iPRO

Governance Spotlight:
Third Party Risks

The Three Lines of Defence Model

Risk management is a fast growing, broad ranging discipline that is spreading to organisations of every size and industry. As boards implement risk management practices, they increasingly find themselves at the centre of a network of analysts, auditors, managers, and specialists, all providing vast amounts of information regarding the risks the organisation faces and how those risks are being managed and mitigated.

The challenge lies in effectively leveraging this wealth of information, coordinating tasks and responsibilities, ensuring the flow of information between stakeholders, and communicating an understanding of risk management to the risk owners on the front line of the organisation.

By now, many organisations have implemented or begun to implement a three lines of defence model, an effective approach for delineating roles and responsibilities wherein the first "line" represents front line employees and the management team, the second line is the board of directors who oversee the risk management program, and the third line is independent verification and audit.

However, this model relies upon an engaged and knowledgeable front line, where employees understand their role in protecting the organisation and are trained and supported with the tools they need. To be successful the model needs to explicitly account for the huge importance of data management and technology adoption for organisations today. Issues like data proliferation – the same data collected from multiple sources and stored in different places – can lead to fractured data storage approaches that are incompatible with one another and reduce the available benefits of data aggregation and analysis.

For the three lines of defence model to be effective, organisations need to take advantage of technological advances that can contribute to their success. Contractor compliance management systems offer software platforms which automate the processes of storing and updating data and evaluating compliance, in order to reduce the risk of human error. These systems can constantly, automatically update and adjust as the regulatory context shifts. This advantage can be incorporated into each of the three lines of defence, adding an additional layer of security while integrating seamlessly with an organisation's overall risk management program.

The First Line of Defence:

Management Implementation

The first of the three lines of defence is made up of the groups that directly make risk decisions, such as operational staff and the management team. This line is responsible for designing internal risk controls, systems and processes, and supervising the running of those processes. For any risk management program to succeed, the support and engagement of operational staff and management is crucial. This requires risk management tools that support staff in taking ownership and embracing accountability for risk decisions.

Third party compliance management systems are a means of supporting and enhancing the capabilities of the first line. Automated processes offload the repetitive and tedious tasks of reviewing documentation, accounting for new regulations and adjusting to new data. Systems of alerts and notifications provide another layer of protection, offering real-time insight into an organisation's third party risk profile. These tools free up management resources for the more demanding work of exercising human judgement, evaluating data trends and making thoughtful risk decisions. Tools like this can support staff engagement by empowering staff to own their risk decisions and to see how those decisions align with the larger risk appetite of the organisation.

The Second Line of Defence:

Board Oversight

The second line of defence involves a risk management committee or similar team that is directly accountable for overseeing the organisation's risk management program. This responsibility is usually adopted at board level to support the management team by setting up monitoring systems and controls to track the performance and consistency of risk management systems, define the organisation's risk appetite, and provide a structure for reporting.

The second line of defence also includes compliance monitoring. This function is dedicated to ensuring that the organisation and, crucially, any third parties with which it does business, are in compliance with the regulatory environment in which they operate.

This line is intended to provide some independence from the first line, but there is a natural tendency for the two lines to get blurred, since they are both run within the organisation. Given the complications of the three lines of defence model, a contractor compliance management system is one means of bringing more independence to the second line, while simultaneously supporting the compliance monitoring operations of the organisation. These systems provide objective data, pre-arranged into dashboards and reports, to verify the performance of first line staff at a glance. By design, compliance management systems are amenable to the purposes of internal audits, and create a common platform that all levels of the organisation can access and refer to, helping to avoid "data silos".

The Third Line of Defence:

Independent Verification

Given that the first two lines are not completely independent of one another, the third line of defence provides independent monitoring and verification. This provides assurance to the board and management team on a wide range of objectives, evaluating the effectiveness of current policies and procedures and of the risk management program as a whole, as well as the performance of the first two lines of defence. Since independent reporting can be provided directly to the board and management team, data trends can be effectively interpreted into recommendations and action items and presented quickly to decision makers. Independent verification or internal audits should be as comprehensive as possible and will certainly include contractor compliance as this is a crucial aspect of third party risk, that is, the risk presented by the vendors, suppliers and service providers that an organisation is involved with.

An example of third party risk is the fact that many data breaches occur, not because of the organisation that originally owned the data, but because of a subcontractor with poor cybersecurity. In the case of the Target data breach in 2013, hackers took advantage of an HVAC provider who had authorisation to pass through Target's firewall to conduct electronic transactions. Third party risk refers to the fact that organisations now face reputational, regulatory and compliance risks from outside parties who may be 2 or even 3 degrees removed from the organisation itself. Given the enormous amount of data collected and stored by a typical organisation, and the rapidly changing compliance environment, software solutions can simplify and automate the process of evaluating compliance for the purposes of risk management.

Conclusion

The three lines of defence model can be used to effectively address the new risk management challenges that organisations face. The increasing pace of technological innovation has created a business environment where organisations must be constantly evolving in order to succeed.

Software platforms that assist with automating data collecting and analysis, particularly regarding compliance risk, are an important tool that can allow organisations to run progressive, well supported risk management programs.

How iPRO Can Help

iPRO offers an intelligent, transparent, real-time solution for compliance monitoring and verification. The iPRO Maturity Model assists organisations in defining best practices for contractor management and identifying gaps in their current methodologies.

Find out more at **ipro.net.**