Strengthening the Three Lines of Defense

By Richard Pike, Product Director, CCH Sword

Strengthening the Three Lines of Defense

By Richard Pike, Product Director, CCH Sword

Without improved communication and coordination, the traditional three lines of defense approach to risk management today is vulnerable. Richard Pike examines the ways in which these lines can be strengthened, ensuring responsibility for risk is understood, coordinated and shared across the organization.

The three lines of defense is a well-established concept that has been deployed across different industries and situations. It consists of:

- The business: The day-to-day running of the operation and the front-office;
- Risk and compliance: The continual monitoring of the business; and
- Audit: The periodic checking of risk and compliance.

This approach has offered thousands of organizations a solid foundation upon which to protect themselves against a range of potential risks, both internal and external. Some organizations adopted it proactively on their own as part of managing risk, and others may have had it forced upon them through regulators' insistence on external audits.

Regardless of circumstance, the three lines of defense concept is reliable and well proven — but it needs to be updated, otherwise, it risks becoming outdated in its ability to meet the rigors of today's market where there are a far greater number of risks and regulations, and an ever-increasing level of complexity.

For the three lines of defense to succeed in the current environment, the communication and relationship between each line needs to be better defined and coordination across all three lines must be clearly established.

This won't be easy to accomplish. In the majority of organizations, management of the various forms of risk — operational risk, compliance risk, legal risk, IT risk, etc. — are each carried out by different teams, creating a pattern of risk silos. This situation leads to a number of negative consequences.

The Negative Impact of Risk Silos

Inefficiency multiplies across silos

Silos may be very efficient at one thing, but that may be at the expense of the overall organization's efficiency.

In the case of risk silos, each gathers the information it needs by asking the business managers to provide various information relating to their daily operations and any potential risks associated with them. Because of the silo structure, the business will find itself being asked for this same information on multiple of occasions by multiple of risk silos. These duplicative efforts are inefficient and counterproductive, and lead to frustrated front-office staff disinclined to engage with risk management in the future.

The level of frustration is such today that when the recently appointed CEO of a large company asked his senior managers what single change would make their life easier, the reply was: Do something to stop the endless questionnaires and check sheets that managers were required to fill out to satisfy risk managers and compliance officers.

Frustration among business managers is never a positive development. But it can fully undermine a company's risk management program as buy-in from the staff is essential.

Inconsistency adds to risks

Silos also tend to lead to inconsistency as the same information will be interpreted in different ways by different risk teams.

This disparate relationship between risk teams can lead to the failure to recognize potential correlations between various risks. For example, the recent sub-prime mortgage crisis that has affected so many banks may have been partially avoided if there had been more coordination and communication between the banks' credit departments and those selling mortgages to people with bad credit.

Similarly the €6.4 billion loss at Société Générale was the result of several risk oversights, combining a lack of controls on individual traders as well as a failure to implement various checks on the trading systems themselves. Also contributing was a negligence of market risk factors with risk management failing to highlight a number of transactions having no clear purpose or economic value.

Tearing down silos

Major risk events rarely result from one risk; rather they commonly involve the accumulation of a number of potential exposures. Consequently, companies need to better coordinate their risk management functions and establish consistent risk reporting mechanisms across their organizations.

Applying this discipline to enterprise-wide risk management can be exceptionally difficult given that risk information is often delivered in inconsistent formats. For example, interest rate risk may be reported as a single Value at Risk number, whereas regulatory compliance or operational risk may be expressed through a traffic-light format. This disparity can make it extremely difficult for a chief risk officer, CEO or any senior executive to accurately rank risk exposures.

As a result, organizations are now recognizing the need to establish a common framework for reporting risk.

This is being undertaken through various initiatives across different industries — ICAS, Solvency II and often the Basel Accord. These initiatives have contributed to the growth of risk and compliance teams. However, the intent of these regulations is not to simply require firms to fulfill their most basic regulatory requirement and to set aside a defined sum of money to cover a list of risk scenarios. Instead, regulators want firms to concentrate on the methodology used to arrive at their risk assessments and to ensure that the risk management process is thoroughly embedded throughout the organization. This requires sound scenario analyses that bring together risk information from all of the various risk silos.

Improving audit coordination

Scenario analysis is very much based on the ability to collate and correlate risk information from all over the organization. This includes not just close coordination across the various risk areas but also with the internal audit teams. This ensures they are more effective and are not simply repeating the work of the risk and compliance teams but rather adding value by rigorously testing this work. Such a task requires using the same common framework as the risk and compliance teams so that information can be seen in the correct context.

When this occurs, everyone benefits.

There is much greater independence and objectivity in the internal audit role today. In an increasing number of organizations the internal audit function is no longer confined to existing within a corner of the finance department and has more direct communication with senior management.

Technology's Critical Role

The use of integrated technology to facilitate the evolution of the three lines of defense is a relatively new development, but will become essential in ensuring coordination across the three lines.

Because it has been hard to clarify the different lines of defense and their relationships, it has been difficult to build a business case for a new system and to build the necessary workflow around these different roles.

However, the current technology situation, where completely separate legacy systems are used in the business, risk and audit departments, is becoming intolerable and simply contributing to risk. Everyone is aware of the weaknesses in their own systems but this knowledge does not always translate across the three lines of defense.

This leaves most companies with two choices. The first is to design a new all-encompassing system from scratch. The second is to deploy a system that supports common processes and reporting while allowing each function to continue using specialist solutions that suit their own needs.

The successful firms will be those that recognize there are different functionalities in these different spaces but they are all able to communicate with each other in a common language and through common systems. For example, observations can be shared and specific risk issues can then be discussed through an e-mail exchange and summary reports can be automatically sent out to managers.

For internal auditors, a lot of their work is manually-based. Technology would enable work to be done more quickly and more accurately. The system would also enable organizations to make certain risk issues generic so that where a risk is identified in one office or department, an alert can be sent to all the relevant risk managers in other departments and offices to see if this risk has been recognized and if there are processes in place to manage this risk. By automating this identification of risk, it enables organizations to take a smarter, more efficient and more global approach to the internal audit function.

For business and risk managers, a system that supports common processes makes risk compliance much simpler. Risk teams have a limited set of resources and must rely on the business to carry out much of the risk process. This includes conducting risk and control self assessments, and recording any losses and control breaches where these losses occur. Using a system that supports common processes means business managers can accurately and efficiently contribute important information, while not being asked to duplicate efforts across risk silos. Risk managers also can then concentrate on the value-added side of their work and their role.

Bringing Business into the Fold

Beyond simply helping get the work done, there are far wider benefits to the organization from using systems that support common processes and the principle behind them. For example, the more that front-office staff is exposed to the mechanics of the risk management process (rather than being repeatedly petitioned for the same information from multiple parties), the more they are aware of its importance and their role in it.

Decades ago, total quality management was a fashionable concept in many organizations. The frailty of this concept was that in having a dedicated management team in this area, the rest of the business could assume that quality was no longer their problem, but someone else's. This same misconception could be applied to risk and compliance, unless the business is kept well-informed of the risk management process and their own role within this process.

Today, it is critically important that everyone realizes that risk is their responsibility. This requires a clear and open line of communication and coordination between the three lines of defense: business, risk and compliance and audit.

About the Author

Richard Pike, CCH Sword product director, has more than 15 years experience in risk management and treasury IT. He has analyzed, designed and managed the development of core treasury and risk management systems for large international financial institutions. He is a regular speaker and writer on risk management issues, and has been named one of the top 50 faces of operational risk by OpRisk & Compliance magazine.

Headquartered in Ireland, CCH Sword is a leading developer and supplier of operational risk control solutions to the global financial services sector. Established in 1995, CCH Sword became part of CCH, a Wolters Kluwer business in 2008 and was renamed from Ci3 to CCH Sword.