KPMG Internal Audit

Top 10 Considerations for 2017

kpmg.nl

Considerations for impactful Internal Audit functions

Competing in a rapidly changing world, companies must grapple with emerging challenges seemingly every day: cyber threats, emerging and potentially disruptive technologies, business performance risk and more. In this increasingly complex environment, Internal Audit ("IA") has a crucial role to play to help the organization in managing risks associated with these diverse business trends. This is also in line with the UK and Dutch Corporate Governance Codes.

An impactful IA function will stay current with these wide-ranging business issues as they emerge so it can help monitor related risks and their potential effects on the organization. To provide the greatest value, IA must find opportunities to challenge the status quo to reduce risk, improve controls and identify potential efficiencies and cost benefits across the organization.

To help IA functions achieve these goals, KPMG surveyed IA functions from companies in multiple industries globally and in the Netherlands. The result is **KPMG Internal Audit: Top 10 Considerations for 2017,** which outlines areas where IA should focus so it can effectively add value across the organization and maximize its influence on the company.

Top 10 Considerations for 2017

1. Cybersecurity
2. Culture/Soft Controls
3. Integrated Assurance
4. Regulatory compliance
5. Third party relationships
6. Anti-bribery/anti-corruption
7. Emerging technologies
8. Data analytics and continuous auditing
9. Performance risk
10. Strategic alignment

The **KPMG Internal Audit: Top 10 Considerations for 2017,** described on the following pages, can help ensure that IA allocates its valuable resources to those areas of highest impact to the organization. This should result in a wide range of competitive benefits, from improvements in internal control environments and enhanced risk management processes to a more confident audit committee.

01 Cybersecurity

Drivers:

- Avoiding and minimizing costly consequences of data breaches such as investigations, legal fines, coverage of customer losses, remediation efforts, loss of executive and mid-level time and focus, and potential loss of customers and business
- Averting reputational damage to the organization, especially with regard to lost customer data
- Avoiding non-compliance with regulatory requirements, i.e. 'Wet Datalekken' and Privacy regulations such as the General Data Protection Regulation (GDPR)
- Preventing loss of intellectual property and capital and other proprietary company information

In today's world of constant connectivity, cybersecurity is a key focal point for many companies. Cybersecurity frequently appears on the top of many Board agendas, and data security breaches now appear to be headline news almost on a weekly basis. Several factors have driven the increased attention paid to cybersecurity issues, including changes in the threat landscape, rapid changes in technology, changing regulatory environments, social change and corporate change. Additionally, new methods are constantly being developed by increasingly sophisticated and well-funded hackers who target companies not only through networks directly but also through connections with key suppliers and technology partners. The consequences of lapses in security can be disastrous as an organization's bottom line and reputation are impacted. It is critical that all companies remain vigilant and up to date regarding recent protection criteria and relevant regulations.

How Internal Audit can help:

- Review the organization's cybersecurity risk assessment, processes and controls to protect its intellectual property, using industry standards as a guide, and provide recommendations for improvements
- Assess implementation of revised technology security models, such as multilayered defenses, enhanced detection methods, and encryption of data leaving the network
- Champion a robust training and education program, including simulated phishing attacks, so that employees play a key role in a comprehensive protection plan
- Assess third-party security providers to evaluate the extent to which they are addressing the most current risks completely and sufficiently
- Demand periodic cyber "fire drills" and review outcomes and procedures followed during such drills and during real-life incidents

02 Culture risk / Soft Controls

Drivers:

- Heightening regulatory scrutiny and increasing cultural expectations
- Increasingly global organizations with much more varied cultural norms and practices
- Governance gaps arising from lack of business unit interrelations
- Stricter governance, oversight and accountability expectations
- Audit findings and internal control issues

Culture risk has gained the attention of company leaders as the cause of many incidents of misconduct that have impacted the public's trust. Even if a company has a well-defined strategy, if the company culture does not support its execution, success is less likely. Culture can be observed, monitored and changed over time to mitigate misconduct and encourage desired behaviors. A broader cultural program, while addressing the specific issues of governance, compliance and risk management, will also focus on understanding how the organization makes decisions to meet the demands of its various stakeholders, and how these decisions influence culture, both current and desired.

How Internal Audit can help:

- Identify organization's cultural drivers related to the core values and other behavioural norms
- Conduct an assessment of the organization's cultural drivers in relation to the organizational norm
- Review the alignment of performance measures to strategy and core values to ensure desired behaviors are being incentivized and rewarded
- Provide assurance regarding the evolution and alignment of the organization's culture with compliance activities, as well as financial objectives and business and operating models
- Assess the quality of the cultural drivers that are preconditions for the operating effectiveness of controls
- Surface culture risk through data analytics and third-party audits
- Lead or participate in investigations into matters involving potential misconduct
- Drive continuous improvement through testing and evaluation of the organization's culture change program, include cultural aspects in reporting
- Perform systematic root cause analysis on audit findings and other non compliance incidents with specific consideration of soft controls

03 Integrated assurance

Drivers:

- Rapidly changing risk environment coupled with increasing need for insights to make decisions
- Collaborating among assurance providers to develop a common view of risk
- Streamlining risk assessment and assurance activities across the enterprise to gain efficiencies and maximize coverage
- Allocating limited resources towards highest risk areas for the enterprise

With a constantly evolving risk landscape, the Board and senior management expect all assurance functions to work together to provide an integrated view of the organization's risk profile. Many companies fail to develop systematic processes for anticipating new and emerging risks, and as a result, critical risks are identified too late to be effectively and efficiently managed. Further, traditional approaches to providing assurance over risk responses are often siloed and uncoordinated. Companies that effectively anticipate and address changes in the risk environment, develop coordinated responses across multiple assurance functions, and maximize enterprise coverage will be well-positioned to provide insights and perspective to senior management and the Board, for the benefit of more effective decision-making and risk management. Companies should identify and manage risks not only as threats, but also as opportunities.

How Internal Audit can help:

- Lead or support coordination of the risk assessment, planning, work execution and reporting across multiple assurance functions, thereby minimizing the footprint on the business
- Develop and execute holistic assurance plans considering enterprise risks, leveraging the various governance, compliance and audit functions across the organization
- Evaluate business implications of emerging trends and their associated risks and opportunities
- Encourage increased utilization of data and analytics to optimize insights into the emerging risk environment

04 Regulatory compliance

Drivers:

- Ensuring compliance with a dramatically increasing number of regulations, both domestically and abroad
- Mitigating the increasing costs of complying with this ever-growing number of regulations
- Developing a strategy to lessen the restraining effects of compliance activities on business operations
- Ensuring compliance operations are aligned following a merger or acquisition

Companies, regardless of industry, are being inundated with new regulatory requirements, both domestically and abroad. These new regulations are putting increased burdens on chief compliance officers and their staffs, raising the possibility that certain compliance requirements are being missed. In addition, meeting this raft of new regulations is adding considerable cost to a company's compliance budget and complexity to internal structures and information needs. Meanwhile, mergers and acquisitions are on the rise, which means companies need to combine their compliance function with that of the acquired entity and ensure a holistic approach to corporate compliance.

How Internal Audit can help:

- Inventory regulatory bodies and requirements affecting the company
- Assess the company's approach to managing its (global) compliance activities, including integration of the requirements of acquired companies
- Evaluate the company's response to any notable instances of noncompliance
- Ensure compliance training programs offered to employees and other stakeholders are appropriate for role and geography
- Perform activities as directed by the compliance department when visiting locations to minimize duplication on the business while still achieving objectives
- Provide assurance with regards to the design and operating effectiveness of the organization's compliance framework

05 Third-party relationships

Drivers:

- Risks associated with an increasing number of third-party relationships and oversight of those relationships
- Enhancing revenue and cost reduction
- Improving contract and vendor governance
- Creating more effective contractual self-reporting processes
- Preventing or timely detecting risk management failures at third party business partners

Although often not deliberate, many business partners fall short due to the complexity of the environment or their agreements leading to overcharging or loss of revenues effecting your bottom-line. To boost productivity and adapt to changing business models, companies are increasingly relying on third parties to carry out vital business functions. However, using third parties opens up companies to numerous new risks and potential service, compliance and other failures that can lead to fines, lawsuits, operational bans and reputational damage. Although often not deliberate, many business partners fall short due to the complexity of the environment or their agreements. Often, third parties have access to the company's networks, increasing the possibility of data breaches, or companies can be unaware that third parties are employing subcontractors that may be lacking in their compliance efforts. Finally, third parties can operate in areas of political uncertainty, exposing contracting companies to further risks. Given all these factors, companies need to ensure they are getting the most benefitsfrom these external relationships while having in place appropriate controls to reduce liabilities.

How Internal Audit can help:

- Review third-party identification, due-diligence, selection and on-boarding processes and controls
- Evaluate contract management processes used by management to track third-party relationships
- Monitor regulatory developments related to third-parties
- Enforce and ensure consistency of right-to-audit clauses
- Enforce third-party compliance with company's information security standards
- Develop, implement and calibrate a continuous monitoring system of self-reported data from third-party business partners

06 Anti-bribery/anti-corruption

Drivers:

- Difficulty in conducting due diligence and compliance audits over foreign agents / third parties
- Identifying emerging regulatory and compliance risk, including cultural issues such as that introduced by organic expansion into new markets, third parties and acquired businesses
- Providing insight to stakeholders regarding the effectiveness of existing anti-bribery and corruption compliance activities
- Preserving the company's ability to control when it discloses a potential violation to the regulators, if at all
- Dealing with the variation in national regulations pertaining to bribery & corruption

The benefits of an effective anti-bribery and corruption compliance program, calibrated for a company's specific risk profile, are clear. Clearly written policies that spell out prohibited activity, the commitment of executive management to anti-bribery and corruption efforts, periodic training, audit clauses in agreements with third parties, and vigilance by compliance personnel can deter bribery and corruption, thereby reducing the risk of costly and disruptive regulatory enforcement activity. Should the unthinkable occur, a well-designed and executed anti-bribery and corruption compliance program may mean the difference between a prosecution and a non-prosecution agreement and may even reduce the amount of monetary fines and penalties levied.

How Internal Audit can help:

- Conduct a gap assessment of the organization's existing anti-bribery and corruption procedures in relation to leading practice regulatory guidance
- Provide assurance regarding the design and operating effectiveness of the organization's applicable preventative and detective controls
- Enhance IA return on investment by embedding anti-bribery and corruption procedures into its existing/scheduled audits and third-party oversight activities
- Surface bribery and corruption risk through data analytics and third-party audits
- Lead or lend resources to investigations into matters involving potential noncompliance
- Conduct an assessment of the current compliance and ethical environment around anti-bribery and corruption

07 Emerging technologies

Drivers:

- Planning the adoption and implementation of cloud computing as an alternative to traditional computing methods
- Rethinking traditional approaches to disaster recovery and business continuity as changes in technology, workforce expectations and unforeseen challenges evolve or are identified
- Considering robotics and other mechanisms which reduce dependence on the human workforce
- Rapidly emerging or disruptive technologies such as fintech and blockchain

Mobile computing, remote computing, cloud computing, social media and big data have allowed us unprecedented access, usage and management of information and have completely altered the business landscape. Emerging technologies are bringing information to the fingertips of employees at companies in the Netherlands and across the globe, allowing organizations to operate more effectively and impacting the way people live and work. These organizations now face a wealth of opportunities to identify and capitalize on these technological advances to drive change and innovation across markets and industries. However, with each new evolution in technology comes risks that companies need to stay on top of to optimize the impact of technology and mitigate concerns over its implementation and use.

How Internal Audit can help:

- Conduct an assessment of the organization's existing and emerging technology systems usage in relation to industry standards
- Evaluate changes in the business model, and related changes in the control structure, that may result from adopted technologies
- Review policies and procedures around the management of technology, including governance and controls, data integrity, security and privacy and supplier management compliance
- Evaluate disaster recovery and business continuity plans, including management's approach to testing those plans, in light of the threat from "denial of service" type attacks
- Consider governance and controls required for digital labor, robotics and related initiatives

08 Data analytics and continuous auditing

Drivers:

- Enabling real-time, continuous risk management
- Increasing overall efficiency of audits being performed (frequency, scope, etc.)
- Taking a "deeper dive" into key risk areas through analysis of key data
- Enabling early detection of potential fraud, errors, and abuse
- Leveraging the benefits of single-platform ERP systems

In the past few years, data analytics have helped to revolutionize the way in which companies assess and monitor themselves, especially in terms of efficiently expanding the scope of audits and improving detail levels to which audits can be performed. Data analytics and continuous auditing can help IA departments simplify and improve their audit processes, resulting in higher quality audits and tangible value to the business. Consider the traditional audit approach, which is based on a cyclical process that involves manually identifying control objectives, assessing and testing controls, performing tests, and sampling only a small population to measure control effectiveness or operational performance. Contrast this with today's methods, which use repeatable and sustainable data analytics that provide a more thorough and risk-based approach. With data analytics, companies have the ability to review every transaction—not just samples—which enables more efficient analysis on a greater scale. Additionally big data techniques such as cognitive analysis and the use of external sources enables companies to pro-actively identifying new trends and related risks such as the early detection of social trends that will likely lead to regulatory changes.

How Internal Audit can help:

- Continuously monitor the business on key risks by creating an effective processes for effective gathering, mapping, analyzing and presenting data extracted from a complex variety of information systems
- Assess the alignment of the strategic goals and objectives of the company to risk management practices and monitoring and prioritization of the strategic objectives and risks on a continuous basis
- Promote data analytics enabled audit programs designed to verify the underlying data analysis and reporting of risk at the business level
- Implement automated auditing focused on root cause analysis and management's responses to risks, including business anomalies and trigger events
- Recommend consistent use of analytics, including descriptive, diagnostic, predictive and prescriptive elements

09

Performance risk

Drivers:

- Ensuring financial performance is linked with operations and strategy
- Providing management with the insights necessary to manage and minimize the risk of not performing
- Integrating the approach to risk management and performance management, leading to smarter risk taking
- Increasing awareness of IA as a strategic partner to the business

Shareholders' expectations of business performance and the risk of not performing are growing increasingly more important. Shareholders expect their IA functions to focus on operations and to truly understand what makes the organization successful and profitable. IA is now being relied on more than ever to help assess risks and to assist in identifying and developing sustainable profit generation. IA is on the front lines of risk analysis across the organization touching on strategic, operational, financial, and compliance risk, all of which affect the performance of the company. Risk analysis findings can be linked quantitatively and qualitatively to a number of value drivers including revenue, operating expenses and investments, which makes IA's perspective essential to maximizing performance.

How Internal Audit can help:

- Shift allocation of IA resources to enterprise initiatives and demonstrate return on investment beyond compliance
- Execute a holistic approach to assess management's effectiveness in managing the risk of not performing, by focusing audit activities on operations and performance in addition to finance and compliance
- Evaluate how the company is measuring performance and identifying initiatives for improvement

10

Strategic alignment

Drivers:

- Ensuring IA aligns to the company's strategic priorities and remains relevant in light of organizational and other transformational changes
- Ensuring IA is involved in key strategic initiatives of the company, whether through consultation or reviewing progress/outcomes

Business transformation has taken hold across the broad corporate landscape due to the confluence of several important triggers, including a tipping point in globalization, a continuing slowdown in Western economies, significant shifts in technology and energy costs, and the challenges of regulatory compliance. When a company's transformational and other goals lead to strategic objectives and initiatives, IA should be an active participant in considering impacts to risk and related governance and controls. Often, efforts to bring about strategic change can sometimes neglect to revise internal controls to conform to new business models. IA brings a unique perspective to strategic change and should be present and active in key strategic initiatives.

How Internal Audit can help:

- Ensure IA resources are allocated toward the most important objectives and initiatives of the organization
- Focus on long term value creation subjects as described in the UK and Dutch Corporate Governance Codes such as culture/ soft controls, cyber risks and ensure that IA include these topics in the IA plan
- Determine how the company is assessing risk related to major strategic initiatives and how it is managing change related to those initiatives, and related governance and controls
- Gather internal and external signals of change for consideration by the corporate strategy group
- Facilitate deep dive analysis of strategic decisions and risk events to provide insights to management for future decision making

Contact us

drs. Bart van Loon RA
Partner Internal Audit,
Risk & Compliance Services

T: +31 (0)20 656 77 96
E: vanloon.bart@kpmg.nl

drs. Pamela de Maaijer
Senior Manager Internal Audit,
Risk & Compliance Services

T: +31 (0)20 656 24 02
E: demaaijer.pamela@kpmg.nl

Leah Jin CPA CISA
Partner Internal Audit,
Risk & Compliance Services

T: +31 (0)20 656 29 89
E: jin.leah@kpmg.nl

drs. Huck Chuah RA RO
Senior Manager Internal Audit,
Risk & Compliance Services

T: +31 (0)20 656 45 01
E: chuah.huck@kpmg.nl

kpmg.nl/internal audit