Internal audit insights
High-impact areas of focus
Introduction

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
High-impact areas of focus for Internal Audit

- Strategic Planning
- Third Party Management
- Internal Audit Analytics
- Integrated Risk Assurance
- Cyber Security
- Digitalization
- Risk Culture
- Strategic and Emerging Risks
- Sustainability Assurance
- Media Audits
- New Ways of Reporting
Strategic planning

The review of organization’s strategic planning process is critical in these times of disruption, if only to ensure that the process is keeping pace with marketplace changes and emerging risks.

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.

Steps to consider:

- Review all key components of the strategic planning process, including parties involved, data and intelligence, models, assumptions, scenarios, approvals, and communication and use of the plan.
- Review the governance over the related models, including model access, formula integrity, and data governance.
- Provide recommendations to strengthen the strategic planning process.
  - 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.

Boards are asking CAEs about third-party risks, and regulators, customers, investors, and the media are expressing concerns as well.

Companies faced a disruptive incident with third parties in the past two to three years: 28%

Confidence in the tools and technology used to manage third-party risk: 94%

- Major disruption with third parties
- A complete third-party failure
- Disruptive incident with third parties

Steps to consider:
- Begin with an assessment of management’s process for managing third party relationships and risks across the relationship lifecycle.
  - The 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.
- 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.

Source: Deloitte’s research

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

Why? Because analytics can boost efficiency and effectiveness in a range of Internal Audit activities.

- Dynamic audit planning - plan based on evolving risks rather than on those of the past
- Analytics - provide insight and foresight regarding risks and issues of interest to stakeholders, as well as the insight driven dynamic reporting.
- Visualization tools - increase stakeholder engagement
- 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

Steps to consider:

- Embrace analytics and accept the related challenges.
- 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.
- Analytics can be applied to a whole range of issues. Key examples include
  - Employee absenteeism
  - Culture change
  - Conduct risk
  - IT cost containment,
  - Risks related to capital projects, IT installations, organizational transformations, and product development initiatives

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.
Steps to consider:

- Internal Audit's position as third line of defense positions the function to develop and deliver integrated risk assurance.
- 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.
- Integrated risk assurance enables Internal Audit to generate more useful reports with the same or fewer resources.

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.

Integrated risk assurance may be the more useful approach from the planning, execution, and reporting perspectives:

- In audit planning - generate more meaningful information and insights for stakeholders.
- In audit execution - improve coordination among the first and second lines of defense, and allocation of audit and risk management resources.
- In reporting - improve the quality of information, risk anticipation, and insights delivered to stakeholders.

Audit plans should start with the business strategy, goals, and means of achieving them and the associated risks.
Cyber

The term cyber goes beyond cyber security, recognizing that the board’s cyber concerns extend well beyond cyber incidents and security risks.

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.

Steps to consider:

- Monitor the requirements, understand the types of reviews and assurance stakeholders will seek, and develop the needed capabilities.
- Look to co-sourcing to help develop capabilities, or simply outsource cyber audits.
- Define a cyber auditing approach that meets the needs of the organization, industry, and stakeholders, including regulators, third-party partners, and external auditors.
- 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.

Prepare to conduct independent, objective reviews (rather than continuing to wait for things to gel) because the risks are too high and varied and stakeholders and those charged with governance want greater assurance now.
Digitalization

Virtual forms are potentially more flexible, far-ranging, and profitable—and more challenging to audit.

Different applications present very different issues, risks, and opportunities, depending on the business, stakeholders, and vulnerabilities—and on the organization’s digital maturity.

Digitalization converts currencies, transactions, services, products, experiences, and relationships into virtual forms.

Steps to consider:

- At a minimum, gauge the impact of internal or external digitalization on the organization and its businesses and functions.
- 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.
- Positions Internal Audit as forward-looking and as a source of strategic advice, and avoids the audit-planning-as-usual rut.
Risk culture

Regulators 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.

Gauging risk culture within organizations on a periodic basis is becoming more critical across all industries.

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:**

- The organization must define risk culture so all parties have the same view.
- 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
  - 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.

While less technically complex than some auditable areas, risk culture demands knowledge of how to measure culture, frame questions, and seek insights.
Strategic and emerging risks

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.

In general, organizations tend to focus on near-term, well-known, less strategic risks that are more controllable.

Risk management may lack enough of a forward-looking, outward-looking focus to identify emerging risks.

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?
• Internal Audit should review the framework, processes, and mechanisms for identifying, assessing, and managing strategic and emerging risks.
• 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.

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.
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.

Internal Audit should provide assurance to the board and management regarding:
- Accuracy and integrity of public disclosures related to sustainability
- Management of operational and regulatory risks, as this will influence stakeholders’ evaluation of sustainability performance

Steps to consider:
- 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
- Mature sustainability environments have formal processes and reports to review. In less mature environments, Internal Audit should advise management on enhancements.
- 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.

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.
Media audits

Recent changes in the advertising landscape have led to agency transparency and advertising performance concerns.

An Association of National Advertisers (ANA) study\(^3\) identified several nontransparent media buying practices by agencies that lead to higher advertising costs. For example:

- Agencies not passing discounts and rebates through to the advertiser
- Purchasing media from suppliers it owns or other related entities as principal (vs. agent)

Other concerns include:

- Digital ads being viewed by robots rather than humans
- 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:

- Review advertising expenses and reconcile billings with contract provisions and agency reports.
- Recommend advertising procurement procedures, for example for selecting and contracting, and new methods of monitoring advertising costs and performance.
- 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?

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.

The current advertising landscape presents complexities that often make this area challenging for Internal Audit groups without specialized expertise.

\(^3\) 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-initiativemedia-transparency-report](https://www.ana.net/content/show/id/industry-initiativemedia-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.

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.

Interactive tools enable drill-down and increased user engagement.

Dashboards and infographics let stakeholders access reports on their devices.

More visual and dynamic reporting meets stakeholders’ need for at-a-glance insights in a changing landscape.

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.
• Dashboards enable dynamic, timely, prioritized reporting on a process, project, or risk area—with readers controlling the level of detail.

New modes of reporting are essential to increasing Internal Audit’s impact and influence.
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.
Local Omaha Points of Contact

Alan West
Senior Manager
alwest@deloitte.com

Mike Thielen
Senior Consultant
mthielen@deloitte.com