20 key risks to consider by Internal Audit before 2020

Are you aware of the risks concerning Internal Audit today and in the near future?

kpmg.nl

Editorial

Huck Chuah
Partner, Internal Audit,
Risk and Compliance Services,
KPMG Netherlands

Traditionally, Internal Audit develops its risk-based audit plan based on a methodical approach that enables the organization to focus on key risk areas. However, as the business landscape continues to be disrupted and evolves with the rapid advancements of technology, regulatory requirements and business models, the underlying risk landscape becomes more dynamic and complex. In turn, this means that it is essential for Internal Audit to adapt and remain agile in its audit framework and methodology.

A modern internal audit function (hereinafter: IAF) should focus on understanding the organization's key risks and pro-actively identify emerging risks that would disrupt the execution of the business strategy. The Institute of Internal Auditors (IIA) in Europe also published a Top-10 Risks in focus, like many other organisations. Like the traditional annual audit plan, these audit plans are quite static, while a more dynamic risk assessment and audit planning is required nowadays. Additionally, Internal Audit should also allow for flexible and dynamic internal audit planning in order to manage the rapidly evolving business landscape.

We believe that this publication serves to provide insights to Chief Audit Executives on the key changes to the risk environment and assist IAF in identifying opportunities to respond to these risks. As further guidance, we have mapped the top 20 risks on a Risk Radar (refer to page 4). The Radar presents two spectrums:
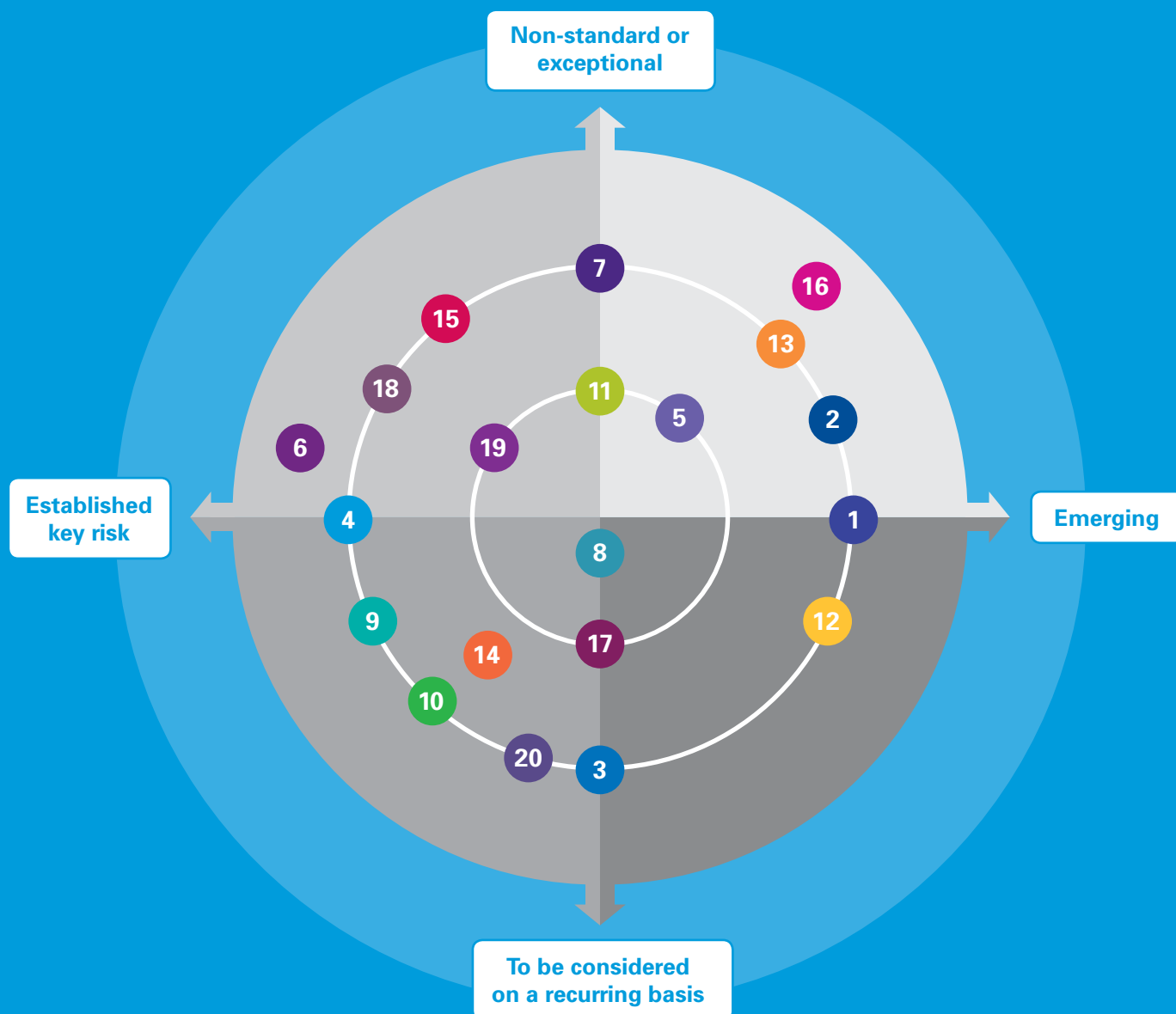
1 **Established key risks** that should have been identified and understood by the IAF vs. **emerging risks** which are developing but full understanding has yet to be obtained.

2 **Non-standard/exceptional risks** that should be considered for a one- time audit vs. **standard risks** that should be considered on an ongoing basis.

In summary, the IAF should ensure that it is able to add value to the organization by leveraging the use of technology and by having a clear and profound understanding of the business strategy and operations. We hope that through this publication, we would be able to provide insights on areas where Internal Audit functions should focus on in the upcoming year in order to establish a strategic role in the organization.

Top 20 risks before 2020

1. Digitalization & the Internet of Things
2. Cloud computing
3. EU General Data Protection Regulation (EU-GDPR)
4. Cyber security
5. Business continuity and crisis response
6. Net working capital management
7. Non-GAAP financial measures
8. Data analytics and Big Data
9. Treasury management
10. Enterprise Project Management
11. Effective talent management
12. Trade environment and customs
13. Alignment of operations to organization's strategy and objectives
14. Culture and behavior and Soft controls
15. Effectiveness and efficiency of operational processes
16. Mergers, acquisitions, and divestitures
17. Integrated enterprise risk management and monitoring
18. IT governance
19. Outsourcing and managing third-party relationships
20. Tax compliance

Risk Radar – Top 20 risks before 2020

Non-standard or exceptional

Established key risk

Emerging

To be considered on a recurring basis

7
16
13
15
11
18
5
2
6
19
4
1
8
9
12
14
17
10
20
3

Emerging and exceptional risks, categorized as a current, high priority by stakeholders

Established and exceptional key risks requiring highly technical & specialized audit and subject matter expertise

Established key risks to be audited on a cyclical basis and considered by management on a continuous basis

Emerging risks to be considered on an ongoing basis and included in assurance activities where possible

Digitalization & the Internet of Things (IoT)

01

Drivers

Digitalization has continuously spread throughout all aspects of our life. Organizations are increasingly investing in technologies such as IoT, robotics, RPA, machine learning, data & analytics and artificial intelligence. As our digital and physical worlds continue to merge and co-exist, we continue to explore the various possibilities in order to maximize the benefits of what technology has to offer. Some of the benefits of digitalization include the following:

- Allows for seamless integration of consumer goods with smart chips/IoT, machines and systems promoting exchange of information without human intervention.

- Providing management with an increased level of information and real-time data, thus improving their ability to manage risks and opportunities as and when they arise.

- Increased productivity and efficiency by automating simple, repetitive tasks.

As digitalization continues to disrupt operations, business processes and business models, it ultimately brings about a new facet of challenges. The following risks should be considered in the face of this digital age:

- Ensuring that the right data is collected and analyzed to aid in the organization's strategy and operations.

- Keeping abreast of the regulatory changes as regulators continue to develop and design the appropriate regulatory framework.

- Maintaining an appropriate level of governance despite the complexity of information systems and tools.

- Maintaining productivity and growth by ensuring that personnel are equipped with the right skills and experience.

The role of Internal Audit

- Assist organizations through the change management process by developing a company-wide digital transformation strategy and assessing if these objectives have been achieved throughout the transformation journey.

- Assist organizations in the design and implementation of appropriate governance and control frameworks within their various systems and tools.

- Provide recommendations on reporting and dashboards by leveraging the use of technology to deploy the use of Continuous Auditing and Continuous Monitoring leading to better and timely insights.

- Provide training to the organization in order to bridge the gap between the digital skills required and the needs of the organization.

The path forward for Internal Audit

- Be aware of upcoming developments and latest technology i.e. regulatory landscape and digital advancements.

- Continuous learning and application of technology enablers such as RPA and data & analyticsin the audit planning and process.

- Enhance our understanding of the various business processes and the influence of digitalization on the processes.

- Possess an analytical mindset to identify, assess and mitigate the risks associated with the impact of digitalization.

- Improve our expertise on using data & analytics in our audits and enabling data & analytics tooling.

- Improve our expertise on general IT controls (GITC) such as data access, integrity, change protocols and IT security.

02

Cloud computing

Drivers

Cloud computing refers to the delivery of services, such as networks, servers, storage, applications and services over the internet. There are three different service models in cloud computing - Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Cloud computing services will continue to grow in the foreseeable future as more companies begin to adopt these services as part of their operations. The following are some of the key benefits of cloud computing:

- Scalability – pay only for the service required, granting businesses the ability to scale up or down depending on their needs without having to incur large capital investment.
- Collaboration efficiency – ability to work across different locations and departments due to the shared access to the same files.
- Flexibility of work – remote access to the information allows employees to be more flexible in their work practices.
- Business continuity – with the data stored in the cloud, it can be easily accessed without interruption, minimizing downtime.

To realize the benefits of cloud computing, companies should be careful and understand the implications of such technology:

- Data Security and Regulatory – dependent on the security and control features of the service providers.
- Technology – as technology continues to evolve, constant upgrade to the security features and training of staff may result in additional cost.
- Operational – challenges in the integration of development and operational responsibilities, which used to function in relative silos, could impact task execution. Additionally, for public cloud, there is limited customizability would result in operational challenges.
- Vendor – due to association with and reliance on service providers, risks faced by vendors could impact businesses.
- Financial – poor planning, changing business needs and lack of understanding in the technology may result in overspending and loss of revenue.

The path forward for Internal Audit

- Keep abreast of changes in the guidelines and standards for data privacy, data security and cloud usage.
- Understand that governance oversight of the cloud system is a responsibility of both the organization and the cloud vendor.
- Gain further experience in IT controls such as logging and monitoring, network configuration, data management, IT asset protection and vulnerability.
- Continue to refine the compliance framework for cloud environments in order to keep up with the technology and remain effective in our audits.
- Audit the third parties and vendors related to cloud computing, business continuity and adherence to contractual compliance.

The role of Internal Audit

- Assist the organization to perform due diligence on the cloud service vendor and ascertain if the vendor's strategic direction and capability is in line with the organization's business development.
- Assist the organization to perform the risk assessment of the environment of the cloud system and to identify appropriate measures to mitigate these specific risks.
- Assess the current level of alignment of business needs to the integration of cloud computing to operations.
- Perform reviews of the Service Level Agreements of cloud vendors to assess contractual compliance and regulatory compliance.
- Perform independent audits of the cloud computing setup to assess the level of security controls and to provide potential areas of improvement.
- Assist the organization to develop ongoing monitoring mechanisms to monitor the performance of the cloud service vendor.

03

EU General Data Protection Regulation (EU-GDPR)

Drivers

The European Union General Data Protection Regulation (EU-GDPR) was approved in April 2016 and enforced in May 2018. The regulation applies to all companies processing and holding any personal data of data subjects residing in the European Union, regardless of the company's location[1]. In the Netherlands it is called "Algemene verordening gegevensbescherming" (AVG).

The Dutch Data Protection Authority (Autoriteit Persoongegevens) released an AVG fining policy to provide guidelines and clarity to the enforcement of GDPR.

In June 2019, the first fine for AVG violations was imposed in the Netherlands. We can expect further fines to be imposed across the European Union as companies adapt to the new regulations. The potential fines for violators of AVG / GDPR may be as high as EUR 20 million, or 4% of the businesses' global revenue, whichever is higher.

In addition to the penalties, organizations also face increased reputational risk due to heightened focus on the topic of data privacy and data security. It is not possible to attain full compliance with the law at the early stages of implementation, hence it is important that organizations continue to focus their efforts on continuous compliance. This can include:

- Understand the nature of the personal data that the organization holds – where it came from, for what purpose was it collected for, who it is being shared with, where it is being stored.

- Increase awareness of the importance of data privacy and data security across the organization.

- Establish procedures to detect, report and investigate any potential personal data breaches.

- Appoint independent Data Protection Officers to support the organization on data protection compliance.

The role of Internal Audit

- Assess the organization's data strategies and governance against the corporate strategy and objectives, ensuring that high standards of data security and regulatory compliance are maintained.

- Assess the organization's current level of compliance against the EU-GDPR guidelines and to identify recommendations and impact on the organization.

- Assess the compliance of third-party providers and understand the initiatives undertaken by them with regards to data protection and data security.

- Assess the level of risk exposure with regards to data security and data protection and identify the relevant mitigation measures.

- Assist the organization in developing the audit program to include the review of EU-GDPR.

- Assist the organization to develop the data security policy ensuring that the policy promotes a continuous process to remain compliant.

The path forward for Internal Audit

- Gain deeper understanding of the EU-GDPR requirements and the Dutch implementation and how it impacts organizations and businesses one and half year after implementation.

- Understand that EU-GDPR goes beyond the EU and may affect organizations with operations or business partners residing outside the EU.

- Consolidate best practices and key risk areas across the different business sectors on GDPR.

[1]   EUGDPR.org (2018) https://www.eugdpr.org/gdpr-faqs.html

Cyber security

04

Drivers

The widespread use of technology brought along with it a rise in cyber-crime, and thus the need for cyber security. It has increasingly become a key focus for many organizations, often appearing at the top of many board agendas. Data security breaches now appear in the headlines almost on a weekly basis.

There are several factors driving the increased focus on cyber security, including:

- Changes in the regulatory environment, such as the EU-GDPR, which may result in penalties, fines and reputational loss.

- Evolution and growing sophistication of the capabilities and techniques used by hackers, especially in their ability to target specific information or individuals.

- Ability of hackers to now target companies, not only through networks, but also through connections with other third party providers.

'You are only as strong as your weakest link'. Cyber security is everybody's responsibility and it is essential that the organization works together to enhance its cyber resilience. The consequences of cyber security breaches can be detrimental to an organization's bottom line and reputation and can affect the growth of the entire organization. There are three key main principles behind effective cyber security:

- Confidentiality – Establishing framework to determine the level of sensitivity of information and ensure that access to sensitive information is restricted.

- Integrity – Ensuring that there are no unauthorized alterations to data and information i.e. malware attacks.

- Availability – Ensuring that the people in the organization has ready access to accurate information.

Cyber security, in essence, should be seen as something more than a defensive or mitigating capability.

The role of Internal Audit

- Conduct cyber risk assessment to assess the organization's capabilities in managing the associated risks and to ensure that key risks have been considered by management.

- Perform benchmarking of the organization's cyber security processes against best practices and identify possible recommendations.

- Assist the organization to develop a cyber security program, which must include the elements of prevention, detection and correction.

- Integrate the cybersecurity audit program as part of the organization's overall risk management process.

- Conduct specialized cybersecurity audits such as vulnerability assessments and penetration testing.

- Provide training to the organization in order to increase their awareness of the need for an integrated approach when it comes to cyber security.

The path forward for Internal Audit

- Access to cybersecurity internal audit experts with the appropriate technical skillsets and understanding of the current risk environment.

- Clear understanding of the interdependencies between organizations, its subsidiaries, and third party providers and how they might impact the overall cyber risk environment.

- Ensure that the internal audit capabilities and resources have the right cyber expertise.

- Stay current with the developments in the cyber risk environment and at the same time grow expertise in other key aspects of cyber security such as data security and data integrity.

Business continuity and crisis response

05

Drivers

With the rapidly evolving business environment, organizations must respond and adapt to these challenges and the threats that these changes may bring. This includes:

- Cyber threats – Technological advancements and the growth of the Internet brought about a new set of IT risks, including cyber security attacks.

- Geographical threats – Natural disasters, disease outbreaks may affect business operations.

- Political threat – Political instability, and the globalization of terrorism may disrupt businesses.

- Digital and social media threat - The speed, nature and impact of information dissemination is increased thus, potentially affecting reputational and branding risk.

Many organizations may have developed a disaster recovery plan and business continuity procedure but have rarely put them to the test in a real crisis situation. However, it is still essential to have adequate business continuity planning and crisis management to ensure that disruption is kept to a minimum.

The role of Internal Audit

- Assist the organization to develop a business continuity plan and crisis management framework by identifying the organization's priorities and needs and the respective recommendations to address potential disruptive threats.

- Assess the quality of the overall crisis management system, ensuring that key threats have been identified and appropriate response plans have been prepared.

- Perform an independent assessment of the leadership's readiness and awareness for crisis situations by conducting a survey with key questions.

- Assisting the organization to test the readiness of the business continuity plan and crisis management response in order to evaluate the organization's level of knowledge and understanding of the framework.

- Perform periodic reviews of the business continuity plan and crisis management framework to ensure that emerging risk and evolving key threats have been considered.

The path forward for Internal Audit

- Keep abreast of potential and emerging risks and threats that may impact organizations and businesses in the various industries.

- Thorough understanding of the organization and its interdependencies with other subsidiaries and third party vendors.

- Conduct an audit and assess from a top-down and 'holistic' point of view on Business continuity and crisis response for key stakeholders such as the audit committee.

- Possess a critical thinking mindset when evaluating the existing business continuity plans and crisis management frameworks.

- Increase knowledge in disaster recovery and run test simulations in order to evaluate the readiness and adequacy of the business continuity plans.

Net working capital management

06

Drivers

An efficient net working capital management is essential to the operational success of the organization. They help to maintain smooth operations and can also improve earnings and profitability.

When managed effectively, a healthy net working capital management can bring about the following key benefits:

- Sufficient liquidity – Ensures the solvency of the organization.

- Operational efficiency – Allows for optimum level of resource allocation and utilization.

- Debtor's management – Ensures prompt and on-time payments that helps to build trust, reputation and a good credit rating.

- Meeting market expectations – Healthy net working capital ensures that dividends are and can be regularly paid.

- Resilience – Ability to survive through crisis and changes to businesses.

Some of the considerations in having an effective net working capital management includes:

- Leveraging the use of technology to access to working capital data, run simulations and to drive continuous improvements in the management of net working capital.

- Improve forecast accuracy by understanding the nature of business and the business needs

- Ensuring that the net working capital strategy is sustainable and not a knee-jerk reaction to a particular problem.

- Aligning the importance of net working capital management throughout the organization.

The role of Internal Audit

- Conduct a review over the adequacy and effectiveness of the net working capital management process, focusing on cash, accounts payable, accounts receivable and inventory.

- Review and assess the quality of periodic reporting of key working capital ratios and measurements, including the collection, calculation, distribution and analysis of the information.

- Benchmarking key working capital ratios and measure against organizations of similar size, industry and location.

- Assist the organization to identify possible recommendations to enhance and integrate the process over working capital management with technology.

The path forward for Internal Audit

- Thorough understanding of the organization's business structures, risk environment and processes.
- Gain insights over industry-specific best practices regarding the management of cash, accounts payable, accounts receivable and inventory.

- Ensure that the internal audit capabilities and resources have the right working capital management.

- Understand the benefits of financial technology enabled solutions in the net working capital management process.

Non-GAAP financial measure

07

Drivers

A non-GAAP financial measure is defined in Regulation G[2] of the U.S Securities and Exchange Commission (SEC) as a numerical measure of a company's historical or future financial performance, financial position or cash flows that excludes amounts or is subject to adjustments that have the effect of excluding amounts included in the most directly comparable measure calculated and presented in general or in accordance with U.S. Generally Accepted Accounting Principles (GAAP).

As part of the requirements of Regulation G, it requires companies to present a reconciliation of the non-GAAP financial measure to the most directly comparable GAAP financial measure.

The SEC has issued a series of guidance and statements to address the increase of the use of non-GAAP financial measures. In January 2019, SEC issued its first enforcement action against a company for disclosing non-GAAP financial measures without giving equal or greater prominence to its most directly comparable GAAP financial measure. More specifically, this is in relation to adjusted EBITDA, adjusted net income, and adjusted net income per share. The SEC will continue to focus on the use of non-GAAP financial measures to ensure transparency and consistency in the disclosures.

In a study conducted by Audit Analytics[3], 97% of the S&P 500 companies used at least 1 non-GAAP financial metric in the financial statements. The growing use of such measures may be linked to:

- Use of non-GAAP measures to determine executive compensation.

- Organizations believe that non-GAAP measures offer better insights into the core business earnings.

- Investors use non-GAAP measures to assist them in the evaluation of the businesses.

There are also dangers in the use of non-GAAP financial measures, especially:

- Method of calculation of non-GAAP financial measures is at the discretion of management which could result in bias perspectives due to varied adjustments used by companies in the calculation process.

- Non-GAAP measures are not covered by the external auditor's opinion.

- Increased compliance risk due to greater SEC scrutiny on non-GAAP measures and its relevant regulatory requirements.

The role of Internal Audit

- Review and assess the reasonableness of the assumptions used in the calculation process of non-GAAP financial measures.

- Assess the design and effectiveness of controls over the preparation and use of the non-GAAP financial measures.

- Assist the organization with compliance with relevant regulatory requirements over the use and publication of non-GAAP financial measures.

The path forward for Internal Audit

- Develop the relevant skill to reconcile non-GAAP financial measures to the most directly comparable GAAP financial measures.

- Understand the relevant benchmarks and assumptions used the calculation of non-GAAP financial measures in the relevant industries.

- Adopt a critical mindset to challenge the underlying assumptions used by the organizations in the preparation of non-GAAP financial measures.

[2] SEC Regulation G, https://www.sec.gov/rules/final/33-8176.htm (January 24, 2002)
[3] Audit Analytics, "Long-Term Trends in Non-GAAP Disclosures: A Three-Year Overview" (October 2018)

Data analytics and Big Data

08

Drivers

We live in a data-driven world, where data is constantly collected, aggregated and refined. With technological advances, it is essential that organizations identify the possibilities of integrating these technological capabilities into their business operations and strategies. It becomes increasingly important for organizations to adopt the use of data analytics to enhance productivity and to make smart business decisions.

With data analytics, some of the benefits may include:

- Allows for real-time and continuous monitoring of key indicators and information to identify business anomalies.

- Enable early detection of potential fraud and errors.

- Trending and analysis of data allows organizations to find opportunities in the market and to gain insights on businesses.

- Reduced costs associated with auditing and monitoring.

To unlock the full benefits of data analytics, organizations should bear in mind the following:

- Identify what information is required to meet business objectives.

- Identify relevant data required to make the required analysis.

- Obtain a comprehensive view of data by breaking out of an organization's data silos.

- Appropriate data sources are in place, especially in the areas of data integrity, accuracy, security and completeness.

- Data used for data analytics is cleaned and ready for use.

The role of Internal Audit

- Assist the organization with the creation and implementation of data analytics tools and dashboard reporting that is aligned with business needs

- Assist the organization with developing system-generated exception reporting in order to monitor key risk areas.

- Shift from traditional audit approach to a more sustainable approach by incorporating data analytics into audit methodology.

- Ensuring that audit assurances are made stronger by 'deep-diving' into the root causes and the development of appropriate recommendations.

The path forward for Internal Audit

- Refine audit programs by integrating the use of data analytics and tooling into audit methodology, ensuring that it is aligned to the relevant risk and controls.

- Gain understanding of the organization's data management system (storage, security, usage, IT applications and infrastructure).

- Develop skillsets in auditing database architectures, database setups and algorithms.

- Possess a critical mindset to question the assumptions used in the analysis of the organization.

Treasury management

09

Drivers

In the current business landscape, where constant changes are happening to disrupt the financial sector, the Treasury function has gradually evolved to take on a more strategic role. To address these challenges, organizations should consider the following developments:

- Treasury functions should be placed strategically where it can be integrated with the core business to bring about added value.

- Identify opportunities to build or implement a treasury management system where automation and robotics can be integrated to deliver insights that are aligned with business objectives.

- With continuous digitization and introduction of Financial Technology, commonly known as 'FinTech', Treasury functions should understand the impact of these technologies and help identify possible solutions for businesses to remain competitive. These technologies include Artificial Intelligence, Blockchain and Cloud solutions.

- Be aware of continuous changes to the regulatory landscape due to the technological advancements and globalization in the financial sector.

- Advancements of technology also increase the sophistication and frequency of cyber security attacks and frauds. Treasury functions, thus, should identify possible proactive solutions to prevent and disrupt these fraudulent activities.

- Changes to the political landscape bring about impacts to the organization such as tax reforms, interest rates and sanctions. It is essential for Treasury functions to be updated and ensure that the organizations are prepared and ready for these changes.

The role of Internal Audit

- Assist the organization to implement possible automation and analytics to financial processes and administration tasks.

- Assist the organization to implement a treasury management system that incorporates best practices, addressing the relevant risks and controls.

- Conduct review of the organization's financial risk management structure and financial reporting processes, ensuring that it is aligned with business objectives and strategies.

- Review cash management processes, including cash pooling and liquidity.

- Conduct a review of the adoption of new solutions such as instant payment systems to determine whether fraud and cyber risks have been adequately managed.

- Conduct compliance audits to assist the organizations to identify non-compliances with regulations.

The path forward for Internal Audit

- Be aware of the developments in FinTech and understand the relevant risks that are present in these new solutions.

- Gain expertise in financial market regulations and ensure that they are kept updated with changes to the regulations.

- Improve understanding of cyber security risks and identify possible mitigation strategies to these risks.

- Gain skillsets relevant to the assessment of new and complex technologies, which includes security and database architecture.

Enterprise Project Management

10

Drivers

The project management landscape is dynamic and fast-paced, often influenced by how the market changes. Some of the upcoming trends to be considered include:

- Advancements of technology allows organizations to leverage the use of these solutions to deliver value.

- Increase emphasis on a more collaborative approach and involvement of more stakeholders to enhance efficiency.

- Establishing Centres of Excellence to monitor the development of projects, ensuring that they are in line with strategic objectives and to develop a strategic roadmap.

- Use of data analytics to make smart and informed decisions.

Without a proper governance framework surrounding project management, may result in a lack of accountability hence exposing the organization to potential budget overruns, inefficient utilization of resources and poor quality in project delivery.

Hence, for an effective governance framework, organizations should consider the following key attributes:

- Designated roles and responsibility for the project to promote accountability for the success of the project.

- Segregation of management duties and project decision making activities.

- Clear reporting structure.

The role of Internal Audit

- Assist the organization with developing a project management framework and reporting structure.

- Perform a risk assessment on the enterprise projects, assisting the organization to identify risk events, assess the overall level of risk exposure to the project and ascertain if controls have been adequately put in place.

- Assist the organization to establish Key Performance Indicators ('KPI') as a basis of monitoring project developments.

- Conduct periodic reviews on the project to ensure that established risk appetite have not been breached and progress is in line with defined objectives and scope.

- Conduct pre and post-implementation reviews of enterprise projects providing assurances over key areas such as project costs and quality of project delivery.

The path forward for Internal Audit

- Integrate the use of data visualization tools and other technology solutions to assist the organization in executing the administrative project management functions.

- Establish a risk-based audit plan on the project objectives.

- Have a multi-disciplinary audit team in auditing project information management systems due to the complexity of projects.

- Develop skillsets in analyzing project planning and delivery in aspects such as costs, time taken and quality.

- Be well-equipped in the international standards relating to effective organizational change and project management such as ISO 21500.

11

Effective talent management

Drivers

As fresh perspectives and technologies are introduced to the business world, having the right skills becomes important for change to be brought about to the organization. In order to be future-ready, organizations are beginning to invest in human capital, in aspects such as recruitment, retention and training. Some key considerations include:

- Identify the relevant skillsets that are essential to driving change initiatives in the organization.

- More collaborative approach where there is knowledge sharing and learning within the team.

- Open, rapid and frequent performance feedbacks to assess short and long terms goals.

- Conduct benchmarking on compensation packages to remain attractive to talents.

- Develop transition strategies to manage the internal disruption to the business units.

The key challenge is to ensure that the right individuals are hired, retained, motivated and developed to help the organization achieve its business objectives.

With the integration of technology into the businesses and bringing about the Fourth Industrial revolution, there could be change resistance from within the organization. Hence, it is important for organizations to consider the following while pursuing rapid innovations:

- Talent development programs not personalized and suited for the individuals.

- Poor communication between management and staff resulting in a lack of understanding of strategic direction by the staff.

- Misalignment of resource needs due to multiple business demands.

For continuous success, organizations should leverage their human capital as a strategic asset, to develop a competitive advantage and to drive success. In doing so, organizations should also pay attention to the long term succession planning for key organizational roles.

The role of Internal Audit

- Perform a gap analysis of the HR processes and benchmark them to good practices and identify potential business process improvements.

- Assess the adequacy of the organization's succession planning for key organization roles.

- Benchmark budget and resources allocated to talent management against industry standards.

- Assist the organization to develop talent metrics that are in line with the relevant business risks.

- Assist the organization to develop a long term talent management strategic road map that is aligned with the growth of the business.

The path forward for Internal Audit

- Understand the key changes and developments to businesses in the industry and the impact on the talent management strategy.

- Ensure that the internal audit capabilities have a multi-disciplinary workforce with IT, data analytics and culture & behavior/ soft controls skillset.

- Understand the best practices in the talent management process of different industries, including the use of metrics to measure the success of the talent management program.

Trade environment and customs

12

Drivers

In recent years, there has been increasing trade uncertainty due to ongoing political and economic developments. Some recent developments include:

- US trade protectionist measures such as the introduction of trade tariffs on steel and aluminium production in the EU.

- With the UK being one of the main trading partners of the Netherlands, the completion of Brexit will ultimately have a direct impact on trading between the UK, Netherlands, the EU and other nation-states.

- The introduction of the Framework of Base Erosion and Profit Shifting (BEPS) may impact trading arrangements and multinational organizations and additional compliance costs.

- The recent escalation of the US-China trade wars may impact the global economy and affect the trade growth in the Netherlands.

The role of Internal Audit

- Perform a risk assessment of the different key trade developments i.e. Brexit, to identify the risks and impacts to the organizations.

- Facilitate internal discussions with management to and identify challenges and solutions in the trade environment that the organization face.

- Assess the readiness of the organization in the face of the trade uncertainties with the outcomes of the audit.

- Assist the organization with compliance checks against trade-related regulations including adherence to trade sanctions, transfer pricing and BEPS.

The path forward for Internal Audit

- Keep abreast of the upcoming developments and changes in the global trade environment.

- Have a multi-disciplinary team that is able to review and assess the cross-country impacts of the trade developments to the organizations.

- Identify potential opportunities arising from the trade developments that might impact the organizations.

- Develop skillsets to comprehensively assess and analyze complex global supply chain structures and evaluate the potential impacts of trade developments on the organization, especially in areas such as import taxes.

Alignment of operations to organization's strategy and objectives

13

Drivers

In recent years, businesses and organizations have been continuously disrupted. Some of the key factors include:

- Digitalization and the Internet of Things (IoT).

- Shift in focus to an agile development methodology.

- Shift in customer's preferences.

- Globalized and interconnected markets.

- Rise of other emerging economies, such as China and India.

With the constant developments, organizations need to remain adaptable to change, and ensure that their strategy remains relevant to the current and future market trends and needs.

When undergoing business transformations, organizations should look out for new risks that may surface during these transitions. They include:

- Changes to business operating models often lead to changes in business processes and new controls have to be identified in order to manage these changes.

- Integration of technological solutions into business processes increases the need for certain specific skill sets in order to lead the change.

- Ensuring that objective for the business transformation has been fulfilled and effectively carried out.

- Be mindful of change resistance faced within the organization and ensure clarity in communications.

The role of Internal Audit

- Conduct a risk assessment with senior management to understand the current risk landscape, identify the emerging risks and determine the impact on the organization.

- Establish a risk-based internal audit plan based on the risk assessment performed in order to manage key risks and activities of the organizations.

- Assist the organization during the implementation of the business transformation, ensuring that execution is in line with a defined strategy and key performance metrics are established to monitor the results and outcomes of the transformation.

- Audit the change management processes in operational areas and ensure that resources allocation is in line with the business objectives and that risks and controls are identified.

- Perform a post-mortem review upon the completion of the business transformation and monitor the effectiveness of the transformation against the defined objectives and determine the need for further actions.

The path forward for Internal Audit

- Keep abreast of recent developments in the different industries in order to be aware of emerging risks.

- Identify emerging strategies and the relevant risks that are increasingly adopted by the organizations.

- Gain relevant skillset and experience in conducting strategy audit and establishing KPI measurement and scorecards.

- Form multi-disciplinary team including technology experts in order to provide assurance to the organization with regards to business transformation.

14

Culture and behavior and Soft controls

Drivers

In December 2016, culture was introduced as a separate element in the Dutch Corporate Governance Code. This suggests the growing importance of ensuring that organizations encourage the appropriate culture and standards of integrity. This is not surprising as more often than not, it is the behavior of people that drives decision making thus influencing organizational performance and the effectiveness of the controls present.

In a model developed by Prof. Muel Kaptein, a Partner from KPMG Netherlands, there are 8 key principles in measuring and analyzing the effectiveness of culture:

- Clarity – Are the desired behavior, rules and procedures clearly communicated?

- Role Modelling – Is management setting a good example?

- Commitment – Are the members of the organization committed and motivated to follow the rules?

- Achievability – Are the activities and targets set realistic to be achieved?

- Accountability – Are the right people held accountable for their own misconduct?

- Enforcement – How do we enforce the established rules in the organization? Are desired behaviors rewarded and undesired behaviors punished?

- Discussability – Are the people able to voice their feedback in an open environment?

- Transparency – Are people's behaviors visible to others?

As part of the culture of ethics, a culture of compliance is also of equal importance. It embeds compliance into the daily business operations and workflows and helps to set the expectations of what is needed from each individual in the organization. For a successful Compliance Management System, organizations should consider the following:

- Adequate oversight from the management in setting clear policies and expectations.

- Formal compliance program with the requirements embedded in the system.

- Allows for checks and balances on the business operations.

- Takes corrective action, where necessary.

The role of Internal Audit

- Conduct an audit on soft controls in the organization and provide assurance over the current culture in the organization and its impact on the effectiveness of the controls set in place.

- Conduct a gap analysis of the organizations processes against the Anit-Bribery & Corruption Laws and Regulations.

- Identify potential fraud risk through the use of data analytics.

The path forward for Internal Audit

- Identify strategies that may assist the organization in promoting ethical behavior.

- Develop expertise in performing cross-border bribery and corruption investigations.

- Develop an analytical mindset when performing data analytics and in identifying potential fraud risk.

- Ensure that soft controls and behavior are part of the internal audit plan and execution.

Effectiveness and efficiency of operational processes

15

Drivers

Operational processes are the fundamental activities of the organization's businesses. The execution of these processes is essential to a successful business. As a response to the internal and external factors influencing the business landscape, the organization develops a response and operational processes are updated as a means to adapt to these factors. It is important for organizations to conduct a proactive, periodic review of key operational processes in order to identify inefficiencies or weaknesses.

Some common internal and external environmental factors influencing organizational processes include:

- Digital disruption (discussed in Risk 1).

- Changes to regulatory requirements to address emerging risks (discussed in Risks 3, 9, 12 and 20).

- Increased emphasis for greater collaboration amongst business units (discussed in Risk 10).

- Increased mobility of employees (discussed in Risk 11)

- Developments in organizational culture (discussed in Risk 14)

- Mergers and acquisitions (discussed in Risk 16)

- Changes in governance frameworks and methodologies (discussed in Risk 17)

- Outsourcing of key business processes (discussed in Risk 19)

The role of Internal Audit

- Conduct enterprise risk assessment to identify key risks and controls.

- Establish a risk-based audit plan based on the results of the enterprise risk assessment.

- Conduct audits on key operational processes and provide the organization with assurance over the effectiveness and adequacy of these processes.

- Conduct gap analysis of these key operational processes and to provide recommendations to improve the processes, including the expected benefits and costs involved.

- Assess the corporate governance structures of the organization and ascertain if there is adequate corporate oversight such as periodic monitoring and management reporting within the organization.

The path forward for Internal Audit

- Integrate the use of technology into the internal audit methodology i.e. data analytics and dashboard reporting.

- Keep abreast of developments in the business landscape and its relevant impact on the different industries.

- Develop understanding and knowledge in auditing organizational change and project management, such as expertise in ISO 21500.

- Have a multi-disciplinary team with experts in the field of legal, technology and operations to assist the organization in IT projects.

16
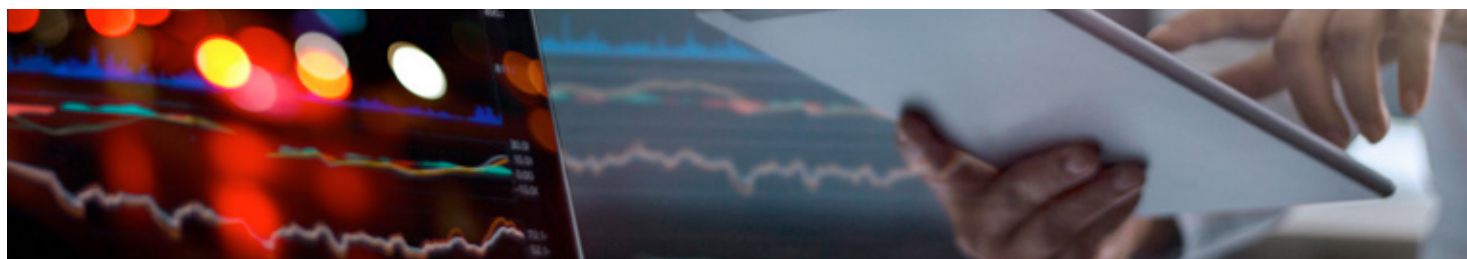
Mergers, acquisitions, and divestitures

Drivers

Mergers and acquisitions ("M&A") refers to the consolidation of businesses or assets and often requires the need for proper due diligence. Some of the reasons for engaging in M&A activities:

- Increase in market share by merging or acquiring established companies.

- Increase cost efficiency by creating economies of scale when merging operations.

- Potential tax gains in the M&A transaction.

- Access to intangible assets such as business processes, patents, trademarks and copyrights.

The benefits of M&A are often accompanied by a myriad of risks:

- Lack of synergy due to the lack of integration – structural or cultural - between the businesses.

- Inaccuracies in the valuation of assets or poor feasibility studies conducted prior to M&A.

- Legal risks arising from the M&A.

- Loss of strategic direction due to poor execution of the M&A plan.

The role of Internal Audit

- Assist the organization with the due diligence process by reviewing the control environment, internal controls and the financial information provided.

- Perform a post-mortem review upon the completion of M&A processes and assess the effectiveness and the assumptions of the M&A transaction and determine if further follow up actions are required.

- Perform a risk management exercise to determine the changes to the risk landscape of the organizations including soft controls and identify the relevant mitigating controls.

- Perform a gap analysis on the current processes of the acquired assets and provide recommendations on the future state of operations upon the completion of the M&A.

- Assess the corporate strategy process and ensure that the M&A is in line with business strategy.

- Assist the organization with the monitoring process and ensure that execution of the M&A is in line with the established milestones.

The path forward for Internal Audit

- Multi-disciplinary team comprising of tax experts, legal experts and auditors to assist with the due diligence process.

- Gain skillset to conduct strategy audit, including providing recommendations relevant to the specific industry.

- Ability to assess and identify business areas where there are opportunities for increased collaboration between the business operations and also key integration risks for enhanced monitoring.

- Ability to understand the risks associated with emerging markets and identify the impacts that it might have on the organization.

Integrated enterprise risk management and monitoring

17

Drivers

As the business landscape continues to evolve, business risks get more multifaceted, more complex and more interconnected. This increases the need for a more dynamic risk assessment process which allows for a more holistic view of risk. It also emphasizes the need for organizations to have a more collaborative approach throughout the business units in order to manage the risks.

A dynamic risk assessment process should contain the following:

- Aligning the risk management process with the business strategy.

- A standardized risk management framework which includes risk appetite and risk threshold to assess risk ratings.

- A centralized risk reporting mechanisms to allow for the escalation and reporting of key risks.

- Identify the risk interconnectivity among the identified risks to assess the overall level of impact to the organization.

- Assigning the relevant risk owners to the identified risks.

- Creating risk metrics and to monitor the risk development.

In the traditional approach of internal audit, where an annual risk assessment is conducted to establish the organization's risk-based internal audit plan. With dynamic risk assessment, this represents a continuous risk monitoring process and brings about greater value for the organization.

Some of the key challenges to an effective integrated enterprise risk management process:

- Costs involved in the integration of systems and information.

- Lack of cross-organization collaboration due to the teams working in silos.

- Lack of risk awareness in the organizational culture.

- Difficulties in identifying and forecasting critical risks that are most impactful to the business strategy.

The role of Internal Audit

- Provide training to the organization to assist in the development of a risk-aware and risk-engaged culture, taking into account the root causes of the relevant shortcomings.

- Assist the organization to develop the risk management framework, including the risk appetite statement, risk threshold and risk metrics.

- Facilitate risk workshop as part of an enterprise risk management process to assist the organization to identify the key risks.

- Assist the organization with the dynamic risk assessment framework to align risk management with business strategy.

- Develop centralized risk reporting mechanisms such as thematic reports or technology-enabled dashboard reporting.

The path forward for Internal Audit

- Develop leading risk indicators relevant to the specific industry to assist the organization with the risk management process.

- Gain skillset relevant to the execution and implementation of dynamic risk assessment framework, including the relevant technological expertise.

- Be aware of risk management frameworks and international standards (e.g. COSO Enterprise Risk Management (ERM) Integrated Framework, ISO 31000).

IT governance

18

Drivers

An effective IT governance framework ensures that the organization's IT management and control framework is aligned with its business strategy, objectives and goals.

According to the International Standard for the Corporate Governance of Information Technology ISO 38500, there are 6 key principles of an IT Governance framework:

- Responsibility – Each member of the organization is responsible for the appropriate use of IT and this should be clearly allocated.

- Strategy – The use of IT should be aligned with the business strategy and requirements.

- Acquisition – In acquiring the systems, organizations should consider the feasibility, risk and cost involved as well as the extent of adoption of technology in its business.

- Performance – To ensure that IT systems are well utilized, the growth of these systems should be in tandem with business growth.

- Conformance – IT controls should be established and clearly communicated.

- Human Behavior – Effectiveness of IT governance is also influenced by the characteristics and needs of the stakeholders involved.

Technology will continue to advance and the use of IT systems will be even more prevalent in the future. It is essential for organizations to have awareness. One of the most widely deployed IT governance control frameworks, Control Objectives for Information and related Technology (COBIT®), provides guidance to assist organizations in the areas of regulatory compliance, IT risk management, alignment of IT with business needs, resource management and performance management. There are also other standards available, such as IT Governance Institute (ITGI), ISO 17799 for security or the IT Infrastructure Library (ITIL).

The role of Internal Audit

- Perform a gap analysis of the IT controls and ensure that it is in line with business needs and relevant regulations.

- Benchmark the organization's IT governance framework against established standards and identify possible recommendations.

- Audit the level of service delivery and ascertain if it is in line with business strategy and requirements.

- Assist the organization to perform a risk assessment of the IT systems and ascertain if key risks have been identified and relevant controls are in place.

- Assist the organization to develop IT metrics that measure the performance level of IT systems.

The path forward for Internal Audit

- Gain thorough understanding of the different IT governance frameworks as well as the application of such frameworks in the different industries.

- Develop skill sets to ascertain the level of maturity of IT governance across the organization, from management to executive.

- Keep abreast of technological changes and identify if they may bring enhancements to the organization.

- Be aware of the interaction between these technological changes and 'the human factor'.

- Gain expertise in the different international regulations that may influence the implementation of IT Governance frameworks.

Outsourcing and managing third-party relationships

Drivers

Third-party risk management has grown in importance over the years as organizations choose to outsource their business functions to third-party vendors. For example, organizations have turned to Shared Service Centres ("SSC") to execute specific administrative and operational tasks. This allowed organizations to concentrate on corporate governance and strategic activities without compromising on the quality of their internal processes.

This increases the exposure of organizations to new risk areas surrounding outsourcing and third-party relationships. Such key risk areas include:

- Loss of control over quality standards and process technologies and/or improvement.

- Potential losses of information confidentiality as third parties are granted access to organization data and networks.

- Hidden costs in the outsourcing arrangements due to inaccurate assumptions or unexpected costs.

- Complexity of outsourcing or third party arrangements and uncertain regulatory landscapes due to more sophisticated nature of services being outsourced.

- Geolocation of the outsourced location may bring about other risks such as language barriers, differences in organizational culture, additional regulatory compliance and political uncertainty.

For effective third-party management, an organization should consider the following:

- Improve monitoring mechanisms to include ongoing monitoring of third-party relationships and contract performance.

- Establish escalation procedures to detect and report of contract failures with third-party vendors.

- Tight budget monitoring of outsourced arrangement.

The role of Internal Audit

- Conduct a review of the selection of vendors, including the due diligence processes and evaluation of the vendors against preset criteria.

- Assist the organization to establish a contract management framework, scorecards to monitor third-party relationships on an ongoing basis, and comprehensive overview of all the outsourcing arrangements, including all the contractual obligations and regulatory requirements.

- Assist the organization to conduct a risk assessment of all the outsourcing arrangements and ascertain if key risks have been identified and addressed.

- Conduct a review of the service delivery process, ensuring that key strategy and key milestones have clearly established.

- Conduct a post mortem review to ensure that service delivery is in line with the initial strategy.

- Conduct a contract compliance review of the outsourced vendor's contract against delivery standards.

The path forward for Internal Audit

- Identify automated, end-to-end work flow solutions to assist organizations with contract management and contract compliance.

- Gain understanding over technology advancements such as smart contracts that are relevant to contract management.

- Gain expertise in assessing the maturity level of the implementation of outsourced arrangements.

- Understand the best practices of the different nature of outsourced arrangements, including SLA measurements, costs and processes.

- Multi-disciplinary team with the ability to perform third-party audits depending on the nature of the outsourced arrangement.

Tax compliance

20

Drivers

Tax change has been an important agenda in the Netherlands recently, with the Dutch position previously seen as a tax avoidance centre. With anticipated tax changes in the upcoming years, it becomes increasingly complex for organizations to ensure compliance with and address the changes to the regulations. Some of the international and domestic highlights include:

- Led by OECD, Base Erosion and Profit Shifting (BEPS) reforms have been introduced to enhance transparency in tax matters. An example includes the OECD country-by-country reporting implementation package that requires certain companies to maintain a master and local files containing information on transfer pricing and other information of intragroup transactions.

- European Union Anti-Tax Avoidance Directive to address issues on tax avoidance is to be implemented by all EU member states into domestic law no later than 31 December 2019 which may have far-reaching impacts on businesses.

- In November 2018, tax rulings resulted in more stringent requirements for international organizations. This change serves to enhance the transparency and integrity of the tax rulings for businesses and is effective from 1 July 2019.

- 2020 Dutch budget including tax reforms have been submitted by the Dutch Ministry of Finance for confirmation. These reforms are expected to come into force on 1 January 2020.

The role of Internal Audit

- Assist the organizations to establish tax risk assessment and tax control frameworks to ensure compliance with tax regulations.

- Assist the organizations to define tax governance structure, including the clarity and allocation of roles and responsibilities with respect to tax reporting.

- Assist the organizations to understand the impacts resulting from the tax changes and to identify possible solutions to address these changes.

- Conduct tax compliance audits to assess key controls and to identify further recommendations with respect to key tax legislation and reporting of taxes.
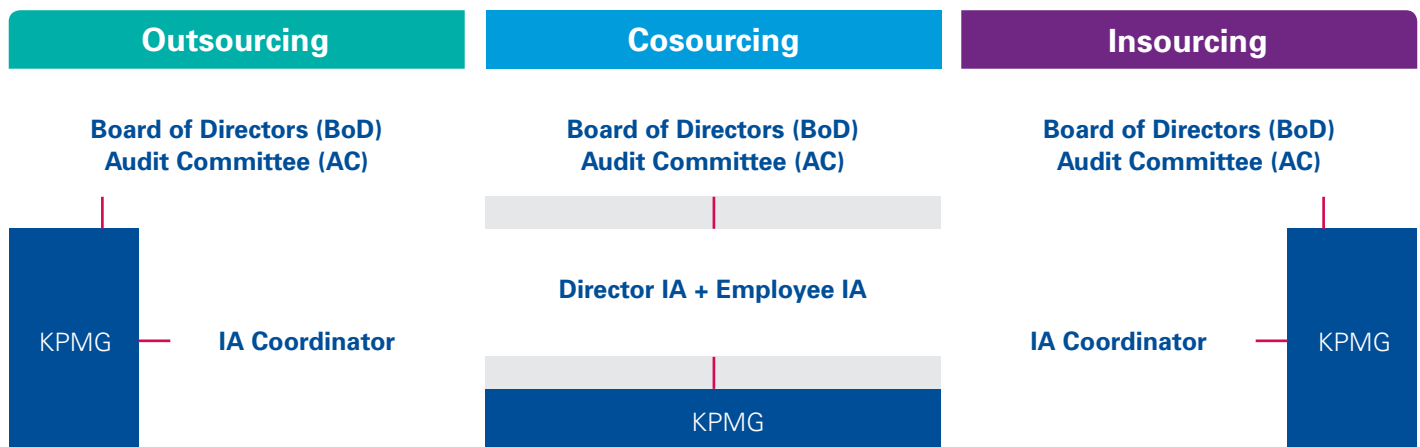
The path forward for Internal Audit

- Keep abreast of the changes and updates to the tax regulations and its impact on the businesses.

- Ability to apply tax knowledge and offer solutions to organizations with complex organizational structures operating in multiple tax jurisdictions.

- Ability to conduct business process analysis and supply chain mapping in order to understand the impact of BEPS to the organization.

- Gain expertise on tax structures and understanding in certain industries in order to assist with the benchmarking of key tax practices.

- Ability to audit local tax returns of the organization vs. local tax law (i.e. VAT, income, fringe benefits etc.).

KPMG as Internal Audit partner

Forms of cooperation with KPMG

Outsourcing	Cosourcing	Insourcing

Board of Directors (BoD)
Audit Committee (AC)

KPMG — IA Coordinator

Board of Directors (BoD)
Audit Committee (AC)

Director IA + Employee IA

KPMG

Board of Directors (BoD)
Audit Committee (AC)

IA Coordinator — KPMG

In the **Outsourcing model**, KPMG assumes the role of the Internal Audit function and works closely together with the IA coordinator and the Audit Committee.

In the **Co-sourcing model**, KPMG acts as an extension of the in-house Internal Audit function, works together with the IA employees and reports to the head of IA.

The **Insourcing model** means that the Internal Audit function consists of its own employees and is supported by KPMG with subject matter specialists' knowledge on an ad hoc basis.

Characteristics of Outsourcing

- Variable costs, great flexibility
- Quick responsiveness
- Access to best practice
- Access to specialists and newest technology
- Access to global network
- More cost-effective for small- sized Internal Audit functions

Characteristics of Co-sourcing

- Partial variable costs, medium flexibility
- Access to global network
- Requires an Internal Audit with the necessary critical mass
- Access to specialists

Characteristics of Insourcing

- Fixed costs, little flexibility Control and execution remain in-house
- Integrated in the company on an ad-hoc basis
- Specialists and technologies are not included

Whether you opt for an Outsourcing, Co-sourcing or Insourcing solution, we can provide the following services:

- Act as sparring partner for all issues related to the role, position and audit agenda of the Internal Audit function.
- Support all process steps of an Internal Audit function, from planning to execution of audits, reporting and tracking.
- Provide specialists (e.g. compliance & legal, IT systems, risk management, treasury, tax, security) with deep understanding of your business and processes.

- Offer worldwide local support with specific language skills and knowledge regarding local regulatory requirements.
- Provide the latest audit methodology (KPMG Internal Audit methodology, DA, Internal Audit tools).
- Provide access to best practice and benchmarking.

Through our proven methodology, our experience and extensive expertise, we are the right partner for you to fully exploit the potential of your Internal Audit

KPMG NL
Laan van Langerhuize 1
1186 DS Amstelveen
Postbus 74500
1070 DB Amsterdam

Contact

Bart van Loon
Partner, Internal Audit,
Risk and Compliance Services
T: L+31 6 532 493 28
E: VanLoon.Bart@kpmg.nl

Huck Chuah
Partner, Internal Audit,
Risk & Compliance
T: +31 6 463 660 13
E: Chuah.Huck@kpmg.nl

Samantha Yeo Shi Yun,
Senior Consultant,
Internal Audit, Risk & Compliance
T: +31206 567395
E: YeoShiYun.Samantha@kpmg.nl

www.kpmg.nl

Top 20 risks in Internal Audit before 2020 November 2019