KPMG

The New Head of Internal Audit

First 100 days as newly appointed Chief Audit Executive (CAE)

kpmg.ch

Editorial

Luka Zupan
Partner
Head Internal Audit
Risk and Compliance
Services (IARCS)

The appointment as the new Head of Internal Audit (IA) presents an array of exciting prospects and challenges for a Chief Audit Executive (CAE).

Stepping into this role allows for a new perspective on how internal audit should be defined and executed within an organization and presents a unique opportunity to introduce fresh ideas and effective and sustainable change to the internal audit organization.

However, as the newly appointed Head of IA one must also be aware of the high expectations of various stakeholders, be it the IA team, the broader organization, executive management or the board/audit committee.

It is thus crucial for a CAE to build their credibility within the organization and quickly become operational.

This paper provides guidance on how to navigate through the first 100 days as a newly appointed Chief Audit Executive (CAE). With topics ranging from the structure of the Three Lines of Defense, to the sourcing of your IA function as well as current and emerging risks for consideration; this paper provides various perspectives and ideas to guide you and provide insights on the upcoming journey. It suggests timeframes for key activities and a detailed implementation checklist to ensure that progress and momentum is achieved.

KPMG as a professional internal audit service provider is enthusiastic to support you in your journey as CAE in setting up/re-organizing the IA function, assisting you to drive momentum and provide insights on industry and IA best practices.

With a highly capable, multi-disciplinary and global team we can assist you with various service offerings including methodology that is aligned to the IIA standards and modern approaches such as data analytics; delivery of internal audit missions on a global scale; conducting enterprise risk management exercises; support in executing forensic and fraud prevention activities as well as assisting in driving the compliance agenda.

Additionally, we can provide a quick and effective performance assessment on the current state of the IA function which can help you in the initial assessment of the IA function and identify areas for improvement.

Content

As the head of an Internal Audit (IA) department one has to lead an independent department providing assurance to the Board of Directors (BoD) regarding risk management, control and governance processes. The Audit Committee (AC) of the BoD expects IA to be able to provide meaningful insights and unbiased opinions, which add value and improve an organization's operations. The top concerns of ACs are listed below:

Top concerns of Audit Committees

1. **Strategy:** Continuous development, implementation and monitoring of strategic objectives for the organization.
2. **Corporate Governance:** Enhancing the value and efficiency of corporate governance and compliance processes including effective reporting to internal and external stakeholders.
3. **Data Analytics:** Fully utilizing the potential of data analytics, continuous auditing and robotics to improve business processes and audit efficiency.
4. **IT risk:** Effectively managing emerging IT risks such as cyber security whilst also maintaining a cost-efficient IT environment.
5. **Third parties:** Optimized assessment, monitoring and controlling of the risks, relations and returns related to dealing with third parties.
6. **Tax:** Evaluating the organizational impact of the Corporate Tax Reform III including effect on financial results and potential tax function transformation.
7. **Assurance:** Independent, concise and relevant assurance reporting from both internal and external auditors on all key aspects required for informed decision making.
8. **Regulations:** Ensuring a sustainable yet effective approach to regulatory compliance on a global, regional and local level (e.g. FCPA, Dodd-Frank Act).
9. **EU Audit Reform:** Understanding and evaluating the impact of the EU Audit Reform on corporations at a global and local level.
10. **Corporate culture:** Ensuring long-term, sustainable organization growth through ongoing enhancement of corporate culture and implementation of talent development and employee-retention programs.
11. **Risk Management:** Ability of the risk management process to effectively identify emerging risks, provide accurate risk assessment and implement cost-efficient counter-measures.
12. **Changing business landscape:** Ensuring that the organization is well-equipped to respond to a changing environment, new operating models, emerging competitors and game changers such as the economy 4.0. or geopolitical influences (Brexit).

Introduction

With companies navigating through a volatile economic landscape, Chief Audit Executives (CAE) face difficult choices when addressing the evolving issues and related risk factors of their organizations. Changing stakeholder expectations and a new view of risk management have prompted an important shift in the role of IA in many organizations. New demands from the board, senior organizational leaders, and regulators require IA to refocus its efforts beyond regulatory compliance issues. As a result the task becomes all the more difficult for a new CAE to move forward in the role.

Setting the scene:

The universe we face today

External factors driving change

- Regulatory pressures
- Emergence of new business risks
- Increased focus on risk and controls from shareholders and investors
- Demands for greater accountability from stakeholders
- Higher levels of macroeconomic and political uncertainty
- Financial market volatility
- Increased use of offshoring

Internal factors driving change

- Increased focus on risk and controls by senior management and the board
- Focus on cost reduction and efficiency
- Market expansion (e.g. new product / service development)
- Geographic expansion
- Emergence of new operations risks
- Stronger risk awareness culture instilled within the organization
- Postmerger process integration

The three lines of defense:

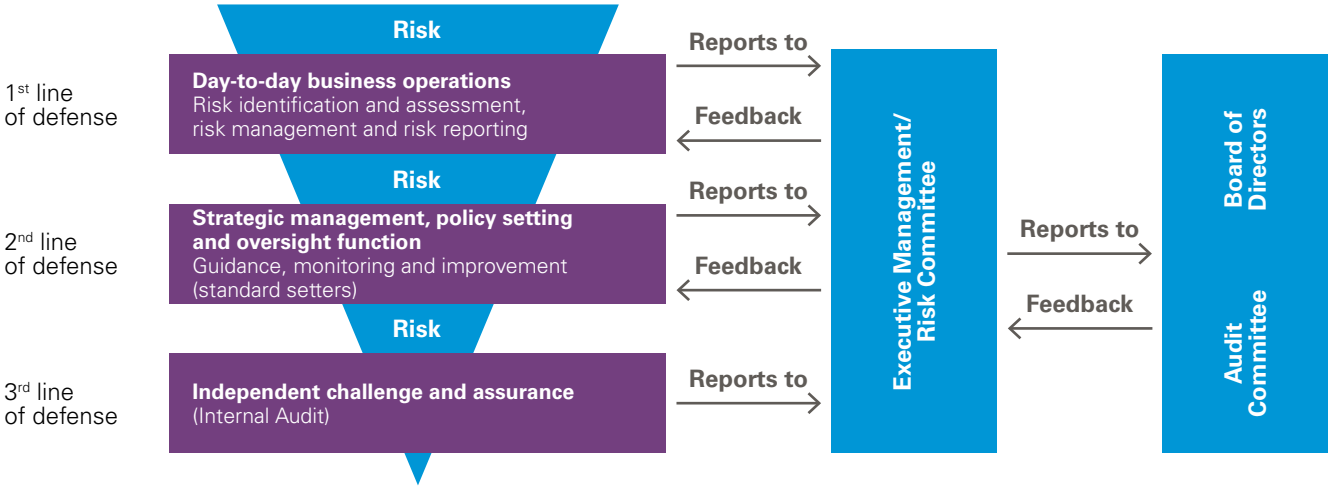
Risk governance

The "three lines of defense" model helps to understand relationships and interactions between the various layers of an organization regarding risk and control ownership, facilitation/monitoring and independent assessment.

The model outlines that the business as the first line of defense is responsible to make sure that risks are managed at an acceptable level and controls executed effectively.

The second line of defense summarizes the supervisory functions that typically support and monitor the management of key risks and report to Executive Management. Examples of functions include Risk Management, Compliance, Legal, Quality Control etc.

The highest level of assurance in terms of independence comprises the internal and external audit functions – defined as the third line of defense. Their focus lies in providing in-depth assurance to the BoD that the key risks of the organization have been identified, are effectively and efficiently managed by the first and second lines of defense. In addition to independent assurance provided by the IA function, IA also helps organizations to create business value, i.e. insights into best practice, or identify process efficiencies.



Where does your Internal Audit department stand?

Get a grasp on the maturity of your IA department based on the characteristics of a leading IA organization.

From an underperforming IA function…	… to …	… an excelling IA function	Characteristics
Individual assurance silos, no coordinated risk perspective	Coordinated approach to understanding key risks	Single view and understanding of key risks across the organization	
Focus on internal controls (ICoFR) assurance and partially on internal compliance	Risk-based assurance across operations, financials and compliance processes	Strategic value creation is actively incorporated into risk-based auditing	
Misaligned skill sets, underleveraged staff, limited career prospects, no rotation program	Active talent management within the organization and continuous development of skill sets	Operational experience, «skills on demand» including guest auditor and rotation programs	
Ad hoc use of data analytics (DA)	More frequent use of DA to assess processes	Leveraging DA to assess the impact of business strategy; assess effectiveness and efficiency of processes and controls; DA incorporated into IA methodology	
Reactive, annual risk assessment	Enhanced risk identification and effective management; ad hoc response	Proactive monitoring of key risk indicators using DA (e.g. dashboards); forward rolling of the strategic audit plan	

Current issues and emerging risks for Internal Audit

IA needs to proactively identify emerging business issues and trends to maintain relevance within the organization. Emerging business trends carry new risks, and IA needs to continually monitor these risks and their potential impact on the organization. To provide the greatest value, IA must act quickly when confronted with emerging risks and identify opportunities to challenge the status quo in order to reduce risk, enhance controls, and realize efficiencies and cost benefits across the organization. The top 12 key risks indicated below, highlight opportunities where IA can proactively assist in the management of emerging risks. Management of current issues and key risks will enhance IA's ability to add value and maximize its influence across the organization.

Top 12 key risks	How IA can help
1. Cyber Security	• Perform a top-down risk assessment of the organization's cyber security process. • Audit cyber security proof of concept and perform operational readiness review. • Assess organizations current cyber security threats. • Assess organizations existing cyber incident reporting.
2. Global regulatory compliance	• Review the inventory of regulatory bodies and requirements affecting the organisation. • Assess the organization's approach to managing its global compliance activities. • Evaluate the organization's response to any notable instances of non-compliance. • Review the appropriateness of compliance training programs.
3. Ethics and integrity of organizations	• Conduct a gap assessment of the organization's existing anti-bribery and anti-corruption procedures in relation to leading practice regulatory guidance (e.g. ISO 19600, ISO 27001). • Review business practices and any potential code of ethics violations, anti-bribery or anti-corruption issues. • Provide assurance regarding applicable preventative and detective controls. • Surface bribery and corruption risk through data analytics and third-party audits. • Allocate resources to investigations involving potential non-compliance. • Drive continuous improvement through controls testing. • Evaluate the organization's anti-bribery and anti-corruption program.
4. Operational effectiveness and efficiency	• Review key organizational processes and assess existing control environment. • Assess communication of the organization's risks, controls and best practices to employees. • Evaluate adherence to policies and procedures affecting key business processes, e.g. supply chain management. • Review effectiveness of key policies and procedures, e.g. Health, Safety and Environment.
5. Third-party relationships	• Review third-party engagement processes including identification, due diligence, selection, on-boarding processes and governance. • Evaluate contract management processes. • Align regulatory developments related to third parties. • Review consistency of right-to-audit clauses. • Assess third-party compliance with the organization's information security standards.
6. Mergers, acquisitions, and divestitures	• Perform «post mortem» reviews on prior deals or divestitures. • Assess adherence to due diligence checklists that address accounting and internal controls. • Review communication processes between finance, Internal Audit, and deal teams. • Perform a project risk assessment review of the business integration or divestiture process.

Top 12 key risks	How IA can help
7. Strategic alignment of the organization's operations	• Assess if resources are being allocated towards the most important objectives and initiatives of the organization. • Provide assurance on other areas than corporate governance (e.g. selected management processes, IT and data management and operational risks). • Evaluate how the company is assessing risk related to major strategic initiatives. • Align IA with the company's strategy.
8. Integrated ERM and continuous monitoring	• Facilitate an integrated risk assessment including all relevant functions within an organization. • Analyze the benefits of continuous risk assessment for a small subgroup of risks. • Evaluate the company's ongoing approach to risk management in light of enterprise risk assessment results.
9. Data analytics and mass data usage	• Review automated extract, transform, and load (ETL) processes, along with system-generated analytics and dashboards. • Make use of data analytics-enabled Internal Audit programs. • Review the organization's data management (security, storage, usage, IT applications and infrastructure).
10. Talent management	• Review IA resourcing requirements based on the annual IA plan. • Assess new resource needs as IA becomes more involved in the business' strategic initiatives. • Conduct internal competency assessment for current resources to understand skill gaps. • Determine scope areas requiring subject-matter specialists. • Build relationships with external service providers. • Provide IA professionals with training and development programs tied to regulatory developments. • Ensure company recruitment practices actively consider IA needs.
11. IT governance	• Review the organization's IT governance structure. • Assess the strategic alignment between business and IT. • Assess the risk framework that guides IT processes. • Assess performance measures such as IT Balanced Scorecards.
12. Organization-wide initiatives/projects	• Analyze contract compliance and cost recovery. • Assess program or project risks. • Provide independent assurance over project setup / monitoring for large company-wide implementation (such as finance transformation).

Questions to ask about your Internal Audit department

Is Internal Audit…

- actively supporting the BoD/AC by providing effective assurance on the key risks of the organization?
- linked to the business strategy and supporting the C-level agenda?
- willing to challenge the business strategy?
- a valued advisor to the organization, expanding its focus to areas like business strategy implementation, fraud prevention, operational excellence and regulatory compliance?
- employing the right people with the appropriate skill sets?
- approaching risks as a "siloed" function or truly integrated and coordinated with other assurance functions?
- anticipatory or proactive to situations within the organization?
- providing applicable cost-saving suggestion and efficiency gains?
- able to identify improvements to the design of risk and control environments?
- perceived positively, as an added-value-bringing function by all stakeholders?
- producing concise and timely reports?
- effectively leveraging modern technologies such as mass DA to provide more accurate assurance opinions or suggestions for efficiency gains?
- appropriately collaborating with the three lines of defense across the organization?

The first 100 days

The decisions made in the first 100 days are essential and will create the basis for the future success of the Internal Audit department. The first questions a new CAE should ask are: «How can I establish a strategic plan for success?», «Do I have the appropriate resources available?», and «How can I build a strong team?».

With this in mind, the new CAE has a lot of tasks to consider. The below outline can support the 100 days agenda and act as a «to-do list.» While not all activities might be relevant to every CAE, there are certainly additional actions and considerations to be taken, based on the individual circumstances within each organization. The need to regularly communicate with the IA team and the key stakeholders to better understand the environment that IA operates in, should be satisfied on a permanent basis.

The following areas should be part of the 100 days agenda of a new CAE:

- **Clarifying and defining the positioning and effectiveness of IA –** establishing a team and infrastructure sponsored by the BoD that can support the needs of the business and execute on the CAE's vision of the function.
- **Assessing regulatory and compliance standards relevant for the assurance objective of IA –** understanding the industry and regulatory requirements and developing a framework to proactively identify risks threatening the achievement of organizational objectives.
- **Aligning IA operations with the corporate governance framework –** ensuring IA's operations are congruent with the company objectives.
- **Using risk management to define the strategic IA plan –** establishing an effective Enterprise Risk Management (ERM) program that embeds risk management across the organization and proactively identifies emerging risks, which may then be appropriately mitigated.
- **Assessing the expectations of stakeholders and aligning IA operations accordingly –** understanding the needs and perspectives of each key stakeholder and establishing a plan to proactively respond to these needs.

A 100 days plan is summarized on the next page.

Executing the CAE agenda

1. Clarifying and defining the positioning and effectiveness of IA

Focus area	CAE's objectives/activities	Recommended timing
Open communication	• Engage in a culture of open dialogue to begin building presence and establish relationships across the organization.	0 – 30 days
People	• Evaluate Internal Audit staff competencies and review performance evaluations.	0 – 30 days
Best practices	• Fully utilize data analytics to enhance Internal Audit capability. • Proactively identify and manage emerging risks. • Benchmark Internal Audit function in terms of size, investment, sourcing model and approach, e.g. compliance or strategic focus.	30 – 60 days
Risk-based approach	• Utilize Enterprise Risk Management methodologies to ensure focus is on key strategic business and process risks. • Understand existing risk assessment and risk management frameworks used within the organization.	60 – 90 days
IA governance	• Assess current compliance with IIA Standards and good practice procedures. • Review and update the IA charter and IA manual and align IA operations accordingly. • Ensure IA is well positioned, having the support of the BoD.	0 – 90 days
Technology	• Assess ability to utilize data analytics in evaluating the effectiveness of controls.	Over 90 days

2. Assessing regulatory and compliance standards relevant for the assurance objective of IA

Focus area	CAE's objectives/activities	Recommended timing
Requirements	• Outline the regulatory environment the organization is operating in. • Assert the responsibilities of the organization regarding these requirements.	0 – 30 days
Risk assessment	• Identify the key risks, align assurance level expectations with stakeholders. • Determine the maturity level of risk responses across the organization.	0 – 30 days
Company-wide implementation	• Assess if the compliance requirements of the organization are incorporated into the business processes.	30 – 60 days
Training and guidance	• Assess what awareness training programs are provided within the organization.	30 – 60 days
Compliance Management System (CMS) maturity	• Conduct independent audit and provide assurance on the maturity level of the CMS to key stakeholders.	60 – 90 days
Remediation actions	• Provide assurance on the corrective actions taken by the organization.	Over 90 days

3. Aligning IA activities with the corporate governance framework

Focus area	CAE's objectives/activities	Recommended timing
Internal control	• Benchmark the internal control framework to COSO 2013 and assess maturity level. • Assess the impact of regulatory internal control requirements on the IA function.	0 – 30 days
Fraud management	• Evaluate the effectiveness of the fraud prevention program and incorporate fraud auditing procedures into fieldwork.	30 – 60 days
Governance process	• Add value by providing an opinion on the effectiveness of the governance process including risks, internal control and organizational culture.	60 – 90 days
Control evaluation	• Align the activities of IA, external audit and other assurance functions by using common understanding of the key risks of the organization and by mapping an assurance landscape.	Over 90 days

4. Using risk management to define the strategic IA plan

Focus area	CAE's objectives/activities	Recommended timing
Risk evaluation	• Review the Enterprise Risk Management process and align/benchmark with internationally accepted frameworks (e.g. ISO31000, COSO ERM).	0 – 30 days
Emerging risks	• Establish processes/procedures to identify, monitor and incorporate emerging risks into the risk assessment.	30 – 60 days
Mitigating strategy	• Determine whether there is an organization-wide approach to identification and monitoring of multiple and cross-enterprise risks. • Assess if risk management processes are embedded within each business unit.	60 – 90 days
Returns	• Consolidate and align processes to drive efficiency and gain positive returns. • Lay an agenda for all future risk management strategies, focusing on ensuring returns.	Over 90 days

5. Assessing the expectations of stakeholders and aligning IA operations accordingly

Focus area	CAE's objectives/activities	Recommended timing
Stakeholders	• Identify key stakeholders and assess their expectations regarding assurance levels.	0 – 30 days
Action plan	• Develop a robust stakeholder strategy and an action plan to address their assurance needs.	30 – 60 days
Leadership and direction	• Ensure the right kind of leadership and direction are provided to staff internal auditors. • Hire and retain people with the appropriate skill sets. • Support staff development proactively and assess possibilities for guest auditors/rotation programs. • Involve subject matter specialists where possible to build credibility, provide deeper insights and added value, e.g. best practice and benchmarking.	60 – 90 days
Improvement plans	• Conduct regular quality assessments. • Improve the quality of audits and their outcomes.	Over 90 days

Checklist and time line

	0 – 30 days	30 – 60 days	60 – 90 days	Over 90 days
1. Clarifying and defining the positioning and effectiveness of IA	• Engage in a culture of open dialogue to begin building presence and establish relationships across the organization. • Evaluate Internal Audit staff competencies and review performance evaluations.	• Fully utilize data analytics to enhance Internal Audit capability. • Proactively identify and manage emerging risks. • Benchmark Internal Audit function in terms of size, investment, sourcing model and approach, e.g. compliance or strategic focus.	• Utilize Enterprise Risk Management methodologies to ensure focus is on key strategic business and process risks. • Understand existing risk assessment and risk management frameworks used within the organization. **0 – 90 days** • Assess current compliance with IIA Standards and good practice procedures. • Review and update the IA charter and IA manual and align IA operations accordingly. • Ensure IA is well positioned, having the support of the BoD.	• Assess ability to utilize data analytics in evaluating the effectiveness of controls.
2. Assessing regulatory and compliance standards relevant for the assurance objective of IA	• Outline the regulatory environment the organization is operating in. • Assert the responsibilities of the organization regarding these requirements. • Identify the key risks, align assurance level expectations with stakeholders. • Determine the maturity level of risk responses across the organization.	• Assess if the compliance requirements of the organization are incorporated into the business processes. • Assess what awareness training programs are provided within the organization.	• Conduct independent audit and provide assurance on the maturity level of the CMS to key stakeholders.	• Provide assurance on the corrective actions taken by the organization.

	0 – 30 days	30 – 60 days	60 – 90 days	Over 90 days
3. Aligning IA activities with the corporate governance framework	• Benchmark the internal control framework to COSO 2013 and assess maturity level. • Assess the impact of regulatory internal control requirements on the IA function.	• Evaluate the effectiveness of the fraud prevention program and incorporate fraud auditing procedures into fieldwork.	• Add value by providing an opinion on the effectiveness of the governance process including risks, internal control and organizational culture.	• Align the activities of IA, external audit and other assurance functions by using common understanding of the key risks of the organization and by mapping an assurance landscape.
4. Using risk management to define the strategic IA plan	• Review the Enterprise Risk Management process and align/ benchmark with internationally accepted frameworks (e.g. ISO31000, COSO ERM).	• Establish processe/ procedures to identify, monitor and incorporate emerging risks into the risk assessment.	• Determine whether there is an organization-wide approach to identification and monitoring of multiple and cross-enterprise risks. • Assess if risk management processes are embedded within each business unit.	• Consolidate and align processes to drive efficiency and gain positive returns. • Lay an agenda for all future risk management strategies, focusing on ensuring returns.
5. Assessing the expectations of stakeholders and aligning IA operations accordingly	• Identify key stakeholders and assess their expectations regarding assurance levels.	• Develop a robust stakeholder strategy and an action plan to address their assurance needs.	• Ensure the right kind of leadership and direction are provided to staff internal auditors. • Hire and retain people with the appropriate skill sets. • Support staff development proactively and assess possibilities for guest auditors/ rotation programs. • Involve subject matter specialists where possible to build credibility, provide deeper insights and added value, e.g. best practice and benchmarking.	• Conduct regular quality assessments. • Improve the quality of audits and their outcomes.

How we can help

Service offerings

Internal Audit (IA) function	• IA strategic sourcing (outsourcing, cosourcing, insourcing) • Strategic IA quality assurance and performance assessment • Establishing an IA function • Supporting risk-based annual planning and execution • Develop and expand IA methodology to include new approach such as DA • Provide subject matter specialists • Provide local KPMG staff
Data Analytics (DA) / Continuous auditing / Continuous monitoring	• DA-enabled IA including development of scripts, providing training and incorporating DA into the IA methodology • Use of DA to assess risk management including risk dashboards • Use of Computer-Aided Audit Techniques (CAAT) (e.g. IDEA) including development of interface with ERP systems (SAP, Oracle, MS Dynamics, etc.)
Forensic services	• Forensic DA • Industry-, company- or process-specific tests • Global investigations • Anti-bribery and anti-corruption proactive and reactive methodologies • Corporate intelligence • Fraud risk (prevention) management • Global Evidence Tracking System (GETS)
Enterprise Risk Management (ERM)	• Enterprise risk assessment • Assurance on the risk management processes including auditing based on ISO 31000 standard • Assurance that risks are correctly evaluated • ERM design and implementation coaching • Evaluation of the reporting of key risks to stakeholders
Internal Control System (ICS)	• Supporting the implementation of an ICS • Review and assessment of the ICS framework based on the new COSO 2013 principles • Benchmarking with comparable companies • Recurring assessment of the ICS • Supporting the update of the ICS documentation • Assisting with the assessment of controls outsourced to external service providers based on ISAE 3402
Compliance Management System (CMS)	• Compliance maturity assessment • Assessment of CMS • Assessment of compliance policies and procedures • Review of integration of compliance controls with existing ICS • Review of third-party compliance • Assessment of code of conduct compliance

Quality assurance and performance assessment of Internal Audit

Added value of external quality assessment by an independent auditor:

- An external, independent view to highlight areas where IA can be optimized.
- An independent assessment of how well IA work complies with IIA Standards and a comparison with best practices.
- Constructive recommendations (including suggestions on which measures to take) based on experience from the relevant sector and best practice.
- Support for external auditing in terms of evaluating the suitability of IA (auditing standard 610).

When to start?

As part of the positioning and effectiveness assessment of the IA function, performing a quality assurance and performance assessment will provide you with a transparent and independent evaluation of the IA department, including benchmarking with best practices and a comparable size of IA based on global data.

Why monitor the quality IA?

Corporate governance, risk management, and the many varied providers of assurance, including IA, represent the core management, monitoring, and control functions within a company. As such, their remit constantly brings them under the scrutiny of various stakeholders, such as the BoD, AC, or executive management. It is not simply a question of whether the results of their work satisfy stakeholder requirements, but also how effectively and efficiently these services are delivered. In terms of the remit for IA, the key questions in this area are as follows:

- What added value do the services provided by IA generate for stakeholders?
- How effective is IA as an independent line of defense within the company's corporate governance framework?

How well does the company's own IA compare with similar companies and best practice?

Our quality assurance of IA focuses on these issues and comes up with recommendations to help bring the current situation in line with what is actually required.

What regulatory provisions apply to the quality assessment of IA?

- IIAS/IIA Standard (1312): "External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization."

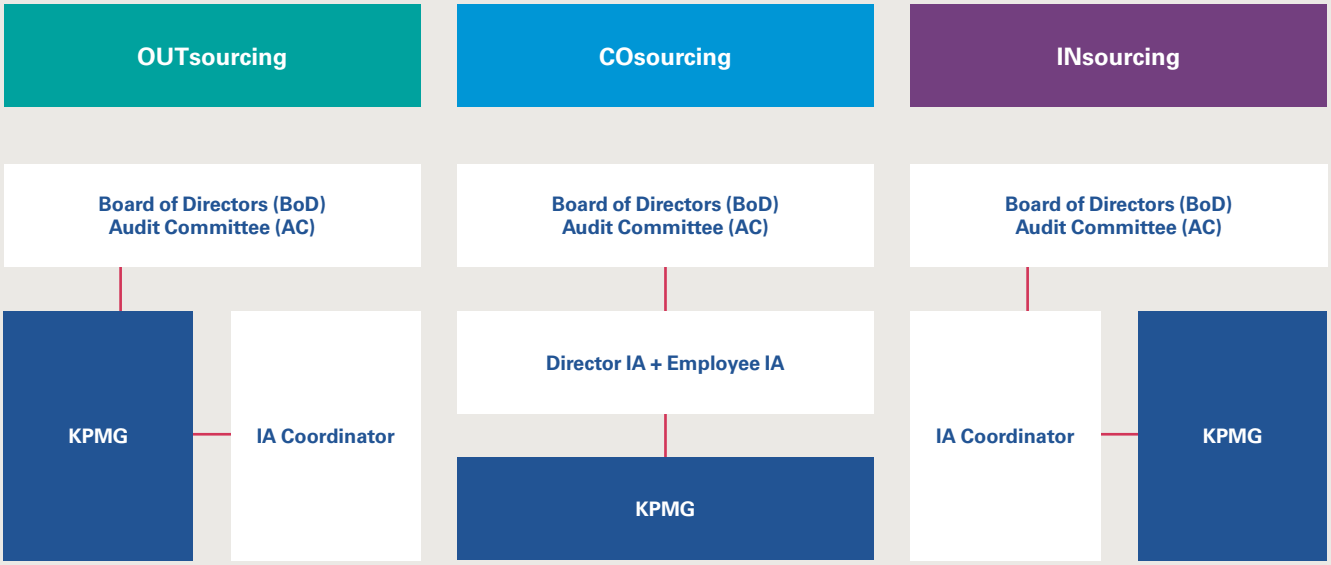
How we can help

The KPMG methodology KSPRint (KPMG Strategic Performance Review of IA) provides the framework for the quality assessment of IA. It is based on IIA Standards and the extensive practical experience acquired during our work for national and international companies. KSPRint is modular and scalable and can be tailored to suit your needs. The methodology is based on the success factors associated with IA and focuses on the following three main areas:

- Positioning: Is IA correctly positioned, in strategic terms, to make a contribution to the company's success?
- Staff: Does IA have the right strategy, human resources, and capacity to fulfill its remit?
- Processes: Are IA processes in line with business needs?

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 **Cosourcing 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-effictive for small-sized Internal Audit functions

Characteristics of Cosourcing
- 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, Cosourcing 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.

Sustainability of Internal Controls

Since 2008 Swiss companies have been audited on the existence of a formal Internal Control System (ICS) regarding financial reporting. KPMG conducted a survey to assess the sustainability of ICS related processes focusing on the design and setup of the ICS, the benefits it provides to the business and the initiatives taken by the companies to optimize their control frameworks. The survey allows for qualitative benchmarking.

KPMG survey

on "Sustainability of Internal Controls"
Companies surveyed: Medium to large Swiss companies (incl. multinationals)

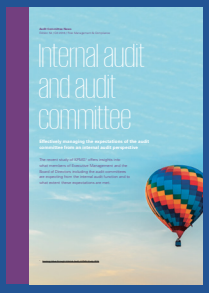
Benchmark: More than 60 companies assessed for the set-up and sustainability of the Internal Controls System

Represented industries:
- Chemicals & Pharmaceuticals
- Communication & Media
- Retail
- Energy
- Technology
- Transport
- Public Sector

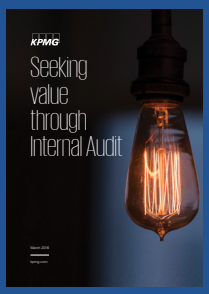
Our competencies in the area of ICS

- **Implementation:** Supporting the implementation of an ICS based on KPMG's proven ICS methodology.
- **Optimization:** Analyzing the current ICS framework and assess the potential for improvements (e.g. control reduction and automation, configuration of the ICS testing procedures, development of a sustainability concept).
- **Benchmarking:** Performing peer review of the ICS with comparable companies and identify possible areas for improvement; supporting the assessment of recurring ICS costs for ICS maintenance, control execution and testing.
- **Testing:** Supporting the recurring assessment (control design and control effectiveness) of the ICS, including support at local sites, design testing procedures and assisting with the development of self-assessment procedures.
- **Update:** Supporting the update of the ICS documentation, e.g. revision of process and control descriptions, re-performance of the scoping exercise, or review of the ICS manual.
- **Sustainability/Development:** Supporting the development and implementation of a long-term ICS sustainability concept.
- **COSO 2013:** Review & assess the ICS framework based on the new COSO 2013 principles.
- **IT General Controls:** Supporting the implementation, updating and testing of IT General Controls.
- **Tools:** Supporting the development of a business case to implement an ICS tool (e.g. define requirements catalogue, perform market analysis and product selection, analyze interfaces with other IT applications, and support implementation).
- **Control Automation:** Analyzing the current ICS control catalogue, and identifying and assessing the potential for control automation based on functionality of existing IT applications including assessment of cost saving potentials.
- **Segregation of Duty Concepts:** Defining, documenting, implementing or auditing Segregation Of Duty (SOD) concepts in full, including user access management using specific IT tools.
- **ISAE 3402:** Assisting with the assessment of controls outsourced to external service providers (e.g. certification of control design, fairness of presentation and assessment of control effectiveness).
- **Integration:** Supporting the consolidation of Governance, Risk & Compliance initiatives and tools and assist with setting up an integrated Enterprise Risk Management framework.

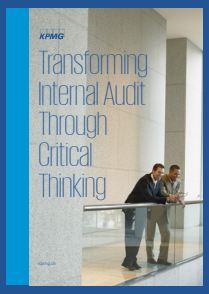
KPMG thought leadership on Internal Audit



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.



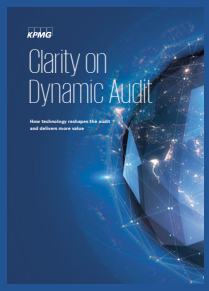
Seeking value through Internal Audit – KPMG and Forbes recently surveyed more than 400 Chief Financial Officers and Audit Committee Chairs on a host of issues regarding the performance, focus, value, and future of Internal Audit functions at their organizations. The findings call attention to a "value 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 Compliance – the white paper "Clarity on Compliance" covers some leading practices and shares insights into building an even more effective compliance function.

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.

Closing perspective

Our expertise in the area of Internal Audit, Risk and Compliance Services can support your Internal Audit department:

- Providing advisory services for the design, implementation and transformation of Internal Audit functions
- Managing Internal Audit functions within the scope of cosourcing and outsourcing contracts
- Performing independent reviews of the Internal Audit function based on standards of The Institute of Internal Auditors (IIA)
- Designing, implementing and reviewing risk management systems
- Providing advisory services on the development, documentation, transformation and organization of sustainable Internal Control Systems (ICS)
- Developing, implementing and reviewing Compliance Management Systems
- Developing and implementing a sustainable corporate governance model (coordinated assurance)
- Carrying out assurance engagements based on the International Standard on Assurance Engagements (ISAE) 3000

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

Robin Gerber
Director, Internal Audit, Risk and Compliance Services (IARCS)

+41 58 249 77 42
robingerber@kpmg.com

Alessandro Gabriele
Senior Manager, Internal Audit, Risk and Compliance Services (IARCS)

+41 58 249 28 39
alessandrogabriele@kpmg.com