SAP Standard for Security
SAP Solution Manager 7.2

Document version 1.0 – 2017-03-31
LEGAL DISCLAIMER

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. This presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has 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’s strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP 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. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This document is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP’s willful misconduct or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from exceptions. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

DOCUMENT HISTORY

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>2017-03-31</td>
<td>First version created</td>
</tr>
</tbody>
</table>
## TYPOGRAPHIC CONVENTIONS

<table>
<thead>
<tr>
<th>Type Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example</strong></td>
<td>Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Textual cross-references to other documents.</td>
</tr>
<tr>
<td><strong>EXAMPLE</strong></td>
<td>Emphasized words or expressions.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.</td>
</tr>
<tr>
<td><strong>&lt;Example&gt;</strong></td>
<td>Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.</td>
</tr>
<tr>
<td><strong>EXAMPLE</strong></td>
<td>Keys on the keyboard, for example, [F2] or [ENTER].</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1. **SAP STANDARDS FOR END-TO-END SOLUTION OPERATIONS** ................................................................. 5
   1.1 Control Center Approach .................................................................................................................. 7

2. **OVERVIEW OF THE SAP STANDARD FOR SECURITY** ........................................................................ 10
   2.1 Secure Operations Map ................................................................................................................... 10
   2.2 Security in Implementation Phases .................................................................................................. 12
   2.3 Security Principles ........................................................................................................................... 13
   2.4 People and Roles .............................................................................................................................. 14

3. **IMPLEMENTATION OF SECURITY** ............................................................................................... 16
   3.1 Plan phase ........................................................................................................................................ 17
   3.2 Build phase ..................................................................................................................................... 18
   3.3 Run phase ....................................................................................................................................... 19
   3.4 Optimize phase ............................................................................................................................... 20

4. **DRIVING CONTINUOUS IMPROVEMENT** .................................................................................. 22
   4.1 Quality Assurance Tasks ................................................................................................................ 22
   4.2 Quality Targets and KPIs ................................................................................................................ 22

5. **TRAINING** ....................................................................................................................................... 24
1 SAP STANDARDS FOR END-TO-END SOLUTION OPERATIONS

IT organizations face new challenges every day as they attempt to remain effective and future safe while also keeping costs for day-to-day operations as low as possible. They are also being challenged more than ever to demonstrate their value to the business. Therefore, it is important to optimize the day-to-day tasks that appear to have less obvious business value and to use KPI and benchmark-based reporting to make IT processes more visible, demonstrating the real value that IT can provide.

In order to minimize the costs of IT, it is necessary to standardize and automate the end-to-end IT processes without reducing the SLAs required by the business, such as stability, availability, performance, process and data transparency, data consistency, IT process compliance, and so on. Based on the experience gained by SAP Digital Business Services (DBS) while serving more than 36,000 customers, SAP has defined process standards and best practices to help customers set up and run end-to-end solution operations for their SAP-centric solutions.

The Build phase of SAP best practices supports a Build SAP Like a Factory approach, consisting of the following processes:

- Custom code management
- Change, test, and release management
- Incident, problem, and request management
- Solution documentation

During the Run phase of a solution, adapting your IT infrastructure to a Run SAP Like a Factory operation impacts both application operations and business process operations. Therefore, operations processes, such as end-to-end root-cause analysis, system monitoring, system administration, and data volume management need to be optimized to achieve state-of-the-art application operations. In business process operations, the same applies to business process and interface monitoring (including performance optimization), data consistency management, and job management.

Quality management processes and tasks need to be established throughout the lifecycle to guarantee continuous improvement of the end-to-end solution operations processes while simultaneously ensuring the flexibility needed to react to changing requirements.
The figure 1 shows an organizational model for solution operations that aligns SAP best practice topics and SAP standards for End-to-End Solution Operations with SAP's control center approach. The Operations Control Center executes and controls the Run SAP Like a Factory processes, while the Innovation Control Center ensures optimal custom code management and a smooth transition to production with integration validation procedures. SAP connects to these control centers from the Mission Control Center to ensure that professional support is available to the customer. The following Application Lifecycle Management (ALM) functions are not provided directly in one of the control centers because they must be handled across different areas:

- Change, test, and release management
- Incident, problem, and request management
- Solution documentation

The quality management methodologies are an essential part of SAP's Advanced Customer Center of Expertise (Advanced CCoE) concept and ensure that the KPI-driven processes are continuously improved across all processes and teams. In addition, the quality manager roles ensure consistent and value-centric reporting to the business and management. This unified reporting platform is known as the Single Source of Truth.
1.1 Control Center Approach

The control center approach consists of three components:

- Mission Control Center (MCC)
- Innovation Control Center (ICC)
- Operations Control Center (OCC)

Both the ICC and OCC are made available at your IT facility, while the MCC is located at regional SAP sites. All three approaches are linked together through the SAP Solution Manager application management solution.

Mission Control Center (MCC)

The purpose of SAP Mission Control Centers (MCCs) is to support the ICCs and OCCs at customer locations, enabling proactive identification and fast resolution on critical issues operating the SAP solutions and helping to apply standard SAP software functionality that addresses business requirements. The MCCs are serving as the central inbound channels for all complex and business critical request of our customers. MCCs connecting customers to experts from SAP that are ready to provide support across all solution areas and phases of the application lifecycle. SAP MCCs are located on North America, Latin America, Europe and Asia regions. All MCC’s are networked, use a common infrastructure and service management system, providing 24x7 year around coverage for critical customer situations.

Figure 2: Interaction Between ICC, OCC, and MCC
Innovation Control Center (ICC)

SAP’s Innovation Control Center (ICC) is the delivery framework to deliver mid to long term innovation programs. The ICC combines a set of experts, services, tools and templates and represents a lean front office at the customer location that is connected to all offerings of a very strong back office, called the Mission Control Center (MCC). This ensures access to the expertise of the entire SAP ecosystem in a structured way.

The Innovation Framework is the foundation of an ICC and is led by a certified ICC Lead. The Lead delivers against a long-term, value based roadmap, sets-up collaboration tools and dashboards for the connection to the MCC and creates innovation service plans for the underlying projects. ICC services are available for all phase of innovation projects

- Discover/Prepare: e.g. Prototyping
- Explore/Design: e.g. Gap Validation or Design Review
- Realization/Deploy: e.g. Integration Validation (Safeguarding)
- Run: Transition to Operations

The overall concept of ICC/MCC establish a long-term relationship to SAP and helps saving implementation costs and time for our customers.

Operations Control Center (OCC)

The Operations Control Center (OCC) is the physical manifestation of the Run SAP Like a Factory philosophy. The Operation Control Center (OCC) is a service of an IT organization that

- creates the relevant transparency to business and other stakeholders along the IT aspects of the seamless execution of E2E critical or core business processes
- provides the relevant transparency on health of the end to end IT landscape and underlying software components
- manages critical exceptions and continuous improvement on the above aspects based on data driven insights
- is supported by standardized IT processes

Figure 3: SAP Mission Control Centers – Customer Innovation Control Center collaboration model
An Operation Control Center is sitting as a layer across / above typical IT departments (who are responsible for the day to day IT operations). It is the job of the OCC to immerse itself in the landscape and processes to fully understand the operational challenges facing the business. Centralized tools and standardized monitoring procedures provide much-needed transparency into these challenges. Meanwhile, a focus on continuous improvement and optimization can improve operations over the long term. As a result, IT departments can realize reduced costs and better capitalize on new opportunities for innovation. To achieve these goals, OCC relies on a close interaction with both the Innovation Control Center (ICC) and the SAP Mission Control Center (MCC).

The OCC is typically equipped with large screens that display the status of business processes, IT landscape components, as well as exceptions and alerts. If problems occur, a video link can be used to obtain live support from SAP and partners. The customer is responsible for managing the OCC.

The OCC is most effective when closely integrated with other IT processes, such as IT Service Management (ITSM) and Change Management. Central monitors and dashboards based on application and business process operations display the current status of business and IT-related processes. This data can also be used to drive continuous improvement.

An effective system monitoring and alerting infrastructure is fundamental to the success of an OCC and feeding the OCC. The OCC is safeguarding all relevant IT aspects, and the execution of the end to end business processes in scope. The OCC reacts and manages on exception along this critical business processes according to predefined error-resolution activities. The OCC manages follow-up activities for error handling if the relevant tasks are not completed within a certain timeframe.
2 OVERVIEW OF THE SAP STANDARD FOR SECURITY

The SAP Standard for Security aims to assist you in setting up efficient procedures and techniques to protect the company’s critical business processes and assets, as well as to ensure compliance with external regulations and standards, such as data protection laws and the Sarbanes Oxley Act (SOX). By following it, you should be able to secure the availability and integrity of critical business processes – both company internal processes as well as collaborative processes with your own customers or other contractors – and to protect the confidentiality and integrity of sensitive information.

To achieve this, the standard follows the structure of SAP’s Secure Operations Map, a framework that has evolved over time to make the individual topics be handled in a more efficient way.

2.1 Secure Operations Map

The objective to secure all the company’s assets are accomplished by addressing sixteen different compliance and security topics, known as secure operations tracks, as shown in the following Secure Operations Map.

![Secure Operations Map](image)

Each track relates to one of the following five principal areas:
- Security Compliance
- Secure Operation
- Secure Setup
- Secure Code
- Infrastructure Security

The individual tracks are can be summarized with the following tasks:
Security Compliance

- **Security Governance**: Adopt security policies for your SAP landscape, create and implement an SAP Security Baseline.
- **Audit**: Ensure and verify the compliance of a company’s IT infrastructure and operation with internal and external guidelines
- **Cloud Security**: Ensure secure operation in cloud and outsourcing scenarios
- **Emergency Concept**: Prepare for and react to emergency situations

Secure Operation

- **Users and Authorizations**: Manage IT users and authorizations including special users like administrators
- **Authentication and Single Sign-On**: Authenticate users properly – but only as often as really required
- **Support Security**: Resolve software incidents in a secure manner
- **Security Review and Monitoring**: Review and monitor the security of your SAP systems on a regular basis

Secure Setup

- **Secure Configuration**: Establish and maintain a secure configuration of standard and custom business applications
- **Communication Security**: Utilize communication security measures available in your SAP software
- **Data Security**: Secure critical data beyond pure authorization protection

Secure Code

- **Security Maintenance of SAP Code**: Establish an effective process to maintain the security of SAP delivered code
- **Custom Code Security**: Develop secure custom code and maintain the security of it

Infrastructure Security

- **Network Security**: Ensure a secure network environment covering SAP requirements
- **Operating System and Database Security**: Cover SAP requirements towards the OS and DB level
- **Frontend Security**: Establish proper security on the frontend including workstations and mobile devices

For more information about each operations track, see the SAP Security Optimization page on SAP Support Portal at [https://support.sap.com/sos](https://support.sap.com/sos).

Note

The secure operations tracks only describe security measures for SAP business solutions. Other security measures that constitute a comprehensive and complete security concept, such as physical measures that control access to facilities or sites, are not covered by this document.
2.2 Security in Implementation Phases

SAP recommends performing the typical design, setup, and operation phases within all of the secure operations tracks to ensure comprehensive security for your SAP systems. Although some of the principal areas already suggest a certain phase to be affected more directly (e.g., Secure Operations is mainly an operational activity while Security Compliance seems to address the design phase), the activities have to be done for all areas.

For low or medium security requirements, you can follow the best practice recommendations provided for each secure operations track. However, for elevated security requirements, you need to perform a comprehensive threat modeling and risk analysis in order to determine the appropriate security measures. These activities (threat modeling & risk analysis) are based on a profound knowledge of the company’s critical business processes and must be performed during the Plan (Design) phase. Successfully designing, implementing, and operating a comprehensive IT security concept requires support and commitment from top-level management. In addition, you need personnel with the relevant knowledge of security and an understanding of the company’s critical business processes. As part of their commitment to security, management must implement the following measures:

- Create a company-wide security policy that outlines general security principles and guidelines. This document should manifest the company’s commitment to security.
- Define dedicated security roles and establish a clear reporting line with the overall responsibility at board level.
- Provide those responsible for security with a dedicated security budget.

Consequently, before going into more detail for the individual activities to be done within the respective implementation phases - also called the “Lifecycle of Security” - important common security principles as well as roles and an overview of typical activities associated with each role are outlined in the next sections.
2.3 Security Principles

Before even going into the first design phase of each of the security tracks mentioned above, your company has to settle down to certain base principles as well as the underlying security philosophy it would like to enact. While some of the principles are non-negotiable - they always hold when dealing with security issues - others reflect the risk averseness of the company or the importance of efficiency to the company. These elements typically have a trade-off associated with negative and positive side-effects - and the company's management has to decide what is more important: lesser risk but more effort, or the other way around. Typically these principles have already been defined outside the context of SAP applications - please ask your internal security team for details.

The weakest link - secure everything

Security is always only as strong as its weakest link. Hence security always has to be considered holistically. Considering only one aspect of security or considering security only in some areas fails to secure a system landscape. Following this "weakest link" paradigm, security fairly often starts in lower systems. In an integrated landscape of topmost importance to the company, almost every system is "critical". Example: Development systems may not hold any data from production. However the software which gets transported into the production is created in the development system. If the system is compromised it might be possible to have malicious code transported into the production system. SAP recommends to take every business process, asset, application, system and network element into consideration and only leave short-living sandbox elements aside (as long as they are operated in a separate network segment and cannot endanger other important systems).

Secure first, open later

This is also known as "whitelisting vs. blacklisting" - or, in case of whitelisting, "principle of least privilege": If not explicitly allowed, access is forbidden. In particular for user authorizations, this has been traditionally demanded by auditors. However, this principle can be applied to database, operating system or even network level access as well. On the other hand, an organization may also decide to follow the blacklisting principle. Because denying everything upfront leads to higher efforts in most cases (e.g. asking for permission, granting permission etc.). Your management should decide which principle to follow for which types of systems or technical layer. SAP recommends to start new implementations with a completely closed up system. Everything that is needed should be opened explicitly. For example, a new user should always start without any authorizations and should be granted only the authorizations he needs for his work.

Threat models and risk assessments

In particular for higher security demand, a threat model should be developed for all processes that touch the SAP system under consideration. Threat models significantly help to structure possible security issues and to make sure that nothing is forgotten (see above: weakest link). Your company's management should decide whether threat modeling must be applied in certain cases. As outlined above, certain security measures bring a trade-off with them. Your company's management should setup a risk assessment process which evaluates both negative and positive effects of a specific measure. Only when assessed in a structured, comprehensible way, risks can be communicated correctly and revaluated in the future.

Skills, knowledge and budget

While certain technical aspects are eligible for outsourcing, security as a whole cannot be bought. Employees must be educated about IT security risks such as social engineering, phishing, spear phishing, tailgating, open Wi-Fi, clean desk, USB devices, email attachments and so on. This affects
SAP applications as well, because they are typically heavily integrated with office data exchange and any failure to protect that may affect SAP application data as well. Furthermore, creating security policies, choosing the right technology, tools and partners require a security team with corresponding knowledge in the field, including SAP products. Your company's management must decide which roles should be present and equipped with a certain level of budget - see "Roles and People" section below. Finally: security costs. As an example, increased checks within user and role maintenance costs because of longer time it takes the affected employees to get through a more complex process. Mitigating this additional effort with more efficient tools like identity management carries other costs. Not providing a budget that matches the company's willingness to take additional risk will fail.

### 2.4 People and Roles

The following overview is not a complete guide to roles and is not intended for use as a fixed blueprint. Role concepts are unique to each company because they vary depending on both the size of the organization and how it is structured. However, the organizational model of each company must still comply with the Segregation of Duties (SoD) requirements imposed by legal regulations, such as the Sarbanes-Oxley Act (SOX). The following table may be used as a template to start designing the (SAP) security organization of the company if not already existing:

<table>
<thead>
<tr>
<th>Group</th>
<th>Role</th>
<th>Activities and Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>Network Administrator</td>
<td>Network segmentation, firewall configuration, communication channel encryption</td>
</tr>
<tr>
<td></td>
<td>Operating System Administrator</td>
<td>Maintains technical systems, defines backup and recovery concept, performs emergency response process</td>
</tr>
<tr>
<td></td>
<td>Database Administrator</td>
<td>Configuration of database, implementing encryption</td>
</tr>
<tr>
<td></td>
<td>SAP Basis Administrator</td>
<td>Operates the SAP application layer, deploys patches, sets security relevant SAP profile parameters or customizing entries</td>
</tr>
<tr>
<td></td>
<td>Application Management</td>
<td>Policy definition on application level, definition of security requirements, design of application authorization structure</td>
</tr>
<tr>
<td></td>
<td>Quality and Test Management</td>
<td>Test concepts for in-house or third-party developments, quality checks on deliverables</td>
</tr>
<tr>
<td></td>
<td>Internal Help Desk Personnel</td>
<td>Management of support connections, handling or forwarding of incidents, incident reproduction on test systems</td>
</tr>
<tr>
<td>Security Team</td>
<td>Security Administrator</td>
<td>Day to day operation of the security monitoring, alerting and emergency responses</td>
</tr>
<tr>
<td></td>
<td>Authorization Administrator</td>
<td>Creates and maintains roles and authorizations</td>
</tr>
<tr>
<td></td>
<td>User Administrator</td>
<td>Creates and manages users, performs risk analysis of user authorization assignment, ensures user-appropriate provisioning and deprovisioning of roles</td>
</tr>
<tr>
<td></td>
<td>Security Management</td>
<td>Policy and emergency response definition, approval and publication, requirements definition, selection and assessment of security measures</td>
</tr>
<tr>
<td></td>
<td>Data Protection Office</td>
<td>Identification and verification of privacy requirements with regard to employees and customers</td>
</tr>
<tr>
<td></td>
<td>Internal Auditor</td>
<td>Verification of legal (external) or internal requirements</td>
</tr>
<tr>
<td></td>
<td>Security Analyst</td>
<td>In-depth security assessments, including forensics, works on security incidents and determines underlying root causes</td>
</tr>
<tr>
<td>External</td>
<td>Auditor</td>
<td>Independent assessment of the internal security compliance</td>
</tr>
<tr>
<td>Business</td>
<td>• Process Owner (planning of processes)</td>
<td>Identify and document process-specific risks, process monitoring, conflict resolution, role design (SoD)</td>
</tr>
<tr>
<td>Group</td>
<td>Role</td>
<td>Activities and Responsibilities</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Business Management</td>
<td>(responsibility)</td>
</tr>
<tr>
<td></td>
<td>Business Expert</td>
<td>(manages implemented processes)</td>
</tr>
<tr>
<td>IT-Management</td>
<td></td>
<td>Budgeting, requirements definition, decision on tools, selection and assessment of security measures (in accordance with Security Team)</td>
</tr>
<tr>
<td>Risk Analyst</td>
<td></td>
<td>Comprehensive risk analysis, impact and probability estimations, cost/benefit estimations</td>
</tr>
</tbody>
</table>

In smaller companies, many of the listed roles can be taken by one employee, e.g. fairly often database and operating system administrators are the same person. However, particular functions require a 4-eyes principle to make sure that the enacted security requirements are not circumvented. An example is user and role administration: an employee that assigns roles to users should not be the same person that creates or changes these roles. Furthermore, no one should be able to assign roles to his own user. Another example is security requirements definition, monitoring and reporting should not be in the same hands as implementing the requirements - otherwise someone implementing security settings would be monitoring himself.

Following such segregation of duties principles is even more important when no regular internal or external audit is performed. Such audits provide an independent view which would check for missing SoD.
3 IMPLEMENTATION OF SECURITY

This section describes the best practices for the security-relevant activities that you need to perform during the operations and optimization phase. The prerequisite activities of the design and setup phase are only briefly outlined here. For more detailed information, see the SAP Security Optimization Service page on SAP Support Portal at https://support.sap.com/sos. The SAP Security Optimization Service page is structured according to the Secure Operations Map and its secure operations tracks. On the SAP Security Optimization Service page, the relevant chapters for the operations tracks consist of an operations track document describing the relevant prerequisites and best practices for all phases within the track. To address a certain track, the responsible security stakeholders can focus on the relevant section in each of these documents. Each section describes important activities related organizational roles, standard and optional SAP tools, as well as relevant training activities. Activities follow the same pattern in the Design, Setup, and Operations & Optimization phases, regardless of the actual track. This pattern complies with the common understanding of a security process as outlined by international standards, such as ISO/IEC 27001:2005, and refinements by national standardization bodies, for example, the German Federal Office for Information Security (BSI).

![Figure 8: Security Process for All Secure Operations Tracks](image-url)
3.1 Plan phase

All areas from the Secure Operations Map require proper and upfront planning. Make sure that adequate policies are developed and consistent with your company’s management demand:

**Security Compliance:** Determine who’s responsible for the security of your company’s applications. Discuss and formulate security policies valid for all SAP applications. Check for external regulation and internal requirements that need to be incorporated into these policies. Validate the policies with external and internal auditors. Discuss possible emergency scenarios and document mitigating processes. Write down requirements that result from your internal policies to be adapted to cloud scenarios. Assess which cloud solution matches the requirements best. Check whether SAP’s GRC Suite or similar partner solutions may provide the basis for a more efficient handling of policies, regulations and risks.

**Secure Operation:** Document the process with which users may get access to systems and which departments are involved for checking, granting and maintaining users and roles. Determine the procedures for maintaining roles and checking user credentials, this includes determining valid authentication procedures and single sign-on scenarios. Document valid procedures by which vendors and partners may access systems remotely for support purposes. Check whether SAP Access Control, SAP Identity Management and SAP Single Sign-On or similar partner solutions can assist for controlling users and authorizations in larger environments in a more efficient way.

**Secure Setup:** Plan ahead how and by whom important security settings are to be made and how the correctness of the settings is validated. Discuss which types of communication has to be secured by which kind of technique (example: shall SNC be used to encrypt all SAPGUI communications?). Do the same for data storage: shall database content be encrypted? If so, how and where? All database content or just selected content? Additionally, investigate whether all demanded security settings match important SAP security recommendation documents from https://support.sap.com/securitywp (see also Section 6 “More Information”).

**Secure Code:** Design a process that makes sure all vendor security patches (operating system, database, SAP Security Notes) get into the systems in a timely manner, based on their priority. Which department is responsible for retrieval of the patches each month? Make sure that the patches get evaluated and documented in which time they have to be applied. Align the corresponding process with your release management. Determine how custom coding is checked for important vulnerabilities and whether additional tools - such as SAP's Add-On for Code Vulnerability Analysis or similar partner products - have to be deployed to assist with this task. Outline the approval processes for exceptions with both vendor security patches and vulnerable custom code that exists in production systems.

**Infrastructure Security:** Discuss whether all SAP applications can be run inside one single network segment or whether individual segments shall be deployed to shield applications of different security classification from each other. Plan for regular penetration testing activities to make sure that your firewall and network security setup matches the expectation that no direct access to internal systems is possible from the outside. Investigate whether solutions such as SAP Enterprise Threat Detection or similar partner products are required for real-time monitoring.

The criticality of each business process affects how you need to design your security processes. For standard security requirements, you can simply follow a best practice approach; however, for critical business processes, you need to perform a comprehensive risk analysis and additional supporting processes.

For more information about how to design a risk analysis in the design phase, as well as the specific responsibilities and future actions, see the **Design Operations** chapter of the relevant operations track document on SAP Support Portal at https://support.sap.com/sos. Please also consult the new SAP Activate Roadmap at https://go.support.sap.com/roadmapviewer/# (S/4HANA Roadmap, On Premise). Within SAP Activate, the phases DISCOVER, PREPARE and EXPLORE compose the traditional plan phase. In these phases, specific security steps are now embedded that may help you to determine the correct planning activities.
3.2 Build phase

During implementation it is vital to make sure that everything is setup the right way, i.e. that no items are forgotten or wrong settings open the new applications in an improper way:

Security Compliance: Thoroughly test the policies and accompanying processes and responsibilities. Do they work properly as designed? Or have unexpected limitations set restrictions on what can be done? If so, rephrase your policies, adapt their documentation - it is important that the overall design still matches the implementation after finalization. For cloud solutions, conduct an audit whether the partner fulfills all requirements properly. Run a full drill on your emergency procedures.

Secure Operation: Implement all required tools and techniques - as well as additional solutions or partner products - to run your user and role maintenance process the correct way. Test exceptions, e.g. what happens when certain workflow requirements are not met, does proper escape routing exist or alternative ways to access systems in case user management tools fail? Make the underlying authentication infrastructure fail-safe and test access from different environments.

Secure Setup: Make sure all important recommendations from https://support.sap.com/securitywp, in particular Secure Configuration ABAP, Securing RFC communication and Protecting Applications Against Common Attacks have been followed unless your internal guidelines do not demand different settings. As a minimum, the configurations from the SAP Security Baseline Template (see Section 6 "More Information") should be implemented. Check for proper implementation of TLS and SNC or other cryptographic techniques. Thoroughly test that insecure settings do not exist and that insecure communications are properly blocked.

Secure Code: Implement security patching tools and test the corresponding processes. Make sure that emergency transport routes for critical SAP Security Notes work efficiently and that regression testing procedures after implementing Support Packages have been correctly documented. Write down secure programming guides to be followed when creating custom code and implement (automatic, tool based) checks to scan your custom code before it leaves the development systems.

Infrastructure Security: Setup the network segmentation structure that has been designed in the planning phase and perform thorough testing on the respective network borders whether all filters and firewall engines work as expected. When everything is ready, run tests from the outside whether internal systems are shielded properly. In particular make sure that Fiori Apps that are accessed from untrusted networks are run on hardened platforms and that their network traffic can be screened on the application layer for malicious input. Setup logging inside the SAP systems, in particular you should switch on and configure the Security Audit Log.

Implementing the security concepts usually involves several steps and various installation and configuration activities. For a list of all typical activities as well as details about testing and review, see the Setup Operations chapter of the relevant operations track document on SAP Support Portal at https://support.sap.com/sos. Please also consult the new SAP Activate Roadmap at https://go.support.sap.com/roadmapviewer/ (S/4HANA Roadmap, On Premise). Within SAP Activate, the phases REALIZE and DEPLOY compose the traditional build phase. In these phases, specific security steps are now embedded that may help you to determine the correct security implementation activities.
3.3 Run phase

While the implementation phase ensured that your new solutions are setup in a secure manner, a secure run phase is vital to stay protected. Most importantly, all measures that have been implemented must be monitored to quickly become aware when the security level degrades somewhere or when attacks are run:

**Security Compliance:** Check whether the policies are effective. Investigate regularly if the policies can be followed and provide the desired level of security without having too negative side-effects. In order to do this, it is important to have measurable KPIs in place (see also section "Continuous Improvement" below). Measure the activities of internal and external auditors: Are the policies understandable to them, and can they conduct their investigations in an efficient way?

**Secure Operation:** Monitor the efficacy of your user and authorizations maintenance processes. Check whether workflows don't take too long and user lifecycles follow changes in employee positions in a timely manner. If passwords based authentication mechanisms are used, regularly check the business case of simpler techniques and measure costs of the user administration desk that has to reset passwords.

**Secure Setup:** It is quite common that security settings degrade over time when systems are copied or critical customizing requires opening of clients for changes (which is often forgotten to be closed afterwards). Therefor you should implement a regular validation of all security settings. SAP recommends to make use of the Configuration Validation application inside SAP Solution Manager to see differing settings as soon as possible. This should include a validation of encryption techniques, e.g. that it is still properly enforced to use TLS and SNC on all communications. Make use of the SAP Security Baseline Template, it includes content for the Configuration Validation application. When not utilizing Configuration Validation, use the Early Watch Alert application inside SAP Solution Manager as a minimum.

**Secure Code:** Setup a reporting about (not) implemented security patches. SAP recommends to make use of the System Recommendations and Configuration Validation applications inside SAP Solution Manager to check for open SAP Security Notes. Measure the efficiency of the custom code security check procedures and whether secure programming guides are followed properly.

**Infrastructure Security:** Monitor on network and operating system level whether attacks are run from unauthorized personnel. Check the logs regularly for anomalies or use additional solutions that provide automated attack detection and incident investigation techniques. Run a team that performs thorough forensic analysis on validated security incidents.

Dedicated review processes conducted by administrative roles verify the successful enforcement of the company’s security policy and ensure that the correct implementation of security measures is not harmed by changes to systems and applications. For detailed information about who should be involved in the review processes, how to measure the defined security KPIs, and references to the company’s security policy, see the Operations & Optimization chapter of the relevant operations track document on SAP Support Portal at https://support.sap.com/sos. Please also consult the new SAP Activate Roadmap at https://go.support.sap.com/roadmapviewer/ (S/4HANA Roadmap, On Premise). In its RUN phase, specific security steps are now embedded that may help you to determine the correct operational activities.
3.4 Optimize phase

This section introduces a series of general criteria that allow organizations to measure the quality or maturity of information security management systems (ISMS) as well as individual secure operations tracks as they are used in the SAP Standard for Security. You can then use this information to optimize security in your organization.

Note

These criteria only provide initial guidance; you need to continuously monitor and evaluate them during operation to determine their effectiveness and drive improvement.

Depending on individual needs and requirements, you should define a different set of objectives for each of the secure operations tracks to compare with the actual situation.

The different criteria are categorized as follows:

- **Process criteria:** Concern the quality and type of security-related workflows within the company
- **Organizational criteria:** Indicate the commitment and support of security by top-level management
- **Tool criteria:** Describe the quality and extent of tool support
- **Measurement and improvement criteria:** Describe feedback and improvement cycles

**Process Criteria**

- **Predefined security workflows**
  Without predefined workflows, security-related activities are performed on an ad-hoc basis, that is, without a clear concept and procedure description. In such cases, the same type of security incident may result in entirely different mitigations. Predefined processes for specific incidents result in effective, reliable, and controllable mitigation activities that are always performed in the same manner, regardless of who actually executes the workflow.

- **Proactive security-related activities**
  Less mature organizations only perform security-related activities if there is an immediate need, for example, if there is a security breach, an external audit, or they need to import a new support package. In such companies, security-related activities are primarily reactive or event driven.

  More mature companies operate proactively. They continuously prepare for and plan security activities, without an immediate need but with a planned and controlled schedule, for example, in terms of review processes and internal audits that help verify the compliance of the company’s security implementation with internal and external requirements.

- **Documentation of activities**
  More advanced security implementations ensure comprehensive documentation of security activities. Ideally, the documentation is available from a central information repository that also provides access to all relevant security concepts and, for example, a full description of the IT infrastructure.

**Organizational Criteria**

- **Company-wide security policy**
  A company-wide security policy ensures that top-level management is committed to the objectives, value, scope, and direction of all security activities performed within the company. This policy should be made available to all employees, for example, from the company’s internal portal.

- **Dedicated budget and personnel**
There should be a dedicated budget for security. Security-related activities should also be performed by trained security experts who are assigned to specific areas. In less mature organizations, security activities are performed by other administrative personnel, such as system administrators, which can eventually cause SoD conflicts.

- Regular training and awareness campaigns
  There should be regular training activities and campaigns to increase awareness of security issues among all personnel.

**Tool Criteria**

- Workflow tools
  Tools should be implemented to enforce and document security workflows during operations. In less mature organizations, workflows might exist on paper, but compliance and execution are not enforced. The Change Request Management and Change Control Management components of SAP Solution Manager can provide significant support in this context.

- Monitoring and review tools
  Security-related information should be monitored and reviewed as close to real-time as possible using intrusion detection systems. Configuration and authorization settings should also be verified on a periodic basis, for example, using the SAP Security Optimization Service.

- Automatically triggered workflows
  Incidents detected by monitoring and review tools must automatically trigger the corresponding workflows for incident resolution.

**Measurement and Improvement Criteria**

- Continuous measurement and periodic evaluation of KPIs
  Continuously measuring and evaluating KPI results steadily optimizes implemented processes, without the need to repeat the design and setup phases.

- Systematic and extensive approach to the operations & optimization phase
  Bigger optimization measures after go-live usually involve substantial changes to the company’s security concept. For such large-scale optimizations, you should repeat all phases for the given secure operations track. These changes improve the company’s standard security level by introducing qualitative measures, for example, tool support of security processes. The maturity of an organization in this regard depends on the extent and systematic approach with which such automations are performed during the operations & optimization phase.
4 DRIVING CONTINUOUS IMPROVEMENT

It is important that your organization learns from the day-to-day operations of security-related activities so that security measures become increasingly effective and efficient. This section describes some key steps you can take to drive continuous improvement and increased value for your security processes.

4.1 Quality Assurance Tasks

From a quality management perspective the key tasks are as follows:

- Track implementation status of SAP Security Notes (implementation vs. release date)
- Track results of security audit and ensure follow-up
- Track compliance to security controls
- Evaluate results of security-related SLA agreements
- Ensure action items are identified for SLA deviations
- Deploy security awareness campaigns
- Request an SAP Security Optimization Service Portfolio (or comparable services from SAP Activate, RUN phase)

For an indication of appropriate KPI setup and measurement, consider the answers to the following questions to ensure that security for users and systems are under control and are communicated within all related parties:

- How do you decide to implement SAP Security Notes?
- How and how often do you review user authorizations?
- How and how often do you review infrastructure security?
- How often do you hold security meeting and who (what roles) must participate?

4.2 Quality Targets and KPIs

To ensure continuous improvement of the security management process and drive the value recognition of IT, the most important quality targets are as follows:

- Increase trust and reliability of SAP solutions by keeping them secure, confidential, and available
- Ensure legal compliance through transparency and authenticity
- Protect investment and reduce TCO

To assess the quality of the security management process, clearly-defined parameters and measurable objectives are required. The key parameters should be collated and evaluated in regular reports. The historical data that is created in this way can be used to identify trends and then derive the necessary measures to take.
The following table describes the main challenges for each of these quality targets and which KPIs can be used to measure the success of your implementation:

<table>
<thead>
<tr>
<th>Quality Targets</th>
<th>Challenges</th>
<th>KPIs</th>
</tr>
</thead>
</table>
| Increase trust and reliability of SAP solutions by keeping them secure, confidential, and available | • Taking action proactively before severe security problems occur  
• Identifying and prioritizing risks  
• Reviewing security maintenance processes as described in this standard  
• Reviewing secure programming policy adherence  
• Ensuring appropriate SAP landscape security monitoring  
• Setting up individual security thresholds                                                                                                                                                                                                                                                                                                   | • Coverage of identified security threats with implemented preventive measures  
• Rate of response for high-risk incidents  
• Number of incidents related to remediation of security issues  
• Number of vulnerabilities not proactively identified                                                                                                                                                                                                                                                                                  |
| Ensure Legal Compliance Through Transparency and Authenticity                   | • Transparency  
• Ensuring that security for users and systems is under control and communicated within all related parties according to updated policy  
• Maintenance and review of authorizations to make sure that they meet legal and company-specific requirements  
• Review of managed access  
• Communication within different departments                                                                                                                                                                                                                                                                                       | • Number of security reviews  
• Number of security alignment meetings  
• Percentage of IT staff who participated in trainings in one year  
• Gap between implemented SAP Security Note from released SAP Security Note  
• Number of incidents caused by missing SAP Security Note  
• Number of reviews of assigned roles vs. actual requirements  
• Ratio of changes in standards/policies leading to IT reviews                                                                                                                                                                                                                                                                               |
| Protect Investment and Reduce TCO                                              | • Reducing the risk of costly downtime due to wrong user interaction                                                                                                                                                                                                                                                                                                                                  | • Number of security-related downtimes  
• Ratio of profile changes for users in one year  
• Number of incidents caused by incorrect or missing roles                                                                                                                                                                                                                                                                              |
5 TRAINING

ADM960 – SAP NetWeaver Application Server Security

Course Content
- Computer Security Overview
- Network Basics
- Basic Security for SAP Systems
- Introduction to Cryptography
- Secure Network Communication (SNC)
- Setting Up SNC for SAP NetWeaver AS ABAP
- Setting Up SNC for Non-ABAP Components
- Secure Socket Layer (SSL)
- Authentication and Single Sign-On (SSO) Mechanisms in SAP Systems

ADM950 – Secure SAP System Management

Course Content
- Introduction to Internal Security Auditing
- Customize and Usage of AIS
- Users and Authorizations Audit
- System Audit
- Repository and Table Audit
- Security in Change Management
- Security Assessment

HA240 – Authorization, Security and Scenarios

Course Content
- Creation of authorizations and authorization roles
- User management
- Access control for HANA native models
- Authorization trace
- Auditing
- Authentication and Single Sign-On options
- Encryption options
- Security considerations for Multitenant Database Containers
- SAP GRC Integration for Governance Risk and Compliance
- HANA use case scenarios and security requirements
- SAP Netweaver Identity Management integration.
- Reusing of BW authorizations for SAP HANA applications
- HANA Cloud Platform (HCP) security
- HANA Enterprise Cloud security

ADM940 – AS ABAP – Authorization Concept

Course Content
- Authorizations in General
- Basic Terminology of Authorizations
- User Settings
- Working with the Role Maintenance
- Basic Settings
- Using Traces
- Transporting Authorizations
- Integration into Organizational Management

FIN900 – System Audit with SAP

Course Content
- Impact of the Sarbanes-Oxley Act and other auditing standards (for example, ISA) that are relevant for the auditors on the audit process
- Compact overview of the authorization concept
- Role-based setup of the AIS and commercial audits with the AIS
- Basic system settings and logs
- Organizational units and organizational structure within an SAP system
- Practical analysis of the risks and controls using test cases
- General Customizing and controls in Accounting while taking into account the impact on the audit process
- Auditing business processes, for example, Procurement, Production, and Sales Order Processing
- Auditing the end of period financial statements
- Auditing of specific evaluation methods
- Transfer of the financial accounting data, balances, and document information to the auditor’s computer in standard format for further analysis (for example, in ACL, IDEA, Excel)

FIN910 – Management of Internal Controls

Course Content
- MIC positioning
- Maintaining the organizational structure
- Maintaining the central process catalog
• Scheduling assessments and testing
• Performing assessments and testing
• Management controls
• Roles and responsibilities in MIC
• Sign off and reporting
• MIC Dashboard

GRC300 – SAP Access Control Implementation and Configuration

Course Content
• Introduction to SAP Access Control
• Architecture, Security, and Authorizations
• Authorization Risks and the SoD Risk Management Process
• Shared Configuration Settings
• SAP Access Control Repository
• Business Rule Framework (BRF)
• MSMP Workflow
• Analyze and Manage Risk
• Emergency Access Management
• Design and Manage Roles
• Provision and Manage Users
• Periodic Access Review Process
• Reports and Custom Fields
• SAP Access Control Implementation

ADM920 – SAP Identity Management

Course Content
• SAP Identity Management (IdM)
• Forms
• Jobs
• Provisioning and Workflow
• Roles
• Approval Workflow
• Context-Based Assignments
• SAP IdM and Other SAP Systems
• Advanced Tasks
• SAP IdM Installation and Configuration