CEP Magazine - October 2019
Vendor risk management

By Ian Shaw

Ian Shaw (ian.shaw@sword-activerisk.com) is Product Manager at Sword GRC in the UK.

As more and more organizations outsource business functions such as IT, the question arises: Just how reliable are the vendors providing the services? What happens if/when something goes wrong? Just because you've outsourced the function, doesn't mean that you've also outsourced all responsibility. As a business, you still need to meet regulatory and legal requirements, and any transgressions by the vendors you use could reflect badly on your own brand.

The Deloitte global survey on third-party governance and risk management[1] highlighted how leading organizations are those that are able to protect their value through risk management and that third-party relationships, being a key part of the extended enterprise, need to be managed just as closely as every other part of the business. Furthermore, many of those leading organizations are looking to enhance the value of their third-party relationships with positive risk management.

What is vendor risk management?

Third-party vendor risk management is markedly different from supply chain risk, but every bit as important. Supply chain risk in a manufacturing company is typically where you rely on suppliers for goods as part of the manufacturing process, and the risk associated might be price fluctuations in raw materials, transportation issues, even geopolitical unrest when dealing with overseas suppliers.

Vendor risk management is where an organization outsources operational elements of the business, typically IT, facilities management, payroll and HR/recruitment, or finance, and these days such services are typically hosted in the cloud. Some desktop business functions have become so deeply entrenched in the cloud that we might not even think of them at first, for example, Microsoft Office 365 and Salesforce. You are placing a great deal of trust in the vendor to deliver the service on demand, and to take care of your corporate information, and while the risk might be with the vendor, as a business you are still liable if anything goes wrong, and the responsibility is ultimately yours.

Reports of third-party risk incidents are on the rise. Indeed, 87% of the respondents in Deloitte's survey said they had faced a disruptive incident with parties in the previous two to three years.

In short, you might think that you have outsourced the risk, but you haven't! Any slip-ups and it is the reputation, brand value, and even share price of your business that will suffer, not to mention regulatory fines as a result. For this reason, any third party that your business deals with should be able to comply with your own internal standards, regulations, and ethics. Knowing what these standards are, and ensuring that your own staff understand and comply, is the first step.