RISK NZ

RISKPOST

ENTERPRISE RISK MANAGEMENT AND INTERNAL AUDIT – WORKING TOGETHER TO LIFT RISK MATURITY WITHIN ORGANISATIONS

SURALDA TIMMERMAN – *Chartered Accountant (SA)*

As a risk professional, I understand the confidence and comfort which independent and objective assurance can provide the governing body of an organisation. And as an internal auditor, I see the immense value of a fully integrated risk management system rather than having a bolt-on process.

My career spans two countries and positions in the private and public sector. I collect interesting audits and risk assessments like treasured mementos. I have worked at Robben Island Museum, a UNESCO World Heritage Site, where operations included cultural and political heritage, endangered species and ferry operations. I have audited strategies and processes in healthcare, insurance, railway operations, fisheries, retail property management and social services. In all these roles, I have always strived to understand what the strategies and objectives are which make these organisations so unique.

In an organisational context, risk is inherent in the pursuit of objectives. How well an organisation navigates uncertain times and volatile environments, depends on their investment into the structures and processes that enable organisations to succeed.

The Institute of Internal Auditors (IIA) issued the updated Three Lines Model in July 2020. The Three Lines Model helps organisations identify structures and processes which best assist with the achievement of objectives and facilitate strong governance and risk management.

In this article I will focus on the roles of Enterprise Risk Management (second line function) and Internal Audit (third line function) within an organisation based on the Three Lines Model. I will also provide practical suggestions for the improved working relationship between these two functions, to ultimately enable a higher level of risk maturity within an organisation.

The role of enterprise risk management

Enterprise risk management (ERM) and other specialist second line functions provide first line management with expertise, support, monitoring and challenge on risk-related matters. [i]

Risk management is not static and is more than the listing of risks in risk registers. Risk management is the culture, capabilities and practices which organisations integrate within strategy-setting and apply when carrying out of the strategy, with the purpose of managing risk in creating, preserving and realising value. [ii]

The ERM function plays a vital role in embedding risk management culture, capabilities and practices within the organisation. ERM achieves this by ensuring that risk management becomes part of the organisation's management philosophy and not an add-on practice.

The role of internal audit

Internal audit (IA) provides independent and objective assurance and advice on all matters related to the achievement of objectives.

A helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes (IIA definition of internal auditing).

Internal auditors are not limited to focusing on the financial aspects of an organisation, but also consider risks related to strategy, operations, compliance, environmental and social responsibilities.

Why is there sometimes friction between enterprise risk management and internal audit functions?

I have noted over the years some of the issues which contribute toward friction between ERM and IA are:

- Lack of alignment.
- Poor communication and coordination.
- Not knowing how to work together while still maintaining the independence of their functions.

As a risk manager, I could see how frustrated management would become when Internal Audit proposed solutions which were just not viable in their current operating environment. Could the risk be addressed in another way? I would spend many hours as a go-between for management and the internal auditors to resolve these kinds of issues.

As an internal auditor, I could not always rely on the risk profiles or risk registers produced by the organisation. Good risk profiles and registers are one of the key components to a good internal audit plan and it influences the commitment of audit resources.

Practical suggestions for working together

Alignment

It is important for ERM and IA to use the same risk and control language when interacting with first line management. A well-developed risk management framework takes into consideration the strategy, operational environment and culture of the organisation. First line management become frustrated when ERM and IA use different impact and likelihood scales to rate risks or have conflicting definitions of what a control is.

At Robben Island Museum we had to develop a risk impact scale which could capture the different levels of risk within a hybrid organisation that includes heritage, ferry, ecological, educational, archival and tourism operations. Measuring risk on a generic risk impact scale was not possible. To develop this framework inputs from first and third line were crucial.

Communication and coordination

ERM works very closely with management to support them in the development and delivery of the organisation's strategy. Internal audit has a risk-based internal audit plan, designed to provide assurance and advice on very specific areas of risk within a given period.

The sharing of the risk work plan and internal audit plans is necessary for the following reasons:

- Shared understanding of the key focus areas for each function, to identify potential areas of duplication or key projects for collaboration.
- Coordinating timing of work to ensure that the first line staff are not inundated by requests from multiple units performing risk and assurance activities at the same time.
- Current and emerging risk trends which the ERM team is observing within the organisation, as this information could impact the delivery of the internal audit plan.
- Understanding the risk maturity of the organisation and how this impacts the delivery of planned work for both functions.

Frequent communication and engagement between ERM and IA are key to a better working relationship.

Collaboration

In building a better working relationship that will benefit the organisation, it is also important to consider areas where ERM and IA can collaborate.

IA and ERM can work collaboratively to explore root causes for internal control failures and come up with solutions which will be cost effective and address the risk adequately.

ERM can then use internal audit reports to facilitate informed discussions with the risk owner.

As risk manager I worked closely with an outsourced internal audit function to incorporate a control effectiveness rating scale into the audit reporting. This same scale was then used in risk registers to show how the effectiveness of controls impacted the residual risk rating.

Cross-discipline development

ERM and IA are two complementary specialist fields. Creating opportunities for team members to seconded into these roles, enables professionals to view the full risk management and assurance cycle from a more holistic perspective. This creates the opportunity for risk and internal audit specialists to develop new skillsets and enhance their capabilities.

It should be noted these secondments should be carefully considered to safeguard the independence and objectivity of the internal audit team members. Once internal auditors return from secondment to ERM, they should not audit any key risk areas which they were involved with during their secondment

In conclusion, ERM and IA have a significant role to play in how an organisation manages its risk while developing and implementing its strategic. By working together in a coordinated and collaborative way, with open communication and the willingness to learn from each other, these two functions can enhance the risk maturity level within their organisation.

REFERENCES

i. https://global.theiia.org/about/about-internal-auditing/Public%20Documents/Three-Lines-Model-Updated.pdf
ii. https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

SURALDA TIMMERMAN

Suralda Timmerman is a Principal Internal Audit Advisor at ACC. She has over 15 years' experience in external audit, internal audit and enterprise risk management. Suralda has worked at EY South Africa, PwC New Zealand and Robben Island Museum. During her time at Provisional Government Western Cape she was the internal audit manager for the Department of Health. She assists organisations in implementing practical risk management and assurance frameworks which ensure benefits to the organisations' stakeholders.