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

Integrated Security Solutions to Mitigate Risks on All Fronts

How SAP's GRC and Security Framework Protects Companies in the Digital Age

by Thomas Frénéhard, SAP

In the wake of a transition into the digital economy, data starts flowing into the enterprise at an unprecedented rate. Companies must then determine what constitutes sensitive data and who in the company has access to that data, more closely integrating security and governance, risk, and compliance (GRC) efforts into the organization's overall operational strategy. Guarding against malicious data and preventing the misuse of data create both challenges and opportunities for businesses as they better integrate security concerns with their overall digital transformation strategy.

New and different types of structured and unstructured data — not just transactions, but social media data, customer sentiment information, and signals from devices connected to the Internet of Things (IoT) — bring new risks. These risks create a demand for integrated GRC solutions that not only can ward off new lines of attacks and threats, but can also create a single enterprise risk assessment picture. This is accomplished when an integrated solution set is aligned with a security strategy that encompasses three tightly knit lines of defense[1] — operational management, risk and compliance management, and independent assurance — replacing what for many companies had been a false sense of security with comprehensive protection.

SAP's GRC and security platform for the digital age is built with the understanding that the automation of controls is just the tip of the iceberg for end-to-end security. A proactive approach to risk mitigation necessitates operations working in concert with a robust risk and policy framework that is created specifically for the unique needs of the enterprise. An independent internal audit team closes the loop by providing independent assurance that a sound risk and control framework is in place, while also retaining the ability to tailor the audit mission according to new risks, failure in controls, or other potential threats.

[1] For more about the three lines of defense, see Bruce McCuaig's article "Gain Control and Mitigate Risk" on page 12.

Create an Enterprise-Specific Risk Catalog

SAP Risk Management, SAP Process Control, and the SAP Regulation Management application by Greenlight form an integrated toolset that a company can use to create a sound risk and control framework based on the identified risks. SAP Risk Management is used to create and automate a comprehensive risk catalog relevant to a specific organization or industry. While SAP Process Control is used to create processes and controls in line with a specific risk catalog, SAP Regulation Management by Greenlight is used for intake, bringing new regulations and frameworks into the fold and handling them accordingly.

Prior to the current business environment, in which companies are increasingly embarking on digital transformations, SAP Process Control and SAP Risk Management were more loosely connected. This was somewhat by design, as a single risk assessment for the enterprise was considered less important than the ability to perform individual risk assessments and reporting by line of business. With a single risk assessment and a tailored risk catalog, however, a continuous link — along with operations to manage both the risks and controls that have been implemented — becomes important.

For many SAP customers, the creation of a risk catalog with SAP Risk Management and SAP Process Control is known as the second line of enterprise defense, and will be distributed and associated with the risks and controls managed by operations, known as the first line

of defense. Within this risk framework, stakeholders are assured that a single view of risk assessment for the enterprise is under continual review, with newly identified functions and risks easily logged and monitored in the system. Operations uses the same solutions — SAP Risk Management, SAP Process Control, and SAP Regulation Management by Greenlight — but to manage its processes, risks, and controls rather than to create a risk framework.

Ease the Audit Mission

An independent assurance of the validity of a risk assessment framework provides an added layer of enterprise security as a third line of defense. Internal auditors can create and tailor an audit strategy by copying the risk and control universe from SAP Process Control and SAP Risk Management into SAP Audit Management. This means that any new risks or functions added to a risk framework are immediately viewable in SAP Audit Management, allowing auditors to modify an audit mission according to changing risk levels.

Audit teams struggle with data classification and digital access; a failure to guard against sensitive data presents risk, as does over-protecting against non-sensitive data. Before data volumes presented this challenge, auditors in a more static, manual controls environment had relative confidence in the gathering, planning, and testing of data. In a digital enterprise, however, true peace of mind requires an integrated GRC platform; with native integration between SAP Process Control, SAP Risk Management, and SAP Audit Management, information is pushed directly to auditors. This not only significantly reduces the amount of time devoted to planning, but it also helps ensure that auditors are working with a single source of truth.

Ensure Policy Compliance

Another important component of an integrated, streamlined GRC platform is assurance of stakeholder compliance. If SAP Regulation Management by Greenlight is the intake mechanism that ensures new regulations are factored into a complete risk assessment, SAP Policy Management is the solution that ensures employees are aware of, and compliant with, changing policies that an organization implements in response to a fluid risk environment.

An organization's employees represent not only a first layer of protection, but also a first threat. Precautions against this threat should never be taken lightly, but are of particular importance for the digital enterprise — nearly 80% of cybersecurity risk relates to human behavior. With SAP Policy Management, teams that create a risk assessment picture can tailor policies according to current assessments and push these policies to operations. Operations then verifies compliance by implementing the necessary controls, such as training, surveys, quizzes, and sign-off forms acknowledging receipt and understanding of a company-specific policy.

An integrated GRC platform enables a proactive approach and the opportunity to continuously adjust controls and access governance according to real-time risk assessment.

Satisfy the Boardroom

A digital enterprise that has data increasing by the day does not have the luxury of relying on manual controls for alerts that are triggered only after something goes wrong. Within such a landscape, a controls environment that is refreshed monthly or even weekly is akin to closing the barn door after the horse has already escaped. An integrated GRC platform enables a proactive approach and the opportunity to continuously adjust controls and access governance according to real-time risk assessment.

While the new digital economy has created a seismic shift in how companies look at enterprise security, the bottom line and boardroom concern remains unchanged: Is the organization safe? To answer confidently in the affirmative, more companies are aligning what had previously been three loosely linked lines of enterprise defense within the comprehensive, integrated framework of SAP's GRC and security landscape. Visit **http://blog-sap.com/analytics/category/grc** for more information. ■

Thomas Frénéhard (thomas.frenehard@sap.com) is a Director in the Governance, Risk, and Compliance Solution Management team at SAP. His particular responsibility is with SAP Risk Management. Thomas's other functional areas of focus are in internal control and compliance, and audit management.