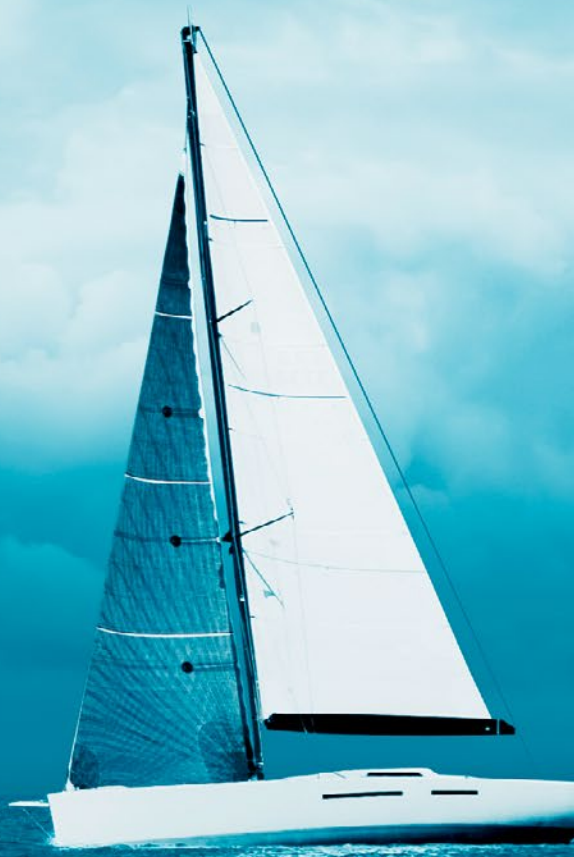
KPMG

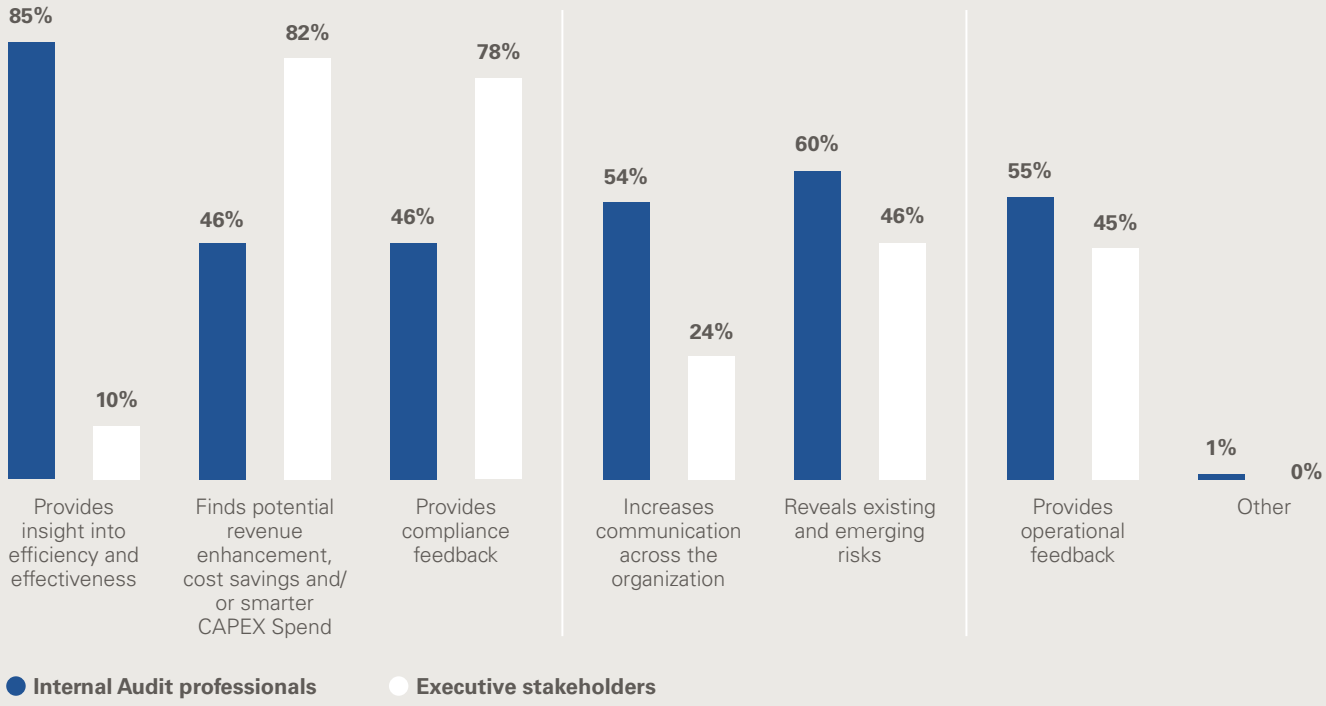
Key risks for Internal Audit

16 key risks for Internal Audit
to consider in 2017/18



kpmg.ch

Survey highlighting the differing perceptions of Internal Audit within organizations



The Strategic Role of IA

Recent studies highlighted a general misperception regarding the role of Internal Audit (IA) within organizations. Traditionally, IA functions have mostly focused on topics related to compliance and internal control systems (ICS). Adding value and providing insights on the key risks of an organization has typically not been a key priority of IA.

A modern IA function should understand the organizations key risks and proactively identify emerging risks in order to add value to the organization. This allows IA to assist the organization in efficiently and effectively allocating resources to mitigate risks and further develop their strategic role.

This publication highlights key risks that IA should consider in the development of the annual strategic audit plan. It will help IA to prioritize topics and will further enhance IA's role as a strategic and value-adding business partner within the organization.

In order to select the key risks that matter to the organization and further develop their strategic role within the organization, IA should:

- **Understand key business matters**
  IA is required to have a deep understanding of the business strategy and operations across all levels of the organization. Once this is achieved, IA can use its expertise to identify key emerging risks, educate the business and partner with them to take advantage of any opportunities.
- **Leverage technology**
  IA must adapt their methodologies to increasingly utilize technology in the execution of their audits. This will not only provide efficiency gains in delivery of IA but also provide deeper insights to the business, further developing the value perception and credibility of IA.
- **Ensure that IA activities create business value**
  IA must ensure that their activities not only provide assurance but also deliver insights to the business which may be leveraged to improve the business processes or gain a competitive advantage.

Top 16 risks in 2017/18

1. Cybersecurity
2. Regulatory compliance
3. Governance, ethics and integrity of the organization
4. Effectiveness and efficiency of operational processes
5. Management of third-party relationships and risks
6. Mergers, acquisitions, and divestitures
7. Alignment of operations to organization's strategy and objectives
8. Integrated enterprise risk management and monitoring
9. Data analytics and mass data usage
10. Effective talent management
11. IT governance
12. Organization-wide initiatives/projects
13. Data Protection and Privacy
14. Outsourcing
15. Tax Compliance
16. Trade Environment and Customs

1 Cybersecurity

Drivers:

- Avoiding costly consequences of data breaches such as investigations, legal fines, liability for customer losses, remediation efforts, inefficient use of executive and mid-level time and attention, and potential loss of new or existing business.
- Preventing reputational damage to the organization, especially with regards to lost customer data.
- Ensuring the security of capital, intellectual property and other privileged organization information.

In today's world of constant connectivity, cybersecurity is a key focal point for many organizations. Cybersecurity frequently appears at the top of many board agendas with data security breaches now appearing in the headline news on almost a weekly basis. There are several factors driving the increased focus on cybersecurity including rapid technological change, changing regulatory environments, an increased number of cybersecurity threats and significant social and corporate change. The capabilities and techniques used by hackers are continuously expanding and evolving, particularly in their ability to target specific information or individuals.

New methods (i.e. ransomware such as Petya) are constantly being developed by increasingly sophisticated and well-funded hackers. In recent times, these hackers not only target organizations through networks directly but also through connections with key suppliers and technology partners. The consequences of cybersecurity breaches can be disastrous to an organization's bottom line and reputation. For this reason, it is critical that all organizations remain vigilant in their management of cybersecurity and continue to implement contemporary practices.

How Internal Audit can help:

- Perform risk assessment of the organization's cybersecurity processes with reference to best practice industry standards, and provide process improvement recommendations.
- Conduct penetration testing of selected IT assets.
- Review existing processes to assess whether management has considered the key threats posed by the constantly evolving IT environment.
- Assess implementation of revised cybersecurity models, such as multi-layered defense mechanisms, enhanced security breach detection and data encryption methods.
- Evaluate the ability of third-party security providers to adequately address emerging cybersecurity risks.

What is needed by Internal Audit:

- Sound understanding of the organization's cybersecurity concept and design, including future IT security strategy.
- Expertise in auditing IT systems from a security perspective, including data security, network security, access management etc.
- Sound understanding of third-party IT dependencies and expertise reviewing third-party cybersecurity providers including Service Level Agreement (SLA) contracts, procurement procedures and any additional control systems applicable to third-party providers.
- Knowledge of good practice in cybersecurity and general IT related processes.
- Ability to conduct penetration testing of key systems to identify potential IT control weaknesses.

2 Regulatory compliance

Drivers:

- Ensuring compliance with a number of regulations, both domestically and abroad.
- Controlling the costs of complying with a growing number of regulations e.g. forthcoming EU General Data Protection Regulation (GDPR) in May 2018.
- Developing a strategy to minimize the burden of compliance activities on business operations.
- Ensuring the alignment of compliance operations following a merger or acquisition.

Organizations, regardless of industry, are being inundated with new regulatory requirements, both domestically and abroad. These new regulations place growing pressure on Executive Management and their employees, increasing the possibility that certain compliance requirements may be unintentionally missed.

Additionally, complying to the growing number of regulations increases compliance costs and adds complexity to the internal organizational governance and controls structure.

In cases of mergers and acquisitions, compliance functions require alignment and consolidation to ensure a holistic and effective approach to integrated corporate compliance.

How Internal Audit can help:

- Perform an inventory over existing regulatory bodies and their requirements applicable to the organization.
- Assess the organization's approach to managing its global compliance activities, including integration of newly acquired organizations.
- Evaluate the organization's response to any notable instances of non-compliance.
- Review compliance training programs offered to employees and other stakeholders and evaluate appropriateness for the respective role and geography.

What is needed by Internal Audit:

- Sound understanding of internationally applicable compliance frameworks and assurance standards (e.g. ISO 19600, ISO 37001, COSO) as well as any additional internal, local or global regulatory requirements (e.g. Sunshine Act, Dodd-Frank Act, EMIR, REMIT).
- Expertise in auditing compliance management systems and drawing comparisons to good organizational business practices.
- Ability to assess the content and delivery structure of any internal or external compliance training programs and tools.

3 Ethics and integrity of the organization

Drivers:

- Limited effectiveness of existing anti-bribery and corruption compliance activities in eliminating such activities.
- Emerging regulatory and compliance risk introduced to the organization by various factors such as organic expansion into new markets, dealings with third parties or business acquisition.
- Introduction of ISO 37001 which is the first international standard on bribery management, designed to help organizations prevent, detect and respond to bribery.

According to some estimates, the average cost related to resolution of a Foreign Corrupt Practices Act (FCPA) matter was more than $80 million in 2013, representing Justice Department and Securities and Exchange Commission fines, penalties, disgorgement, and prejudgment interest. 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 benefits of an effective anti-bribery and corruption compliance program can be: full commitment from and endorsement by Executive Management to eliminate anti-bribery and corruption; clearly defined and documented policies on prohibited activities; periodic compliance training; and audit clauses in third party agreements.

Each program element contributes to the deterrence of bribery and corruption, thereby reducing the risk of costly and disruptive enforcement activity. Should the unthinkable occur, a well-designed and executed anti-bribery and corruption compliance program may be the difference between a prosecution and a non-prosecution agreement and may even reduce the severity of penalties incurred.

How Internal Audit can help:

- Conduct a gap analysis of the organization's existing anti-bribery and corruption procedures in comparison to leading practice or regulatory guidance.
- Provide assurance regarding the design and operating effectiveness of the organization's preventative and detective controls related to anti-bribery and corruption.
- Enhance internal audit 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.
- Provide subject matter specialists to investigations involving potential non-compliance.
- Drive continuous improvement by assessing the organization's anti-bribery and corruption program.
- Conduct reviews of the organization's anti-bribery management system to strive for ISO 37001 certification.
- Perform ongoing periodic audits to maintain the ISO 37001 certification.

What is needed by Internal Audit:

- Sound understanding of the organization's governance structure and ethical framework (using standards such as ISO 37001, ISO 19600 and the Swiss Criminal Code).
- Expertise in assessing strategies that support managerial responsibility for ethical behavior.
- Expertise in performing cross-border bribery and corruption investigations.
- Ability to perform data analytics and third-party audits to provide assurance and identify areas for continuous improvement.
- Assessment of business-driven fraud risk management processes.

4 Efficiency and effectiveness of operational processes

Drivers:

The efficiency and effectiveness of operational processes is often key to the successful execution of an organization's strategy. However as an organization develops and evolves in response to the pressures of it's internal and external environment, so do its operational processes. Without a proactive, periodic review of key operational processes, inefficiencies within these processes may develop over time.

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

- Changes to regulatory requirements (see Risk 2);
- Mergers and acquisitions (see Risk 6);
- Geographic expansion;
- Changes to organizational governance structures or frameworks (see Risk 7);
- Increased mobility of employees (see Risk 10);
- Outsourcing of key business processes (see Risk 14);
- Digital transformation (Industry 4.0) and increasing automation of manual processes; and
- Greater interdependency of business units (see Risk 12).

How Internal Audit can help:

- Perform a detailed process review, including the identification of key risks and controls, possible pain points and improvement opportunities.
- Document and analyze the process control environment to evaluate the efficiency and effectiveness of the control framework in relation to the key risks of the organization.
- Based on independent assessments, provide management with suggestions on prioritizing improvement opportunities, expected benefits and implementation efforts/costs.
- Facilitate workshops with employees to discuss the organization's risks, controls, and better practices to support consistent application of corporate policies and procedures.
- Review corporate governance structures including periodic monitoring and reporting within the organization to assess whether adequate corporate oversight exists.

What is needed by Internal Audit:

- Sound understanding of the organization's operating structure, processes, culture and external environment.
- Excellent knowledge of industry-specific legal and regulatory requirements.
- Expertise in value-chain-based auditing of organizational processes and procedures.
- Experience in application of Lean and Sigma Six methodologies in large and complex organizations.
- Expertise in effective organizational change and project management, including ISO 21500.
- Expertise in design and implementation of IT automation projects.
- Experience in business process analysis including effective use of data analytics and benchmarking.

5 Management of third-party relationships and risks

Drivers:

To boost productivity and efficiency, organizations are increasingly relying on third parties to carry out vital business functions. However, third party relationships expose organizations to new risks and potential compliance failures that may result in fines, lawsuits, operational bans or reputational damage.

Such compliance failures may occur due to complexity of the agreement itself or the business environment that the organization operates in. Additionally, third parties are often granted access to organization networks further increasing the potential for data security breaches.

Third parties may also grant network access to subcontractors who have suboptimal business and compliance practices, further jeopardizing data security.

Finally, third parties may operate in areas of political uncertainty increasing the severity and broadening that nature of risks that the organization is exposed to.

In the context of these risk exposures, organizations need to implement controls to adequately mitigate these risks in order to effectively benefit from its third parties relationships:

- Increasing oversight of third-party relationships.
- Enhancing cost reduction.
- Improving contract governance.
- Creating more effective contractual self-reporting processes.
- Ensuring timely detection of risk management failures occurring within third-party business partners.

How Internal Audit can help:

- Review the third-party selection and due diligence processes.
- Assess the on- and off-boarding processes and controls.
- Evaluate contract management to monitor third-party relationships and contract fulfillment.
- Monitor regulatory developments related to third parties.
- Review inclusion and consistency of right-to-audit clauses in third party agreements.
- Review third-party compliance with generally accepted information security standards.
- Advise management on the development, implementation and calibration of a continuous monitoring system for self-reported data from third-party providers.

What is needed by Internal Audit:

- Expertise in auditing third-parties and supply chain management processes including assessing the level of compliance with local laws and corporate regulations.
- Comprehensive understanding of the organization's third party relationships including contractual obligations and regulatory requirements.
- Sound understanding of local customs and practices as well as experience in comparing local practices to regulatory standards.
- Capability to perform third party audits (e.g. visiting production sites abroad, comparing third-party compliance standards to the organization's corporate regulations).

6 Mergers, acquisitions, and divestitures

Drivers:

Business today is under strong pressure to deliver sustainable results to all stakeholders. One option for an organization to create value is to engage in M&A activities. This encompasses the buying, selling, partnering or funding of business components and emphasizes the need for proper due diligence. It also highlights the importance of implementing effective integration mechanisms to extract the most value from each transaction.

Additional drivers of this key risk may include:

- Impact of M&A and divestiture activities on other parts of the organization;
- The need for a rigorous and consistently executed M&A program to proactively identify and manage risks, e.g. addressing transaction risk prior to shareholder announcement.
- Effective execution planning, timely delivery and performance monitoring throughout the M&A process.
- The possible impact of the integration (or carve-out) processes across all key functions.

How Internal Audit can help:

- Perform "post mortem" reviews on historical transactions to evaluate the effectiveness of the M&A process.
- Assess the proper use and completeness of due diligence checklists regarding financial information and internal controls (e.g. quality of earnings and assets, cash flows, unrecorded liabilities etc.).
- Identify internal control gaps in newly acquired organizational assets and the future state of the business combination.
- Assess the implications of implementing business process change as a result of M&A or divestiture activity on the existing control environment.
- Assess the process for ongoing risk and control assessment during the M&A or divestiture process.

What is needed by Internal Audit:

- Specialized financial, operational and compliance knowledge related to due diligence process.
- Sound understanding of the type of risks faced when acquiring, merging or splitting an organization.
- Ability to identify and assess business areas where integration risks exist and direct focus for future audit work.
- Expertise in assessing the tax related financial impact and the impact of valuation and accounting standards based on local GAAP or applied GAAP.
- Ability to evaluate integration processes including auditing of the effectiveness and efficiency of project management, information systems, communication lines, project planning, and issue escalation.

7 Alignment of operations to organization's strategy and objectives

Drivers:

Recent times have seen widespread business transformation due to the convergence of multiple triggers including:

- Increasingly globalized markets;
- Digitalization, Economy 4.0 and The Internet of Things;
- Major slowdowns of Western economies;
- Entry of new market competitors with innovative business models; and
- Increasing challenges of regulatory compliance.

In the dynamic modern economy, organizations need to be increasingly adaptable to change, constantly analyzing their strategy in order to ensure that they are adapting to the current and future market trends and remain fully aligned to their customers needs.

Significant business transformation also impacts the strategy and operations of an organization, prompting a need to assess new risks and implement or amend controls to effectively mitigate new risk exposures.

Often efforts to bring about strategic change can neglect adequate revision of 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 and implementation of business transformation projects.

How Internal Audit can help:

- Assess whether resource allocation is aligned with key strategic objectives and initiatives of the organization.
- Perform audits over the process of strategy development e.g. evaluate strategy formulation, the degree to which strategy is translated into objectives and key performance measures and evaluate whether delivery has resulted in the desired performance and results.
- Review change management processes in operational areas that are heavily impacted by business transformation and may not typically be associated with the IA function e.g. IT and data management and business as usual processes.
- Participate proactively in Enterprise Risk Management (ERM) activities with Executive Management and Risk Management in order to provide insights into emerging strategic and operational risks and determine a plan for integration into the annual audit plan if necessary.

What is needed by Internal Audit:

- Sound understanding of the organization's mission statement, strategy and objectives.
- Expertise in auditing process re-engineering and change management as well as performance management programs (use of KPIs, balanced scorecards etc.).
- Access to subject matter specialists from key transformation areas e.g. IT or experts in change management itself.
- Expertise in strategy process auditing including assessment of strategy development processes and KPI measurement.

8 Integrated enterprise risk management and monitoring

Drivers:

In the past, an annual risk assessment conducted by the IA function would establish an organization's IA plan for the coming year. However this overlooks various other risk monitoring functions that also conduct risk assessments throughout the organization leading to a constantly evolving corporate risk register. In light of this, organizations have recognized the need for an increasingly integrated view of risk, which should be informed by a coordinated risk identification exercise.

To ensure a coordinated effort, the following components are needed:

- A common risk language including issue ratings;
- A collective risk assessment program to minimize duplication of effort;
- An audit process that allows for participation of other risk and control functions; and
- An aligned and consistent risk reporting regiment.

Combining this approach with the technical ability to gather key risk and performance indicators, IA can create a more dynamic planning process.

A continuous risk assessment process may present challenges (e.g., data quality, data availability etc.), however creates the opportunity to significantly increase the value of IA and other risk and control oversight functions.

Eventually, there is an opportunity for managers to adopt and integrate this approach into their own practices to improve the overall risk and control awareness and environment. Once the latter is achieved, IA can progress to a more advanced level of monitoring and continuous risk assessment.

How Internal Audit can help:

- Assist the Second Line of Defense (risk management) in facilitating an integrated, organization-wide risk assessment.
- Educate and facilitate the consistent usage of common risk language and understanding of organizational key risks.
- Evaluate the organizations risk assessment processes related to major strategic initiatives and how it is managing change related to those initiatives.
- Pilot continuous risk assessments for small sub-groups of risks to demonstrate benefits.
- Evaluate the existing setup of the Three Lines of Defense and assess whether IA can increase presence within the Second Line of Defense and assist in identifying emerging risks.

What is needed by Internal Audit:

- Expert knowledge of risk management frameworks (e.g. COSO ERM Integrated Framework, ISO 31000).
- Good understanding of the organization's risk appetite and risk management processes.
- Expertise in independent assessments of enterprise risk management frameworks including reviewing risk management systems.
- Ability to assess whether key risks are being effectively managed by the organization through the implementation and execution of mitigating controls.
- Ability to coordinate risk assessment activities throughout the entire organization.

9 Data analytics and mass data usage

Drivers:

In recent years, data analytics has strongly impacted the way organizations assess and compile relevant information including monitoring key risks. As such, it has also extended the techniques that IA can apply when executing audits thus providing a higher level of assurance.

The traditional audit approach is based on a cyclical process that involves identifying control objectives, assessing control design, and testing only a small sample of the population to measure control operating effectiveness.

In contrast, contemporary methods use repeatable and sustainable data analytics to develop a more thorough and risk-based approach. With data analytics, organizations have the ability to efficiently review the whole population of transactions — not just samples — thus allowing for conclusions based on the entire number of transactions. This enables a more concise analysis, the identification of the root cause and development of practical recommendations.

IA departments should collaborate within their organization to develop and implement a cohesive strategy to leverage data analytics for the benefit of the whole organization. Some of these benefits may include:

- Enabling real-time, continuous data monitoring.
- Increasing overall efficiency of audits being performed (frequency, scope, etc.).
- Taking a "deeper dive" into key risk areas through data analysis.
- Reducing costs associated with auditing and monitoring.
- Enabling early detection of potential fraud and errors.

How Internal Audit can help:

- Assist in creating automated data extraction, transformation, and loading (ETL) processes.
- Support the development of system-generated analytics tools and dashboards in order to monitor business behavior against specific risk criteria.
- Develop data analytics-enabled audit programs designed to verify the underlying root cause, compile findings and derive remediation actions in order to help the business mitigate risks effectively and efficiently.
- Assist with the implementation of automated auditing tools in order to identify business anomalies and key risk indicators that could trigger certain events.

What is needed by Internal Audit:

- Sound understanding of the organization's data management system (storage, security, usage, IT applications and infrastructure).
- Excellent knowledge in auditing database architectures and capability to understand the underlying dataflow.
- Expertise in incorporating data analytics into audit methodology, aligning data analytics to the risks and assurance scope.
- Expertise in the implementation and usage of data analytics tools/software.

10 Effective talent management

Drivers:

In today's business world, the search for future talents, highly skilled subject matter specialists and key management personnel is challenging. Corporates are investing heavily in recruitment and retention programs in order to develop and maintain an effective pipeline of talented individuals.

Similarly, by becoming a strategic partner to the business, the diversity and multi-disciplinary nature of the IA function has increased. Thus IA also requires access to talented professionals and subject-matter experts.

The challenge is to ensure the right individuals are hired, retained, motivated and developed to help the organization achieve its business objectives. Organizations also need to evaluate risk mitigation plans in case of top talent resignations.

Some of the key factors contributing to a possible high staff turn-over include:

- Limited or non-effective internal talent identification and development programs.
- Non-alignment of staff-needs with the future strategic direction of the organization.
- Poor communication and collaboration between management and staff.
- Misalignment of resource needs i.e. approved FTE budget and actual delivery requirements.

How Internal Audit can help:

- Assess the design, organizational set-up and effectiveness of the talent pool/learning and development programs.
- Benchmark budget and resources contributed to talent management against industry standards.
- Audit the recruiting and hiring procedure and evaluating the efficiency of HR processes, e.g. assess the design and effectiveness of the recruitment and selection process to ensure that the right people are hired.
- Assess whether the recruitment practice actively considers IA needs; remain highly involved in the recruitment process for internal auditors and develop programs that would allow audit-staff-rotation into the business.
- Review the budgeting and resource planning process in order to identify possible misalignments.
- Audit the internal communication process, assess the ability to act upon received feedback and ensure long-term improvements.

What is needed by Internal Audit:

- Sound understanding of the organizational goals and requirements as well as the talent management strategy.
- Expertise in evaluating the organization's talent metrics and identifying and addressing gaps.
- Resource structures using guest auditors and rotation programs.
- Ability to review/benchmark the corporate talent management system against good practices (including use of metrics such as incentives, remuneration, retention ratios, development programs).

11 IT Governance

Drivers:

A comprehensive IT governance system considers all stakeholders when making benefit, risk and resource decisions for IT operations. Good and aligned IT Governance improves the effectiveness of security and privacy controls within the organization.

Management must have a clear understanding of whether the IT infrastructure (including technology, people, processes) is capable of supporting expected organizational needs. This can also include emerging topics such as cybersecurity, the Internet of Things/Industry 4.0 or cloud computing.

Management needs to have a sound understanding and the right awareness of the organization's IT risk exposure and the effectiveness of its existing governance and control setup.

Organizations have an increasing interest in adopting the best practices and standards for IT governance. This can include for example, the standards provided by the IT Governance Institute (ITGI), Control Objectives for Information and related Technology (COBIT®), ISO 17799 for security or IT Infrastructure Library (ITIL). These standards will also drive the IT-related risk assessments performed within organizations.

Additionally, new regulations such as the GDPR require Swiss corporations operating within the European Union to adopt these standards. Consequences of failure may lead to more stringent requirements for the organization, increased reporting demands or fines.

How Internal Audit can help:

- Assess and evaluate processes, procedures and controls over IT Governance by considering applicable requirements from management, stakeholders or national/international regulations.
- Provide observations, recommendations, gap-analysis or benchmarking assessments related to the design and effectiveness of enterprise-wide IT governance systems.
- Assess the level of contract compliance of any external service provider that supports or delivers parts of the overall IT governance framework.
- Prioritize and develop a time frame for implementing missing governance key topics, procedural requirements or key controls.

What is needed by Internal Audit:

- Expertise in auditing organization-wide functions that have a significant IT infrastructure supporting their operations.
- Sound understanding of the organization's IT governance concept and design, including strategy.
- Good knowledge and overview of third-party IT dependencies and expertise in auditing third-party providers such as Service Level Agreement (SLA) contracts, procurement procedures and any additional control systems applicable to third- party providers.
- Broad knowledge of good practice and national/ international regulations in the field of IT governance.
- Ability to ascertain the maturity of organization processes in mitigating existing IT risks.
- Evaluate if the design of the IT organization is appropriate to maximize added-value from IT.

12 Organization-wide initiatives/projects

Drivers:

The very nature of projects presents organizations with risks and challenges:

- Projects tend to be complex in delivery, have a large number of stakeholders, a significant number of project partners and vary in scale.
- Project managers, engineers, commercial officers and other project custodians often face considerable pressures regarding time, money and other resources – especially when involved in complex global projects with multi-layered work streams.

A lack of standardization and accountability around project controls (i.e. using an effective Project Management Organization Tool) exposes an organization to an increased potential for budget overruns, waste and misuse of resources, and obscures the transparency required to assess the root cause of project issues.

Every project governance structure should have core components that drive project governance at all levels of the organization's project portfolio. This can include:

- Designated accountability for the success of the project.
- Clear project ownership independent of asset ownership.
- Segregation of management and project decision making activities.
- Segregation of project and organizational structures.

How Internal Audit can help:

- Provide independent assurance over project governance structure and project setup/monitoring for large organization-wide implementations (e.g. finance transformation).
- Assess the monitoring processes concerning return on investment of organization-wide initiatives/projects.
- Evaluate contract compliance of any project-specific service providers.
- Provide assurance on the risk management process of initiatives/projects.
- Conduct pre or post implementation reviews of material projects and provide assurance to key stakeholders on project outcomes.

What is needed by Internal Audit:

- Sound understanding of the organization's short, medium and long-term strategies and objectives.
- Expertise in auditing projects including project rollout, costs analysis, IT systems and documentation.
- Experience in auditing project information management systems (incl. reporting to the Steering Committee and Board of Directors).
- Ability to analyze project planning and delivery against initial budget (i.e. FTE resources, monetary funds, timeline).
- Expertise in effective organizational change and project management, including ISO 21500.

13 Data Protection and Privacy

Drivers:

The European Commission finalized the introduction of the General Data Protection Regulation (GDPR) in December 2015; its official adoption was in May 2016.

The GDPR 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.

The GDPR will be a fundamental game changer. It introduces a broader geographic reach, meaning that provisions of the EU regulation will be applicable to organizations outside the EU i.e. Switzerland.

In addition, Swiss data protection legislation changes aligned to the GDPR are also under development.

As a result, organizations need to demonstrate continuous data protection compliance. This can include for example:

- Obligation to report personal data breaches.
- Implementation of data privacy by designing relevant processes and systems.
- Appointment of data protection officers positioned independently within the organization.

Potential impact of the GDPR on the organization's bottom line can include fines as high as 4 percent of global turnover and increase reputational risks.

How Internal Audit can help:

- Assess the potential impact of the GDPR on the organizations strategic goals and more specifically the information governance strategy and budget.
- Evaluate the organizations current degree of data protection compliance and areas for improvement.
- Assess the data protection risk exposure and what actions should be taken to mitigate emerging risks.
- Assess the compliance of business partners or third party providers and understand what compliance initiatives they are undertaking.
- Assess the organizations GDPR compliance roadmap to determine whether the plan is adequate for the organization to become compliant. For example by conducting a Data Protection Impact Assessment (DPIA) or assisting with the appointment of a mandatory Data Protection Officer (DPO).
- Integrate GDPR requirements into the annual audit program to assist the organization in improving compliance to the GDPR.

What is needed by Internal Audit:

- Strong understanding of the existing regulatory landscape that the organization operates in (i.e. local data privacy legislation).
- In-depth knowledge of the GDPR requirements that affect the organization.
- Access to benchmarking and good practice examples on how to effectively implement GDPR strategies and ensure long-term compliance.
- The ability to evaluate how the GDPR will impact an organizations subsidiaries, affiliates or business partners outside the EU.

14 Outsourcing

Drivers:

Shared service centers (SSC) have grown exponentially in the past decades due to globalization and powerful new technologies. It has allowed organizations to concentrate on key activities and optimize costs without compromising effectiveness and efficiency of their internal processes. The services outsourced by organizations are becoming increasingly complex as outsourcing capabilities mature and willingness to outsource increases.

Outsourcing can be driven by an organizations desire to:

- Centralize support functions including IT, HR or finance to achieve economies of scale and reduce duplication of efforts.
- Allow external service providers with superior practice, skills or infrastructure to take on organizational functions to improve efficiency and effectiveness.

The growth in outsourcing non-standardised and complex services has lead to the need for customised and tailored outsourcing services and thus increased the complexity of outsourcing contracts (Service Level Agreements – SLA).

Additionally with the increasing level of outsourcing, data security continues to be a major concern for organizations, as service providers are also responsible for upholding their clients' protection standard (also refer to the GDPR risk).

How Internal Audit can help:

- Assess and evaluate outsourcing risks related to tax, regulation, accounting, technology and other areas.
- Provide subject matter expertise input when assessing the maturity level of the Service Delivery Lifecycle.
- Audit the Service Delivery Lifecycle model including strategy, design of the future target operating model and the roadmap for getting there.
- Evaluate the implementation plan including the transition to the new operating model.
- Review the ongoing governance and contract management of outsourced service providers (i.e. independent assessment of the level of service delivery vs. actual costs).
- Assess service providers compliance to various compliance requirements e.g. data protection.

What is needed by Internal Audit:

- Expert knowledge in sourcing and shared services methodology (i.e. Business Services Maturity Model – BSM) that covers all angles of the sourcing lifecycle.
- Ability to assess key risks and opportunities relating to outsourcing (i.e. evaluate SSC business plan).
- Capability to benchmark current SLA agreement against good practice (i.e. using the correct KPIs, compare budget and actual costs against industry standards etc.).

15 Tax Compliance

Drivers:

As tax compliance becomes increasingly complex and heavily monitored, organizations must be at the forefront of changes to manage their obligations strategically.

Some significant developments in the tax landscape include:

- OECD Base Erosion and Profit Shifting (BEPS) reforms regarding transfer pricing (TP) including three layered TP reporting of a master file, local file and country-by-country file (CbCR).
- Swiss Corporate Tax Reform III – Despite the rejection of the referendum in February 2017, many still believe that reform is required. The balance between maintaining adequate tax revenues whilst ensuring global acceptance of Switzerland's tax legislation remains an ongoing challenge. Future reform is likely to have far-reaching impacts on multi-nationals and local Swiss organizations alike.
- Automatic Exchange of Information (AEoI) – Enforced as of 1 January 2017, the AEoI requires Swiss banks to provide tax authorities with detailed information about their foreign clients' accounts – unprompted and annually.
- Growing trend towards the introduction of legislation that requires organizations to publish or file their tax strategy e.g. UK.
- The impact of OECD BEPs on indirect taxes such as VAT. For example, re-qualification for VAT in a particular country as a result of the changes.

How Internal Audit can help:

- Design an IA program to review compliance with key tax legislation on a periodic basis and assessment of key controls with respect to the correct calculation and reporting of taxes.
- Assess the organizations capability to proactively review and react to changes in its tax compliance landscape (e.g. emerging tax rulings, foreign tax laws) to maintain compliance.
- Use IA process mapping of the organizations supply chain processes to assess tax implications of OECD BEPS rules.
- Evaluate the organizations capabilities to periodically assess tax compliance from a holistic organizational point of view and whether it is incorporated into the appropriate levels of decision-making.
- Assess the clarity and allocation of roles and responsibilities with respect to tax reporting (group level vs. local level).

What is needed by Internal Audit:

- Subject matter expertise on upcoming developments in the global and local tax environment relevant to the organization.
- Ability to apply tax knowledge and internal audit expertise to complex organizational structures operating in multiple tax jurisdictions and evaluate the impact.
- Experience in business process analysis and supply chain mapping in order to better evaluate BEPS compliance.
- Capability to benchmark the current tax organization to good practice (i.e. organizational setup, roles and responsibilities, local vs. group accountabilities etc).
- Ability to audit local tax returns of the organization vs. local tax law (i.e. VAT, income, fringe benefits etc).

16 Trade Environment and Customs

Drivers:

The global trading environment is continuously evolving due to ongoing political and economical developments. Examples of recent developments include:

- USA trade policy uncertainties including potential for increased protectionism or overturning of trade agreements.
- The impact of Brexit on trade volume between the UK, Switzerland, EU and other nation states; whether the UK market will require new regulatory product approvals and whether the cost of UK products will change.
- The impact of Base Erosion and Profit Shifting (BEPS) on trading and multinational organizations as the tax incentives of cross-border activities may decrease.
- Increasing trade barriers and inward-looking policies have the potential to derail economic improvements and diminish the international growth prospects in organizations.
- Union Customs Code (UCC) effective as of May 2016 which provides a new framework regulation on rules and procedures for customs throughout the EU.

How Internal Audit can help:

- Conduct an independent review of the risks and impact of new trade agreements or dissolutions (Brexit) on the organization.
- Facilitate internal discussions and identify challenges based on expertise related to the trade environment the organization faces.
- Assist and facilitate subject matter specialists to develop terms-of-trade mapping to quantify potential costs and assess the risks from changing trade agreements.
- Assess compliance with trade related regulations including adherence to trade sanctions, transfer pricing and BEPS.

What is needed by Internal Audit:

- Sound understanding of upcoming developments in the global trade environment.
- Subject matter expertise of existing trade agreements, customs and import taxes applicable to countries the organization deals with.
- Ability to comprehensively assess and analyse complex global supply chain structures and evaluate the impact of customs and trade agreements.
- Use outcomes of audits to assess risk and opportunities related to trade impacting the organization.

Contacts

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch

Luka Zupan
Partner, Head Internal Audit, Risk and Compliance Services (IARCS)
+41 58 249 36 61
lzupan@kpmg.com

François Rouiller
Partner, Head of Assurance Audit Corporates

+41 58 249 79 14
frouiller@kpmg.com

Michael Schneebeli
Partner, Head Markets Financial Services

+41 58 249 41 06
mschneebeli@kpmg.com

Mark Meuldijk
Partner, Head of Assurance Technology

+41 58 249 49 94
markmeuldijk@kpmg.com

Matthias Bossardt
Partner, Head of Cyber Security, Technology Risk and Data Protection Services
+41 58 249 36 98
mbossardt@kpmg.com

Matthias Kiener
Partner, Advisory, Forensic

+41 58 249 21 35
mkiener@kpmg.com