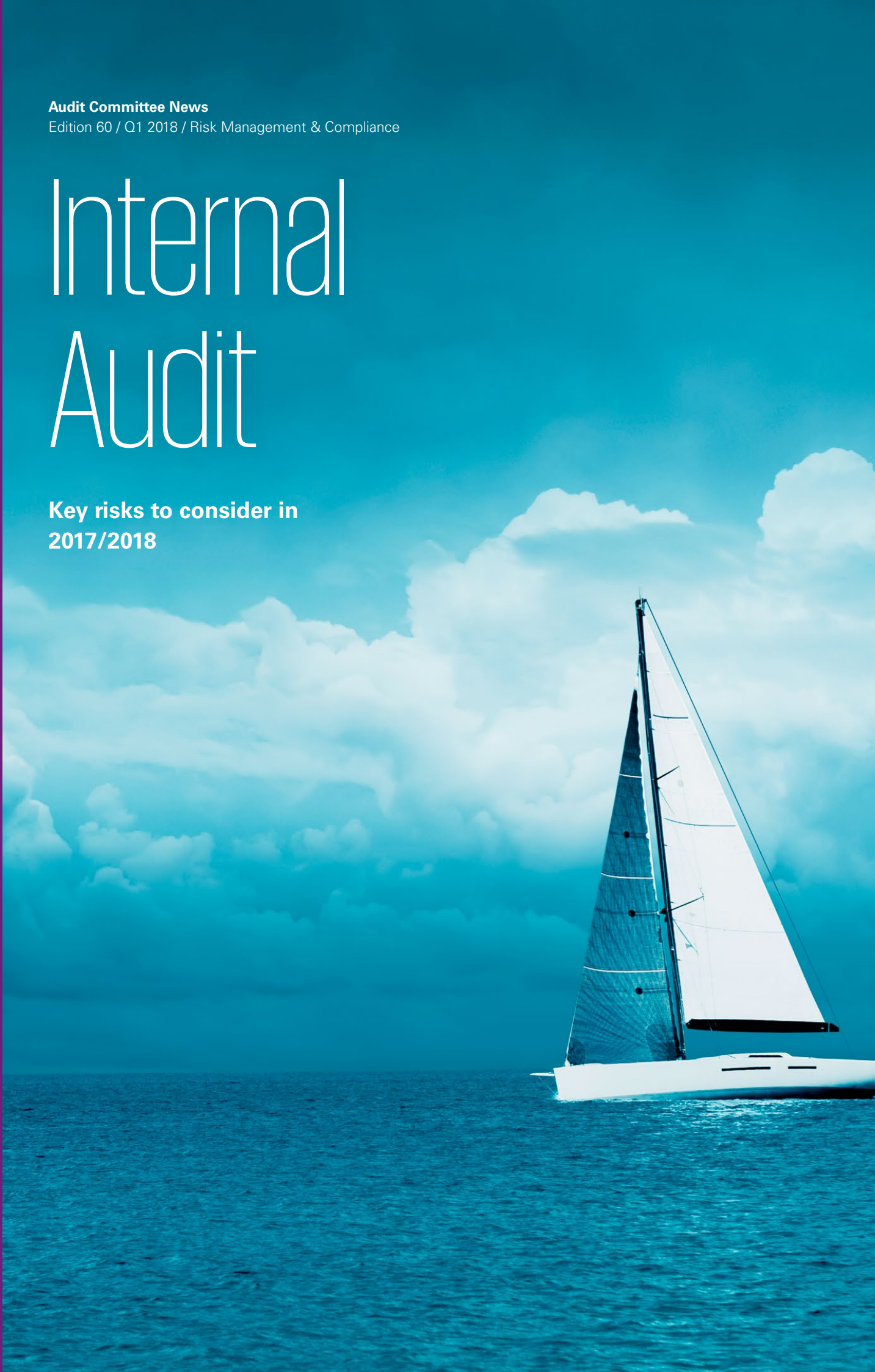
Audit Committee News
Edition 60 / Q1 2018 / Risk Management & Compliance

Internal Audit

Key risks to consider in 2017/2018



The Internal Audit (IA) function is required to provide assurance to the Board of Directors, the Audit Committee and Executive Management that the key risks within the organization are effectively mitigated by the organization's control environment. Therefore as part of the strategic planning process, the IA function must identify the key risks within the organization, assess how well they are managed and the level of assurance that can be provided. Based on our experience and numerous interviews with key stakeholders, this article outlines what we consider to be the key risks that many organizations face today and how IA can assist in the mitigation of these risks.

Traditionally, IA functions have focused on topics related to internal control systems (ICS) and compliance and only provided limited insights on the broader existing and emerging risks within the organization. Changes to the traditional paradigm of the IA function have led to a more modern approach to the identification of key risks and also changed the focus and activities of the IA function in order to address these key risks.

Today, a modern IA function must have a broad awareness of the key risks and opportunities faced by the organization, and use this understanding as additional context when reviewing the processes, organizational culture, corporate governance and controls of the organization.

This will allow the IA function to assist the organization in efficiently and effectively allocating resources to mitigate risks and further develop their strategic role. This article highlights selected key risks that IA should consider in the development of the annual strategic audit plan[1].

It is designed to provoke thought and challenge and also facilitate brainstorming sessions amongst Members of the Board, Audit Committee, Executive Management and Internal and External Audit within an organization during their annual audit planning process.

It aims to assist in broadening the discussion on key risks and enhancing the strategic value of governance functions such as IA to ensure that key and emerging risks are captured within their review. This way IA can assist the organization in mitigating key risks effectively whilst also seizing new opportunities as they emerge.

- Cybersecurity: Cybersecurity continues to frequently appear at the top of many board agendas with data security breaches now appearing in the headline news on almost a daily basis. The capabilities and techniques used by hackers are continuously expanding and evolving, particularly in their ability to target specific information or individuals.

  The IA function should consider performing a risk and readiness assessment of the organization's cybersecurity processes with reference to best practice, conduct penetration testing of selected IT assets (preferably with a skilled outsourced service provider) and assess implementation of revised cybersecurity models and counter measures.

- Data protection and privacy: The General Data Protection Regulation (GDPR) (Regulation 2016/679 EU) is the biggest and most impactful change on privacy and data protection in recent history and introduces a range of new requirements for organizations in relation to data protection. As a result, organizations need to demonstrate continuous data protection compliance including for example: reporting of data breaches, introduction of a data privacy policy, appointment of data protection officers etc. The potential impact of the GDPR on the organization's bottom line can include fines as high as 4 percent of global turnover and greater exposure to reputational risks.

  The IA function should consider assessing the potential impact of the GDPR on the organization through performance of a Data Protection Impact Assessment (DPIA); reviewing the current degree of data protection compliance and areas for improvement and evaluating the organization's GDPR compliance roadmap to determine whether the plan is adequate for the organization to become compliant.

- Management of third-party relationships and risks: To improve productivity and efficiency, organizations increasingly rely on third parties to carry out vital business functions through outsourcing agreements. However, third party relationships expose organizations to new risks and potential compliance failures that may result in fines, lawsuits, operational bans or reputational damage. Additionally, third parties are often granted access to organization networks, thereby further increasing the potential for data security breaches.

[1] For a comprehensive list of key risks to consider for the strategic internal audit plan 2017/2018 refer to the following KPMG publication: https://assets.kpmg.com/content/dam/kpmg/ch/pdf/key-risks-internal-audit-en.pdf

The IA function should consider assessing their third-party selection and due diligence processes; evaluating contract management processes to monitor third-party relationships and contract fulfillment and reviewing third-party compliance with generally accepted standards and regulations (e.g. supplier audit).

- Governance, ethics and integrity of the organization: The average cost related to the resolution of a Foreign Corrupt Practices Act (FCPA) matter was more than $80 million in 2013, representing fines, penalties, disgorgement and prejudgment interests from both the US-Justice Department and the Securities and Exchange Commission (SEC). Viewed in this context, it is clear why organizations have focused their attention on understanding their exposure to bribery and corruption and evaluating their existing compliance programs.

  The IA function should consider conducting a gap analysis of the organization's existing anti-bribery and corruption procedures in comparison to leading practice or regulatory guidance (e.g. ISO 37001), assessing the design and operating effectiveness of the organization's preventative and detective controls, providing subject matter specialists to investigations involving potential non-compliance and performing ongoing periodic audits to maintain an ISO 37001 certification.

- Alignment of operations to the organization's strategy and objectives: Multiple triggers including globalization of markets, digitalization, Economy 4.0 and the Internet of Things are driving widespread business transformation. In a dynamic economy, organizations need to become increasingly adaptable to change and constantly assess new risks and implement or amend controls to effectively mitigate new risk exposures. Often strategic change can neglect adequate revision of internal controls, bringing IA into a unique perspective to link both worlds and ensuring a continuing effective corporate governance structure.

  The IA function should consider performing audits over the process of strategy development, e.g. the degree to which strategy is translated into objectives and key performance measures and also evaluate whether delivery has resulted in the desired performance and results. Furthermore IA can review change management processes in operational areas that are heavily impacted by business transformation.

- Effective talent management: The search for future talents and highly skilled subject matter specialists is challenging. Organizations are investing heavily in recruitment and retention programs in order to develop and maintain an effective pipeline of talented individuals.

  The IA function should consider performing a review of the design, organizational set-up and effectiveness of the talent pool/learning and development programs; performing an audit of the recruiting and hiring procedure and evaluating the efficiency of HR processes in general.

Cyber security, data protection and privacy, third party relationships, governance of ethics and integrity as well as alignment with the organization's strategy and effective talent management are but a few of the trending topics that can represent significant risk and under-utilized opportunities within the organization.

The annual strategic audit planning process presents an opportunity to draw focus upon such topics and evaluate whether opportunities have been fully exploited, risks have been appropriately mitigated and adequate resources have been allocated.

Luka Zupan
Internal Audit, Risk and
Compliance Services (IARCS)
lzupan@kpmg.com

Stephanie Föhn
Internal Audit, Risk and
Compliance Services (IARCS)
sfoehn@kpmg.com