How to Build a Strong Security and Compliance Foundation for Your SAP Landscape

Ensure a Secure Environment Using SAP Solutions and the NIST Cybersecurity Framework

by **Martin Müller**, Presales Expert Security, SAP Deutschland, and **Arndt Lingscheid**, Product Manager of SAP Enterprise Threat Detection, SAP SE

Attacks that come from outside of a company often target its IT infrastructure layer to interrupt business operations. Most successful attacks are carried out by insiders or individuals compromised via phishing or malware attacks, and sometimes employees are recruited by suspicious organizations and used as vehicles to carry out an attack. These attacks often focus on the company's application layer and use privileged user accounts. Unfortunately, many security departments see the SAP application layer as a "black box," and they view the security of SAP applications as the responsibility of their Basis or SAP application colleagues, leaving these applications at risk.

In cases where an organization's SAP applications are run by a service provider, the security team might even expect the service provider to be responsible for the security of these applications. While the provider might be responsible for the IT infrastructure layer, depending on the service level agreement (SLA) in place, technologies used for securing this layer often cannot prevent or detect attacks and data breaches at the application layer, where the most important business-critical data is usually stored. And responsibility for the data always lies with the customer organization.

For these reasons, the security of the application layer can often be a blind spot within organizations. Compounding this issue are myriad factors at play. For example, small-size companies have requirements that are different from mid-size or large organizations. Some businesses run their SAP software on premise, others use cloud-based SAP applications, and still others run their SAP applications in heterogeneous landscapes. And auditors have varying expectations of companies depending on variables such as the legal and geographical structure of an organization, its use of solutions, and the distribution models it uses, which leads

to very individual audit requirements for companies, even if they operate in the same industry.

This article helps SAP decision makers (CIOs, CFOs, and CISOs) and IT operations managers successfully meet these challenges and secure their SAP landscapes. The article first looks at how security frameworks can help lay the foundation for a strong security strategy. It then walks through SAP's portfolio of security and compliance solutions through the lens of the Cybersecurity Framework provided by the National Institute of Standards and Technology (NIST) — a framework that is widely used for establishing standard security guidelines and best practices within organizations — to provide SAP customers with a toolkit for creating a comprehensive security strategy that meets their unique and varied needs. Lastly, it explains how to control the activities with a security infrastructure to meet compliance and business requirements and to provide insight that helps those at the C level make better decisions.

Solid Security Strategies Start with a Framework

A framework of guidelines, standards, and best practices is a critical tool for ensuring the security of an organization's landscape. One resource that SAP provides for its customers for this purpose is the SAP Security Optimization Services Portfolio, which provides Best Practices centered on three key areas: Security Overview, which provides overall SAP security recommendations; Security Topics Area, which provides recommendations for areas such as security patch management and configuration analysis; and Security Services, Tools and Information, which recommends additional resources on service offerings. For those seeking to create a structured overall SAP security strategy, the Security Overview area is an ideal place to start, and the SAP Secure Operations Map at its center provides an overview of the SAP-specific topics that need to be covered.

Another resource that is widely used by many organizations is the NIST Cybersecurity Framework. The NIST Cybersecurity Framework can be used in a complementary way with the SAP Secure Operations Map, as it is orthogonally oriented and provides a more general approach to structuring a security strategy. The framework is divided into three components: core, profiles, and tiers. The core component, which is the focus of this article, contains an array of activities, desired outcomes, and information about aspects of and approaches to cybersecurity, while profiles and tiers center on aligning the core information with an organization's objectives and practices.

The SAP Secure Operations Map

The SAP Secure Operations Map serves as a reference model for structuring the overall security of an organization, and for serving as the basis for discussions about the needs and solutions required for specific security areas. These areas include: organization, processes,

MARTIN MÜLLER (mart.mueller@sap.com) obtained an engineering degree from HFT Stuttgart, and went on to hold various positions in application development and product management in Germany and abroad. He joined SAP in July 1998 and worked in SAP Business Information Warehouse development until June 2000. Martin has been responsible for presales and program management for SAP's various security products for more than 15 years, focusing on cybersecurity for the past six.

ARNDT LINGSCHEID (a.lingscheid@sap.com) studied general mechanical engineering at the University of Applied Sciences in Cologne. He then worked in Germany and abroad in the areas of SAP NetWeaver Basis, ABAP application development, and ABAP product development. Beginning in 2007, Arndt served as Product Manager for various SAP add-on products, and then in 2013, became Pre-Sales and Product Manager for SAP security add-on products. Since September 2019, he has been Product Manager for SAP Enterprise Threat Detection.

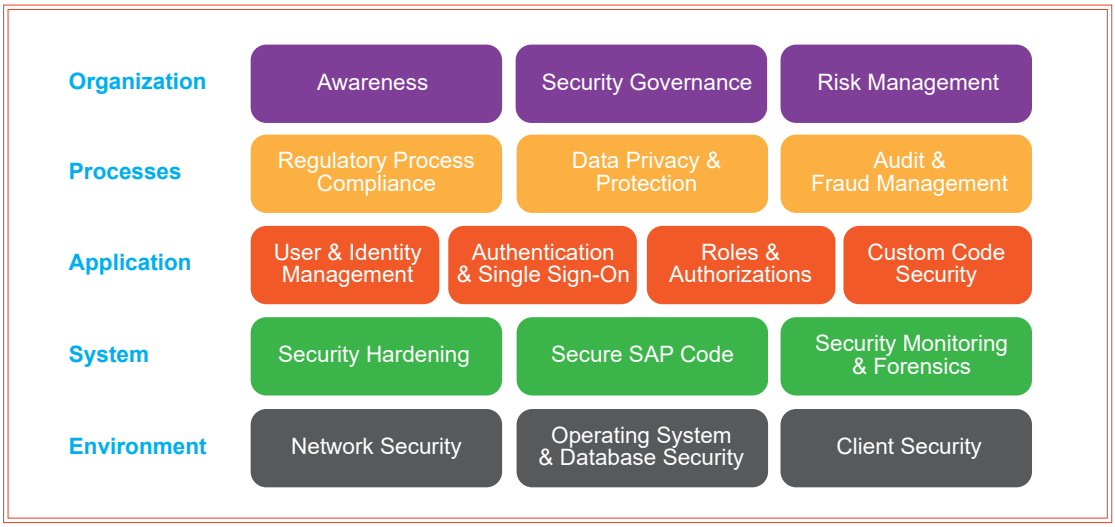

Figure 1 The SAP Secure Operations Map provides a 360-degree view of security in an organization's SAP landscape

application, system, and environment (see **Figure 1**). The focus is on the operational aspects of security — that is, the tasks and considerations that a customer or service provider needs to consider to maintain and operate its systems and landscapes safely.

This most recent version of the map, which was updated in January 2020, includes the addition of two new areas: organization and processes. To establish the processes, data protection measures, and technologies that are necessary to effectively secure the business, all employees — including those at the board level — must be aware of the issue of security in the organization. To this end, the organization layer describes activities such as awareness campaigns and general knowledge of security governance and risk management. The process layer completes the known paradigm of people (organization), processes, and technology. It covers areas such as regulatory process compliance, data privacy and protection, and audit and fraud management, and it deals with the correct behavior of applications concerning policies and legal demands.

The application layer consists of typical SAP applications that cover areas such as identity access management, roles and authorization management, and typical custom code security. It is important to note that the application layer is separate from the system and environment layers (many organizations do not see it as separate, which can have security ramifications, as mentioned earlier). The system layer covers typical elements such as security hardening, secure code from SAP (via SAP security patches), and continuous security monitoring and event management of the application layer. The environment layer collects the security actions needed for SAP operations on a network, operating system, and client level.

The NIST Cybersecurity Framework

Established in 2014, the NIST Cybersecurity Framework is used by many organizations — IDC estimates that more than half of Fortune 500 companies with US headquarters have adopted this framework as their primary control framework for cybersecurity. This framework helps IT security teams assess and improve their ability to prevent, detect, and respond to cyberattacks. Through its core component — which provides the foundation for the framework's other two components, profiles and tiers — the NIST framework provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes (see **Figure 2**).

An NIST-Based Overview of SAP's Security and Compliance Solutions

Figure 3 provides an overview of SAP's security and compliance solutions through the lens of the NIST Cybersecurity Framework. At the lower right is a legend that describes the focus of the product or service, which is indicated by color in the diagram. Some tools are SAP standard tools (shipped with SAP's core software), some focus on cybersecurity, and others

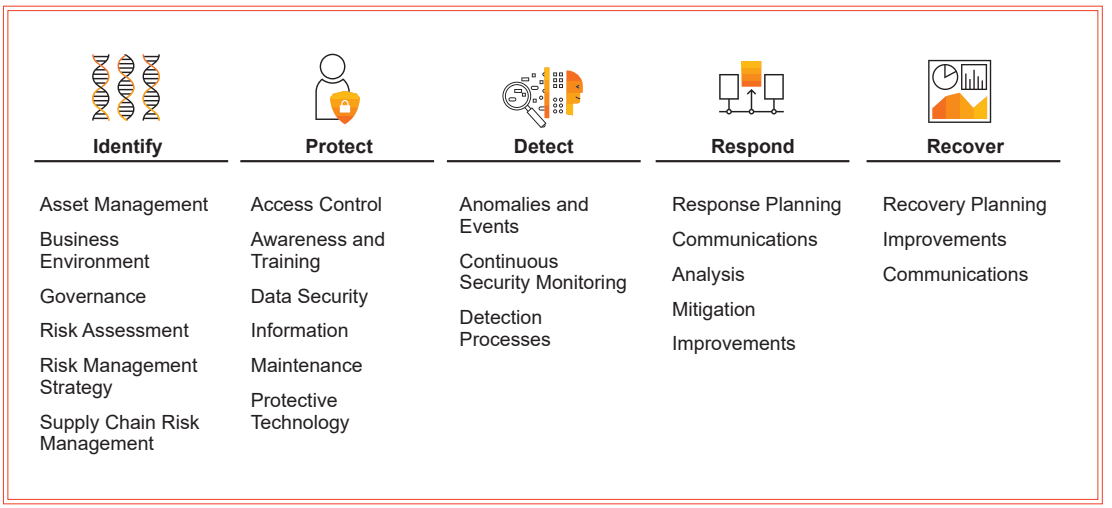

Figure 2 The NIST Cybersecurity Framework helps organizations assess and improve their ability to prevent, detect, and respond to cyberattacks

focus on compliance. In addition, several support services are available to help organizations improve their enterprise security environments. The length of the bars indicates where to position the solutions in the NIST framework. Across the top are solutions that provide overarching control over the activities performed with these tools as part of the defined security strategy, along with transparency for executives. Next, we will walk through the key features and functionality of the solutions shown in the diagram.

SAP EarlyWatch Alert Workspace

According to the NIST framework, one of the first steps in assessing an SAP application is to identify the

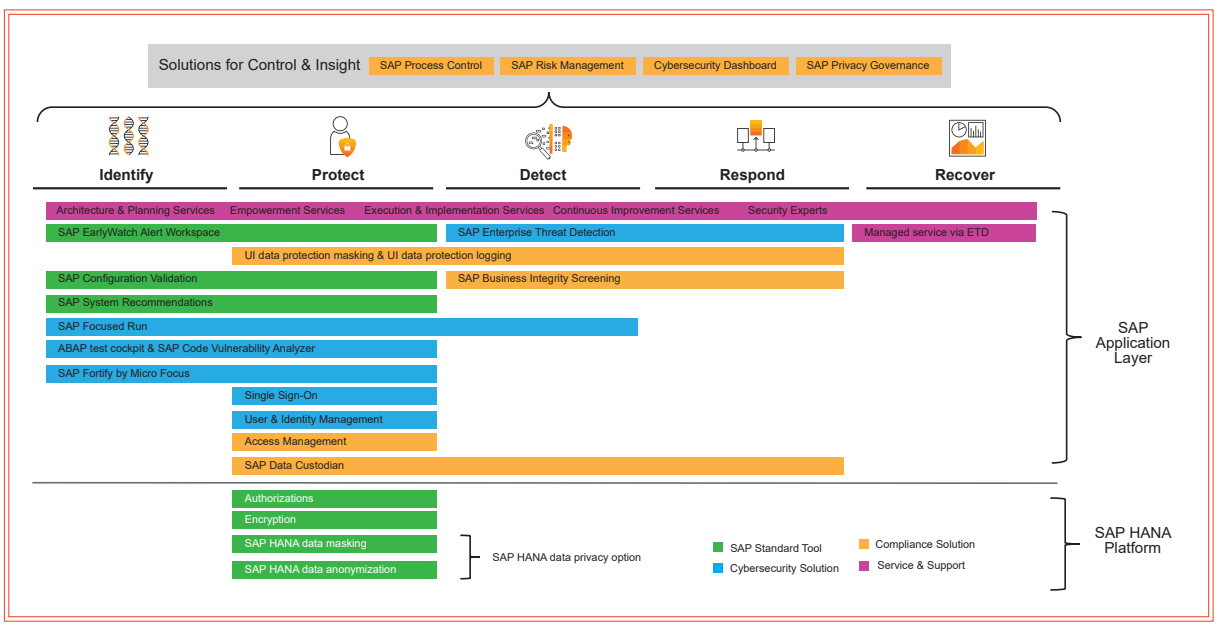

Figure 3 An overview of SAP's security and compliance solutions based on the NIST Cybersecurity Framework

most important systems and applications and how users are accessing the most important data in these systems, so that you can then take steps to protect it. The SAP EarlyWatch Alert Workspace service, which helps address the "identify" and "protect" areas of the NIST framework, is a free, automated SAP standard tool that scans all productive SAP instances on a weekly basis, collecting and analyzing a comprehensive set of critical settings and vulnerabilities, and highlighting missing security patches. This service can also be used for an initial security assessment of all productive SAP instances to identify vulnerabilities and to visualize unpatched systems.

Introduced more than 20 years ago as SAP EarlyWatch Alert, the service originally ran within SAP Solution Manager or via the customer's SAP Service Backbone connection. In 2018, SAP EarlyWatch Alert was completely redesigned as a cloud-based tool called EarlyWatch Alert Workspace and accessed through SAP ONE Support Launchpad, and that same year received an SAP Product Excellence Award from SAP User Group Executive Network (SUGEN) customers.

The goal of SAP EarlyWatch Alert Workspace is to identify critical security issues across an organization's productive landscape and to provide a prioritized worklist to share and track progress — for example, it offers an easy way to view how many systems are vulnerable and in what ways. Despite the advantages of using this tool, however, many organizations are often unaware of it or don't understand its benefits. Be sure to take advantage of this freely available service to help ensure a comprehensive security strategy based on the NIST framework.

SAP Configuration Validation

SAP Configuration Validation uses data from SAP Solution Manager to help determine whether the SAP systems in an organization's landscape are configured consistently and in accordance with the company's requirements. This SAP standard tool, which helps address the "identify" and "protect" areas of the NIST framework, can help validate the current configuration of a system against the configuration data of other systems, or against a defined target system, for example, and can help fulfill standard requirements from auditors.

This tool enables the execution of validation reports to compare the current configuration of one or more systems with a reference system. The reference system can be either a real, existing system or a virtual target system containing user-defined configuration criteria. Each configuration element is checked, and if the value of the element in the comparison system fulfills the conditions defined in the reference system, it is rated compliant. If any element in a configuration store is not compliant, the entire configuration store is rated noncompliant. The same applies to a system: if any element in a configuration store is noncompliant, the entire system is rated noncompliant.

System Recommendations

System Recommendations is an SAP standard tool that also helps address the "identify" and "protect" areas of the NIST framework. Included with SAP Solution Manager, this tool provides a tailored list of SAP Notes, including security notes, that should be applied to a selected managed system. Details of the notes, including any prerequisites for a particular note, can be viewed in a user-friendly SAP Fiori interface.

SAP Focused Run

SAP Focused Run, a solution originally developed by SAP's cloud operations team, helps address the "identify," "protect," and "detect" areas of the NIST framework. It is a solution that uses SAP HANA to support high-volume monitoring, alerting, diagnostics, and analytics, and it is available for all SAP customers and service providers with an additional license via SAP Service Marketplace. SAP Focused Run helps organizations maintain their SAP applications using a central, scalable, safe, and automated environment.

While SAP Focused Run is not solely focused on security, it includes many security features that can help ensure a secure system landscape, including:

- Predefined and policy-based security and compliance validation of configurations
- Monitoring of server-side certificates
- Security note deployment validation, including transparency about gaps versus achievement

- Integration into operational processes
- Insights into actual usage, including system communication, document flow, and user behavior
- Graphical charts and built-in dashboarding capabilities that can also be used by auditors and management

SAP Code Vulnerability Analyzer

Many SAP customers use the ABAP programming language to create their own and extend existing SAP applications. While the ability to customize and enhance applications is a useful capability, incorrect programming can lead to severe security issues, such as data theft and costly compliance violations. For this reason, SAP recommends using SAP Code Vulnerability Analyzer for all custom ABAP code development. At SAP, ABAP code must be checked using this cybersecurity solution before it can leave the development system, which has led to a significant decrease in vulnerabilities.

SAP Code Vulnerability Analyzer, which helps address the "identify" and "protect" areas of the NIST framework, fits seamlessly into the well-known ABAP test cockpit. Within the ABAP test cockpit, developers can review their code and perform tests for code robustness, performance, and usability. When a customer licenses SAP Code Vulnerability Analyzer, ABAP developers receive an additional option within the ABAP test cockpit to perform SAP Code Vulnerability Analyzer security checks within the ABAP test cockpit.

SAP Fortify by Micro Focus

SAP Fortify software by Micro Focus helps secure applications wherever they are deployed — in house, on the web, in the cloud, or on mobile devices around the world. The software integrates with SAP Code Vulnerability Analyzer across the solution life cycle and automates key processes for developing and deploying highly secure technology and services.

This cybersecurity solution helps address the "identify" and "protect" areas of the NIST framework. It supports a cohesive approach to application quality management and security testing, and it helps identify and address security vulnerabilities throughout the software life cycle. Through its intuitive web interface, SAP Fortify provides line-of-code guidance specific to the programming language used. Additional functionality includes real-time security vulnerability testing and verification for web applications and services, a sophisticated software security center, a static code analyzer for different development languages, and web inspect functionality.

SAP Fortify helps organizations comply with internal and external security and quality mandates and establish continuous, automated procedures to address security issues in deployed software and reduce risk in software that is in development or being acquired.

UI Data Protection Masking and UI Data Protection Logging

Controlling which data can be viewed and tracking who has viewed critical data is crucial in an SAP environment. SAP provides two functionalities via the UI data protection masking and UI data protection logging add-ons, which require an additional license. These compliance solutions help SAP customers meet this need, and they help address the "identify" and "protect" areas of the NIST framework.

UI data protection masking enables SAP customers to reduce the visibility of their sensitive data — such as salary data, bank account information, and social security numbers — via easy configuration settings. The UI masking technology allows security administrators to hide, mask, or block data on a business transaction. The data is not displayed because it is never sent to the client system, providing the strongest possible data protection. Dynamic authorizations enable the configuration of output based on attribute and role information, so that only those with a specific role see the unmasked data, while all others are shown only the masked data. For example, in an HR scenario, not every HR employee should view the salary details of all employees.

UI data protection logging helps provide transparency around who has viewed which data, how often, and when to help spot access misuse. The UI logging technology provides a detailed, screen-exact data access protocol for both user input and system output. It is also possible to configure real-time alerts upon access to predefined data, or to enable more advanced alerting via native integration with SAP Enterprise Threat Detection (more on this tool later).

SAP Business Integrity Screening

Fraudulent transactions can have a costly effect on an organization's profitability, but it can be difficult to identify these types of transactions before they occur.

SAP Business Integrity Screening is a compliance solution that helps address the "detect" and "respond" areas of the NIST framework. It helps organizations prevent risky transactions and reduce processing errors, fraud risk, and losses by identifying anomalies early enough to stop the transaction. The software uses SAP HANA technology to scan large volumes of data, identify risks and suspicious patterns, and generate alerts so you can react to compliance violation checks immediately and avoid transactions with suspicious third parties.

Single Sign-On, User and Identity Management, and Access Management

Different types of users (such as employees, customers, and business partners) work with SAP applications in heterogeneous landscapes (on premise, in the cloud, or both). These users need functions such as single sign-on, user provisioning, and segregation of duties in parallel with self-services, workflows, and role management, while security administrators need identity and access management solutions that ensure consistent and compliant identity management and access control.

SAP has several cybersecurity and compliance solutions and services that support the identity and access management needs of users and security administrators in a secure way, both on premise and in the cloud, and that help address the "protect" area of the NIST framework. These include SAP Cloud Identity Services, SAP Identity Management, SAP Single Sign-On, SAP Cloud Identity Access Governance, and SAP Access Control, which were discussed in detail in a previous SAPinsider article.

SAP Data Custodian

Maintaining data security and regulatory compliance is a primary concern with public cloud deployments. SAP Data Custodian, which helps address the "protect" area of the NIST framework, is a software-as-a-service (SaaS) product that is designed to give public cloud users insight into their public cloud resources and applications, along with data transparency, protection, and control in public cloud deployments.

This compliance solution provides monitoring and reporting functionality for data access, storage, movement, and location in the public cloud. In addition, security administrators can create and enforce access restrictions with policy-based controls and use encryption features across cloud applications to further strengthen data security and regulatory compliance.

SAP Enterprise Threat Detection

SAP Enterprise Threat Detection, which helps address the "detect" and "respond" areas of the NIST framework, is a real-time security event management and monitoring solution that is tailored to the needs of SAP applications and provides insight into SAP systems out of the box. It helps security administrators detect, analyze, and neutralize cyberattacks as they are happening, and before serious damage occurs. This solution provides a single source of truth for centrally audited SAP systems and provides all connected log types in a readable format. It recognizes any unusual or critical behavior inside the SAP system, such as brute force attacks, activation and use of highly privileged user accounts, and extraction of confidential information.

Using SAP HANA technology, all log types can be processed and correlated in real time, instantly creating a complete picture of what is happening instead of producing puzzle pieces that need to be assembled, which enables the early interception of hacking attacks. The generic approach of SAP Enterprise Threat Detection and its semantic understanding of SAP logs help the solution quickly and easily adapt to new threats with no additional development required.

The risk-based, step-by-step implementation process for SAP Enterprise Threat Detection allows organizations to start quickly with small ("alarm") system scenarios that focus on the most important applications using a manageable amount of detection patterns and different log types. This helps quickly close security and audit gaps and protect the organization's most valuable assets. More information on SAP Enterprise Threat Detection is available in a previous SAPinsider article.

SAP Services and Support

The SAP Services and Support organization provides resources that can help SAP customers take the right steps to strengthen cybersecurity protections and increase compliance throughout their SAP landscapes.

With the SAP Consulting Security Services offering, the support team at SAP evaluates the customer's IT landscape, creates the architectural plan and defines the necessary steps, and then supports the realization and implementation of the plan.

Through its SAP Cloud Application Services organization, SAP also offers managed security services for cybersecurity based on SAP Enterprise Threat Detection. With SAP managed security services for SAP Enterprise Threat Detection, the SAP managed services team monitors an organization's SAP applications and, optionally, non-SAP applications. To meet the individual requirements of different organizations, several packages are available, ranging from basic event monitoring to highly complex threat hunting services. The agreed-upon SLA describes the exact content and extent of the managed service, including the monitoring time (from six days per month to 24 hours per day, seven days per week).

SAP HANA Platform Security

SAP HANA is designed as a multi-purpose business data platform for the intelligent enterprise that supports analytical and transactional scenarios in different deployment modes, both on premise and in the cloud. The security approach used for SAP HANA enables SAP customers to address the security requirements for this type of multi-purpose platform.

SAP HANA comes with a comprehensive security framework for secure data access and applications, with SAP standard functions for authentication, user management, authorization, encryption, and auditing. The SAP HANA data privacy option (data anonymization and masking) allows for the cautious treatment of sensitive and confidential data.

SAP HANA is designed to be set up and run securely in different environments. Tools, settings, and information help organizations configure, manage, and monitor SAP HANA security in their specific environment. SAP HANA cockpit provides a role-based security dashboard, security configuration, and user and role management screens.

Controlling Security Activities and Providing Insight to the C Level

An important component of a comprehensive security strategy is control over the activities performed for that strategy to ensure the compliance of the SAP landscape, which involves monitoring the behavior of applications in terms of the guidelines and legal requirements, such as data privacy requirements, in place where SAP systems are operating. It is also important to create transparency about cybersecurity risks, and to quantify these risks in monetary terms, to help those at the C level, and CISOs in particular, balance risks against appropriate business value and make better decisions. SAP offers several solutions to meet these needs, including SAP Process Control, SAP Risk Management, a cybersecurity dashboard concept, and SAP Privacy Governance.

It is also important to create transparency about cybersecurity risks, and to quantify these risks in monetary terms, to help those at the C level, and CISOs in particular, balance risks against appropriate business value and make better decisions.

SAP Process Control

Regulatory pressures are increasing as organizations expand into different geographical areas. While in the past, companies could set up a team to handle a new regulation, regulations are now increasing at a rate that outpaces the resources of most companies. In addition, organizations tend to have duplicate controls in place due to a siloed approach to managing regulatory compliance, which can be costly during tough economic times that require reduced costs and streamlined processes.

SAP Process Control provides a robust compliance framework that helps businesses document, test, and report across regulations and company initiatives, thus reducing effort, increasing visibility, and enabling more streamlined and harmonized processes. For example, a control can be documented once and assigned to as many regulations and initiatives as

necessary, while still ensuring that data specific to each regulation is captured as required. If the result of a single evaluation is relevant for other scenarios, the evaluation can also be shared as appropriate. This not only saves time and effort, but also makes it easier to expand into new geographies and adopt new regulations and initiatives. It also establishes clear accountability by control, subprocess, regulation, or initiative.

SAP Risk Management

SAP Risk Management helps organizations integrate and coordinate risk management activities, gain a deeper understanding of risk, and plan timely, reliable responses. It provides reliable, accurate information for making better decisions and ultimately improving and sustaining the profitability of the business.

The solution enables companies to see and assess current and future risks, link them to business value drivers, and preserve and build on that value. It enables insights into how value is created and destroyed by linking risk drivers, key risk indicators, and related impacts, and it provides the ability to easily integrate and coordinate risk management activities across the organization, from corporate and executive levels to audit committees and operating managers. The instant access to information from key risk indicators and integration with SAP S/4HANA means businesses can act quickly and decisively on emerging risks and opportunities.

Cybersecurity Dashboard

When it comes to securing business applications, organizations tend to face three key challenges:

- How to enable the application security team to prioritize the necessary cybersecurity actions
- How to give the CISO insight into application security risk activities
- How to bridge the gap between the problems faced by the CISO and the problems faced by the rest of the C-suite

One potential way to address these challenges is by building a cybersecurity dashboard using SAP Analytics Cloud and its integration with SAP security solutions, a concept in which several SAP customers have expressed interest, and which SAP is planning to build by working together with customers.

The idea is to create a customizable dashboard that combines the feeds from various cybersecurity solutions, analyzes attacks, and suggests actions for the application security team to prioritize. The dashboard would also give CISOs a snapshot of what their teams are doing at any point in time so they can adjust operations if necessary. In addition, the dashboard would help the board understand how cybersecurity risks can affect strategic business objectives, and make better decisions based on risk mitigation, by providing insight into the monetary value of cybersecurity risks and into the company's overall risk management status.

SAP Privacy Governance

Complex data privacy regulations are emerging worldwide, from the EU's General Data Protection Regulation (GDPR) to the first-of-its-kind California Consumer Privacy Act (CCPA) and India's sweeping new privacy laws. Tracking which regulations affect a business and how they affect a business is no small task, and monitoring whether a business is in compliance is equally challenging.

SAP Privacy Governance addresses this by providing purpose-built automated tools to help organizations bring order and transparency to privacy compliance. This SaaS offering establishes data protection and privacy governance for the enterprise, supported by automation, transparency, and reporting that provides real-time insight into where the organization stands when it comes to complying with security and privacy regulations, and what needs attention before it's too late and costly fines are imposed.

Summary

The security and compliance challenges faced by SAP customers across their technology landscapes vary widely and can be overwhelming. By establishing a solid security foundation for your organization — using the guidance of a framework such as the NIST Cybersecurity Framework and the resources provided by SAP for security and compliance — you have everything you need to overcome these challenges and succeed.