SAPinsider

This article appeared in the Apr ▪ May ▪ Jun 2016 issue of *SAPinsider* (www.SAPinsiderOnline.com) and appears here with permission from the publisher, WIS Publishing.

WIS pubs

Gain Control and Mitigate Risk

Leveraging 3 Lines of Defense for a Holistic Security Framework

by Bruce McCuaig, SAP

Technology is connecting people, devices, and companies around the world like never before. And while this connection presents nearly boundless business opportunities, it also brings forth greater security threats to both companies and their customers. Cybercriminals are advancing as quickly as the technologies they are tapping into, obtaining access to intellectual property (IP) and customer account information — and disrupting business. A cyber breach not only can shut down a company's website or its entire operations, it can also damage its reputation.

Organizations must safeguard against a mounting variety of points of exposure. Because of the rapidly proliferating Internet of Things (IoT), hackers can access sensitive information not just through enterprise software, but also through various other systems. And a single system in a vast, connected network is enough — once attackers get into one system, they can easily get into anything else. In addition to protecting against external threats, it's critical to make sure that employees are properly trained to know what to watch for, what to do, and what not to do.

With all these risks present, businesses need to protect their systems with a consistent security framework across the entire organization. This framework should identify each entry point into your system and provide a checklist for securing and monitoring vulnerabilities. Are you updating your security systems properly? Are you using passwords? Can you monitor the status of your entry points? Can you detect when those points are under attack?

This is the mindset behind SAP's cybersecurity framework, which follows a three-lines-of-defense approach. This method provides a unified process that ensures risk, compliance, and audit systems work together for maximized security, protecting you against threats both inside and outside of the organization.

3 Lines of Defense

Let's look at the three lines of defense (see **Figure 1** on page 14) in more detail.

1. Operational Management

The first line of defense focuses on identifying and assessing each risk so you can then determine where to manage that risk. This is a critical step for establishing clear responsibilities. Determine the risks in a particular environment and ensure that the accountability for managing those risks is clear. In this line of defense, the organization is focused on maintaining effective controls and implementing and complying with internal policies and procedures.

2. Risk and Compliance Management

This second step ensures that the people on the first line of defense are using the right tools and frameworks — in other words, this step verifies that the first line of defense is operating as designed. For example, if you have a data center using ISO 2700, the standard computer security framework, and another area of the company is using an entirely different type of framework, you will want to correct this so that there is a consistent approach to managing risk across the enterprise. The key to this second line of defense is to provide quality assurance and completeness — to ensure that all the risks identified by the first line of defense are managed consistently across the organization by setting

Figure 1 The three lines of defense provide for a comprehensive security framework

up continuous monitoring of all risk, control, and compliance requirements.

3. Independent Assurance

The third line of defense provides comprehensive and independent assurance, typically by internal auditors. These auditors are responsible for making sure the first two lines of defense are working — first, that all controls are in place and working, and second, that risk management is consistent across the entire enterprise. Should the auditors find anything that needs improvement, they can provide feedback to the first two lines for how to better carry out their tasks.

Realizing the Value

The three lines of defense serve as a framework for managing risks and monitoring efficiency, but to ensure that your organization is truly safeguarded against an attack, there must also be a system in place for reporting and determining performance metrics. This means getting reports and the overall status of IT and cybersecurity to executives, who can then make decisions and allocate resources as necessary.

Additionally, to get the biggest return on the three lines of defense, its principles must be applied to strategic processes as well as operating processes. There is less value in placing the framework around only payroll, accounts payable, or inventory processes; the real benefit is applying the framework to the strategic business processes that add value, such as new product development. The technology behind this framework also vastly streamlines GRC processes, eliminating overlaps and duplications with the auditing process, and dramatically reducing the overall GRC footprint of the company.

A multinational conglomerate has seen a number of benefits since launching the three-lines-of-defense model powered by SAP solutions for GRC, including SAP Access Control, SAP Process Control, and SAP Risk Management. The company was in need of a consistent, standardized, and speedy way to stay compliant across the business. The platform also needed to fit within the company's existing ecosystem, expand with the organization, and leverage the tools it already had.

SAP solutions for GRC gave the company the ability to integrate with its existing access control environment and have a standard language across its SAP ERP environment.[1] It was also able to reduce the number of controls that needed to be manually audited and reviewed by 40% and move to continuous monitoring. The company also gained a stronger understanding of the measures required to track risks, as well as refined reporting capabilities and enhanced risk tolerance.

Becoming Strategic

The three lines of defense model is not just about protection — it is about giving GRC professionals the tools and freedom they need to focus their resources on more strategic types of risks. By the same token, it also provides much more complete, comprehensive information to executives. More informed decision makers can begin to manage operations from a GRC perspective in a more strategic way, allowing them to better allocate resources and deploy new technologies. For more information, visit **www.sap.com/grc**. ■

Bruce McCuaig (bruce.mccuaig@sap.com) is Director, GRC Product Marketing at SAP. Bruce has executive and board-level experience in implementing and managing three-lines-of-defense solutions.

[1] For more about SAP solutions for GRC, see Thomas Frénéhard's article "Integrated Security Solutions to Mitigate Risks on All Fronts" on the next page.