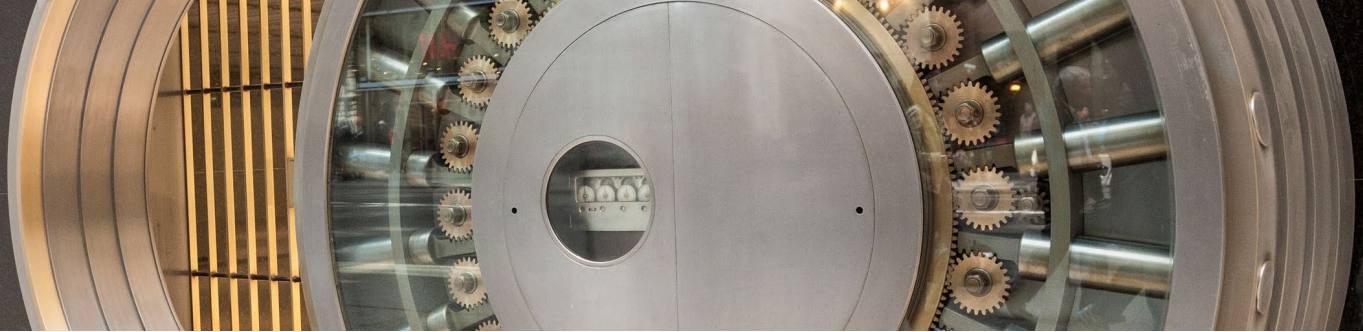


Managing Security with SAP® Solution Manager

May 2015

Table of Contents

-
- 3** Security in Three Phases: Build, Setup, Operate
-
- 7** The Role of ITSOM Tools for Security
-
- 16** Conclusion: The Center of a Secure System Landscape
-
- 17** Additional Information and References



Running a secure system landscape requires more than just secure software. System setup and operation are key to protecting against and detecting attacks to prevent downtime. **IT services and operations management (ITSOM)** tools play an important role for security, collecting information about a system landscape, providing alert mechanisms, and helping distribute security patches. The SAP® Solution Manager application management solution is the ITSOM product of choice for SAP software landscapes.

This paper introduces the various aspects of building, setting up, and operating a secure system landscape and shows how SAP Solution Manager supports these tasks.

Running and maintaining secure landscapes requires a strategy. And with the increasing need to collaborate with customers, partners, and employees anytime and anywhere, you need a strategy that makes things simpler to use and manage. A strategy requires an overall plan and with it a central controlling element that executes the plan or at least keeps it up-to-date for everyone to refer to. If you fight many small battles against vulnerabilities in a new setup, you may win some, but you will lose in the long run. Think of the well-meant but uncoordinated actions taken by individual citizens during fires, threats to public security, or natural disasters: these may be useful on the spot, but they will never keep an entire infrastructure or social system safe over time or be able to rebuild it. A central headquarters is necessary to coordinate all the measures

and activities and provide them as efficiently as possible, at the right time and in the right place.

This paper argues for such a headquarters for IT landscapes in the form of a central solution for **IT services and operations management** – particularly in SAP software landscapes, which are similar in complexity to the real-world social systems and infrastructures mentioned above. With complex systems, security is always a concern, primarily in the areas of monitoring and alerting, the software lifecycle, and software logistics. In large part, security requires knowing what is going on and knowing the landscape and its processes, so you can identify issues and fix them quickly when they first arise – and automate these functions as much as possible.

In the following sections, we will examine the role of ITSOM tools, particularly SAP Solution Manager, in software security, along with the process of implementing, configuring, and operating secure solution landscapes.

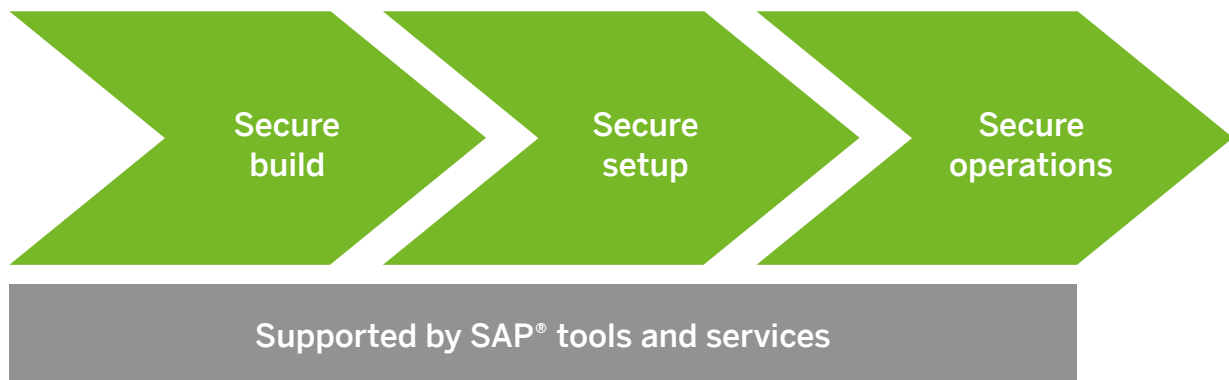


Security in Three Phases: Build, Setup, Operate

There are numerous ways to approach and subdivide the extensive topic of software, system, and landscape security.¹ This paper will follow the high-level process: you need to first **build secure software**, then **set up secure systems** and system landscapes in which this software runs, and finally **keep these landscapes secure** during operations.

Within these three phases, we will focus on those areas in which ITSOM tools make a strong contribution to securing system landscapes – particularly the many areas supported by SAP Solution Manager.

Figure 1: Three Main Phases Helping to Ensure Security



1. Another possibility is to structure the topic with security of data, channels and interactions, and identities on the first level, as shown in *SAP CIO Guide: IT Security in Cloud and Mobile Environments*.

BUILD SECURE SOFTWARE

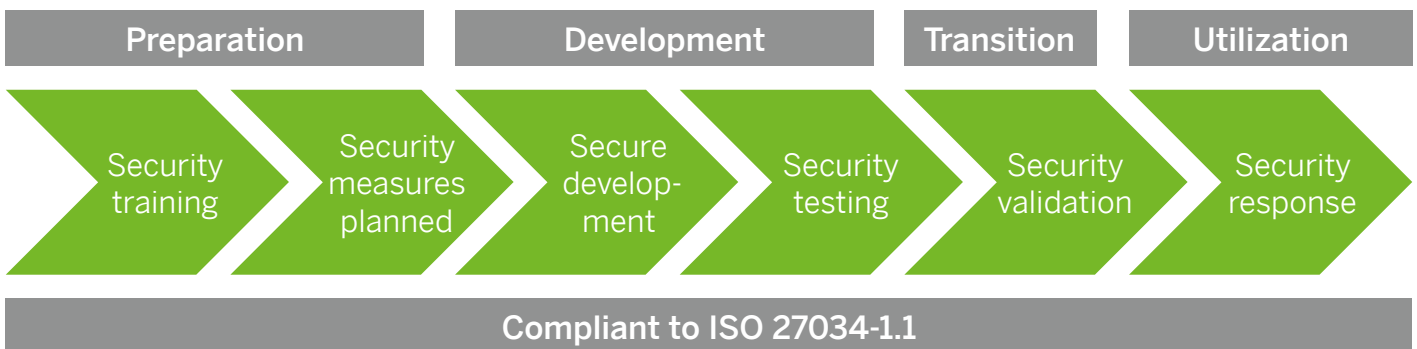
Security for software systems obviously starts with what developers do. They are the ones responsible for delivering secure code. They also deliver security fixes and prepare interfaces for secure communications, monitoring, and alerting. Developers need to answer questions such as these: Is the code well protected against manipulations or injections? Are interfaces designed for secure use? Are there no credentials hard-coded anywhere? Have the proper interfaces for monitoring, methods for alerting, and so forth been implemented? SAP developers follow the secure software development lifecycle shown in Figure 2.

This paper focuses on ITSOM tasks to keep landscapes secure, but the section “[Secure Code](#)” will also briefly examine some tools to validate coding with respect to security.

SET UP SECURE SYSTEMS

Setting up secure systems, system interactions, and thus system landscapes is the first step in subsequently operating a secure environment. Many tasks that must be performed once during setup reoccur, periodically or continuously, in the operations phase to ensure security, managed by an ITSOM solution. Setup is a highly critical phase, as missing security tends to be invisible, especially in a yet-unused system landscape. If the configuration is not checked actively, the detection of security flaws usually happens during operations – often when some damage has already been done. Fixing security issues during ongoing operations is usually expensive and often heavily restricted by the risk of breaking business-critical processes in productive environments.

Figure 2: Secure Software Development Lifecycle from SAP





KEEP LANDSCAPES SECURE

In the operations phase, powerful ITSOM tools become mission critical. This holds true for many operations tasks, which play important roles in keeping the operated landscape secure. An initially secure configuration is important, but you also need to ensure that changes to this configuration are deployed in a structured and monitored way. And security fixes alone will not be very useful if you do not know where to apply them or what their possible impact might be. These, among many other things, are recurring tasks for ITSOM – the central management of information pointing to possible vulnerabilities and attacks, as well as the coordination and routing of the corresponding fixes and defensive measures.

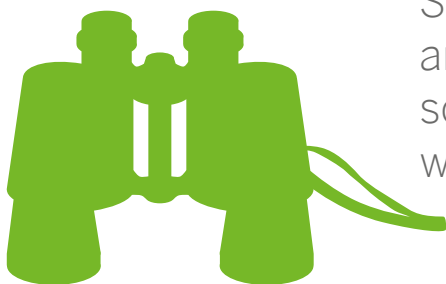
From the security perspective, timing is a critical factor, because the elapsed time between when a new threat or vulnerability occurs and when it is fixed defines the likeliness of damage. The ease and speed of fixing security issues is therefore crucial, and the security of a system landscape rises with the speed at which fixes can be deployed to the entire landscape.

The speed at which threats and vulnerabilities can be fixed increases with a number of factors, some of which are:

- Homogeneity of the landscape
- Completeness and consistence of information about the landscape
- Consistency of the fixing method(s)
- Completeness and quality of information about changes to the landscape
- Continuity of security maintenance

On the business side of the equation, time is also a critical factor. Security breaches and subsequent service downtime often cost organizations millions in lost revenue. Preventive network and systems security management can avoid these losses and make the difference in whether a business is profitable or not.

These effects are boosted by today's trend toward the cloud, combining cloud and on-premise landscapes, and providing more and more solutions for remote and mobile access. Many of the same mechanisms apply across these deployment scenarios, so we will not differentiate between them here.



Security requires knowing what is going on and knowing the landscape and its processes, so you can identify issues and fix them quickly when they first arise.



SECURE OPERATIONS MAP FROM SAP

SAP provides a Secure Operations Map that covers the three phases mentioned above and serves as a reference (see the final section of this paper) to match the capabilities of ITSOM tools to the requirements for a secure system.

Phase 1 – secure build – maps to “secure code” in Figure 3. Phases 2 and 3 – secure setup and secure operation – are named the same in

Figure 3. Phase 3 also covers the contribution of ITSOM tools to infrastructure security. “Security compliance” in Figure 3 applies to all phases and is typically not the focus of ITSOM tools.

The following section will introduce SAP Solution Manager as a comprehensive ITSOM tool and map some of its features to tasks in this Secure Operations Map.

Figure 3: Secure Operations Map from SAP

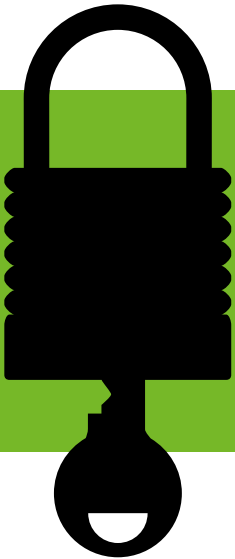
Security compliance	Security governance	Audit	Cloud security	Emergency concept
Secure operation	Users and authorizations	Authentication and single sign-on	Support security	Security review and monitoring
Secure setup	Secure configuration	Communication security	Data security	
Secure code	Security maintenance of SAP® code		Custom code security	
Infrastructure security	Network security	Operating system and database security	Front-end security	



The Role of ITSOM Tools for Security

We can define ITSOM tools covering the tasks of the three phases of security as follows: ITSOM tools are any products and services that help to **monitor** an IT landscape and all services therein and to **detect any abnormal behavior**. They also include any products that improve **control** over the **IT infrastructure** (asset management, change management, and configuration management), over **processes** (job scheduling and workflow management), and over **service workflows** (service and support desk, service-level management, and business service management).

SAP Solution Manager is SAP's well-recognized offering for ITSOM. With respect to security, it is accompanied by a set of services offered in the SAP Service and Support portfolio, which are often based on or controlled by SAP Solution Manager. In the following discussion, the tasks of the secure operations map in **Figure 3** are mapped to the capabilities of SAP Solution Manager.



Setting up secure systems, system interactions, and thus system landscapes is the first step in subsequently operating a secure environment.





THE ROLE OF SAP SOLUTION MANAGER

As shown in **Figure 4**, SAP Solution Manager plays a central role in managing the system landscape. In addition to many other tasks, SAP Solution Manager is involved in the installation, update, and management of all systems of a local system landscape. Operating under the guiding principle of a single source of truth, SAP Solution Manager stores information about the system landscape and software versions. It also connects to the SAP Service Marketplace extranet to retrieve patches, support packages, and security updates. Furthermore, SAP Solution Manager monitors the systems on various levels – such as the operating system level (such as for CPU load, memory consumption, or disk allocation), the platform level (such as for health of work processes on application servers), and the application level.

To fulfill these tasks, SAP Solution Manager uses so-called agents (shown as dark rectangles in the diagram) that provide management access to the machines and the applications running on them and forward event notifications. Using this mechanism, SAP Solution Manager can also send notifications on security-related exceptions that are detected in the system landscape and help to fix problems where they occur.

SECURE CODE

At the beginning of software system security is secure code. At the very beginning, this means the code as it has been shipped by SAP and is installed on multiple machines in the system

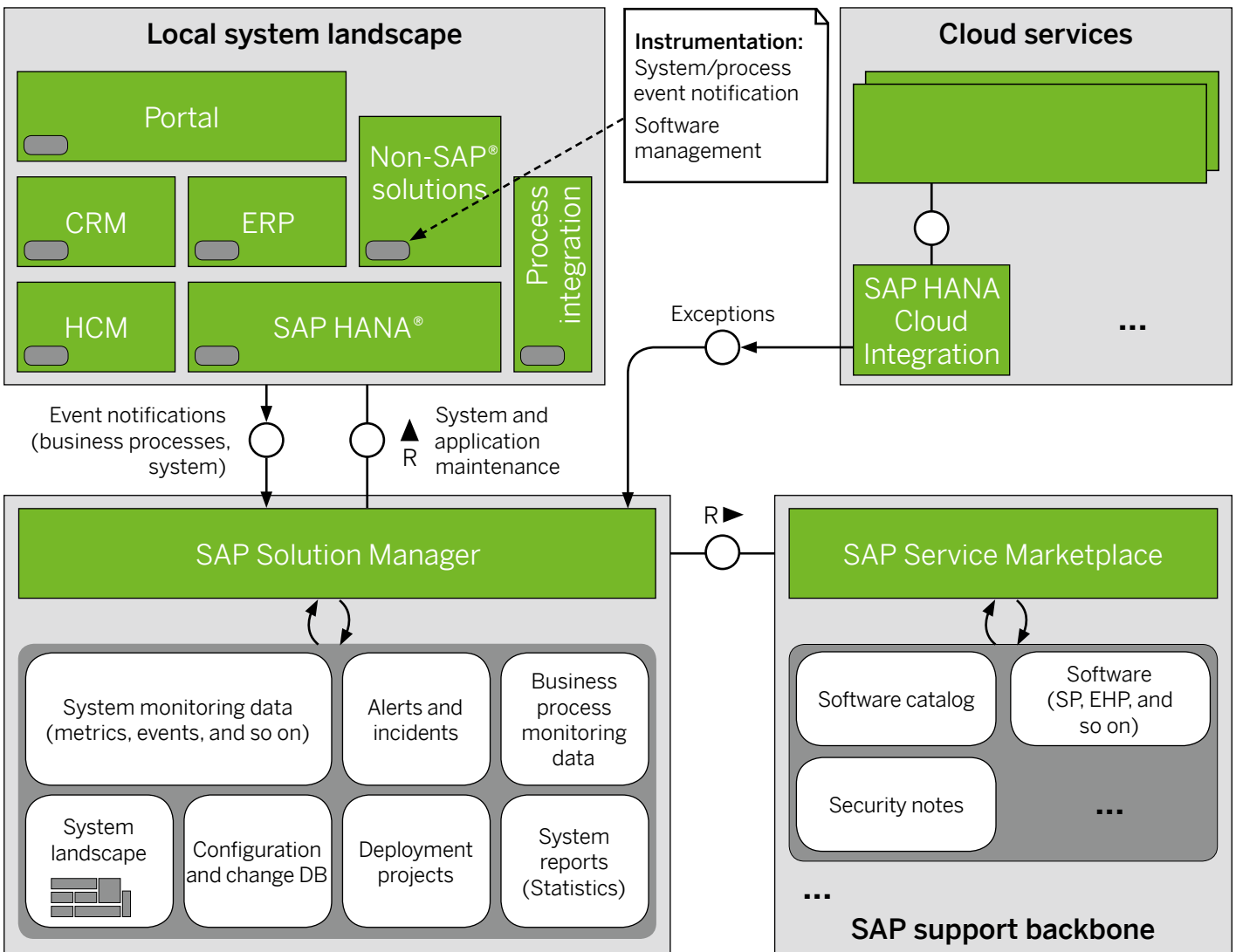
landscape during setup. During the course of continuous change and operations, the security of the installed code will need to be optimized and fixed. A strong knowledge of the landscape is required to manage software versions and keep them in sync.


Security Maintenance of SAP Code

The **system recommendations** functionality in SAP Solution Manager determines which SAP Notes from the SAP Notes tool are valid for systems in a landscape and is thus crucial to keeping systems secure. SAP Solution Manager uses the information about installed components and their release levels for all systems in the landscape and matches them with the available SAP Notes in the SAP Support Portal destination (which is part of SAP Service Marketplace, as shown in **Figure 4**). This matching is actually performed by an algorithm in the SAP support backbone, where SAP Solution Manager sends the information about configurations, release versions, and patch (SAP Note) levels for the systems it manages and receives recommended SAP Notes, including security notes, in return. Because system recommendations can directly integrate with **change request management** through SAP Solution Manager, the change processes to implement the required SAP Notes can immediately be triggered and subsequently logged to keep system security up-to-date at all times – in full compliance to the ITIL standard (see the section “**Security Compliance**”).



Figure 4: Overview of Managed System Landscape for SAP Solution Manager





Also available in system recommendations is information on which objects are touched by recommended SAP Notes. The **business process change analyzer** in SAP Solution Manager can use this information to evaluate the potential impact of SAP Notes on business processes. Data from the usage procedure logging (UPL) framework can be used to assess whether and how often code touched by an SAP Note is in use at all. On that basis, it is possible, for example, to get an assisted analysis of the consequences of implementing an SAP Note.

For planning support package updates, the **maintenance optimizer** is the tool of choice. It calculates which software packages you have to load and analyzes which SAP Notes (including security notes) are needed after a system update.

Custom Code Security

For customers, a straightforward way of extending SAP software without modification is to copy code and modify the copy. The downside is that

copied code will not be subject to security patches. From a security standpoint this creates an inherent risk, because this copied – or cloned – coding often appears to add functionality to the system, when in reality it does not. This is why SAP Solution Manager features the **clone finder** and some other tools for analysis of custom code usage, to identify redundancies in custom code as well as unused code. This superfluous code can then be suggested for deletion.

In addition to SAP Solution Manager, SAP and our partners offer further products and services to help customers check their code. Among these is the **SAP NetWeaver® Application Server component, add-on for code vulnerability analysis**, which covers the ABAP® programming language and helps detect critical code patterns, injection dangers, hard-coded credentials, and so forth. For Java and C++, there is **SAP Fortify software by HP**, which identifies and addresses software security vulnerabilities across the software lifecycle.



From the security perspective, timing is a critical factor, because the elapsed time between when a new threat or vulnerability occurs and when it is fixed defines the likeliness of damage. The ease and speed of fixing security issues is therefore crucial.





SECURE SETUP

Simply having secure code is not sufficient to run a secure system. After deploying software, it is important to set up the system's configuration to be secure right from the beginning. Some security problems have their origin in the setup phase when system parts are deployed but not used (and therefore not checked). Secure setup also includes the definition of security standards for systems against which later changes can be verified (see the section "[Secure Operations](#)").

Secure Configuration

A set of services to help ensure secure configuration during initial system setup is based on information gathered in SAP Solution Manager. The general (not completely security specific) SAP EarlyWatch® Alert service (security-related content described in SAP Note 863362) and the more detailed [security optimization services \(SOS\)](#) compare customer settings (configurations

and critical basis authorizations) with SAP-recommended standards. Based on these checks, a customer-specific security baseline can be derived that also takes into account customer-specific conditions and security regulations. Any changes during operations can subsequently be monitored with the help of [change diagnostics](#) and be compared against this customer-specific security baseline using [configuration validation](#), to help ensure that no unwanted change goes unnoticed (see the section "[Secure Operations](#)").

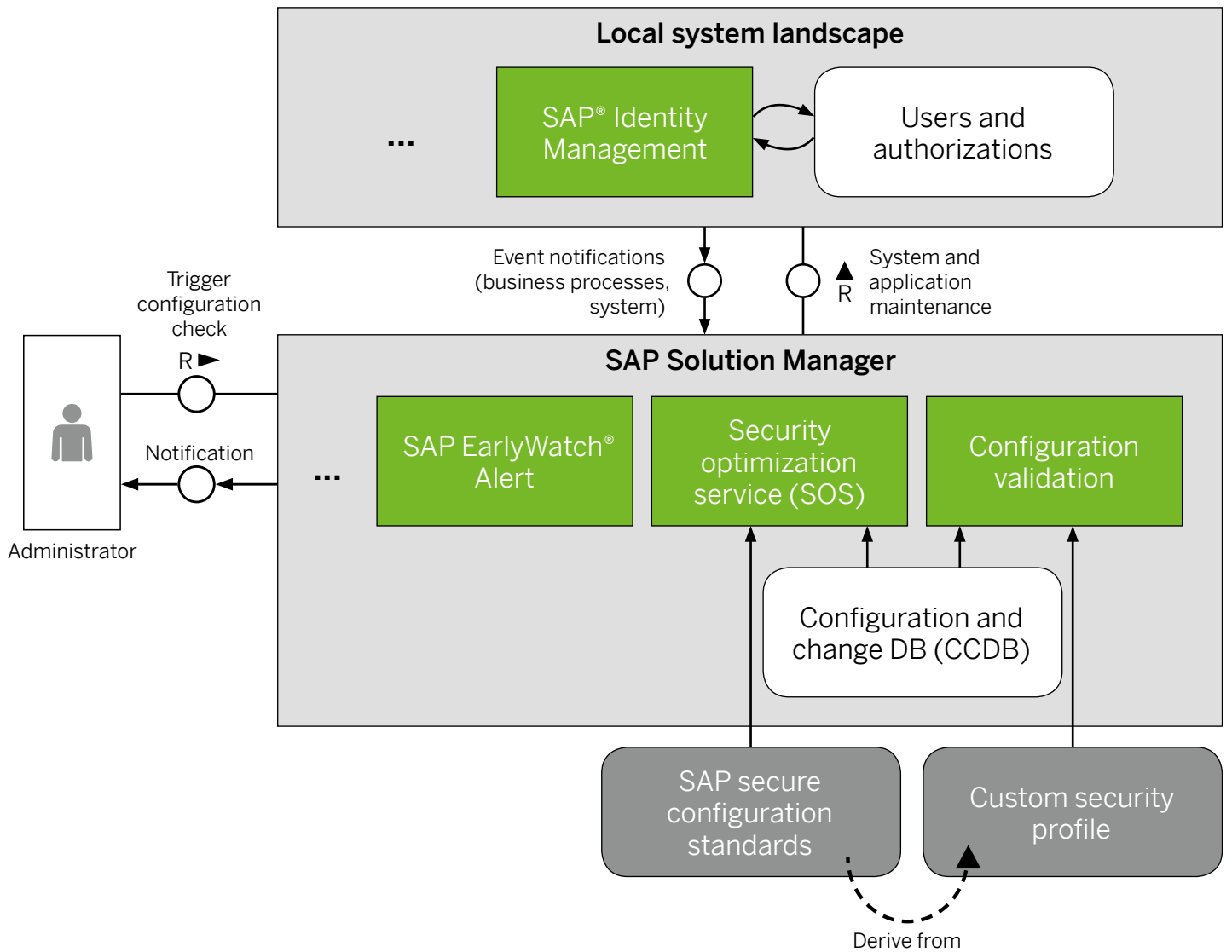
On top of regular monitoring, SAP advises running the complete set of reports from SOS or SAP EarlyWatch Alert periodically to help ensure compliance of the landscape, since not only may systems change, but also the threat landscape around the systems will likely evolve and new recommendations from SAP may come up over time.



Within the customer's operations center, SAP Solution Manager can be operated as a central instance for all monitoring and alerting information.



Figure 5: Checking and Monitoring Secure Configuration





Communication Security

Just as SAP Solution Manager watches over changes and configurations, it watches interfaces as well, and it helps in assessing the proper configurations for network communications with configuration validation in conjunction with SAP support professionals. However, SAP Solution Manager does not play a role in classic network security questions.

SECURE OPERATIONS

Ongoing operations and their security are the main focus of SAP Solution Manager. It assists operators in all of their main task areas. It provides an overview of the system landscape and its status. It also manages and monitors release and patch levels as well as configuration changes from the compliant and secure baseline configuration defined by the compliance activities (see the section “[Security Compliance](#)”) and established during setup (see the section “[Secure Setup](#)”). An overview of its connections to this system and landscape information is shown in [Figure 5](#). In addition, SAP Solution Manager manages problems and incidents and makes recommended actions (or “guided procedures”) for these issues available in a context-sensitive manner. This makes SAP Solution Manager an important security component.

Users and Authorizations, Authentication, and Single Sign-On

User identities are typically managed by the [SAP Identity Management](#) component. However, the configuration validation functionality in SAP Solution Manager can use data in the [configuration and change database](#) (CCDB) to periodically execute queries such as “all users with SAP_ALL access” to monitor and verify compliance with SAP recommendations and corporate policies.

Authentications and single sign-ons are managed by the [SAP Single Sign-On](#) application, not by SAP Solution Manager directly. However, if set up appropriately, SAP Solution Manager can send alerts about any changes made to authentications in the systems under its watch (see [Figure 5](#)).

Support Security

Support security defines the policies for support personnel, secure support connections to customer systems, and support user roles, accounts, and authorizations. SAP Solution Manager can help you enforce these policies with the mechanisms mentioned in the previous section. In light of the increasing demand for ensuring data protection, this policy enforcement adds an additional layer of security and confidentiality to the system landscape.



Security Review and Monitoring

Your strongest focus will most likely be on the ongoing process of reviewing and monitoring security. This is also an area for which SAP Solution Manager is mission critical, as it facilitates the cooperation of the operations control center and the innovation control center on the customer side with the mission control center on the SAP side.² Within the customer's operations control center, SAP Solution Manager can be operated as a central instance for all monitoring and alerting information; and – in an optimal setup – it should have certain cases defined in which incoming alerts directly and automatically trigger the mission control center at SAP. Most of the security-relevant information is in CCDB, which will send alerts in response to any unexpected configuration changes in the landscape. The [SAP Enterprise Threat Detection](#) application can be used to add more alerting capabilities. Periodic checks of the landscape against the configuration validation data will verify in parallel whether systems still comply with the baseline configuration defined and implemented in the setup phase (see the section "[Secure Setup](#)").

This feature of SAP Solution Manager helps keep a high security level during productive system operations. With continuous monitoring, a single indication can reveal a potential intrusion, giving an administrator the chance to activate countermeasures.

2. See also [Control Center Approach](#).

SECURITY COMPLIANCE

Security compliance is basically the conceptual or theoretical discipline in security. The term summarizes the activities around high-level definitions of security standards for on-premise and cloud environments, their adaptation from SAP policies to customer-specific policies, the auditing processes that inspect the compliance to these standards, and the high-level concepts for incidents and emergencies. Any ITSOM tool will play only a minor role in this area, because no hands-on system tasks are involved.

Security Governance

SAP Solution Manager helps to organize the storage and context-sensitive access to documents concerning recommended actions for security and other operations incidents. However, it will usually have no part in administering the high-level policies that form the basis of an organization's security governance.

Audit

SAP Solution Manager is certified to comply with a number of standards, such as ITIL. Thus, it is one of the main sources for landscape information that is relevant in the auditing process, and it is the source for monitoring information and configuration details relevant in auditing processes (see the sections "[Secure Setup](#)" and "[Secure Code](#)"). It may also itself be subject to auditing.

Cloud Security

This paper will not explicitly differentiate between on-premise and cloud security, because in an ideal world cloud and on-premise environments should be controlled by the same management platform and the same ITSOM tool.





Emergency Concept

This point on the secure operations map summarizes the definition of processes, responsibilities, roles, and countermeasures in the case of incidents. Some of these are enforced with the help of SAP Solution Manager. It does not, however, play a part in this definition phase.

SECURE SAP SOLUTION MANAGER SETUP AND OPERATION

SAP Solution Manager plays a central role in your system landscape. It is connected to all systems with administrative access to control deployment and operation. This also makes SAP Solution Manager a potential target for cyberattacks. SAP Solution Manager must be secured following the [SAP Security Guides](#) (login required).

In a nutshell, you should consider SAP Solution Manager as a **productive system**, just like your productive system for finance or human capital management, and should set it up and operate it accordingly. This includes:

- An authorization concept for SAP Solution Manager
- A security concept for communication around SAP Solution Manager (see [Figure 5](#))

Further information about a secure setup of SAP Solution Manager is available in the [Security Guide for SAP Solution Manager](#) (login required) and in the wiki on SAP Community Network: [SAP Solution Manager – Security and Authorizations](#).

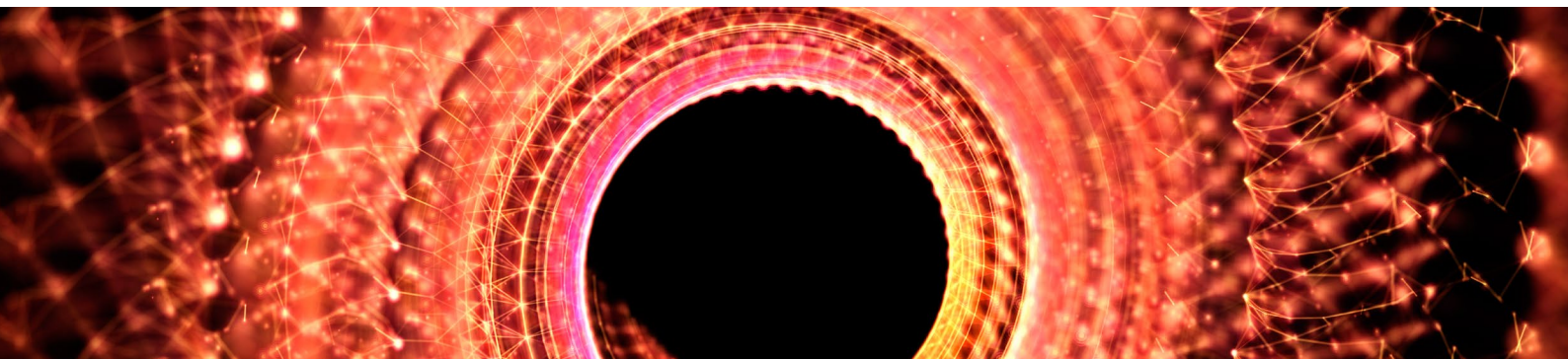


The central position of SAP Solution Manager makes it the tool of choice to define, implement, and sustain a secure system landscape.

Conclusion: The Center of a Secure System Landscape

At the center of managing a highly complex system landscape, SAP Solution Manager performs a large number of different tasks and activities. Here, all information comes together. The central position of SAP Solution Manager makes it the tool of choice to define, implement, and sustain a secure system landscape.

Securing system landscapes is just one role played by SAP Solution Manager. Overall, it is recognized by industry analysts as a powerful (and fully ITIL-certified) ITSOM tool. You will benefit by becoming better acquainted with the full range of possibilities that it offers.



Additional Information and References

Some of the following materials have been intensively used as sources for this document and are also linked from within the above sections, while others are simply interesting to read and are not explicitly used or quoted in the document.

- [**SAP Solution Manager**](#) (book: Marc O. Schäfer and Matthias Melich, SAP Press, 2012)
- [**SAP Security Optimization Services**](#) (SAP Support Portal)
- [**Secure Operations Map**](#)
- [**Maintenance Optimizer**](#) (SAP Community Network)
- [**SAP Solution Manager documentation**](#) (SAP Help Portal)
- [**Configuration and Change Database**](#) (SAP Help Portal site)
- [**Configuration Validation**](#) (SAP Help Portal)
- [**System Recommendations**](#) (SAP Help Portal)
- [**SAP Single Sign-On**](#) (SAP Help Portal)
- [**SAP Solution Manager, the ITIL-Aligned IT Management Tool**](#) (SAP Community Network)
- [**Managing Changes with Change Request Management**](#) (SAP white paper, 2011)
- [**SAP CIO Guide – IT Security in Cloud and Mobile Environments**](#) (PDF, SAP, 2013)
- [**The Dawning of the New Age: Research in Action Vendor Selection Matrix – IT Operations and Service Management for SAP-Centric Environments**](#) (PDF, Research in Action, 2014)
- [**“Mit der Solution Manager Suite findet SAP Anschluss an BMC”**](#) (in German; Computerwoche, January 12, 2015)
- [**Security Management and Operations**](#) (Microsoft Corporation)
- SAP Solution Manager Security Guide (login required): [**SAP Solution Manager Installation & Upgrade Guides**](#) → [**SAP Components**](#) → [**SAP Solution Manager**](#) → [**<Release>**](#) → [**Operations**](#) → [**Security Guide SAP Solution Manager <Release>**](#) (SAP Service Marketplace)
- [**SAP Solution Manager – Security and Authorizations Wiki**](#)

This document provides guidance on how to centrally manage security in an SAP landscape. It contains current and intended strategies, developments, and/or functionalities of SAP® solutions, applications, and technologies and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development; its content is subject to change without notice.



© 2015 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices. 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 SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE 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 platform 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, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.



The Best-Run Businesses Run SAP®

