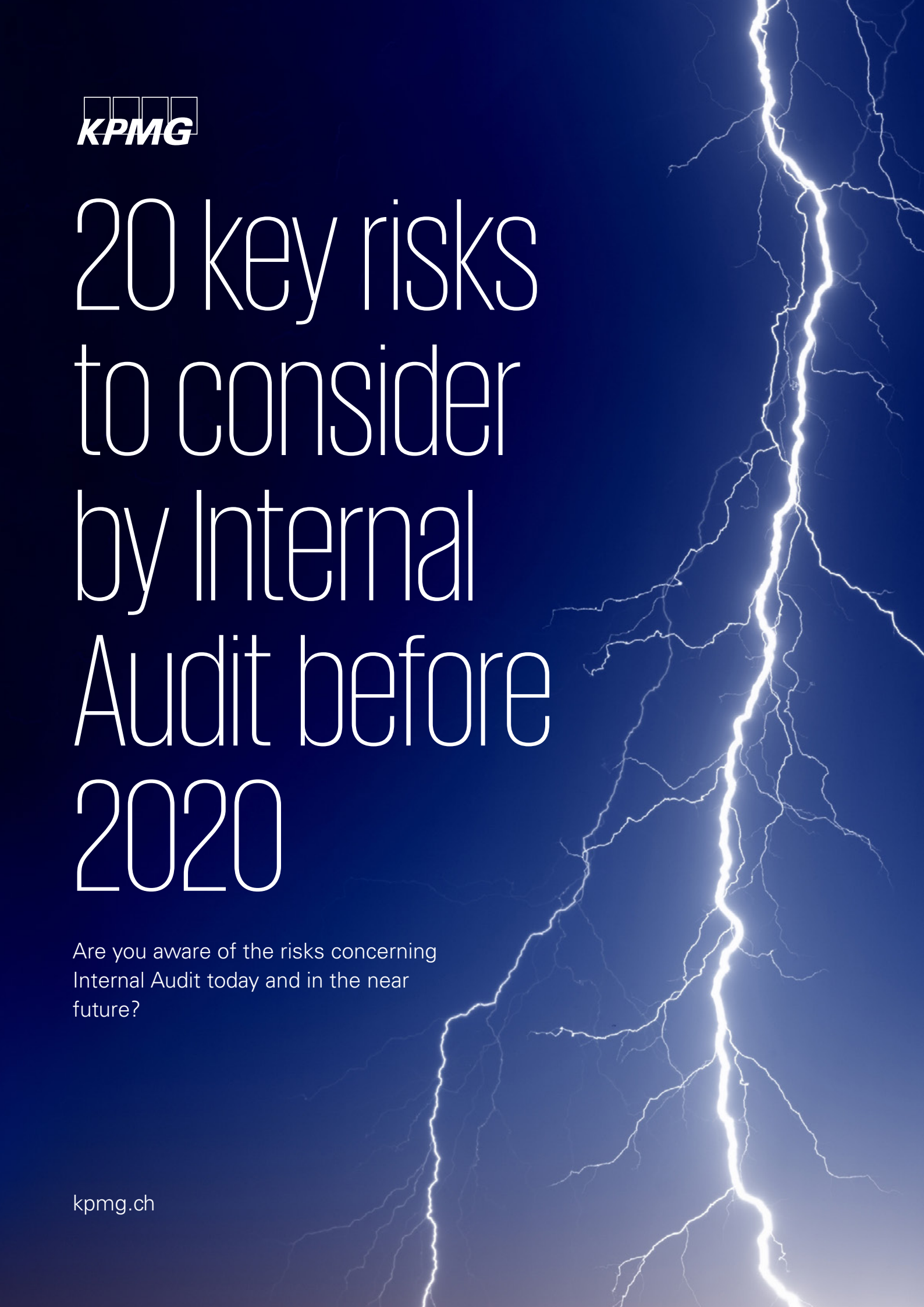
KPMG

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.ch

Luka Zupan
Partner, Head of Internal Audit, Risk and Compliance Services (IARCS), KPMG Switzerland

Member of the global KPMG IARCS Collaboration & Knowledge (C&K) Champion Network

Editorial

An effective and sound risk-based Internal Audit plan is one of the most critical components for determining IA's success as a value-adding and strategic business partner.

The Institute of Internal Auditors (IIA) Standard "2010 – Planning" states that "the Chief Audit Executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals".

This publication aims at assisting Chief Audit Executives (CAE) during their annual audit planning process. Whether provoking thought or facilitating discussions, this publication should assist your governance function to consider a broad range of key risks potentially impacting your organization within the next two years.

In order to allow for a comprehensive strategic assessment, it is key to profoundly understand the underlying risk drivers as well as the potential consequences or impact on the organization. It enables the CAE to determine whether a risk is considered key to the organization or if it's something of a "nice to have". Once the key risks have been established, this publication provides further insights on how internal audit should tackle the topic, how it can help the organization during an audit and what the required crucial skillsets and expertise are in order to ensure an effective, efficient and value-adding outcome by your internal audit team.

As further guidance we have mapped the top 20 risks on a Risk Radar (refer to page 5). The Radar presents two spectrums:

1 **Established key risks** that should be known by the IA function by now vs. **emerging risks** which are not yet fully visible regarding magnitude;

2 **Non-standard/exceptional risks** that should be considered for a one-time audit vs. risks that should be considered on an ongoing basis and form a recurring part of the strategic audit plan

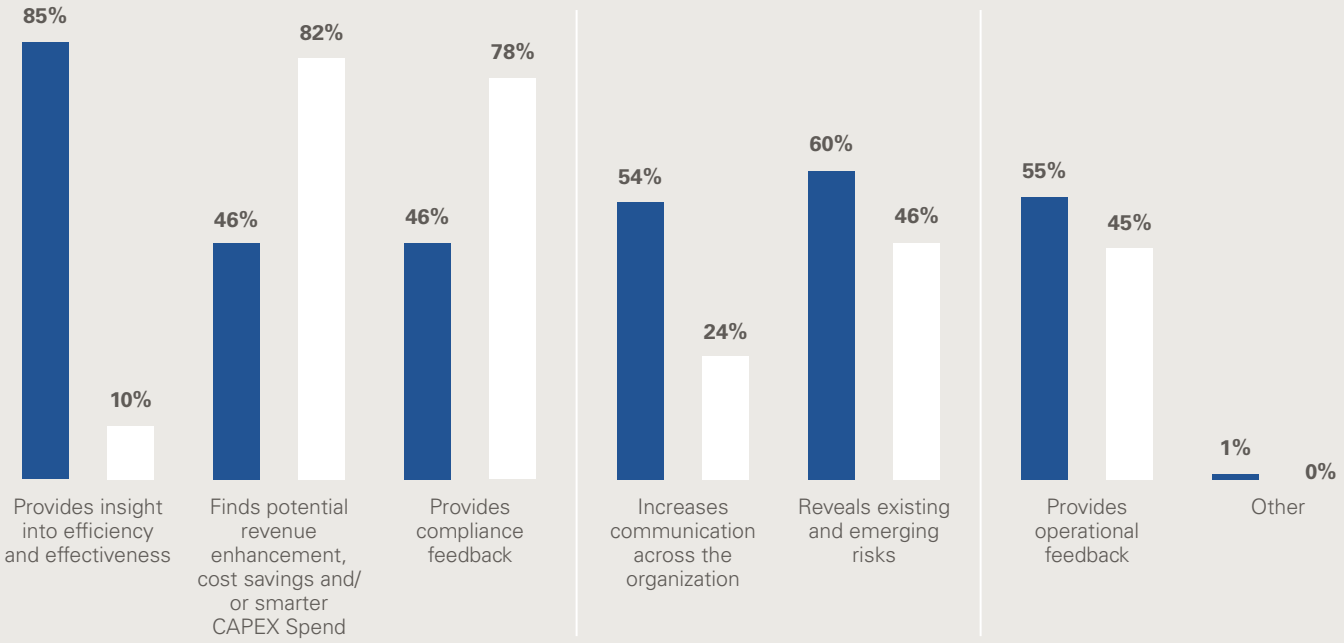
Beyond identifying emerging versus established key risks, the Risk Radar also highlights the recommended level of monitoring of key risks. For instance, IT governance, data analytics and mass data usage are risks that should be continuously considered by IA professionals throughout all governance activities. Non-standard/exceptional risks should be considered based on a triggering event (i.e. merger or acquisition) or due to close scrutiny by stakeholders (i.e. organization-wide project).

For further information you find the distinctive KPMG subject matter specialists for the respective topics on the last page of this publication.

I would like to thank Stephanie Föhn for her tremendous support in collecting and establishing the content.

We are looking forward engaging with you into interesting discussions as to how the future internal audit topic and bring in our extensive experience and thought leadership.

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 organization's 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 its 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 profound 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 collaborate with it to take advantage of any opportunities.

- **Leverage technology**

IA must adapt its methodologies to increasingly utilize technology in the execution of audits. This will provide not only efficiency gains in the delivery of IA but also provide deeper insights into the business, further developing the value perception and credibility of IA.

- **Ensure that IA activities create business value**

IA must ensure that its activities not only provides assurance but also delivers insights into the business, which may be leveraged to improve the business processes or gain a competitive advantage.

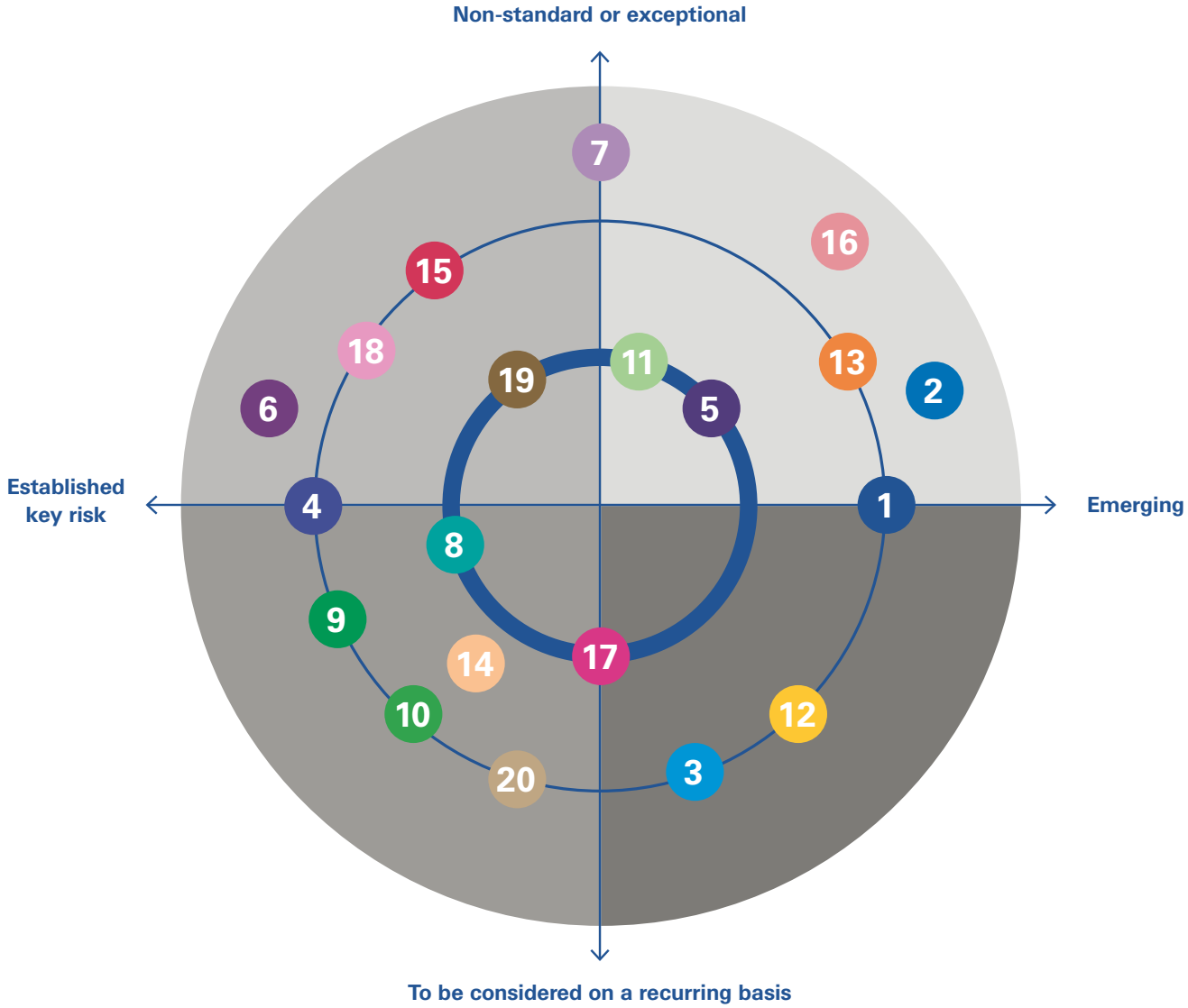
- **Consider the source of demand for assurance**

During the development of the risk-based IA Plan, IA should always consider who is seeking assurance over the specific risk. Once identified, IA should then assess its ability to provide additional insights beyond the stakeholder's current understanding of the topic. This should help IA to prioritize audits which add value and have the potential to provide insights ordinarily not accessible to interested stakeholders.

Top 20 risks before 2020

1. Digitalization, Industry 4.0 & 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 mass data usage
9. Treasury management
10. Organization-wide initiatives/projects
11. Effective talent management
12. Trade environment and customs
13. Alignment of operations to organization's strategy and objectives
14. Compliance Management Systems (CMS), auditing organization culture and ethics
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



- 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

1 Digitalization, Industry 4.0 & the Internet of Things (IoT)

Drivers:

Growing pressure on the efficiency and quality of operational processing continues to drive organizations towards digitalization and automation. Increasing investments in robotics, machine learning, artificial intelligence and advanced analytics is driving a new form of business transformation that is commonly referred to as Industry 4.0.

Key drivers and benefits of digitalization include:

- The increased level of information and transparency achieved through the digitalization of processes. This provides additional context by constructing a virtual copy of the physical production environment to assist management in decision-making.
- The ability of machines and systems to interface and exchange information without human intervention.
- The decentralization of decision-making achieved through delegating simple, repetitive decisions to robotics and machine learning systems.

However alongside the significant benefits, challenges will inherently arise due to the rapid pace of change.
Some of these include:

- Ensuring adequate data protection with regard to intellectual property and production knowledge
- Maintaining production quality with reduced human supervision
- Skill shortage of experienced personnel to implement and operate highly automated processes

How Internal Audit can help:

- Assess whether the objectives and business plans for digital transformation have materialized and organizations are realizing the benefits.
- Assist organizations in the design, implementation and assessment of appropriate governance and control frameworks over digital processes and systems.
- Use the risks and findings identified in Internal Audit reports to drive the digitalization/Industry 4.0 agenda and outline opportunities for process automation.
- Utilize the greater availability of information to conduct audit procedures that provide a higher level of assurance and insights.

What is needed by Internal Audit:

- Subject-matter expertise of upcoming developments and latest technology with respect to automation and digitalization
- Sound understanding of the process to identify, assess and mitigate risks associated with digitalized processes
- Expertise in change management and transformation
- Expertise in general IT controls such as data access, integrity, change protocols and security
- Expertise in data analytics including data extraction, data processing and compiling insightful reports

2 Cloud computing

Drivers:

Cloud computing refers to any type of services where data, applications and/or infrastructure is being stored online and accessible remotely. This can include services such as: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The flexible delivery models and customization of such services has contributed to the widespread adoption of cloud computing. Some of the benefits of cloud computing include:

- Scalability – the ability to scale up or down depending on business needs with reduced CAPEX investment
- Increased mobility of information – remote access to large amounts of data e.g. access to company software via mobile phones
- Business continuity – uninterrupted and reliable central storage of data, accessible to various stakeholders

However, without proper training and security measures, the full benefits of cloud computing may not materialize and thus lead to increased exposure to operational, financial and compliance-related risks. For instance:

- Data security and regulatory risk – data held on a public cloud is entrusted to the governance and controls of a third party
- Operational risk – integration of existing private services with cloud services can be expensive and time-consuming. Additionally, shared cloud service models often provide limited customizability, creating greater integration risks.
- Financial risk – private cloud services require significant initial investment while shared services may vary depending on poor planning and changing business needs
- Vendor risk – vulnerability to risks faced by cloud vendors including regulatory, disaster recovery, reputational and financial exposure

How Internal Audit can help:

- Conduct an independent assessment of the existing governance framework used for operating cloud platforms.
- Assist the organization to identify and define appropriate cloud-computing certifications or provide observations and recommendations in order to create a fit-for-purpose cloud computing governance framework (i.e. ISO 27001 Certification).
- Perform an independent assessment of any third-party cloud service providers on behalf of the organization to identify data security risks.
- Assess the coverage and clarity of the roles and responsibilities assigned between the organization and the cloud service provider, e.g. crisis management.
- Conduct reviews of the Service Level Agreements (SLAs) with third-party cloud computing service providers and assess contractual compliance.
- Perform an independent review of the cloud computing setup in relation to internal and external regulations, i.e. EU-GDPR.

What is needed by Internal Audit:

- In-depth experience in IT audit areas such as logging and monitoring, network configuration, data management, IT asset protection, vulnerability assessments and access control
- Subject matter expertise in various cloud solutions including their technical differences and specific risks of each solution
- Experience in developing controls mitigating key risks associated with cloud usage
- Expertise in the risks and mitigating controls specific to data protection and privacy requirements when using cloud services
- Expertise in guidelines and standards for cloud usage e.g. Cloud Security Alliance

3 EU General Data Protection Regulation (EU-GDPR)

Drivers:

As of May 2018, the European Union General Data Protection Regulation (EU-GDPR) is applicable to:

- Organizations located within the EU; and
- Organizations located outside the EU if they offer goods or services to, or monitor the behavior of data subjects in the EU.

In summary, it 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].

The EU-GDPR is the biggest and most impactful change regarding privacy and data protection in recent history and has introduced a range of new requirements for organizations in relation to data protection.

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

In addition, the Swiss data protection legislation (Swiss Federal Data Protection Act) is currently under revision. One goal is to enhance the alignment of Swiss legislation to the legislative changes in the EU.

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

- Obligation to report personal data breaches within 72 hours
- Implementation of data privacy by designing relevant processes and systems
- Appointment of data protection officers positioned independently within the organization
- Requirements to obtain unambiguous or explicit consent from data subjects regarding the usage of their personal data

Potential impact of the EU-GDPR on the organization's bottom line can include fines as high as 4% of global turnover or up to EUR 20 million, and increased reputational risks.

How Internal Audit can help:

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

What is needed by Internal Audit:

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

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

4 Cyber security

Drivers:

In today's world of constant connectivity, cyber security is a key focal point for many organizations. Cyber security 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 cyber security, including:

- 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.
- The evolution and growing sophistication of capabilities and techniques used by hackers, particularly in their ability to target specific information or individuals i.e. ransomware such as Petya.

In recent times, these hackers target organizations not only through networks directly but also through connections with key suppliers and technology partners. The consequences of cyber security breaches can be disastrous to an organization's bottom line and reputation.

A survey[2] conducted by KPMG Switzerland of 60 companies located in Switzerland found the following:

- 42% of respondents who suffered successful cyber-attacks incurred financial losses as a result (42% disruption of business process, 33% from disclosure of confidential information and 25% reputational damage).
- 82% of cyber response plans do not cover incidents such as attacks against suppliers or business partners.
- 28% of respondents have cyber insurance.
- 44% of respondents say that they have no instruments to enforce their control framework on suppliers and 34% do not require specific cyber security measures in third party contracts.

How Internal Audit can help:

- Perform risk assessment of the organization's cyber security 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 cyber security 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 cyber security risks.

What is needed by Internal Audit:

- 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
- Ability to conduct penetration testing of key systems to identify potential IT control weaknesses

[2] KPMG AG, Clarity on Cyber Security, 2018, https://assets.kpmg.com/content/dam/kpmg/ch/pdf/clarity-on-cyber-security-2018.pdf

5 Business continuity and crisis response

Drivers:

Many organizations have developed a disaster recovery plan and business continuity procedure that have rarely been put to the test in a real crisis situation. With the rapidly evolving business environment, the nature of crises traditionally planned for is changing. For example, in more recent times there is increased exposure to:

- Cyber crises, including cyber security attacks, IT-system outage or data breaches due to greater connectivity and reliance on IT-systems
- Physical crises, including natural disasters, disease outbreaks, workplace violence particularly with respect to multinationals operating in a global market
- Reputational crisis due to digital and social media platforms increasing the speed, nature and impact of information dissemination
- Financial crisis due to the increased volatility and interdependency of the global economy

For these reasons, organizations require adequate planning covering immediate response, decision-making, recovery, communications and contingency plans for various scenarios which may suddenly arise.

How Internal Audit can help:

- Conduct an independent review of the entire crisis management system, including governance, processes and risks, and evaluate the quality and extent of coverage of various crises.
- Assess the leadership's readiness for crisis situations by conducting a survey with key questions to determine the level of preparation for crisis situations.
- Assess the effectiveness and organization knowledge of crisis response plans through simulations of crisis activities and evaluation of the business response.
- Using recent events in the media, knowledge of emerging risks and understanding of the business, facilitate brainstorming workshop with senior management on the various scenarios that may arise.

What is needed by Internal Audit:

- Expertise in effective crisis management and business continuity good practices
- Sound knowledge of the potential and emerging risks and crises which may impact the organization or specific industry
- Subject matter expertise in conducting workshops with senior management to identify risks or conduct drills on crisis scenarios
- Ability to critically analyze existing crisis/business continuity plans and challenge effectiveness

6 Net working capital management

Drivers:

The effective management of net working capital (NWC) is considered to be a key measure of an organization's financial maturity. When managed effectively, organizations can significantly boost capital investments to secure long-term economic success with little or no additional pressure on cash (i.e. cash conversion cycle).

The focus of organizations on the efficiency of NWC can be linked to various factors, including:

- Increasing financing costs due to poor solvency ratios;
- Pressure to meet market analysts' expectations;
- Growing bargaining power of customers to improve payment terms in their favor;
- Increasing use of supply chain finance by large multi-nationals to lengthen payment terms without burdening cash flow management of suppliers;
- Transitioning focus of Senior Management from profit and loss to cash generation as the clearest measure of success;
- Growing use of NWC measures in incentive or bonus schemes for management; and
- Increasing use of technology to access data and drive continuous improvement in the NWC processes.

How Internal Audit can help:

- Perform an internal audit review of the effective and efficient management, monitoring and reporting of NWC, focusing on the three core processes and balance sheet accounts (Accounts Payable (AP), Accounts Receivable (AR) and Inventory (INV)).
- Analyze and document the processes, methods and IT infrastructure as a basis to identify areas for improvement.
- Review and assess periodic reporting of key NWC measures, including collection of information, calculation, distribution of information and usage of measures.
- Perform benchmarking of key NWC processes and measure against organizations of similar size, industry and location.

What is needed by Internal Audit:

- Sound understanding of the organization's operating structure, processes and external environment
- Excellent knowledge of industry-specific better practice regarding the management of AR, AP and INV and its impact on the NWC ratios
- Expertise in financial value chain-based auditing of organizational processes and procedures
- Multi-disciplinary team with experience in the areas of controlling, accounting and treasury
- Experience in business process analysis and modeling including effective use of data analytics and benchmarking

7 Non-GAAP financial measure

Drivers:

According to the U.S Securities and Exchange Commission (SEC) Regulation G[3], a non-GAAP financial measure is 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).

Non-GAAP measures are often presented with GAAP measures in earnings releases and other communications to provide investors with additional information and insight into a company's historical and future financial performance. One common example is adjusted earnings, which may be used to remove non-recurring items from GAAP earnings to better represent year-on-year comparison of financial performance. However, a study in 2017 highlighted that the difference between the GAAP and non-GAAP earnings per share was approximately 54%[4].

In 2017, up to 96% of the S&P 500 presented non-GAAP in their earnings releases[5]. The growing use of such measures may be linked to:

- Management beliefs that non-GAAP measures present a more accurate reflection of business performance.
- Consideration and reliance on non-GAAP measures to determine management compensation and incentive plans, debt covenants or budgets and forecasting.
- Analysts and investors using such information to distinguish performance amongst various businesses within the same industry or using as input for business valuation models.

Despite the relevance and broad user groups of such measures, the risks must also be considered alongside the benefits. For instance:

- The type of measures and the method of calculation of non-GAAP measures are largely open to management discretion, potentially providing users with a biased view and reducing comparability amongst businesses.
- 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 their potential to be misleading.

How Internal Audit can help:

- Assess and challenge the calculation process for non-GAAP financial measures.
- Assess the design and effectiveness of controls related to non-GAAP financial measure calculations in order to maintain consistency and accuracy.
- Develop measures and systems to provide assurance to the Executive Management on the accuracy of non-GAAP measures on a recurring basis.
- Assess compliance with relevant regulatory guidance on the use and publication of non-GAAP measures.

What is needed by Internal Audit:

- Subject matter expertise of GAAP vs. non-GAAP financial measures and standard calculation methods for key measures
- Sound experience in review of non-GAAP measures in order to apply critical thinking (i.e. benchmark across multiple firms and industries)
- Experience in dealing with and being reviewed by regulatory bodies (e.g. the Public Company Accounting Oversight Board (PCAOB)) to understand key risks regarding the calculation and publishing of non-GAAP measures

[3] SEC Regulation G, https://www.sec.gov/rules/final/33-8176.htm (January, 24, 2002)

[4] FactSet Insight, "Did DJIA Companies Report Higher Non-GAAP EPS in Q1'17?" (May 19, 2017).

[5] Audit Analytics, "A Look at Non-GAAP Reporting After New SEC Guidance" (January 2017)

8 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 entire population of transactions — not just samples — thus allowing for conclusions based on the entirety of transactions. This enables a more concise analysis, the identification of an issue's root cause and the 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

9 Treasury management

Drivers:

The role of Group Treasury is evolving towards that of a strategic business partner due to a combination of factors, including:

- Development of sophisticated payment systems resulting from increased prevalence of fraud, competitive pressure to reduce costs and implementation of state-of-the-art technology that is highly automated, integrated and centralized, using encryption for information security purposes.
- With the introduction of **new technology** in payment processing such as Blockchain or Instant Payments, Treasury functions must be aware and knowledgeable of the latest developments in order to help the organization remain competitive and on the cutting edge.
- Emerging Financial Market Regulations such as **FMIA Regulations** in Switzerland. As of 2018/19, all companies are required to provide derivatives reporting to authorities. The regulation is closely aligned to already enforced EU and US regulations (Frank Dodd Act and EMIR).
- Greater volatility in **foreign exchange (FX)** rates leading to increasing use of dynamic hedging strategies.
- **Political interventions** such as trade sanctions and embargos creating compliance challenges and greater need for multinationals to perform transaction screening.
- In the age of digitalization the prevalence of **cyber security attacks** is increasing, with payment processes being a major target area of attackers. Additionally, the sophistication of attacks is developing beyond simple phishing attacks to "Crime-as-a-Service" (CaaS), blackmail, fake president fraud and fraudulent payment diversions.
- Increasing focus on banking relationship management due to growing bank fees, and also limited transparency and benchmarking information regarding bank fees.

How Internal Audit can help:

- Conduct an independent review of the organization's financial risk management structure, focusing on assessment of transparency, predictable business results and cost-effective management of financial risks in accordance with the organization's risk appetite.
- Conduct an independent review of payment systems to determine whether fraud and cyber risks are adequately managed, and identify any opportunities for automation and centralization.
- Review cash management processes, including cash pooling and liquidity.
- Assess financial reporting processes used for financial instruments and structured financing as well as for valuing derivatives and/or stock option plans for FMIA requirements.
- Conduct a review of bank relationship management, including efficiency of bank account structure, and identify opportunities to reduce bank fees.
- Conduct a review of the adequacy of the design of the treasury organization and help evaluate adherence to tax, regulatory and legal requirements such as trade sanctions.

What is needed by Internal Audit:

- Sound understanding of upcoming developments in the Treasury landscape e.g. dynamic hedging, Instant Payments processing, Blockchain etc.
- Subject matter expertise of financial market regulations, e.g. FMIR, trade sanctions and embargos
- Ability to comprehensively assess complex payment processes with multiple geographic locations and systems, and identify opportunities for automation, centralization and integration
- Understanding of cyber security risks specific to payments processing and mitigation strategies to prevent instances of fraud

10 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.
- Resistance to change within the organization due to fear of the unknown, lack of competence, poor consultation, misunderstanding of the need or reason for change, exhaustion and low trust levels.

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 (ROI) 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

11 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 that 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 turnover 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

For these reasons, amongst others, organizations must also be adequately prepared to effectively manage succession planning to ensure business continuity. The development and mentoring of high-potential and talented individuals should lead to a pool of future leaders who will shape the continuing success of the organization.

How Internal Audit can help:

- Assess the design, organizational setup and effectiveness of the talent pool/learning and development programs.
- Benchmark budget and resources allocated to talent management against industry standards.
- Audit the recruiting and hiring procedure and evaluate 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.
- Assess the maturity of the organization's short, medium and long term succession plan for managerial staff and technical roles.
- 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)

12 Trade environment and customs

Drivers:

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

- US trade policy uncertainties including potential for increased protectionism or overturning of trade agreements.
- The impact of Brexit on trade volumes between the UK, Switzerland, the 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.

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 analyze 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 that impact the organization

13 Alignment of operations to organization's strategy and objectives

Drivers:

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

- Increasingly globalized markets;
- Digitalization, Industry 4.0 and the Internet of Things (IoT);
- Major slowdowns of Western economies; and
- Entry of new market competitors with innovative business models.

In the dynamic modern economy, organizations need to be increasingly adaptable to change, constantly analyzing their strategy 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.

When implementing strategic objectives, the organization should not only consider the impact and changes to its operating model but also how effectively the strategy has been executed. For instance, IA should be questioning whether the defined strategy was altered or has evolved during the actual execution. Identified emerging strategies should be assessed to better understand the root cause of the change and the potential impact (i.e. is the change complimentary or contradictory to the defined strategy).

How Internal Audit can help:

- Assess whether resource allocation is aligned with the organization's key strategic objectives and initiatives.
- Perform audits of 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.
- Assess the differences between the defined strategy and the actual, emerging strategy, and assess effectiveness of execution against the actual, emerging strategy.
- 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

14 Compliance Management Systems (CMS), auditing organization culture and ethics

Drivers:

Some of the key drivers of the growing focus on managing organization risks and ethics include:

- Limited effectiveness of existing anti-bribery and corruption compliance activities.
- Emerging regulatory and compliance risk such as organic expansion into new markets, dealings with third parties or business acquisition.
- Increasing expectations on the corporate culture and/or higher prevalence of misconduct incidents due to poor corporate culture, impacting public trust.
- Social media outlets facilitating the ability to quickly and widely broadcast incidents and insights (i.e. corporate culture, misconduct, fraud etc.).
- Growing pressure from key stakeholders on Board effectiveness is driving the need for greater professionalism of Boards in terms of skills, experience, independence etc.
- Introduction of ISO 37001, the first international standard on bribery management, designed to help organizations prevent, detect and respond to bribery.
- Introduction of the Swiss Auditing Standard 980 from 1 January 2019 that highlights the increasing emphasis of Audit Committees on assessing the effectiveness of the Compliance Management System within their organizations.

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 strive for ISO 37001 certification.
- Evaluate whether current performance measures are incentivizing and rewarding desired corporate culture behavior. Provide assurance regarding the design and operating effectiveness of the organization's preventative and detective controls related to anti-bribery and corruption.
- Facilitate a Board self-assessment in order to determine appropriateness of composition, skills, experience, independence, strategy and goal-setting etc.
- Identify bribery and corruption risk through data analytics and third-party audits.
- Review of existing Compliance Management Systems using ISO 19600 as best practice framework and Swiss Auditing Standard 980 to guide audit procedures.

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, Swiss Auditing Standard 980 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

15 Effectiveness and efficiency 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 its 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 Risks 3, 9, 12 and 20);
- Mergers and acquisitions (see Risk 16);
- Geographic expansion;
- Changes to organizational governance structures or frameworks (see Risk 17);
- Increased mobility of employees (see Risk 11);
- Outsourcing of key business processes (see Risk 19);
- Digital transformation (Industry 4.0) and increasing automation of manual processes (see Risk 1); and
- Greater interdependency of business units (see Risk 10).

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

16 Mergers, acquisitions, and divestitures

Drivers:

Organizations today are 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 the 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 on these areas 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

17 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.

Even though a continuous risk assessment process may present challenges (e.g. data quality, data availability etc.), it 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 organization's 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 Enterprise Risk Management (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

18 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, and processes) is capable of supporting expected organizational needs. This can also include emerging topics such as cyber security (refer to Risk 4), the Internet of Things/Industry 4.0 (refer to Risk 1) or cloud computing (refer to Risk 2).

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 the IT Infrastructure Library (ITIL). These standards will also drive the IT-related risk assessments performed within organizations.

Additionally, new regulations such as the EU-GDPR require Swiss corporations operating within the European Union to adopt these standards (refer to Risk 3). Consequences of failure may lead to more stringent requirements for the organization and 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 support or deliver parts of the overall IT governance framework.
- Prioritize and develop a timeframe 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
- If the design of the IT organization is appropriate to maximize added-value from IT

19 Outsourcing and managing third-party relationships

Drivers:

To boost productivity and efficiency, organizations are increasingly relying on third parties to carry out vital business functions. For instance, Shared Service Centers (SSC) have grown exponentially in the past decades. This has allowed organizations to concentrate on key activities and optimize costs without compromising effectiveness and efficiency of their internal processes.

However, third-party relationships also increase exposure of organizations to new risks and potential compliance failures that may result in fines, lawsuits or reputational damage.

Such compliance failures may occur due to:

- Complexity of outsourcing or third party agreements, particularly due to the increasingly customized and sophisticated nature of services being outsourced.
- Third parties being granted access to organization networks further increasing the potential for data security breaches.
- Third parties may operate in areas of political uncertainty, increasing the severity and broadening the nature of risks that the organization is exposed to.

In the context of these risk exposures, organizations need to implement controls to mitigate the risks in order to effectively benefit from third parties relationships. Some considerations may include:

- 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 including on- and off-boarding processes and controls.
- Evaluate contract management to monitor third-party relationships and contract fulfillment.
- Make use of right-to-audit clauses in third-party agreements.
- Assess and evaluate outsourcing risks related to tax, regulation, accounting, technology and other areas.
- Review third-party compliance with generally accepted information security standards.
- 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

What is needed by Internal Audit:

- Expertise in auditing third parties, supply chain management, sourcing and shared services methodology (i.e. Business Services Maturity Model – BSM) 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 benchmark current SLA agreement against good practice (i.e. using the correct KPIs, compare budget and actual costs against industry standards etc.)
- Capability to perform third-party audits (e.g. visiting production sites abroad, comparing third-party compliance standards to the organization's corporate regulations)

20 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 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) – In effect since 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:

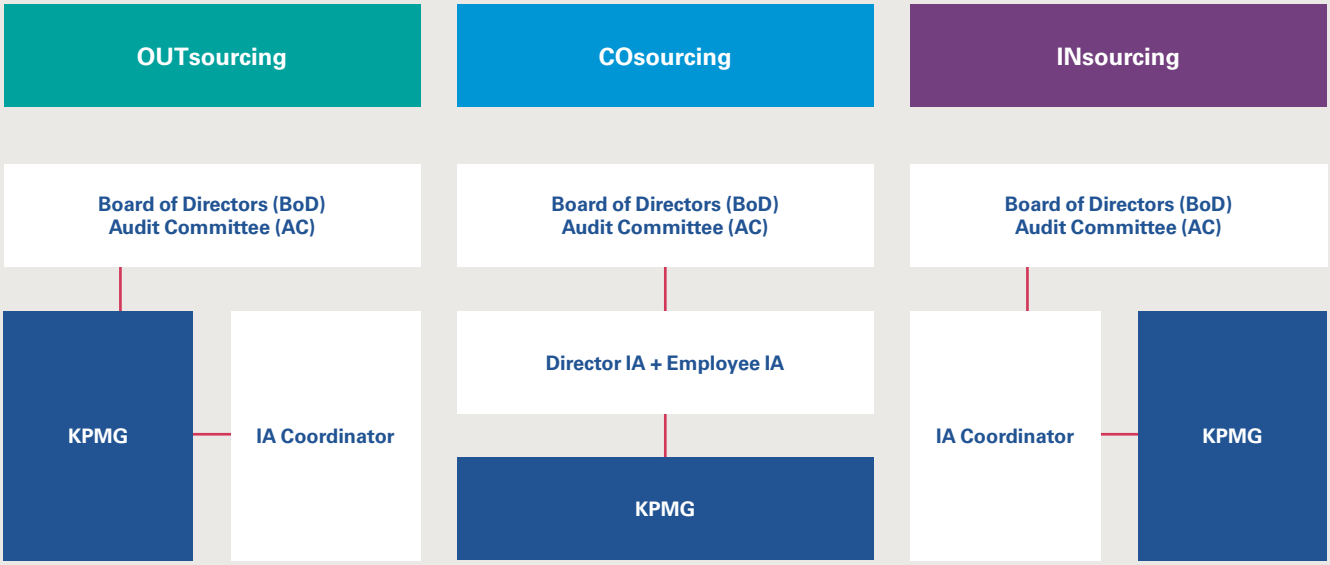
- Design an IA program to periodically review compliance with key tax legislation and assess key controls with respect to the correct calculation and reporting of taxes.
- Assess the organizations capability to proactively review and react to changes in its tax compliance landscape (e.g. emerging tax 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 organization's 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:

- Having 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.
- Having 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.).

KPMG as Internal Audit partner

Forms of cooperation with 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

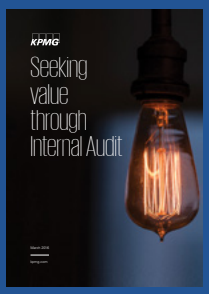
Characteristics of Insourcing
- Fixed costs, little flexibility Control and execution remain in-house
- Integrated in the company on an ad-hoc basis
- Specialists and technologies are not included

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.

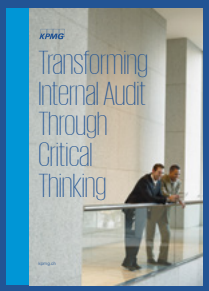
Through our proven methodology, our experience and extensive expertise, we are the right partner for you to fully exploit the potential of your Internal Audit function in an increasingly complex environment.

KPMG thought leadership on Internal Audit

Internal audit and audit committee – the recent study of KPMG offers insights into what members of Executive Management and the Board of Directors including the Audit Committees are expecting from the Internal Audit function and to what extent these expectations are met.



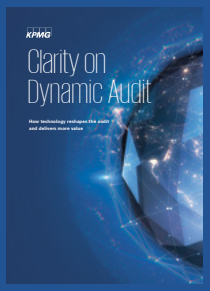
Seeking value through Internal Audit – KPMG and Forbes recently surveyed more than 400 Chief Financial Officers and Audit Committee Chairs on a host of issues regarding the performance, focus, value, and future of Internal Audit functions at their organizations. The findings call attention to a "value gap" between what Audit Committee Chairs and CFOs identify as priorities and what they are receiving from their IA functions.



Transforming Internal Audit through critical thinking – critical thinking is many times a cultural shift for Internal Audit. It can deliver the value creation being sought, and expand or develop the positive perception of the function across the organization.

Clarity on Digital Labor
Clarity on Digital labor outlines relevant insights in how digital labor will change the way we do business and affect the global digital economy.

Clarity on Cyber Security – KPMG's Clarity on Cyber Security explores the most-pressing cyber security topics and analyzes Swiss companies' risk maturity in this field.



Clarity on Dynamic Audit
Clarity on Dynamic Audit explores how technology has changed audits, and what benefits can be drawn from those changes. The publication looks at the expectations in that field of some key Swiss companies and how it has brought additional value for them.

Clarity on Swiss Taxes
Regulatory change is under way in many tax jurisdictions. KPMG's Swiss Tax Report 2018 reflects the fact that it usually takes time for the full effects to unfold.

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

Rolf Hauenstein
Partner, Head of Markets Audit

+41 58 249 42 57
rhauenstein@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, Head of Forensic

+41 58 249 21 35
mkiener@kpmg.com

Daniel Haas
Partner, Head of Accounting Advisory Services

+41 58 249 33 82
dhaas@kpmg.com

Prafull Sharma
Partner, Head of Digital Transformation Advisory

+41 58 249 77 91
prafullsharma@kpmg.com

Stefan Kuhn
Partner, Head of International Corporate Tax

+41 58 249 54 14
stefankuhn@kpmg.com

Top 20 risks in Internal Audit before 2020 April 2019