Security at SAP | PUBLIC

The Secure Operations Map

Highlights and Best Practices for

Securing SAP® Solutions

THE BEST RUN SAP®

Table of Contents

Prioritizing Security

Information security is a top priority for your business. With cyberattackers becoming more sophisticated and relentless, we at SAP are committed to continuously innovating our software to keep your information safe – both on premise and in the cloud. We prioritize security so that you can stay focused on running your business and managing your customer relationships effectively using SAP® solutions, safe in the knowledge that **your data is secured**.

WHY SAP SOFTWARE MUST BE SECURED

Across nearly all of the technology landscapes managed by companies all over the world, one theme is constant: hyperconnectivity. The benefits of this hyperconnectivity are clear: efficiency, convenience, and choice to consumers and businesses alike.

Yet, a hyperconnected economy presents risks as well – risks that SAP takes seriously. Our software, for example, stores and processes a wide range of sensitive and valuable information, such as personal data, prices, and product procedures.

To protect this data and keep information from being intercepted or falsified, we've published a secure operations map that highlights the best practices organizations can adopt for a secure approach to managing SAP solutions during the operations phase.

This paper provides an overview of the secure operations map. More information is available here.

As bad actors continue to devise new modes of attack, and vulnerabilities to these attacks are identified, **SAP continuously provides security updates** for existing code to keep your systems secure.

Securing Daily Operations with SAP

Figure 1 shows the secure operations map that structures our security best practices according to 16 topics across the following five layers:

- Organization
- Process
- Application
- System
- Environment

ENVIRONMENT

The environment layer at the lowest level of the secure operations map focuses on the non-SAP technical infrastructure on which SAP offerings run. Success at this level is important for ongoing operational security.

Network Security

Protection and monitoring mechanisms that are embedded in the underlying network infrastructure act as a critical frontline measure for augmenting corresponding lines of defense at the software level. Practices for protecting networks include network zoning and segmentation as well as the use of network components such as routers, firewalls, and Web application filters. Intrusion detection and prevention systems can also bolster the ongoing monitoring of relevant security events.

Operating System and Database Security

An absence of secure baseline configurations or easily bypassed access controls at the operating system and database levels can put the protection of applications running on them at risk. Relevant security controls in this regard include file-system permissions, database-user security, tenant separation, and data-at-rest encryption methods.

Client Security

Without proper protection at the client-system level, your system is an easy target for adversaries trying to establish a point of entry into the network or injecting bogus data into network traffic. Thus, client-side controls are needed. These include secure maintenance, configuration, control, and monitoring of the client – as well as execution rules for browsers.

SYSTEM

The system layer serves as the foundation on which all SAP applications run. With controls such as authorization tools at the application layer, your organization is more secured and protected from lower-level vulnerabilities such as SQL injections made possible through the use of insecure code.

Organization	Awareness	Security governance	Risk management	
Process	Regulatory process compliance	Data privacy and protection	Audit and fraud management	
Application	User and identity management	Authentication and single sign-on	Roles and authorizations	Custom code security
System	Security hardening	Secure SAP® software code	Security monitoring and forensics	
Environment	Network security	Operating system and database security	Client security	

Figure 1: The Secure Operations Map

Security Hardening

Security hardening focuses on minimizing the overall attack surface of a system. Typically, it deals with the proper setting of system parameters and other aspects of system configuration, including the activation of security features and functionalities. For purposes of backward compatibility or to facilitate a migration project, some of these features and functionalities are sometimes switched off. Wherever possible, it is important to reactivate the proper configuration settings to protect against possible security vulnerabilities.

In the secure operations map, system hardening also encompasses front-end components such as the SAP GUI interface and SAP Business Client software. It also covers infrastructure components such as the SAProuter application and cloud connectors provided by SAP.

Secure SAP Software Code

As bad actors continue to devise new modes of attack, and vulnerabilities to these attacks are identified, SAP continuously provides security updates for existing code to keep your systems secure. SAP delivers these security updates through support packages, which are available for you to install.

On the second Tuesday of every month, as part of our "Security Patch Day," we also publish security notes with the latest security corrections and recommendations. Implementing a security maintenance process to assess and implement recommended security updates is a proven best practice for mitigating security risk.

Security Monitoring and Forensics

While proactive measures such as hardening systems and securing code are critical and necessary, on their own, they are not entirely sufficient for securing SAP systems. Traditional reactive measures, such as comprehensive 24x7 system monitoring, are needed as well. Proper monitoring helps identify security breaches and suspicious system behavior so that you can trigger appropriate countermeasures.

Forensics are important too – which means that maintaining proper system logs for ongoing analysis is critical for learning from past security breaches.

TIPS FOR SECURING SYSTEMS

SAP provides the following services for securing systems:

- SAP EarlyWatch® Alert service, which monitors the essential administrative areas of SAP components and keeps you up to date on performance and stability
- SAP Security Optimization service, which is designed to verify and improve the security of SAP solutions by identifying potential security issues and providing key recommendations
- Engagement services, which offer support to implement security best practices, product security features, and cybersecurity for SAP solutions

APPLICATION

The applications layer focuses on controls available in standard applications delivered by SAP and non-standard applications built by customers. Topics include protective measures regarding user access and privilege levels, as well as proper application design.

User and Identity Management

For proper user and identity management, leading organizations follow a lifecycle approach to the management of user accounts, provisioning, and maintenance – including the approval, assignment, and revocation of authorizations to and from specific users. Technical and emergency users need to be incorporated into this lifecycle approach as well. Federated hybrid environments also aid in effective user and identity management.

Authentication and Single Sign-On

Authentication involves the verification of the true identity of a user. Verification methods range from simple password approvals to trusted system connections in which one system relies on the authentication mechanisms of another system.

One common practice for authentication is to adopt single-sign-on capabilities, where users are authenticated once and granted uniform access to several systems within a given landscape. Communication security mechanisms, such as Transport Layer Security for HTTP connections or secure network communication for remote function call connections, are used to support authentic communications between systems and clients.

Roles and Authorizations

In hybrid system landscapes in particular, ensuring that the right person uses the right application – and blocking unauthorized users from restricted applications – can be a significant challenge. Thus, systematic processes and auditable tools for aligning business roles with properly defined, distributed, and maintained authorization profiles are required. Automated ways to ensure segregation of duties and exert control over compliance-related concerns are also important.

Custom Code Security

Maintaining security for custom code requires a disciplined approached to custom code management. The first step is to remove unnecessary custom code wherever possible – and then maintain the remaining code in a proper lifecycle management system.

Such a system should be designed to cover the end-to-end custom code lifecycle. Critical features and capabilities include secure architecture and design, secure development, code security scanning, security maintenance, and retirement of custom code.

SAP TOOLS FOR SECURING APPLICATIONS

- Identity management tools with single-sign-on capabilities for cloud, on-premise, and hybrid system landscapes
- Governance, risk, and compliance capabilities for critical authorizations and control of segregation-of-duty rules
- Code vulnerability analysis to secure custom code against typical code patterns – such as those from the Open Web Application Security Project (OWASP) Top Ten list
- Enterprise threat detection to analyze security-related events from all kinds of systems

PROCESS

The process layer of the secure operations map deals significantly with regulatory compliance. The objective here is to have the correct application behavior as it pertains to the policies and legal demands associated with the various jurisdictions in which SAP solutions operate.

Regulatory Process Compliance

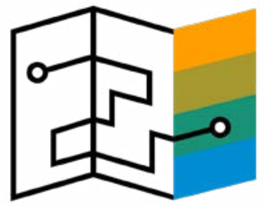
To maintain compliance with regulatory processes, your organization should review application functions in light of their potential to violate legal requirements when not used properly. For issues detected, controls such as double invoice checks or special tax-statement controls can be implemented to help minimize the risk of such violations. Typical regulations within purview include HIPAA, Basel II and III, and the Sarbanes-Oxley Act, to name just a few.

Data Privacy and Protection

Data privacy and protection regulations such as the General Data Protection Regulation in Europe require organizations to implement mechanisms that control the proper handling of relevant personal data. Practices to help ensure compliance include tools to manage blocking and deletion, consent management, right of access, and validation. Strong confidentiality measures such as field tokenizing or encryption at rest are also important.

Audit and Fraud Management

While regulatory compliance is mission critical for legal reasons, your organization will likely seek additional capabilities to detect fraudulent behavior and have appropriate controls in place. Thus, tools that automate auditing and fraud detection are also highly valuable.



You'll be in a strong position to **devise your own company action plan** and create a security road map that is tailored to the unique needs of your organization.

ORGANIZATION

The organization layer focuses on the people aspect of the secure operations map. Here, general awareness of security measures enterprise-wide are emphasized.

Awareness

While it is certainly unreasonable for any organization to expect all employees and partners to become security experts, a baseline security awareness should be reflected in your organizational culture – at least to the extent that everyone understands their role and does their part. For example, employees should be trained to understand the nature of situations or events in which security experts should be enlisted. Tools that prevent users from circumventing security regulations and mechanisms are also important. Intuitive interfaces that guide users to take the appropriate security actions are a critical best practice.

Security Governance

Organizations that achieve security excellence understand that a standardized and systematic approach to security governance plays a central role in success. Security governance is broad – touching almost everything involved in operational security – including organizational awareness, procedures, regulations, setup, configuration, integration, and the operation of SAP solutions.

Risk Management

Risk management comprises all elements of identifying, handling, mitigating, and resolving risks, including services or SAP solutions in this area. Your organization needs to assess risk, track and report on risk status, and identify key risk indicators – all beyond simple tracking of financial activity. Managing what drives values, determining how the value is created or eroded, and identifying emerging risk and opportunity help you to quickly define risk priorities. Risk management should include a framework to control risk and identify opportunities where risk accountability is encouraged.

Organizations that achieve security excellence understand that **a standardized and systematic approach to security governance** plays a central role in success.

TOOLS FOR SECURING ORGANIZATIONS

SAP offers SAP governance, risk, and compliance solutions to help better manage and improve process management. Offerings include:

- Business process control, continuous monitoring, and compliance management tools
- Risk management tools to help manage risks, identify opportunities, and highlight key risk indicators
- Business integrity screening software to help improve the detection and prevention of anomalies for mitigating fraud risk and reducing loss
- Audit management capabilities to automate internal auditing procedures and improve quality (can be integrated with risk management capabilities)

Keeping on Top of Your Security Needs

The guidance provided in this document is designed to help your organization understand that when it comes to secure operations, you are not alone. SAP understands the challenges ahead and is here to help you take the appropriate measures and achieve peace of mind.

Our resources and tools are available to answer your questions, offer expert advice, and provide support. A good starting point would be to familiarize yourself with the various white papers that we've published on security and compare these to actual situations that you are encountering in your own company. These resources go deeper into the many topics covered here.

It's also a good idea to refer to our security guides and security baseline template for further information and support. And take advantage of our tools, which include SAP EarlyWatch Alert, SAP Security Optimization, our system recommendations, and our configuration validation. These tools are available to you as part of your maintenance contract, although additional charges may apply.

From here, you'll be in a strong position to devise your own company action plan and create a security road map that is tailored to the unique needs of your organization. We also recommend making use of existing external offers, which include the guides, working groups, and special-interest groups developed by our regional user groups. Finally, we invite you to actively raise open security questions with us by sending us a message anytime. After all, your security is our priority.

When it comes to secure operations, **you are not alone**. SAP understands the challenges ahead and is here to help you take the appropriate measures and achieve peace of mind.

Additional Information

Further details are available at the following locations (some of these resources require user and password authentication):

- SAP Security Optimization
- Security baseline template
- Secure operations map
- Security white papers
- Security checklists and recommendations for SAP HANA®
- SAP EarlyWatch Alert
- System recommendations for SAP solutions

OUR COMPLIANCE AND SECURITY SOLUTIONS
For more information on the solutions we offer in the area of compliance and security, please refer to the following sources:

- Security
- Cybersecurity and governance, risk, and compliance

Follow us

www.sap.com/contactsap

Studio SAP | 49234enUS (20/08)

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

THE BEST RUN SAP®