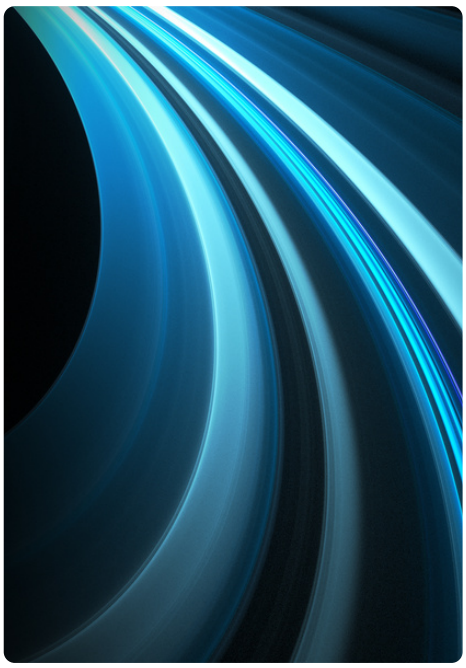
WHITEPAPER

Which cybersecurity framework is the best fit for SAP application security?

Security Bridge™

Executive Summary

As organizations increasingly rely on SAP systems and applications to support their critical business processes, it is crucial to ensure that these systems are secure and protected against cyber threats. Several cybersecurity frameworks exist to help organizations manage and mitigate cyber risks. Unfortunately, they are not specifically for SAP environments. This article will explore some of the best cybersecurity frameworks for SAP and provide an overview of their key features and benefits. By adopting one or more of these frameworks, organizations can improve their security posture and standardize their complex security operations to protect their critical assets from cyber threats.



Who uses a cybersecurity framework?

A wide range of organizations in various industries uses cybersecurity frameworks, including government agencies, healthcare organizations, financial institutions, and large corporations. Small and medium-sized businesses may also use cybersecurity frameworks to help protect their assets and meet regulatory requirements. Adopting a cybersecurity framework can help organizations understand and manage their cyber risks and protect their assets from cyber threats. Some organizations may be required to implement a specific cybersecurity framework as part of regulatory compliance, while others may choose to adopt a framework voluntarily to improve their overall security posture.

What is a cybersecurity framework?

A cybersecurity framework is a set of guidelines, best practices, and processes for managing and protecting an organization's critical assets like SAP S/4 HANA, SAP ERP, CRM, or SRM from cyber threats. The framework helps organizations understand, manage and address the risks they face from cyber threats. It also provides a systematic approach to managing and protecting enterprise-critical SAP applications. Its goal is to reduce the likelihood of a successful cyber-attack and to minimize the impact if an attack does occur. There are several different cybersecurity frameworks that organizations can adopt. Read on to learn which are the most practical for SAP security operations.

What is a cybersecurity framework?

Cybersecurity frameworks for securing SAP systems may include:

- The secure configuration of system security-relevant settings
- The implementation of access controls to ensure that only authorized users have access to SAP systems and applications
- The regular application of security patches and updates to protect against known vulnerabilities
- The implementation of security measures to protect the network infrastructure that SAP systems and applications are running on
- The implementation of measures to protect sensitive data (i.e., DB or interface data encryption) stored in SAP systems and applications
- The development of an incident response plan to help organizations quickly and effectively respond to and recover from cyber incidents.

Moreover, it is essential to include secure application development to eliminate unnecessary attack vectors.

What are the challenges when adopting a cybersecurity framework to secure SAP?

There can be several challenges when adopting a cybersecurity framework to secure SAP systems and applications. Some of the most common challenges include:

Cost:
Implementing a cybersecurity framework can be expensive, as it may require organizations to purchase new hardware and software, hire additional staff, and allocate resources to training and awareness programs.

Complexity:
SAP systems and applications can be complex and securing them can require a deep understanding of the specific technologies and processes involved. Frameworks provide the governance process but cannot provide all the detailed information needed to harden a specific SAP ERP application. This can be a challenge for organizations that do not have strong cybersecurity expertise in-house.

Resource constraints:
Organizations may struggle to allocate sufficient resources to implement a cybersecurity framework, particularly if they are already stretched thin with other priorities.

Integration with existing systems:
It can be challenging for organizations to integrate a cybersecurity framework with their existing ERP systems and SAP processes, particularly if they have a large and complex SAP environment.

Changing regulatory requirements:
Often, cybersecurity frameworks are developed in response to changing regulatory requirements, and organizations may struggle to keep up with the rapid pace of change.

Adopting a cybersecurity framework for SAP systems and applications can be a complicated and resource-intensive process, and organizations should allocate sufficient resources and time for it to be successful. However, one should not forget that the invested efforts are already more than amortized after the successful defense against a few attacks.

How to choose the best cybersecurity framework for SAP?

Choosing the best cybersecurity framework for SAP systems and applications can be a complex process, as there are several factors to consider. Here are some tips to help you make an informed decision:

1. Consider your specific needs and goals when choosing a cybersecurity framework. Different frameworks have different focus areas and may be more or less suitable for different types of organizations. For example, if your primary goal is to protect sensitive data, you may want to look for a framework that includes strong data protection controls. On the other hand, if your primary goal is to ensure the availability of your SAP systems, you may want to look for a framework that includes measures to prevent outages and disruptions.

2. Carefully review the requirements of the frameworks you are considering. Make sure your organization has the resources and expertise to meet the framework requirements and consider whether the framework is scalable and flexible enough to meet your future needs.
   It is also important to consider your budget when choosing a cybersecurity framework. Implementing a framework can be expensive, so look for one that provides the most value for your organization at a price you can afford.

3. Consider is the recognition and respect of the framework in the industry. Choose a widely recognized and respected framework, as this can help demonstrate your commitment to security and make it easier to find trained professionals familiar with the framework.

4. Involve stakeholders in the decision-making process, including IT staff, security professionals, and business leaders. This can help ensure that the chosen framework meets the needs of the entire organization.

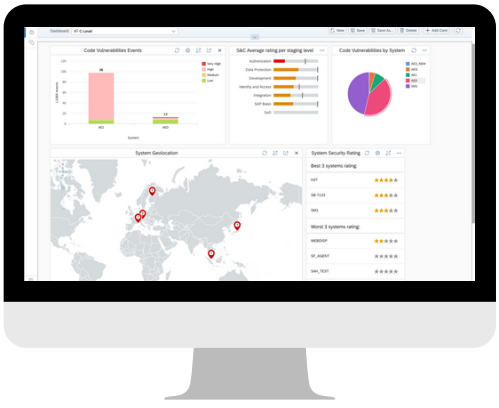
By considering these factors, you can choose the best cybersecurity framework for your SAP systems and applications and help ensure that your critical assets have protection against cyber threats.

Which frameworks exist? How do you rate them for SAP application security?

Organizations can use several cybersecurity frameworks to help secure SAP systems and applications. Some of the most common frameworks that organizations use to protect SAP environments include:

Cybersecurity framework	SAP rating
SAP Cybersecurity Guideline/Framework: This framework was developed by SAP specifically to help organizations secure their SAP systems and applications. It provides a set of best practices and guidelines like the famous SAP Secure Operation Map and tools for protecting SAP environments. Additionally, it can be customized to meet the specific needs of different organizations. *Unfortunately, the guideline is still under constant innovation, meaning that not all chapters are available in the same level of detail. However, our experts believe this guideline is still a must-use for all SAP customers, especially the recommendation for the secure configuration of the more than 2000 system profile parameters.*	★★★
NIST Cybersecurity Framework: The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a widely-used framework that provides a set of best practices for managing and protecting critical assets from cyber threats. *Even SAP itself uses and recommends the use of NIST CSF. However, some translation is required to apply the framework prerequisite to SAP applications. SecurityBridge provides standard mapping that combines all existing security controls with the NIST chapters' requirements. The SAP Security Baseline and the NIST CSF create a solid mix.*	★★★
COBIT: COBIT is a framework that guides the governance and management of information and technology. It can ensure that SAP systems are secure, compliant, and aligned with business goals. *During our careers, we could not connect deeply with the COBIT framework. Some emerging technologies are becoming increasingly important in IT security that COBIT does not address. Although COBIT provides practical guidance and recommendations for implementing effective IT controls and processes, our experts find it very complex. At the same time, it does not provide detailed, step-by-step instructions for implementing specific controls and processes.*	★☆☆

Cybersecurity framework	SAP rating
ISO/IEC 27001: This international standard provides a framework for implementing an information security management system (ISMS). It can help secure SAP systems and applications by providing guidelines and controls for managing and protecting sensitive data. *However, it describes many detailed aspects required for SAP applications superficially, so the users must take care of the SAP security requirements themselves. Although ISO/IEC 27001 is a globally recognized standard, and organizations that are certified as compliant with the standard are required to undergo regular audits to ensure that they are maintaining their security posture, our experts do not feel that the requirement for mission-critical SAP systems is detailed enough as to warrant an unqualified recommendation. ISO27001 shines in the area of data security.*	★★☆
CIS 20 Critical Security Controls: The Center for Internet Security (CIS) 20 Critical Security Controls is a set of best practices for protecting against cyber threats. It can help secure SAP systems and applications as part of an overall cybersecurity program. One of the key differences between the CIS 20 Critical Security Controls and other security frameworks is that it specifically focuses on identifying and prioritizing the most crucial actions organizations can take to protect against cyber threats. Its name comes after its organization into 20 controls that cover a whole range of security areas, including network security, incident response, and data protection. *The SecurityBridge experts conclude that the 20 controls provide a great structure to start the SAP security operation but lack the level of detail needed to implement SAP-specific measures.*	★☆☆



Conclusion

Adopting a cybersecurity framework is a vital step for organizations that rely on SAP systems and applications to support their critical business processes. Cybersecurity frameworks provide guidelines, best practices, and processes for managing and protecting an organization's assets from cyber threats. Organizations can improve their security posture by adopting a framework and standardizing their security operations.

We listed several cybersecurity frameworks organizations can adopt for SAP, including the SAP Cybersecurity Framework, the NIST CSF, the ISO/IEC 27001 standard, and the CIS 20 Critical Security Controls. Each framework has unique features and benefits, and organizations should consider their specific needs and goals when choosing one.

The successful implementation of a cybersecurity framework requires careful planning and allocating sufficient time and resources. However, organizations can help streamline the process and overcome potential challenges by using the right software solution, such as the SecurityBridge Platform for SAP. SecurityBridge supports their chosen framework(s). This can help ensure the framework is efficiently implemented and helps organizations manage and maintain their security posture over time.
Overall, choosing the right cybersecurity framework is a crucial decision for organizations that target to protect their mission-critical SAP systems and applications. By carefully considering their specific needs and goals, and by selecting a widely recognized and respected framework in the industry, organizations can successfully work towards introducing barriers that shield their critical assets from the various threat actors.

CONTACT US

Europe (Headquarters)

+49 (841) 93914840

Munchenerstr. 49

85051 Ingolstadt, Germany

United States

+1 (416) 821 0850

Info@SecurityBridge.com

SecurityBridge.com

SecurityBridge™