Internal audit's own risk assessment

Internal auditors regularly make recommendations about risk management but when's the last time you listened to your own advice? Internal audit faces its own uncertainties which need to be managed: budget cuts, organisational restructure and mergers. In addition to the impact of working arrangements on providing assurance with the potential for permanent hybrid arrangements and ambiguity over an end to social distancing measures.

This piece provides you with the tools to get started on creating your own risk register, or updating an existing one, and will hopefully stretch your thinking.

What is risk identification?

Risk identification is important because it helps you make better decisions...decisions about what to do, what to prioritise and what's no longer relevant. It enables the internal audit team to meet the needs of the organisation by delivering high quality assurance and advice on the subjects that makes a real difference.

Internal audit doesn't own risk….

It's an inherent human flaw to avoid talking about hard to address risks!

Even for audit leaders…..

But all leaders must own risks relevant to their operations; internal audit is no exception.

Everyone has a responsibility to identify risks and take responsibility for the risks which are assigned to them. While internal audit must never take responsibility for organisational risks, they must take ownership of their own risks.

We have strategic goals and audit outcomes, processes to achieve them, standards to abide by and behaviours and values that define our professionalism. Uncertainty is part of life: things that stand in the way of success (threats) and things that can help us excel (opportunities).

Internal audit has its own unique risks to achieving its objectives. They should be documented, managed and shared (with the audit committee) just like any other function is expected to do.

The audit committee together with the head of internal audit must take ownership of internal audit risks.

But I have a QAIP!

Great. So, for you the question is how did you put it together?

If you don't have a QAIP (a quality assurance and improvement programme) you may want to think about creating one as it covers everything… an all-encompassing action plan. It goes hand-in-hand with a risk assessment not to mention that it's a mandatory requirement (IPPF standard 1300) for audit leaders following global best practices.

One element of the QAIP is defined as 'risks impacting the internal audit activity have been identified and managed'.

A risk assessment is more than a line about known problems such as insufficient resource or compromised reporting lines. It's a comprehensive evaluation of an activity or goal. It enables meaningful actions to be agreed.

A QAIP, even a good one, can fall into the trap of being comfortable. As internal auditors we like things to be evidenced, it's part of our professional due diligence. Yet this strength is also our weakness when it comes to risk management. We are prone to fixing our thinking based on what we can prove. Compound this with another human failing of confirmation bias where we favour information that supports our position and you can see where the value of a genuine risk assessment comes into play.

Risk basics

Taking a moment to think about risk is always a good use of time.

We all know that the only certainty is that things will change…with or without our intervention or approval. It's better to be on the front foot, as proven in the early months of the coronavirus pandemic.

Risk is about uncertainty…events that might happen.

If it's never happened it might in the future. It's a risk.

If it's happening now, it's an issue not a risk.

If it's already happened, then there's a risk it might happen again.

To keep it simple, here are three types of risk worth thinking about.

- **Preventable risks** - things we can influence and actively manage in our day to day processes and routines (planning, methodologies, policies, systems, partnerships, recruitment, relationships, skills) with rules-based controls that prevent and/or detect.
- **Strategic risks** – things that take us out of our comfort zone that we do to better our position (projects, trials, initiatives, development, reputation, structure) but that we can only do our best to manage, there are no absolute controls.
- **External risks** – things out of our sphere of influence (funding, partnerships, reputation, relationships, pandemics and stranded ships in the Suez canal, etc) that we need to be alert to and be prepared to deal with.

Internal audit's risk appetite

The organisation will have a risk appetite and culture which internal audit needs to take into account. It would be inappropriate, for example, if the function used a slow, paper-based methodology in an organisation that valued digital innovation. Likewise, in a company operating at high risk, auditors may need to be more cautious at times than their operational colleagues.

Ultimately, the audit committee need to decide the risk appetite for internal audit with the head of internal audit.

As an audit leader, what is your personal risk appetite? Does the audit committee support you when needed? Perhaps this is a conversation to explore with the audit committee chair…

Risk assessment process

There is no one size fits all approach for doing a risk assessment. If you have a small team in one location, a simple 2x2 grid may work with likelihood and impact going from low to high. For a large team split across locations you'll need consistency so a more traditional scoring matrix may be preferable to enable consolidation.

Detailed guidance is available for internal auditors on undertaking a risk assessment of the internal audit function. It has all the tools you need to get started.

One thing is certain: involve the whole team and your stakeholders. The more insight the better, the more diverse perceptions and opinions the richer the evaluation…doing a risk assessment builds strength, it does not demonstrate weakness. Weak leaders are those that avoid risk and its management.

Objectives and goals of internal audit

An effective risk assessment has a solid foundation focusing on objectives: internal audit's strategic and operational imperatives. Whatever these look like for you, relevant to your organisation's needs it is also worth considering the core principles of internal audit effectiveness. What risks can you identify for your team in achieving these requirements?

1. **Demonstrates integrity.**
2. **Demonstrates competence and due professional care.**

3. **Is objective and free from undue influence (independent).**
4. **Aligns with the strategies, objectives, and risks of the organisation.**
5. **Is appropriately positioned and adequately resourced.**
6. **Demonstrates quality and continuous improvement.**
7. **Communicates effectively.**
8. **Provides risk-based assurance.**
9. **Is insightful, proactive, and future-focused.**
10. **Promotes organisational improvement.**

Impacting decisions

The outcome of the risk assessment is invaluable in deciding where to focus precious audit resource: time, skills and funding. There is often little unproductive time in the strategic audit plan, delivering assurance and advice is after all the primary role of internal audit.

Knowing which risks are potentially the most impactful, the most likely to happen means that appropriate risk treatments can be put in place. Using risk information to make informed decisions and prioritising actions to the most important outcomes.

Sharing this information with stakeholders, particularly the audit committee demonstrates strategic leadership and provides those with the ultimate accountability the information needed to oversee the function.

Closing thoughts

Risk identification, evaluation and assessment are essential elements of risk management, one of the cornerstones of good governance. Audit leaders need to be skilled not only in the theory of risk management to deliver assurance but also the practicalities of it to manage the function. Without a genuine risk assessment to back them up even well-presented strategic plans and QAIPs can be reduced to nothing more than assumptions and ideas under robust audit committee scrutiny.

"There are no rules here – we're trying to accomplish something."

Thomas Edison