



Leading with insights
Internal Audit High Impact Areas

28 September 2017

Introduction

The Internal Audit practice is changing...

The changing landscape in which organisations operate require a lot from the internal auditors to stay relevant, to be dynamic in their approach whilst adding value to the stakeholders.

28%

Only 28 percent of CAEs believe their functions have strong impact and influence within their organizations.¹

The increasing importance of the internal audit role as the 'third line of defense' in effective risk management and control has raised the visibility both within and outside the organization.



Therefore, impact and influence increases when Internal Audit attends to areas of greatest risk, importance, and concern to key stakeholders

1. Deloitte's 2016 Global Chief Audit Executive (CAE) survey

The Internal Audit practice is changing...



High Impact Areas for the Future

High Impact Areas



Strategic Planning



The IA function should review the Organisation's strategic planning process to ensure that the process is keeping pace with marketplace changes and emerging risks.

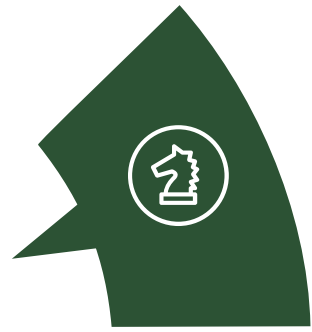


- Validity of assumptions
- Integrity of data sources (market share and growth, sales forecasts, interest rates, input costs, product pricing, funding sources, and regulatory activities.)
- Governance over models used (formula integrity, data governance)
- Scenarios and parties involved
- Approvals
- Communication and use of the plan
- Monitoring performance against objectives

The Role of IA is not to audit the strategy but to provide recommendations to strengthen the strategic planning process.

Internal Audit Analytics

Insight Driven Audits



Analytics can be applied to make audits more efficient:

- **Dynamic audit planning** can enable internal audit to plan based on evolving risks rather than those of the past.
- Provide **insights and foresight** regarding risks and issues of interest to stakeholders using visualization tools & interactive graphics.
- **Predictive analytics** –Provide forward looking analysis of likely control breakdowns and to play an advisory role before and during an initiative

Key examples of where analytics can be applied 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.

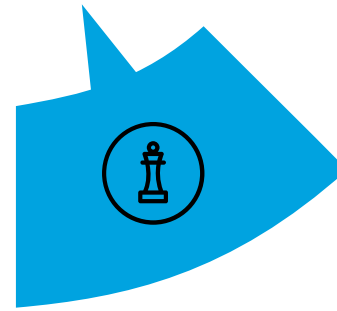
Integrated risk assurance/ Combined assurance

Generating an integrated picture of risk across the Business



Risk Culture

Regulators and boards are focusing on risk culture because it largely determines decisions, conduct, and risk taking within an organization.



Deloitte defines risk culture as a system of values and behaviors present throughout an organization that shape day-to-day risk decisions.

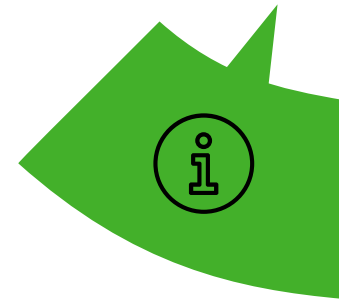
Excessive risk taking is not always the problem. Often, organizations take too little risk (for example in innovation and technology adoption) and this may stifle organisational growth.

Indicators should be used to assess the existing risk culture periodically (e.g. biannually) and monitor desirable and undesirable changes.



Digitization

Digitalizing any aspect of a product, service, transaction, or relationship can transform the risks associated with its traditional form.



Internal Audit should gauge the impact of internal or external digitalization on the bank and its businesses and functions by taking a few key steps:

1. Conduct appropriate risk analyses and rankings
2. Define audit procedures to identify risk exposures
3. Review management's steps to address them.

Cyber

Internal Audit should provide an independent, objective, comprehensive review of cyber risks within the organisation and how these risks are being managed.



1st line of defense Information Technology Unit (Business unit)

- **Integrate cyber risk management into day-to-day decision making and operations**
- **Follow a cyber risk process and apply internal controls and risk responses**

2nd line of defense Technology Risk Management

Establish governance and oversight, monitor security operations, and take action as needed, often under the direction of the chief information security officer (CISO).

3rd line of defense Cyber defense— Internal Audit

- **Integral role in assessing and identifying opportunities to strengthen enterprise security**
- **Independent perceptive and assurance to the board - inform the audit committee and board of directors that the controls for which they are responsible are in place and functioning correctly**

Strategic and Emerging Risks

Strategic risks relate mostly to external disruptions or factors that impact the ability of the organization to achieve strategic objectives. Emerging risks are early-stage developments that could impact ability to achieve business goals.



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?

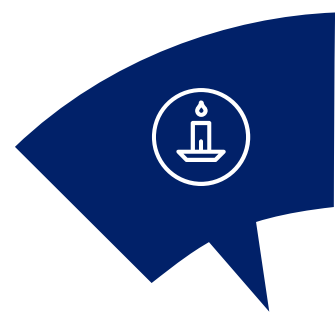
How are these risks being proactively and comprehensively identified?



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.

New ways of reporting



Stakeholder demand is driving Internal Audit to adopt novel 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.

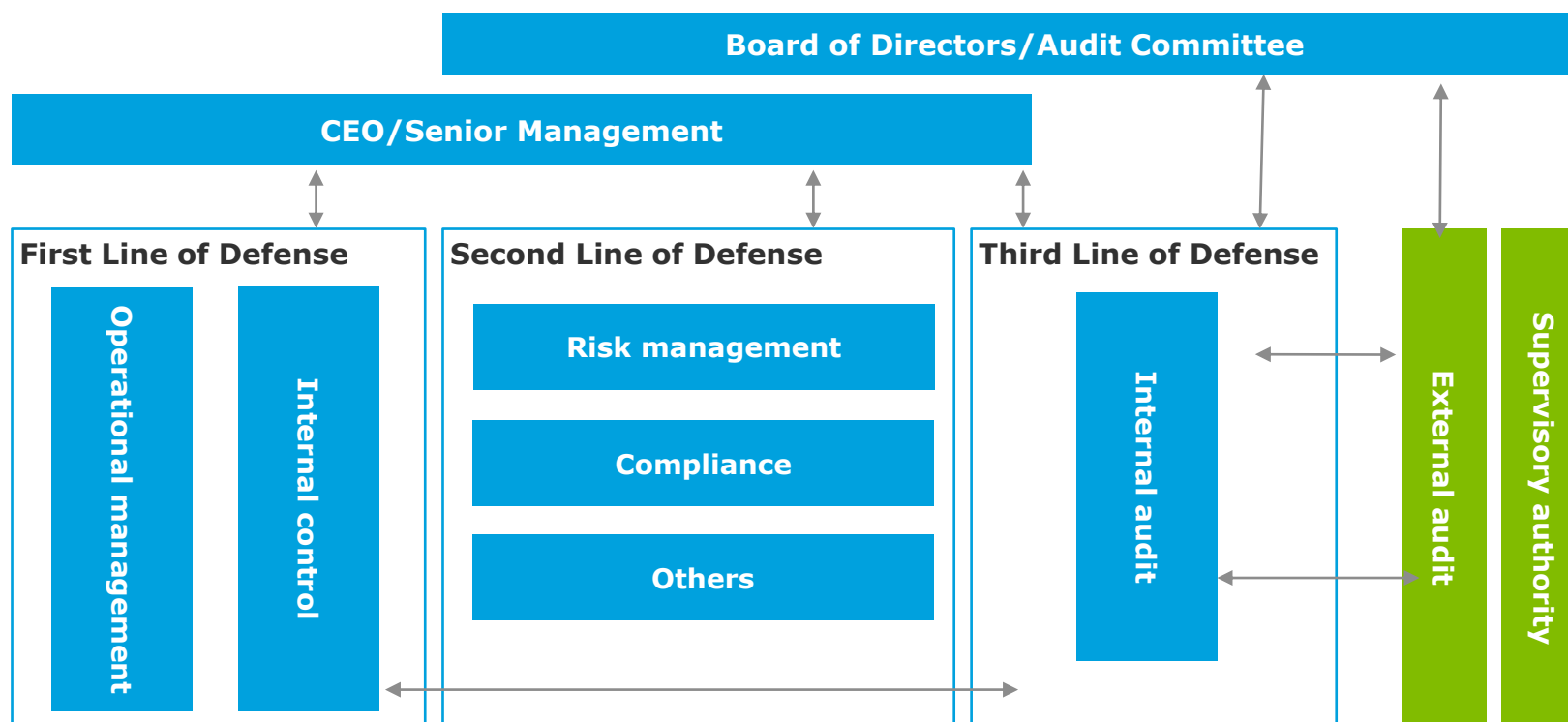
More visual and dynamic reporting meets stakeholders' need for at-a-glance insights in a changing landscape. Dashboards and infographics let stakeholders access reports on their devices—a rising trend—while interactive tools enable drill-down and increased user engagement.



Focusing over the horizon

Leading IA functions focus on the high impact areas

Not all of these areas will be high impact for your stakeholders and Internal Audit group. 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.



Source: Institute of Internal Auditors: The Three Lines of Defense in Effective Risk Management and Control



Deloitte refers to one or more of Deloitte Touché 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.

Akintola Williams Deloitte, a member firm of Deloitte Touche Tohmatsu Limited, is a professional services organization that provides audit, tax, consulting, accounting and business process solutions, financial advisory and risk advisory services.

Deloitte provides audit, tax, consulting and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. The more than 245,000 professionals of Deloitte are committed to becoming the standard of excellence