Deloitte.

Internal audit insights

High-impact areas of focus

2017

In any organization, 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 organizations. 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.

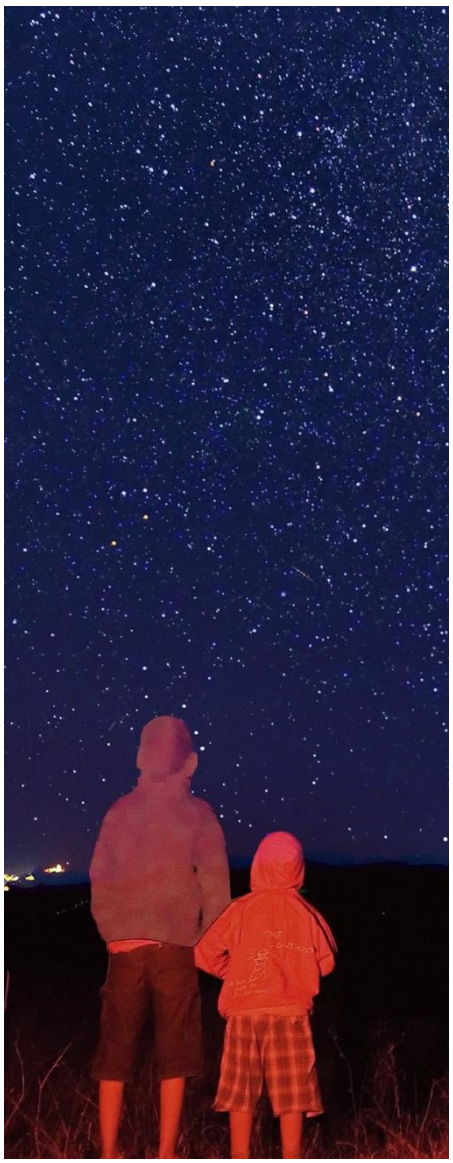
This year's edition of our Internal Audit Insights series identifies eleven areas of high impact for Internal Audit in the year ahead. It also explains why these areas are important to stakeholders and how Internal Audit might approach the area in upcoming audit plans.

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

Strategic planning

In strategic planning, management lays the foundation for the success or failure of the organization going forward. In the above-mentioned survey, 53 percent of CAEs said their Internal Audit functions plan to review their organizations' 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 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.

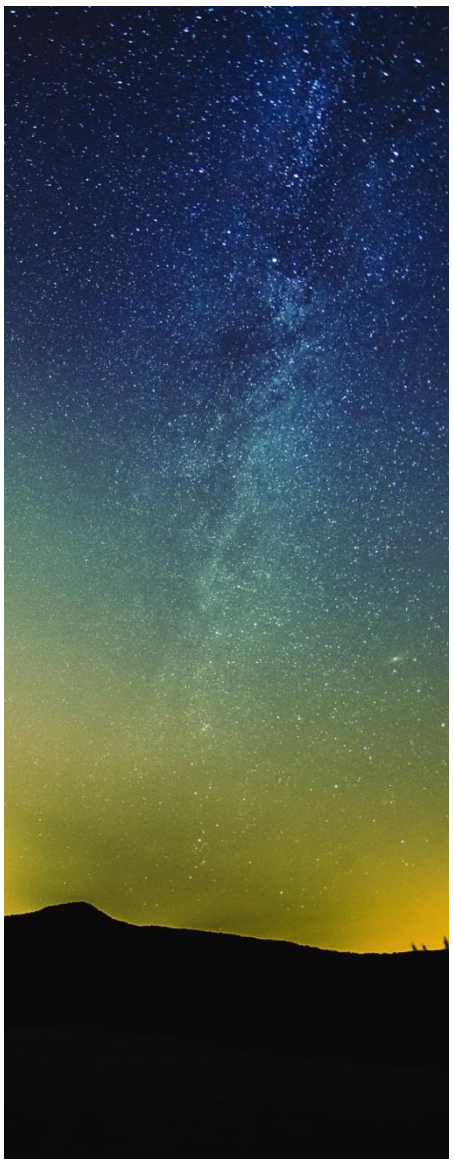
Steps to consider: Internal Audit should review all key components of the strategic planning process: parties involved, data and intelligence, models, assumptions, scenarios, approvals, and communication and use of the plan. Potentially high impact components would include management's key assumptions 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 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.



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.

Steps to consider: Internal Audit should ideally 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. Reviews of third-parties offer potentially high returns in cost savings and cash recovery, which go directly to the bottom line (in contrast to compliance). However, Internal Audit may need specialized skills to assess certain relationships, such as those in advertising, cyber, or capital projects.



[2] Third-party governance and risk management: The threats are real, Extended enterprise risk management global survey 2016, Deloitte <http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-gers-TPGRM.pdf>

Internal audit analytics

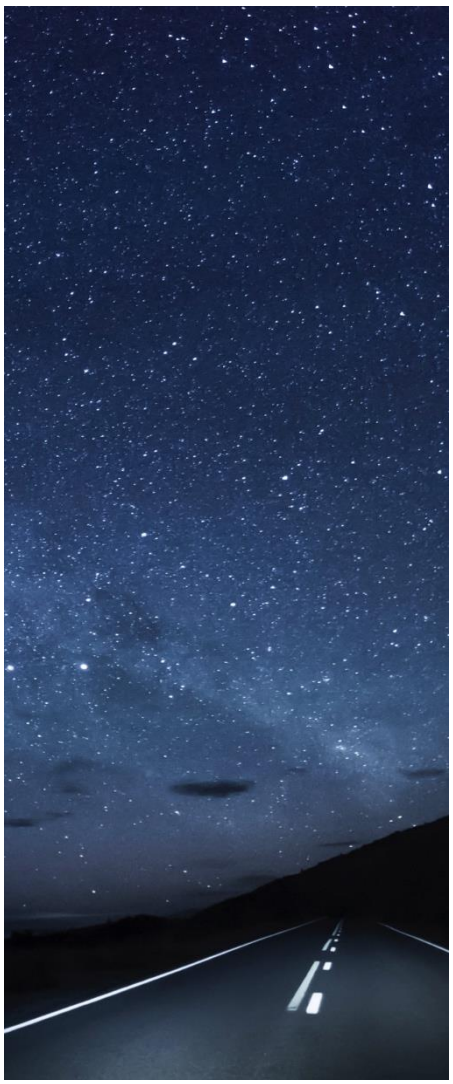
Analytics can boost efficiency and effectiveness in a range of Internal Audit activities. Dynamic audit planning enables Internal Audit to plan based on evolving risks rather than on those of the past. Analytics also enables Internal Audit to provide insight and foresight regarding risks and issues of interest to stakeholders, as well as the insight driven dynamic reporting. To increase stakeholder engagement, Internal Audit groups are using visualization 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 organization'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 visualization. Train technically-inclined internal auditors in analytics tools, then hire data scientists 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 diverse data, a consumer bank predicted potential specific control weakness and noncompliance events at specific branches. Finally, analytics can be applied to a whole range of issues. Key examples include employee absenteeism, culture change, conduct risk, and IT cost containment, as well as execution risks related to capital projects, IT installations, organizational 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 coordination 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, 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 defense 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.



Cyber

The term cyber goes beyond cyber security, recognizing that the board's cyber concerns extend well beyond cyber incidents and security risks. As the ubiquity of cyber has become clear over the past year or so, 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. The Cyber-security Systems and Risks Reporting Act, proposed in the U.S. Congress, could expand Sarbanes-Oxley (SOX) reporting requirements to cybersecurity systems and risks. The Federal Financial Institutions Examination Council (FFIEC) and the Office of the Comptroller of the Currency (OCC) are starting to review organizations' cyber auditing plans. The AICPA is defining guidance for evaluating cybersecurity risk management and governance capabilities to enhance consistency and transparency in cybersecurity reporting. These developments reflect the wide recognition that cyber is critical to organizational performance and security, and must be periodically and rigorously audited.

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 organization, industry, and stakeholders, including regulators, third-party partners, and external auditors. The audit plan should prioritize 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.

Digitization

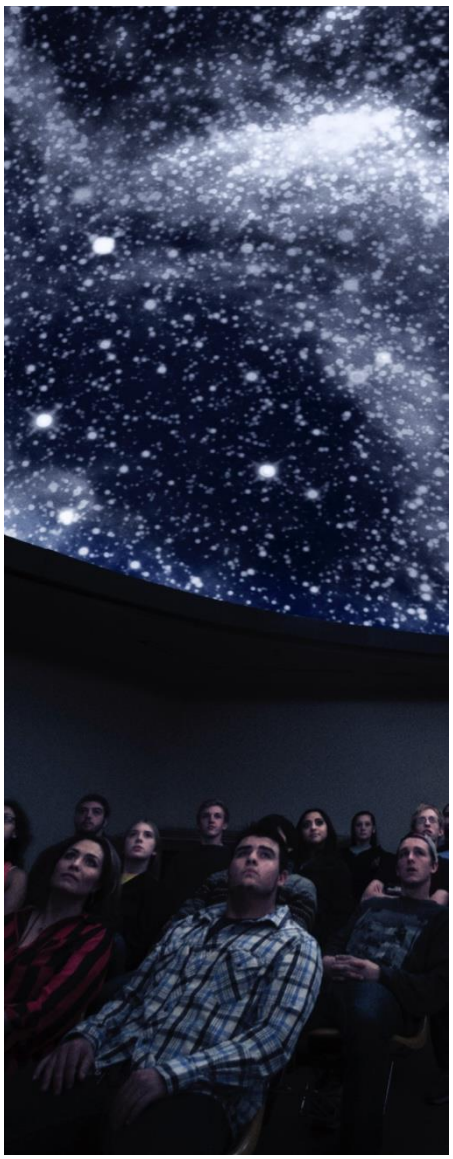
Broadly, digitalization converts currencies, transactions, services, products, experiences, and relationships into virtual forms. Virtual forms are potentially more flexible, far-ranging, and profitable—and more challenging to audit. Digital products (books, movies), services (shopping, ebanking), and disruptive business models, such as ride-sharing or room-sharing applications, augment or replace existing ones. Payment mechanisms from financial and nonfinancial 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 organization's digital maturity. All of this holds true even if your organization is not digitalizing. If competitors are digitalizing and you aren't, you may face diminished sales, profits, and market share such that not digitalizing may be the major risk.

Steps to consider: Digitalization holds profound impacts, which Internal Audit must be aware of and help the organization to address. At a minimum, Internal Audit should gauge the impact of internal or external digitalization on the organization and its businesses and functions. Risks can be easily overlooked amid the enthusiasm with which management can embrace digitalization. Digitalizing any aspect of a product, service, transaction, or relationship can transform the risks associated with its traditional form. Internal Audit should understand how digitalization 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 organization 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 digitalization, Internal Audit positions itself as forward-looking and as a source of strategic advice, and avoids the audit-planning-as-usual rut.

Risk culture

egulators and boards are focusing on risk culture because it largely determines decisions, conduct, and risk taking within an organization. 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, organizations 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 organizations on a periodic basis is becoming more critical across all industries. For example, public sector organizations tend to be sensitive to reputational risk. In life sciences organizations, 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 behaviors around value creation and risk must be clarified and properly directed.

Steps to consider: First, the organization must define risk culture so all parties have the same view. For example, Deloitte defines risk culture as a system of values and behaviors present throughout an organization that shape day-to-day risk decisions. Deloitte identifies a framework with indicators of risk culture[3]. Whatever the framework, indicators should be used to assess the existing risk culture and monitor desirable and undesirable changes. Internal Audit can audit 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 audit of the risk culture management process, metrics, and outcomes. Since risk culture can vary across organizational areas, the results of risk culture reviews should be considered individually and in aggregate. Internal Audit can also make recommendations to strengthen an organization's risk culture through training, incentives, controls, and other mechanism. 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.

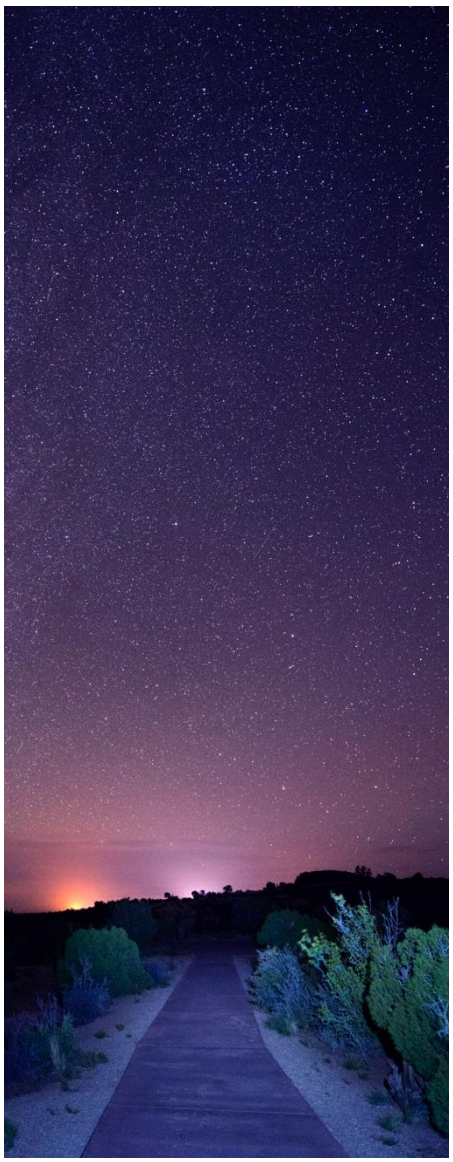


[3] See Cultivating a Risk Intelligent Culture: Understand, measure, strengthen, and report, Deloitte, 2012 <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/center-for-corporate-governance/us-ccg-cultivating-a-risk-intelligent-culture-050212.pdf>

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 organization to achieve strategic objectives. Emerging risks are early-stage developments that could impact an organization'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 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, organizations 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 organization is exposed.

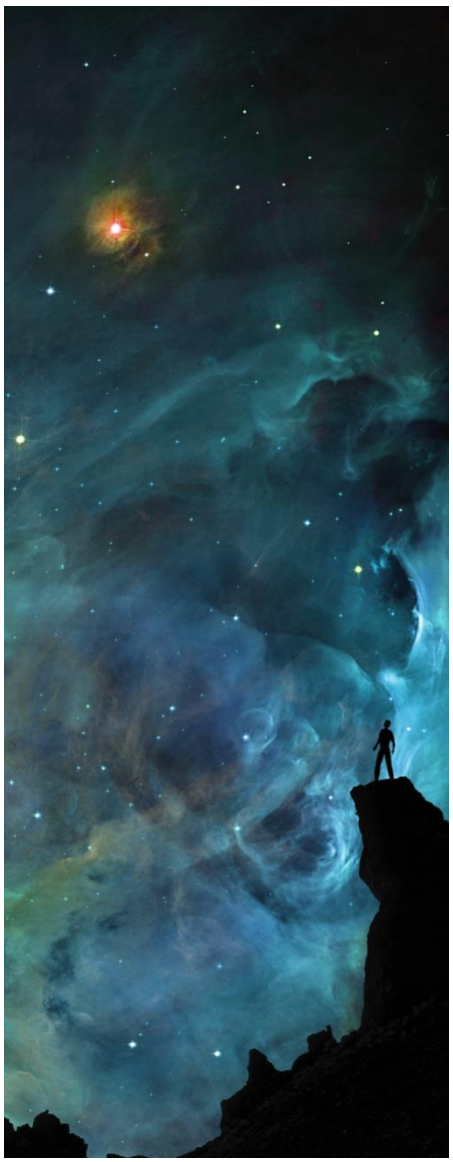
Steps to consider: Internal Audit's involvement can range from informal conversations to formal reviews. Questions might include: How are these risks being proactively and comprehensively identified? How are they being assessed and monitored? Are these risks being considered when setting strategy and 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? Most organizations 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 organization 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 organization faces and then incorporate reviews of them into audit plans.



Sustainability assurance

Regulators, institutional investors, nongovernmental organizations, and the media increasingly seek disclosure on sustainability risks that could materially affect the organization 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.

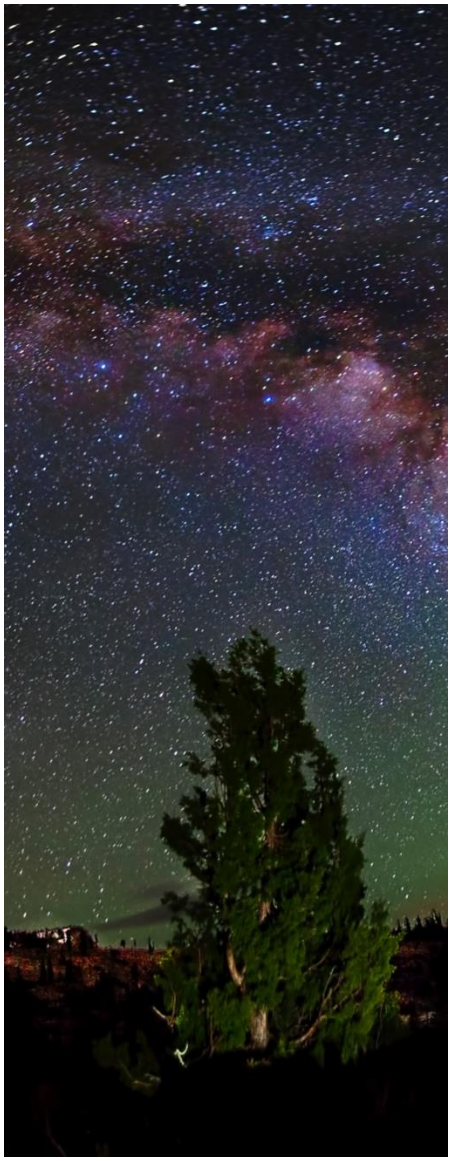
Steps to consider: Absent a comprehensive annual review, Internal Audit should cover at least one area of sustainability per year, such as employee or contractor health and safety, carbon emissions, operations management systems, or community engagement, selected in light of the materiality of the issue. 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. Information from resources like the Global Reporting Initiative (GRI) and the Sustainability Accounting Standards Board (SASB) can help in determining which issues are material.



Media audits

Organizations 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. An Association of National Advertisers (ANA) study [4] identified several nontransparent media buying practices by agencies that 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 organization'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 specialized 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 visualizations 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 specialized expertise.

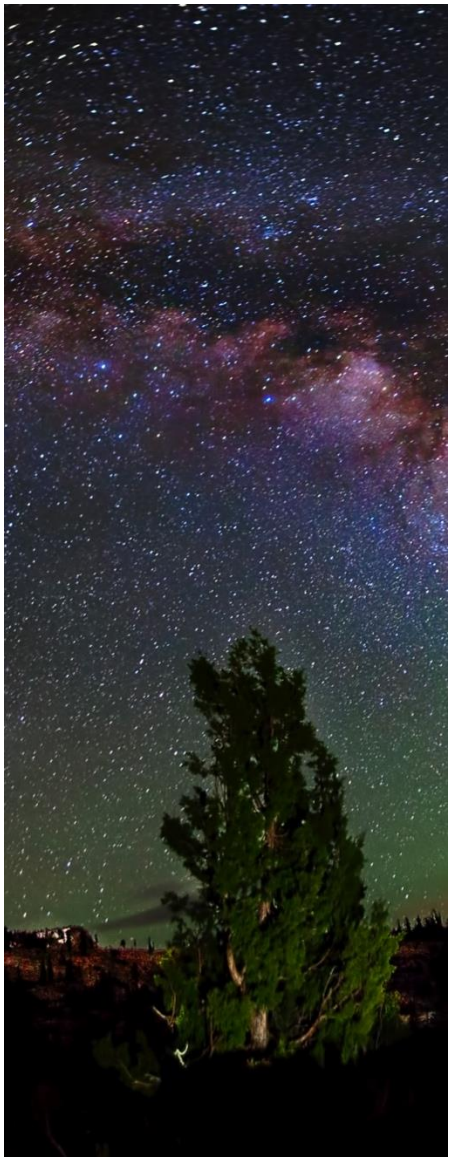


[4] Independent Study of Media Transparency in the U.S. Advertising Industry, prepared by K2 Intelligence for the Association of American Advertisers, June, 2016 <https://www.ana.net/content/show/id/industry-initiative-media-transparency-report>

New ways of reporting

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 organization 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 visualization 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, prioritized 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.



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 organization 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.

Your Contact in Germany

Heinz Wustmann
Partner Risk Advisory
Internal Audit
hwustmann@deloitte.de

Deloitte.