiring, and training can provide them. When Internal Audit is new to an area, providing advisory services on processes, data capture and reporting, and rationales for these efforts can be a good start.
Driven by stakeholder demand, Internal Audit is adopting new modes of reporting that simplify the user experience while generating data-driven insights. The resulting reports are more forward-looking and insightful, briefer and more layered, more visual and dynamic. Forward-looking, insightful reports focus on the risks and issues of most concern to stakeholders. Briefer, more layered reporting avoids dense and complex reports that stakeholders don’t read, but allows for drill-down into data and issues for interested individuals. More visual and dynamic reporting meets stakeholders’ need for at-a-glance insights in a changing landscape. Dashboards and infographics let stakeholders access reports on their devices—a rising trend—while interactive tools enable drill-down and increased user engagement. The larger and more complex the organisation and the busier its stakeholders, the faster Internal Audit needs to adopt these new ways of reporting.

**Steps to consider:** Commit to delivering short, insightful, layered reports with summaries rather than narratives. Tell stakeholders what they need to know, why they need to know it, and what they should do about it. Use visualisation tools and dashboards to leverage the results of whatever analytics you are using. Insights multiply and deepen with advanced analyses based on aggregated data sets, combined internal and external data, and predictive techniques. Even without advanced analytics, Internal Audit can still use heat maps, bubble charts, and infographics to convey findings and insights. Consider leveraging internal or permissible web-based resources for help in creating infographics. Get training if needed. Dashboards enable dynamic, timely, prioritised reporting on a process, project, or risk area—with readers controlling the level of detail. For example, an Internal Audit group developed a SOX reporting tool that identified areas as within bounds, of concern, or potentially material. New modes of reporting are essential to increasing Internal Audit’s impact and influence.
Media audits

Organisations often rely on advertising agencies to plan, execute, and self-report their advertising costs and performance. Recent changes in the advertising landscape have led to agency transparency and advertising performance concerns. There is a risk surrounding nontransparent media buying practices by agencies that can lead to higher advertising costs. Examples include agencies not passing discounts and rebates through to the advertiser and purchasing media from suppliers it owns or other related entities as principal (vs. agent), which removes advertisers’ protections against conflicts of interest. Other concerns include digital ads being viewed by robots rather than humans and ads appearing on inappropriate digital venues. Some agency agreements do not provide advertisers with adequate media transaction details or the ability to trace funds from plan to placement.

Steps to consider: As for all vendors, Internal Audit should review the process for selecting, managing, and monitoring the organisation’s advertising agencies, especially when advertising is a large part of overall expenses. However, the current advertising landscape presents complexities that often make this area challenging for Internal Audit groups without specialised expertise. To get started, Internal Audit might review advertising expenses and reconcile billings with contract provisions and agency reports. Internal Audit may recommend advertising procurement procedures, for example for selecting and contracting, and new methods of monitoring advertising costs and performance. Agency contracts should clearly state costs and fees, treatment of discounts, and performance metrics—and contain a right-to-audit clause. Useful monitoring calls for analytics and data visualisations and a review to verify service levels per the agreement. Initial questions for audit to ask internally would be: Did we get what we paid for? Was the pricing clear and fair? Were contractual requirements met? Again, this area presents complexities that may require specialised expertise.
Digitisation

Broadly, digitisation converts currencies, transactions, services, products, experiences, and relationships into virtual forms. Virtual forms are potentially more flexible, far-ranging, and profitable—and more challenging to audit. Digital products (books, movies), services (shopping, ebanking), and disruptive business models, such as ride-sharing or room-sharing applications, augment or replace existing ones. Payment mechanisms from financial and non-financial companies, and digital currencies enabled by blockchain, present issues for almost any company. Virtual reality is impacting design as well as video gaming. The Internet of things, which affects vehicles, heating and cooling systems, home appliances, to name a few, is coming onstream. Different applications present very different issues, risks, and opportunities, depending on the business, stakeholders, and vulnerabilities—and on the organisation’s digital maturity. All of this holds true even if your organisation is not digitalising. If competitors are digitalising and you aren’t, you may face diminished sales, profits, and market share such that not digitalising may be the major risk.

Steps to consider: Digitisation holds profound impacts, which Internal Audit must be aware of and help the organisation to address. At a minimum, Internal Audit should gauge the impact of internal or external digitisation on the organisation and its businesses and functions. Risks can be easily overlooked amid the enthusiasm with which management can embrace digitisation. Digitalising any aspect of a product, service, transaction, or relationship can transform the risks associated with its traditional form. Internal Audit should understand how digitisation fits management’s strategic vision and plans, conduct appropriate risk analyses and rankings, and define audit procedures to identify risk exposures and review management’s steps to address them. The point at which these steps devolve into actual audits will depend on the organisation and the Internal Audit function. Early efforts might include a facilitated audit, a review, actual sampling and testing, or advisory services. By increasing its awareness of and involvement in digitisation, and how robust the controls over the systems underpinning digitisation are. Internal Audit positions itself as forward-looking and as a source of strategic advice, and avoids the audit-planning-as-usual.
The year ahead

Not all of these areas will be high impact for your stakeholders and Internal Audit group. Nor can you realistically get up to full speed on more than a few (at most) in the coming year. In fact, the highest impact areas within your organisation may reside elsewhere. To locate those most relevant to your stakeholders, ask them, and then listen. Then take steps to develop or acquire the frameworks, skills, tools, and methods that will enable you to provide insights, assurance, and advice that they can use.
Internal Audit Leadership

Colm McDonnell  
Partner  
Risk Advisory  
cmcdonnell@deloitte.ie

David Kinsella  
Partner  
Risk Advisory  
davkinsella@deloitte.ie

Eileen Healy  
Partner  
Risk Advisory  
ehealy@deloitte.ie
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As one of the largest global professional services and consulting networks, with over 220,000 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients. In Ireland, Deloitte has over 2,000 people providing audit, tax, consulting, and corporate finance services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience, and insight to collaborate with clients so they can move forward with confidence.

This 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.

© 2016 Deloitte. All rights reserved