Enhancing value from internal audit

KPMG Netherlands Internal Audit
Risk & Compliance Services

July 2020

Enhancing value from internal audit

The internal audit function was designed to *add value and improve an organization's operations*. How this can be achieved evolves over time.

Here we outline five key challenges that internal auditors are currently facing, which should be addressed to achieve enhanced value from internal audit.

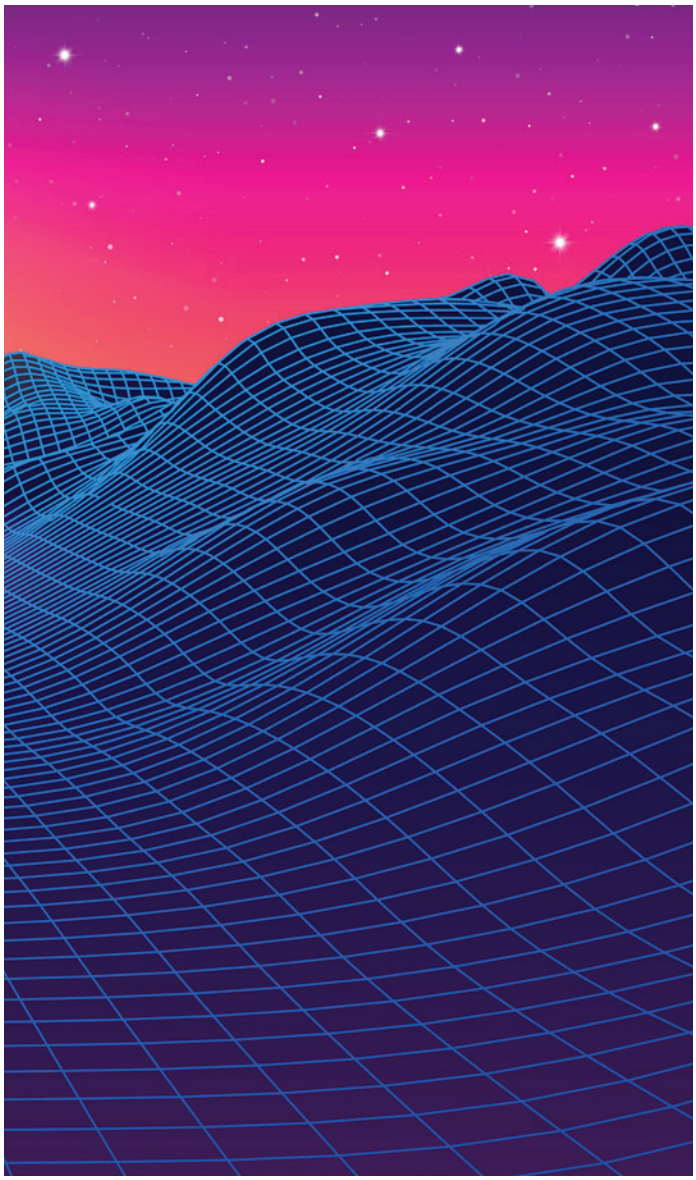
Challenges facing internal audit functions today

1. Increased complexity and volatility in the risk and compliance landscape
2. Stakeholder requirements to provide insights into emerging risks
3. Expectation to go beyond preserving value to creating value
4. Requirement to fill the technology gap – e.g. through the use of data analytics, process mining and other advanced internal audit techniques
5. Creating a multi-disciplinary team that is up for the task

Based on our cross-sector experience, we have identified three main areas internal audit can focus on to address the above-mentioned challenges as a prerequisite for sustainable enhanced value from internal audit:

Internal audit's interactions within its eco-system – achieving integration of GRC activities

Governance, risk and compliance (GRC) is all about defining the playground within which the organization wants to operate in order to achieve its objectives. The borders are defined by the risk appetite, regulatory landscape, desired culture and behavior, and the policies and procedures defined by the organization.



What do we see today?

We often see a very fragmented approach towards GRC, where uncoordinated activities are performed by the different second and third line functions (risk management, compliance, internal control, internal audit, etc.). While internal audit functions are often focused on executing their audit plan, we rarely see them connecting the dots.

This leads to various inefficiencies – on one hand, the business receives an overload of requests, distracting them from running the business and delivering value. On the other hand, fragmented reporting typically lacks the transparency that those charged with risk oversight (i.e. boards and audit committees) need to ensure the risk and compliance landscape is properly identified and addressed.

What does best practice look like?

An integrated Governance, Risk & Compliance (iGRC) system is a key success factor for addressing today's challenges around the increased complexity and speed of risks, as well as the high expectations of stakeholders – including boards, risk and audit committees, and senior management.

Internal audit can, and should, play a key role in achieving iGRC, given their purpose of providing assurance that the organization is in control, and their view on the overall risk and compliance landscape of the organization, its stakeholders, and the actors involved.

They should also limit requests to a 'need to know' basis and coordinate their activities to ensure the business is only interrupted once for the same request.

How can you get there?

Involve your internal audit function, particularly in the assessment phase of your GRC Target Operating Model (TOM) implementation:

— Identify and scope the **risk and compliance landscape**, which will be the basis of your GRC TOM. What are the compliance requirements and types of risks that are relevant for your organization, e.g. GDPR, Credit risk, SOX etc.?

— Define your **risk and compliance appetite and strategy** for each TOM component – what do you want to achieve? For example, you might have a low risk appetite for GDPR if your organization is active in a sector that is sensitive to data privacy. So your strategy might be to have a state-of-the-art GDPR compliance framework. For SOX compliance the strategy might be to minimize the cost of compliance as much as possible.

— **Evaluate the organization's current state** – its strengths and weaknesses; its maturity of the different components – in order to identify and map the gap between the 'as is' and the 'to be' situation.

What will this achieve?

Integrating your governance, risk and compliance components will help your organization to:

- avoid blind spots in your risk and compliance framework, by ensuring that the risk and compliance landscape is sufficiently covered;
- avoid inefficiencies, and thus save costs, by optimizing the cost-efficiency of the second and third line functions; and
- provide integrated reporting and insights to stakeholders.

How internal audit operates - dynamic auditing

Dynamic auditing combines agile auditing with technology and data analytics.

What does best practice look like?

Leading practice internal audit departments are leveraging data analytics and other tools/technologies during all internal audit phases. During risk assessment, it helps to identify (high) risk areas in an automated way. For the execution of the internal audit assignments, it ensures unusual trends or patterns are detected, and enables a more comprehensive understanding of the process. Auditors can then focus their efforts on analyzing the results and investigating outliers.

There are four key agile auditing fundamentals:

— **Interactions.** Sufficient and clear communication is key to an agile way of working. In this way, draft report findings should not be a 'surprise' to the auditee or senior management.

— **Working software.** Small pieces of 'working software' (or phases of an audit process) are delivered to the auditee at set intervals, or 'sprints'. At the end of each sprint, all work papers are reviewed, a workshop is planned, and the root cause analysis and outcome are discussed together with the auditee.

— **Customer collaboration.** Stakeholder involvement is essential to success – internal audit should determine, upfront and with stakeholders, the value to be delivered by an audit; what level of assurance is needed; and what risks are most concerning. Then a cross-functional, self-organizing team should be formed based on business area or technical domain (e.g. data analytics) to define, build, and test during the executions of the audit.

— **Responding to change.** If you are not able to respond to change you will not be able to please customers or to provide business value.

How can we get there?

Data analytics maturity

In assessing your data analytics maturity, consider: the strategy and goals of your organization; your internal audit strategy; the skills of your internal audit staff; the internal audit process and procedures; the available technology within the organization; and the data quality within the organization.

Based on the assessment of each of these components, your internal audit department can set its data analytics goals and ambitions to achieve a certain level in phases.

KPIs are a useful way to follow this up, for example, percentage of audit programs where data analytics is embedded, and percentage increase in audit coverage through use of data analytics.

Agility maturity

In assessing your agility maturity, consider: the strategy and goals of your organization; the skills of your internal audit staff; the internal audit process and procedures; and the available technology (tools) within the organization.

Based on the assessment of each of these components, your internal audit department can set its agility maturity goals and ambitions to achieve a certain level in phases. Clear KPIs should be defined after goals are set, for example, the percentage of agile audit missions.

Your role as a board

Together with your head of internal audit, the board can challenge whether agile principles are considered to enhance the value throughout the different audit phases.

- **Audit risk assessment and planning phase:** Do you have a flexible internal audit plan resulting from periodic or continued assessments and communication? Based on management feedback, can you conclude that key risks were defined and addressed in the audit plan?
- **Audit execution and close out phase:** Do the auditees consider that there was an accelerated and continuous communication of issues? Based on executive committee feedback, does internal audit leverage on reporting practices that are aligned to their needs (e.g. simplified reports)?

What will this achieve?

Dynamic auditing – through the use of technology and data analytics, and agile auditing – will help your organization achieve:

- **Enhanced internal audit planning and risk identification that adapt to the context.** Agile (rather than rigid) internal audit planning maintains a periodically updated planning to be executed with clear goals, prioritizations and resource planning.
- **Improved quality, standardization, and effectiveness, providing a greater level of assurance.** The use of data analytics and technology enables a more effective identification of fraud risk, while the visualized results from the data analytics queries adds value to the reporting, and the focus on business and stakeholder needs provides more valuable insights.
- **Accelerated audit delivery cycles and faster delivery of (sub)products, leading to increased capacity.** Internal audit executes within timed sprints to complete a set of well-defined and prioritized tasks. Sprints set a faster execution cycle for audits by setting out to provide a level of assurance or to confirm a hypothesis.
- **Empowered stakeholders because of the interactions and collaboration focus.**

What internal audit delivers - enhanced insights

Internal auditors are the eyes and ears of the board. They should:

- identify and provide insights into key risks for the organization;
- pro-actively identify emerging risks that could disrupt the execution of the business strategy;
- provide assurance over those key areas impacting the business on a regular basis;
- be aligned with the organization's strategy and should timely adjust its plan to any business changes.

What are some of the key risks that internal audit departments should be considering?

- **Technology-related risks.** Internal audit should possess the knowledge regarding emerging technology-related risks, such as **digitalization**, cloud computing services, and the resulting cybersecurity threats, and must address, if relevant, the coverage in the audit plan. For example, IA must identify and assess the mitigation of the risks associated with the impact of digitalization. They must be able to perform independent audits of the **cloud computing** setup to assess the level of security controls and provide potential areas of improvement, and assist the organization to develop ongoing monitoring mechanisms to monitor the performance of the cloud service vendor. They must conduct specialized **cybersecurity** audits such as vulnerability assessments and penetration testing.

— **Culture, behavior and soft controls.** More often than not, it is the behavior of people that drives decision making, thus influencing organizational performance and the effectiveness of the controls present. Internal audit should conduct an audit on soft controls in the organization and provide assurance over the current culture in the organization and its impact on the effectiveness of the controls set in place.

— **Third-party risk management** has grown in importance over the years as organizations choose to outsource their business functions to third-party vendors. Internal audit should assess whether the organization has established a contract management framework, scorecards to monitor third-party relationships on an ongoing basis, and comprehensive overview of all the outsourcing arrangements, including all the contractual obligations and regulatory requirements.

In addition, the COVID-19 crisis has brought new challenges and new risks. Internal audit functions can bring more added value by engaging more proactively – such as, by participating in key crisis meetings, advising the business on (temporary) changes and workarounds in the business operations, performing quick scans, and limiting the audit scope to key aspects, with a focus on providing assurance on the minimum level of controls that may not be compromised despite the crisis. Additionally, there are risks to reconsider, such as fraud risks, strategic risks, and business continuity and crisis management risks.

How do we move towards a more insightful internal audit?

— **IA strategy.** Ensure a strategic vision is established for your internal audit function. To provide real-time value to the organization, internal audit must align its activities with the organization's vision. Does your internal audit sufficiently focus on the topics that impact the strategic objectives of our entity and on the emerging risks?

What will this achieve?

- Providing insights in new risks and emerging trends / signals of change
- Stronger strategic alignment

— **Positioning.** Ensure internal audit's stature is sufficiently high. It needs a seat at the table, and by demonstrating a deep understanding of organizational needs and delivering greater value with deeper, more relevant and more timely projects, it is likely to get it.

— **Close interaction** with key stakeholders is critical to timely identify any change in priorities.

— **Alignment.** The audit plan and audits should be aligned to business changes.

— **Skills.** Ensure your internal audit function has all delivery capabilities – deep business know-how, and an understanding of the ins and outs of individual business processes and how each ties back to the big picture from a risk perspective.

Conclusion

Which elements of these three pillars are the most important for your organization? Discuss internally whether you meet them or which further actions are needed. For example, do you need a better integrated risk landscape? A shift away from the traditional way of auditing towards more agile auditing, using all available technology? A change of the internal audit plan with a higher focus on new risks, new technologies, or strategically important risks that have been ignored so far?

Contact

Bart van Loon
Partner
Internal Audit, Risk & Compliance Services
T: +31 20 656 77 96
E: vanloon.Bart@kpmg.nl

Huck Chuah
Internal Audit Services
Partner
T: +31 6 463 660 13
E: chuah.huck@kpmg.nl

With contributions of Erik Custers
Consultant Internal Audit, Risk & Compliance Services