Assurance Across the Three Lines

A Collaborative Defense

In day-to-day vocabulary, a line of defense is defined as a structure used to defend against attack. Historically, in a military setting, a line of defense consisted of barriers of felled or live trees with branches (sharpened or entwined with barbed wire) pointed toward the enemy. In an organizational context, a line of defense is defined as a group of people that works together for a common goal.[1] In enterprise risk management, three lines of defense have been defined with separate responsibilities that enable effective risk management against any threat.

One chief operating officer in the financial services industry consistently referred to effective risk management as license to do and continue with business. Effective risk management is essential to enable the operational success of an organization in an industry that is highly regulated. Assurance activities across the three lines of defense can be used as tools to ensure confidence in risk management throughout organizations. As such, this approach has been adopted by a considerable number of organizations.

Assurance as a role that is embedded into risk management is explored here from the perspective of a risk practitioner and assurance provider. Risk management in this context is the practice of evaluating, responding to and monitoring risk and threats in order to mitigate operational losses, regulatory penalties, fraud and cyberattacks.

The three lines of defense are defined here in relation to responsibilities.[2]

The first line of defense is the function where risk ownership and management reside. They define the internal control of an environment by designing the granular processes and associated procedures. Some examples of such functions include business operations and operational management, risk management, and internal control measures.

It is not uncommon to find business operational management and key decision makers who have separated their activities from risk management. The expectation from business operational management has been that risk practitioners and assurance providers should proactively detect key risk and breaches in the business. Business operational management should play an integral part in risk management and demonstrate an understanding of the environment by identifying threats and risk inherent to the business, and collaborate with risk practitioners to manage and mitigate those risk. In many organizations, this is achieved through maintaining a database of risk and controls associated with key processes. Traditionally, risk and control matrices have been maintained in different forms and are updated as living documents. Risk ownership resides at the operational level.

Ability Takuva, CISA
Is a risk governance and control professional who began his career in assurance, IT audit and risk management at EY (formerly Ernst & Young). He currently heads the assurance function as the first line of defense at Absa Card and Payments, South Africa. He has 11 years of experience in risk management, assurance and IT audit, IT security, process optimization, and project management. His passion for the profession includes acting as a subject matter expert reviewer for ISACA® publications such as audit assurance programs on identity management and cybercrime and white papers on incident management response and security as a service.

Operational management must attest to the design and operating effectiveness of controls, and some organizations have testers/assurance providers that reside in the first line of defense. Generally, a risk-based approach is adopted to establish the frequency of key controls testing. In one organization, it was observed that subject matter expert (SME) operators in collaboration with assurance professionals were being tasked to review operational processes and associated controls. Independent SME operators may be, for example, operators from other business units with similar functions. While this collaborative approach encourages skills transfer and promotes effective time management as less time is spent learning while auditing, this could irritate the auditee.

> **"Collaboration is required in governance of risk activities as stakeholders evaluate, respond to and monitor risk."**

The second line of defense is the function that checks and challenges the activities performed by the first line of defense. Stakeholders in this line of defense perform an oversight role and oversee the risk. This is where policies should be set. Implementation and compliance thereof should be monitored here as well. Some examples of such functions include compliance, quality, risk management, security and financial control.

Some level of assurance activities are also performed by the second line of defense as a tool to provide an opinion on compliance to policies and regulations.

The third line of defense is an independent function that is mandated to report directly to the board of directors (BoD). Typical third line of defense functions include internal and external audit. In some organizations, the third line of defense is seldom included in key risk management activities, with the exception of conducting assurance activities. Why is this? Is it because they are mandated to report directly to the BoD and there is fear of not maintaining independence throughout the risk management life cycle? Is there perhaps a lack of trust in the organization that leads to expectations that the third line of defense must objectively participate in workshops that highlight internal control? Or, do third line of defense colleagues prefer to be viewed as policing from the outside? A response from many may simply be that the third line of defense should remain completely independent. Even if this response is true, it does not necessarily mean they should not be included in key risk management discussions throughout the life cycle. They should, however, remain independent from the design of processes/controls, execution and operational accountabilities/ responsibilities within an organization.

Collaboration is required in governance of risk activities as stakeholders evaluate, respond to and monitor risk (**figure 1**).

Assurance has been viewed as an enabler to facilitate risk management, although it is reactive in its nature. However, the value that it provides is significant. Today, most organizations are highly regulated and are driven by stringent regulatory requirements. For example, in the financial services industry in South Africa, a bank operating in the country is subject to many regulations that include and are not limited to the following:

- South African Reserve Bank Act, 1989[3]
- Financial Intelligence Centre Act, 2001[4]
- National Credit Act, 2005[5]
- Prevention of Organized Crime Act[6]
- Consumer Protection Act, 2008[7]

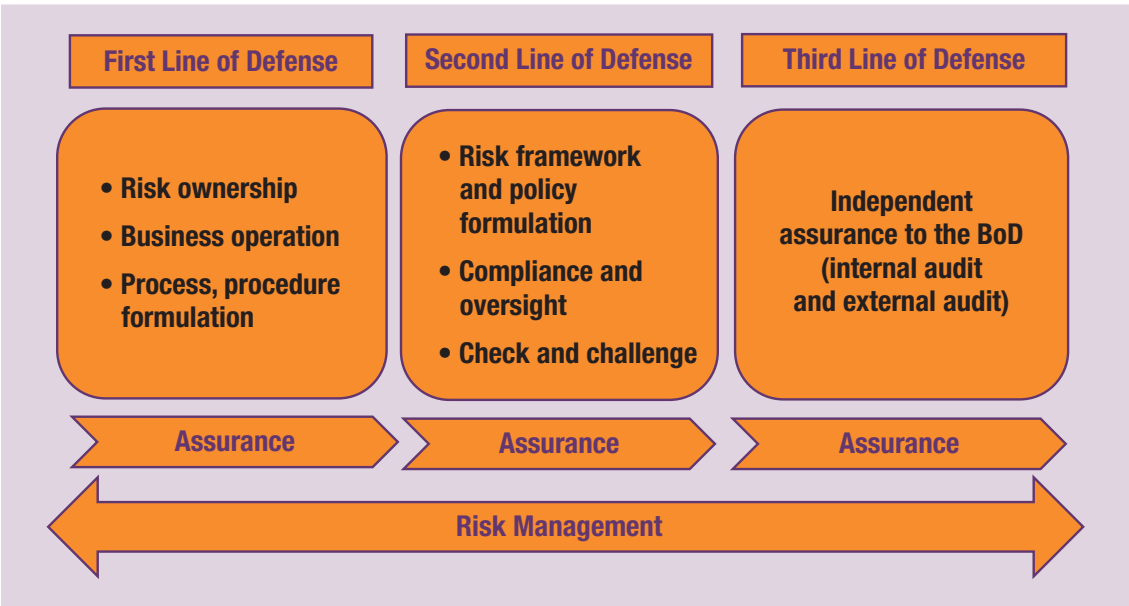
- National Gambling Act, 2004[8]
- Electronic Communications and Transactions Act, 2002[9]
- Protection of Personal Information Act, 2013[10]

Regulations originating outside a country in which an organization is based can also be applicable to the organization, provided they meet certain criteria. As an example, a player in financial services in South Africa is subject to US Sarbanes-Oxley compliance due to US affiliation (i.e., the organization is listed in the US stock exchanges and meets relevant financial criteria).

To ensure compliance with these regulations as a minimum, many specialized assurance areas are used to support the risk management strategy and framework. There is potential for these assurance areas to operate in silos. Traditionally, the assurance activity resides in the third line of defense. However, organizations have found value in assurance activities that are embedded across the three lines of defense as part of risk management to maximize expertise and knowledge. This model only works if implemented correctly.

Duplication and scope convergence become a regular occurrence if not implemented correctly and this can lead to frustrated risk owners and business operational staff. The frustration is due to the aforementioned duplication and endless reviews that span numerous cycles with a focus on similar risk themes. While different disciplines all have a role in assurance activities, collaborative risk management may be another way to effectively manage them. This allows for better scope management, and reliance can be placed on the activities that have been performed by different teams across the three lines of defense. Competent assurance providers are recruited in various disciplines across the three lines, so they can effectively collaborate and rely on each other's work. Auditing standards allow for reliance and, in some instances, limited procedures can be performed; this is according to the International Federation of Accountants (IFAC)'s International Standard on Auditing (ISA) 600.[11] The solution is, perhaps, a risk management approach that promotes joint collaboration assurance activities. This is increasingly becoming known as "integrated or combined assurance" in some organizations. The expectation is, however, that colleagues are operating from the same framework and standards.

Figure 1—High-Level Embedment of Assurance Across Three Lines



To achieve maturity with such collaboration, senior management should facilitate an environment that empowers the three lines of defense and fosters an environment for engagement and improvement. This can be achieved through risk governance forums that include assurance and joint planning of assurance activities. This also optimizes resources and skill.

> **"Assurance across the three lines facilitates improved ownership and accountability, which contributes to effective management of the control environment."**

Where third parties have an interest in the control environment of a service provider and governance thereof, it is worth having an International Standard on Assurance Engagements (ISAE) 3402 (ISAE 3402)[12] review. This is formerly the Statement on Auditing Standards (SAS) No. 70 (SAS 70) model in the United States, which has been replaced by the Statement on Standards for Attestation Engagements (SSAE) No. 16. SSAE No. 16 was issued with the intention of updating the US service organization reporting standard so that it mirrors and complies with the new international service organization reporting standard ISAE 3402.[13] This model encourages a service provider to proactively seek an independent assurance provider to supply an opinion of their control environment. Key controls are defined to support specific control objectives for major known risk factors. The report therefore, can be used by the service organization to give assurance to all their customers, avoiding the need to provide separate reviews on that environment for each customer.

Conclusion

As much as the assurance model described previously seems to detail potential duplicated activities across the three lines of defense, this model is effective if appropriate collaboration and engagement are achieved. Key success factors for effective implementation include:

- Executive management support
- Consistent application of frameworks and standards
- Intentional collaboration
- Joint planning across the various disciplines in the lines of defense
- Reliance on work performed by other assurance providers
- Skills transfer

Assurance across the three lines facilitates improved ownership and accountability, which contributes to effective management of the control environment. Executive management should, therefore, play a pivotal role in defining an overall organizational culture that promotes and enables the successful implementation of effective risk management.

Endnotes

1 Vocabulary.com, "Line of Defense," *https://www.vocabulary.com/dictionary/line%20of%20defense*

2 The Institute of Internal Auditors, *The Three Lines of Defense in Effective Risk Management and Control*, January 2013, *https://na.theiia.*

org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

3 South African Reserve Bank, *South African Reserve Bank Act 90 of 1989*, 1 August 1989, *https://www.resbank.co.za/BanknotesandCoin/Upgrade1Banknotes/Documents/SA%20Reserve%20Bank%20Act%2090%20of%201989.pdf*

4 Financial Intelligence Centre Republic of South Africa, *Anti-Money Laundering and Counter-Terrorism Financing Legislation*, 2012, *https://www.fic.gov.za/Documents/FIC%20Act%20Booklet%20202012.pdf*

5 National Credit Regulator, *National Credit Act, 2005*, vol. 1, 2007, *https://www.ncr.org.za/documents/pages/ENGLISH.pdf*

6 Republic of South Africa Department of Justice and Constitutional Development, Prevention of Organized Crime Act 121 of 1998, 21 January 1999, *www.justice.gov.za/legislation/acts/1998-121.pdf*

7 *Consumer Protection Act, 2008*, 29 April 2009, *https://www.acts.co.za/consumer-protection-act-/index.html*

8 National Gaming Board of South Africa, *National Gambling Act, 2004*, 12 August 2004, *www.ngb.org.za/SiteResources/documents/6_1-National_Gambling_Act.pdf*

9 *Electronic Communications and Transactions Act, 2002*, 2 August 2002, *https://www.acts.co.za/electronic-communications-and-transactions-act-2002/index.html*

10 Republic of South Africa Department of Justice and Constitutional Development, *Protection of Personal Information Act, 2013*, 26 November 2013, *www.justice.gov.za/legislation/acts/2013-004.pdf*

11 International Federation of Accountants, International Standard on Auditing 600 Special Considerations—Audits of Group Financial Statements (Including the Work of Component Auditors), 15 December 2009, *www.ifac.org/system/files/downloads/a033-2010-iaasb-handbook-isa-600.pdf*

12 International Federation of Accountants, International Standard on Assurance Engagements (ISAE) 3402 Assurance Reports on Controls at a Service Organization, 15 June 2011, *www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf*

13 Statement on Auditing Standards No. 70, *http://sas70.com/FAQRetrieve.aspx?ID=33300*