Three Lines of Defense
A methodology for the governance of risk exposure across the enterprise.
Three Lines of Defense

A methodology for the governance of risk exposure across the enterprise.

Reputedly derived from the work by Weike and Sutcliffe, ‘Managing the Unexpected’, published in 2001, Three Lines of Defense (3LOD) is now a risk management governance framework widely adopted by financial institutions internationally. However, much within the 3LOD approach is equally applicable to every enterprise, not just those that operate in the financial sector.

In the modern enterprise many diverse functions and teams may be involved in managing and controlling risk. As well as enterprise risk management specialists, there are also compliance officers, internal auditors, internal control specialists, quality inspectors, fraud investigators and other risk and control professionals involved in different elements of enterprise risk management. The challenge however, is to ensure that all of these different functions communicate effectively, and that specific processes are followed to ensure that there are no gaps in controls, nor duplication of effort. A clear framework that defines roles and responsibilities is required to ensure that the organization has a suitably robust risk and control operation.

The 3LOD approach brings together all of these disciplines within the overall governance of risk. While it is not a risk management standard, process or maturity model in itself, it is a methodology that offers transparency and risk related information. It ensures all areas involved in risk communicate in a meaningful way to better manage risk and, in particular, risk controls within the organization. This being the case, it is therefore also important to note that a risk management standard, process and approach to maturity evolution is still required in addition to the 3LOD model, as this is only one part of an overarching risk management strategy.

3LOD helps provide the governance for risk management as a key piece of management information by helping ensure that the global risk control framework is understood throughout the organization. It helps ensure that everyone understands their role within the risk control framework, and that risk policies and procedures are followed.

This paper aims to explain the 3LOD methodology and how it can be applied to any organization, regardless of size.
What are the Three Lines of Defense

3LOD has been adopted by many organizations internationally and is accepted as a form of best practice for governing current levels of risk by boards, management and regulators. It is a continuous process that focuses most specifically on the controls that are put in place across the enterprise to manage risk exposure down to an acceptable level.

It pulls together the different aspects of risk responsibility across the organization into a single process to ensure that all risk assurance providers are involved in the process of validating the effectiveness and reliability of the enterprise risk control framework.

The ultimate responsibility for risk management sits with the Board who answer to shareholders and regulators. The Board delegate to the CEO or managing director, who in turn would typically delegate this responsibility across the executive management team. The 3LOD model identifies three generic groups, those that own and manage the individual risks, those that oversee the risk and control process, and those that provide independent assurance that key risks and their associated controls are being managed adequately to meet company risk appetite levels and policy directives. In other words ‘do we have confidence that the risk management framework is operating as designed?’.

...It pulls together the different aspects of risk responsibility across the organization into a single process...

First line of defense – Operational Management

The first line of defense is the business, specifically management within operational divisions. Business managers that are managing the commercial activities are by definition the owners of risks. They understand the real risks to the business, whether this is, for example; geo-political risks of selling goods in Russia or China; financial risk of a merger or acquisition; geological risks of opening up a new oil field in the North Sea, or central Asia; workforce direct action within the supply chain; or day to day operational risk that is faced in the course of business, say, keeping a safe working environment for staff.

Importantly, operational management also owns any identified mitigation strategies designed to align the level of risk exposure with defined risk appetite tolerances. Of these mitigation strategies, it is the controls identified and deployed by Operational Management that are of interest to the 3LOD approach. At an enterprise level, the controls are the vehicles used to provide confidence that the inherent risk within the business is being managed down to an acceptable level of risk today.
Second line of defense – Risk Management and Control

The second line of defense is the central risk management function. Ideally lead by a Chief Risk Officer, the risk team reports to the board, providing expertise and advice.

This starts with identifying and quantifying the risk appetite of the organization. It goes on to design and implement an enterprise wide risk management framework that is capable of reporting on risk performance. The risk function provides risk control and mitigation strategies, and collects risk information to ensure that the organization understands where risk procedures are not being adhered to.

The second line of defense is primarily addressing the process and framework deployed to identify and control the risk exposures of the business, and in relation to the 3LOD, they provide the key process governance around the risk control framework.

This management function is often supported by specialized risk management teams in the area of project, health and safety, quality and compliance each looking to deal with risk around specific objectives of the business.
Three Lines of Defense –
Independent Assurance (Audit)

The third line of defense is the audit function. Typically in-house, but with a strong relationship with external audit and industry regulators. Audit provides independent assurance that enterprise risk control procedures are adequate and that they are operating effectively in design and operational terms.

Audit therefore helps ensure the effectiveness of the risk management framework and encourages continuous improvement through reporting and feedback. In relation to the 3LOD model, audit is the ultimate “catch” to ensure that key risks have been identified, that they are being managed by appropriate controls, and that these controls can be relied upon by the business.

Audit provides this assurance back up the tree to both the risk management teams and the ultimate risk owners, pulling together the assurance offered at each of the three levels of the model.

LOD Responsibilities
- Who does what?

Before the first line of defense, the CEO, executive management and governing bodies are responsible for setting the organization’s objectives, defining strategies to meet those objectives, and ensuring that governance structures are in place to define and control risks and opportunities within the business.

The key point when adopting a 3LOD model is that every stakeholder has a place in the process - processes build on each other, and everyone relies on having timely access to accurate data. This means that transparency and collaboration between different functions that may have traditionally seen themselves as completely separate, is the real key to success.

First Line – Operational
Divisions Key Activities

Operational management is responsible for owning and managing the risks within the business; Its first duty is identification and assessment of risks. This includes identifying the real risks taken by the business to achieve its goals and objectives; assessing the impact of each risk both individually and collectively to evaluate possible outcomes, and to set the risk appetite which is aligned to financial objectives.

The second duty is to agree risk mitigation strategies for those risks and appropriate handling controls to manage the level of current risk to an acceptable level. Operational management is responsible for ensuring the assessment of these risks over time, and for the ongoing effectiveness of the controls in managing these risks.
Second Line – Enterprise Risk Management Key

The risk management, compliance, quality and HSE functions are responsible for providing expertise and guidance to the business and the risk owners at an enterprise level. This takes three specific areas which are:

- A risk management function that advises on the most appropriate risk management framework to meet operational and financial requirements. This includes an infrastructure with processes to facilitate the collating of risk data and effective risk management. The risk team should set policies and procedures, and moniotor implementation to ensure operational parameters are maintained, and provide reports on risk management performance, to the business (risk owners), in terms of on-going guidance and training.

- A compliance function, of which there can be various different sub divisions that manage specific types of compliance, for example, health and safety, supply chain, environmental, quality, and risk management.

- A control function, which monitors financial risks and financial reporting.

The key point when adopting a 3LOD model is that every stakeholder has a place in the process...

Third Line – Independent Assurance (Audit) Key Activities

Internal audit, and often external auditors and regulators, provide independent reviews of the enterprise risk control framework. The aim is to provide assurance to the rest of the organization (but specifically the risk owners at Level 1) that the governance and risk framework is fit for purpose, and that controls and processes are effective. The audit team should undertake regular reviews, assessing the effectiveness of all internal procedures, with additional attention for areas where the levels of risk are high or unacceptable, providing feedback and recommendations to improve the risk management framework.
Overall, 3LOD provides a supporting method for good governance. For the Board and the CEO it helps to provide confidence that once the business has identified the key risks to the enterprise and their associated controls, that these are being evaluated, monitored and escalated when weaknesses are detected.

3LOD forces the three areas of risk management, i.e., the business risk owners, the risk and compliance management function, and audit to work together using shared data. In some organizations this can mean that data handling processes must be put in place, as the nature of some risks may be too commercially sensitive for widespread access. However, an enterprise risk management software solution will manage security classifications to ensure that the appropriate people see the appropriate information at the appropriate time.

3LOD gives risk and control owners greater confidence in the assessment of their risks and the stability of their important controls because they have a level of assurance provided by internal audit. This ultimately helps ensure that the business can better deliver against key objectives.

The audit function within the business is able to use 3LOD to prioritize its audit work schedule by identifying the areas of greatest risk significance, giving a lead to audit as to where best to concentrate resources in their audit plans.

3LOD gives risk and control owners greater confidence in the assessment of their risks...

### Key Benefits Summarized

- Helps organizations delegate and coordinate the control aspect of risk management duties across the business using a systemic approach.
- Improves communication on risk and controls by clarifying roles and responsibilities across the business.
- Improves the effectiveness of risk management as it is now being viewed across the business and with the right level of assurance from independent assurance contributors.
- Risk and controls owners have greater confidence in the quality of their assessment of uncertainty around the objectives they are responsible for.
- Assurance providers (auditors) have a method of planning their overall assurance program based upon enterprise risk prioritisation.
- The Board has a pan-organization governance process in place that covers the highest levels of stewardship and protection of future business performance.