



SAP Security Webcast Series (February 16th, 2023): Introduction into the SAP Security Optimization Services Portfolio

Fritz Bauspiess, SAP

Public



Agenda

▪ Introduction

- Why Security Services
- The Secure Operations Map
- Security Services for SAP Cloud Solutions

▪ Information

- Our Security Optimization Services Landing Page
- The Security Notes Webinar
- Additional interesting information sources on SAP Security

▪ Content & Services

- The EarlyWatch Alert Workspace
- Security Optimization (Self) Service
- System Recommendations
- The Security Baseline Template Package
- Security Value Map

▪ Premium Engagement (MaxAttention, ActiveAttention, ValueAssurance)

- Security Engagement
- Deep Dive Components

Agenda

■ Introduction

- Why Security Services
- The Secure Operations Map
- Security Services for SAP Cloud Solutions

■ Information

- Our Security Optimization Services Landing Page
- The Security Notes Webinar
- Additional interesting information sources on SAP Security

■ Content & Services

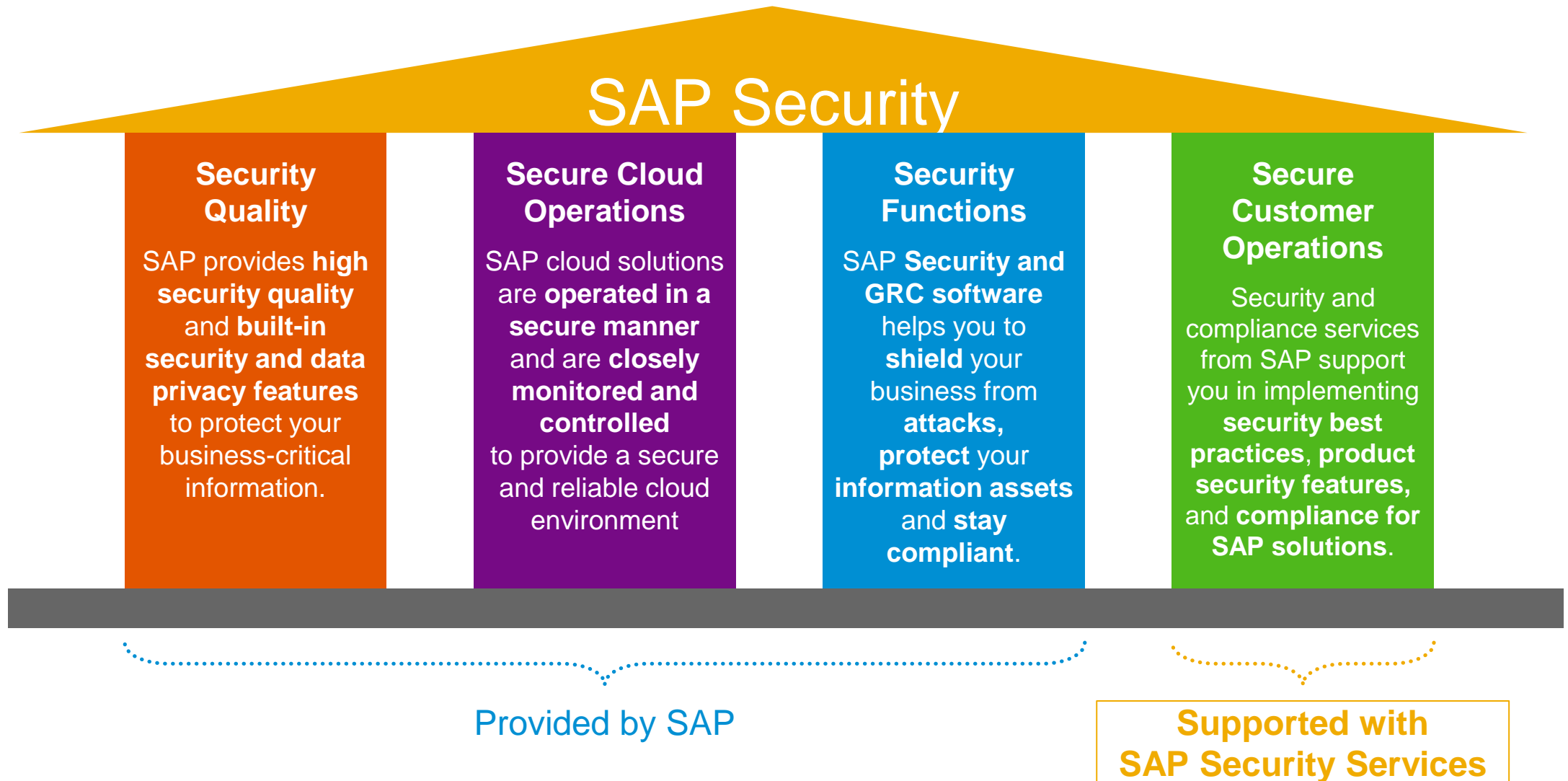
- The EarlyWatch Alert Workspace
- Security Optimization (Self) Service
- System Recommendations
- The Security Baseline Template Package
- Security Value Map

■ Premium Engagement (MaxAttention, ActiveAttention, ValueAssurance)

- Security Engagement
- Deep Dive Components

Why Security Services?

The Pillars of SAP Landscape Security



The Secure Operations Map

Organization

Awareness

Security Governance

Risk Management

Process

Regulatory Process
Compliance

Data Privacy &
Protection

Audit &
Fraud Management

Application

User & Identity
Management

Authentication
& Single Sign-On

Roles &
Authorizations

Custom Code
Security

System

Security Hardening

Secure SAP Code

Security Monitoring
& Forensics

Environment

Network Security

Operating System
& Database Security

Client Security

Secure Operations Map - Fundamentals

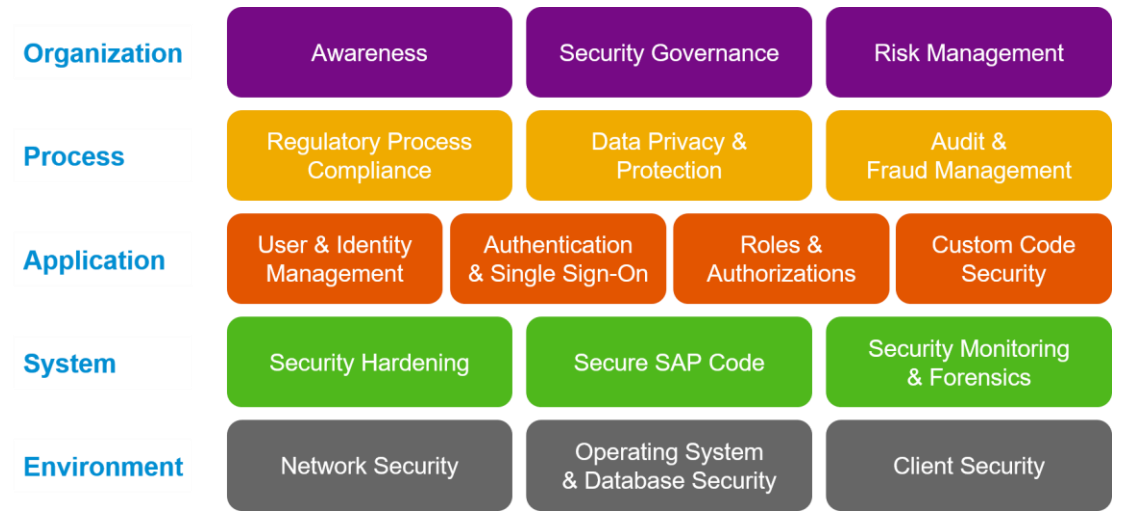
The Secure Operations Map

- is a **Reference Model**
 - to structure the broad area of security for content, discussions and as a basis for a 360° view on security
 - i.e. you can't "order" a block, but you can allocate discussions, needs and solutions to specific security areas
- focuses on the **Operational Aspects** of security
 - i.e. on the tasks and considerations which a customer or service provider has to take into account to maintain and operate their systems and landscapes in a secure manner.
- is further interpreted in the concrete **Context of SAP**, although the model also could be applied to non-SAP realms.

How to use the Secure Operations Map

Be aware:

- **Security** is not a property which you have or don't have. It is a **risk measure**, where you can have a higher or lower level of Security
- Maximum Security is often not what you want, since this requires high effort and may limit functionality. You require **adequate security**:
 - Baseline measures / Security best practices should always be applied.
 - For systems with security needs beyond such baseline measures, a risk analysis is required to derive corresponding suitable additional security measures.
- **Security** often is **invisible**. The fact, that you don't notice security weaknesses or successful attacks, does not mean that there are not any.
- **Security** does not only **protect against malicious attacks** but also **against unintended failures**.



Security for (SAP) Cloud Solutions

- In general, security increases when moving to the cloud
 - Reason:
 - For most customers, security is not part of their core business.
 - For cloud solution providers like SAP it is!
- The overall responsibility for security remains with the customer as it is linked to their business
 - For those parts handed to the cloud solution provider, customers should verify that the cloud solution provider fulfills their security and compliance needs.
 - For SAP, the [SAP Trust Center](#) provides a lot of information on this matter.
 - Some security tasks will remain in the customers' responsibility, depending on the type of cloud solution (Infrastructure-as-a-Service [IaaS], Platform-as-a Service [PaaS], Software-as-a-Service [SaaS])

Security for Cloud Customers

In cloud solutions, many administrative tasks are taken over by the cloud provider. This includes taking care of security protection and secure operation of the cloud solution.

Nevertheless, certain security-relevant topics remain in the responsibility of the customer as they relate to customer-specific decisions and tasks. Without the customer's contribution, the overall solution will not be secure.

Examples for such security tasks in responsibility of the customer are

- **User lifecycle** including processes for creation of users, adaption to changed needs during lifetime and decommissioning.
- Assignment of proper **authorizations** to internal users, external partners, power user and administrators.
- Proper **authentication** of users.
 - Control of those components which verify the true identity of users ("Identity Providers").
 - Control of authentication methods (passwords, chipcards, authentication via mobile devices, two-factor authentication).
- **Connectivity** between systems and components in the landscape.
 - Definition and enforcement of who may communicate with whom.
 - Verification / Authentication of communication partners to prohibit malicious impersonation by attackers.
- **Audit readiness**
 - Definition, evaluation and archiving of security-relevant logs.
 - Definition, enforcement and control of a security policy to not only "get secure" but also "stay secure" over time.
- **Security of the software**
 - Security of custom-developed code – e.g. custom-developed extensions.
 - Security maintenance of standard code. At least the responsibility for triggering such updates may reside with the customer.

Agenda

■ Introduction

- Why Security Services
- The Secure Operations Map
- Security Services for SAP Cloud Solutions

■ Information

- Our Security Optimization Services Landing Page
- The Security Notes Webinar
- Additional interesting information sources on SAP Security

■ Content & Services

- The EarlyWatch Alert Workspace
- Security Optimization (Self) Service
- System Recommendations
- The Security Baseline Template Package
- Security Value Map

■ Premium Engagement (MaxAttention, ActiveAttention, ValueAssurance)

- Security Engagement
- Deep Dive Components

Our “SAP Security Optimization Services Portfolio” Landing Page

<https://support.sap.com/sos>

The screenshot shows a web browser window displaying the SAP Support portal. The address bar shows the URL: support.sap.com/en/offerings-programs/support-services/security-optimization-services-portfolio.html. The page header includes the SAP logo and 'Support' text, followed by navigation links: My Support, Products, Tools, Maintenance, Offerings & Programs, ALM, and Explore SAP. Below the header, there is a breadcrumb trail: SAP Support Portal Home / Offerings & Programs / Support Services. The main heading is 'SAP Security Optimization Services Portfolio'. A sub-heading reads: 'SAP Security Optimization Service Portfolio ensures smooth operation of your SAP solution by taking action proactively, before severe security problems occur.' Below this, a section titled 'Best Practices' contains a paragraph: 'Keeping the security and availability of your SAP solution high is a tremendous value to your business. Analysis will:' followed by a list of four bullet points: decrease the risk of a system intrusion, ensure the confidentiality of your business data, ensure the authenticity of your users, and substantially reduce the risk of costly downtime due to wrong user interaction. To the right of this list is a blue 'Contact Us' button. Below the 'Best Practices' section, there are four columns of links and descriptions: 'Security Overview' (interested in general SAP Security Optimization Services and want an overview), 'Security Topics Area' (entry point into different topic areas such as Security Patch Management or Security Configuration Analysis), 'Security Services, Tools and Information' (overview and links to further information on service offerings, including information and best practices, tools and self-services, remote and on-site service offerings, and more systematic engagement models), and 'Advisories' (SAP Security Notes Advisory (January 2023), Security Notes Webinar (pdf) or https://wiki.scn.sap.com/wiki/x/MIOeJQ (January 2023), and How to register).

The Security Notes Webinar

- The Security Notes Webinar is offered to customers on a monthly basis, typically in the week after the SAP Security Patch Day
- In it, guidance is given on critical SAP Security Notes of the past month. In addition, also general SAP security topics relevant for customers are discussed.
- The Security Notes Webinar is offered
 - in collaboration with ASUG (suitable for the Americas and EMEA time zone, held in English)
 - in collaboration with DSAG, (suitable for the EMEA time zone, held in German)
 - via the SAP Enterprise Support Value Map for Security / Enterprise Support Academy, (suitable for the EMEA and APJ time zone, held in English)
 - in addition, a new series was started for China, held in Chinese
- Information on how to participate as well as the content of the past Security Notes Webinars is available
 - [here](#) on the [SAP Security Optimization Services Portfolio landing page](#)
 - [here](#) on the [Support Wiki](#)

Additional interesting information sources on SAP Security (random incomplete personal selection 😊)

- [SAP Trust Center](#)
 - Including dedicated information on [Security](#), [Compliance](#) and [Privacy](#) by SAP
- [Security Notes Support Portal Page](#)
 - Including
 - Access to the complete list of SAP Security Notes
 - Information on the SAP Security Patch Day as well as the Security Maintenance Strategy
 - Links to further resources related to the subject
- [Recommended Security Configuration for SAP Cloud Services](#)
 - in [My Trust Center - Tools & Documentation](#)
with the option to subscribe for updates

Agenda

■ Introduction

- Why Security Services
- The Secure Operations Map
- Security Services for SAP Cloud Solutions

■ Information

- Our Security Optimization Services Landing Page
- The Security Notes Webinar
- Additional interesting information sources on SAP Security

■ Content & Services

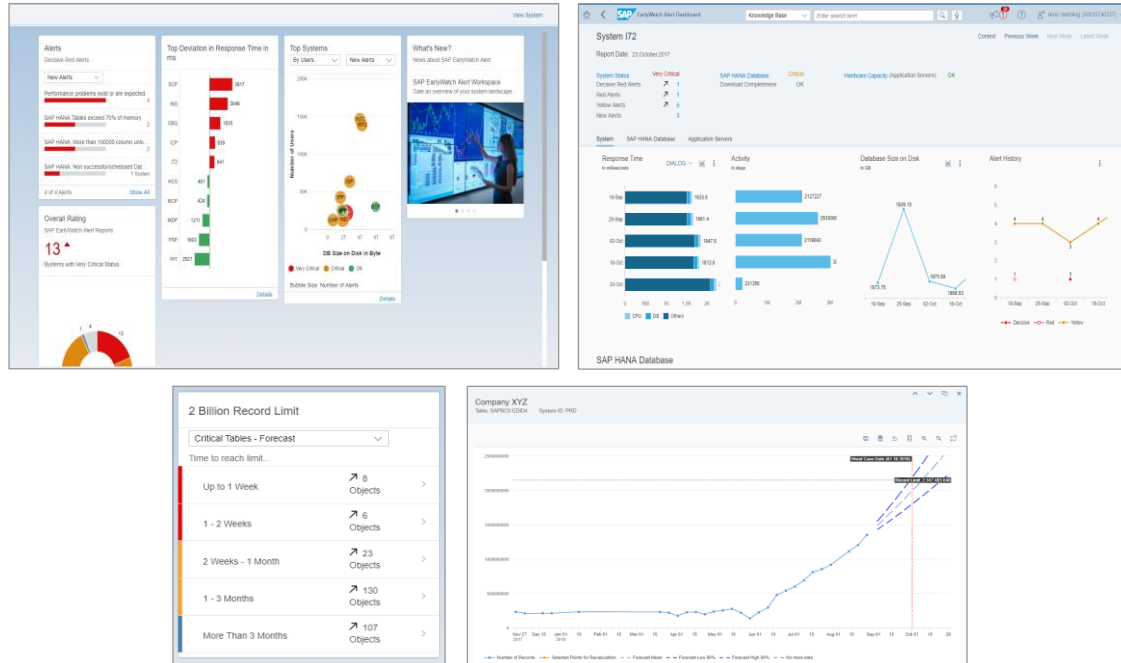
- The EarlyWatch Alert Workspace
- Security Optimization (Self) Service
- System Recommendations
- The Security Baseline Template Package
- Security Value Map

■ Premium Engagement (MaxAttention, ActiveAttention, ValueAssurance)

- Security Engagement
- Deep Dive Components

SAP EarlyWatch Alert Workspace

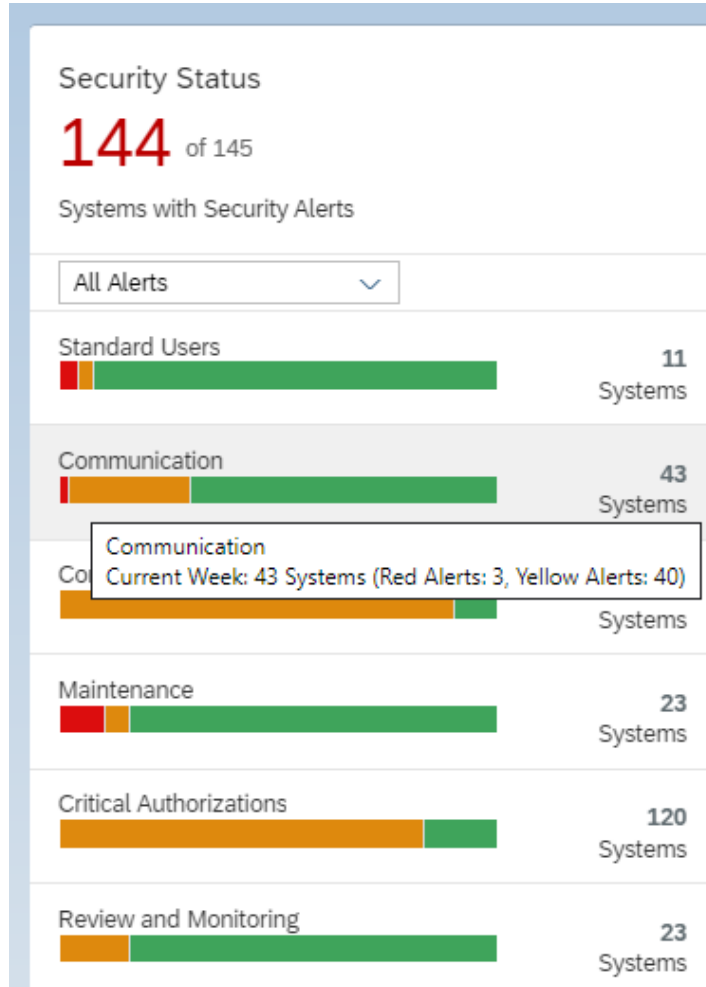
Get empowered to speak the same language across teams



- One common view for all users
- Built for **simplicity** with Design Thinking
- One database with **years of history** of data
- One service engine using rules, predictions, and **Machine Learning**
- Transparency **at all times** for business continuity

Work with proven standards at any place and under all conditions.

SAP EarlyWatch Alert Workspace Security Card – Sample Content



How many systems are vulnerable or even “RED”

- Standard users including SAP* or DDIC have default passwords
- HANA user SYSTEM is active and valid
- RFC Gateway and Message Server security – Doors wide open
- HANA Internal or System Replication Communication is not secured
- Weak Password Policy
- HANA: SQL Trace configured to display actual data
- Systems having outdated Software no longer supported with SAP Security Notes
- Users having critical basis authorizations like SAP_ALL, Debug/Replace, Change all tables,...
- HANA users having critical authorizations like DATA ADMIN privilege
- Audit Log is not active or written to an unsecure audit trail target

Available at <https://launchpad.support.sap.com/#ewaworkspace>

S-User Authorization required: “Display Security Alerts in SAP EarlyWatch Alert Workspace”

Access to the SAP EarlyWatch Alert Workspace

- Access is available to all customers in the context of their maintenance contract.
- Special S-User authorizations is required to view the SAP EarlyWatch Alert Security Card
 - See blog “Displaying Security Alerts in the SAP EarlyWatch Alert Workspace” (<https://blogs.sap.com/2019/10/01/displaying-security-alerts-in-the-sap-earlywatch-alert-workspace/>)
 - In detail, you need the following authorizations:
 - Authorization “**Service Reports and Feedback**” (section Reports) to view SAP EarlyWatch Alert reports and apps.
 - Authorization “**Display Security Alerts in SAP EarlyWatch Alert Workspace**” (section Reports) to use the alert category “Security” in the application SAP EarlyWatch Alert Solution Finder and to access the card “Security Status”.
 - To verify whether you have access, open the EWA Workspace and check whether you can see the “Security Status” card. (<https://launchpad.support.sap.com/#/ewaworkspace>)
 - If you don’t see it, ask your S-User Super Admin to grant the above authorizations to you.

The SAP Security Optimization Service

- The SAP Security Optimization Service (SOS) is designed to analyze, verify, and improve the security of your SAP system by identifying potential security risks and providing recommendations to mitigate these risks within the analyzed systems. There are many different SAP systems that can be analyzed with an SOS
 - SAP NetWeaver Application Server – ABAP
 - SAP NetWeaver Application Server – JAVA
 - SAP S/4HANA on-premise and private cloud
 - SAP HANA on-premise and private cloud
 - SAP Business Technology Platform
- For details and examples see
 - Our landing page <https://support.sap.com/sos> → examples in the “Media Library” at the bottom of the page
 - Blog “[New Security Optimization Service Continuous Quality Check for SAP Business Technology Platform \(CQC SOS for BTP\)](#)”
- In addition, the SOS is also available in pilot delivery for
 - IBP (Integrated Business Planning)
 - IAS (Identity Authentication Service)
 - SAP S/4HANA public cloud

System Recommendations – see <https://support.sap.com/sysrec>

SAP Support Portal Home / Application Lifecycle Management / SAP Solution Manager / Processes for 7.2

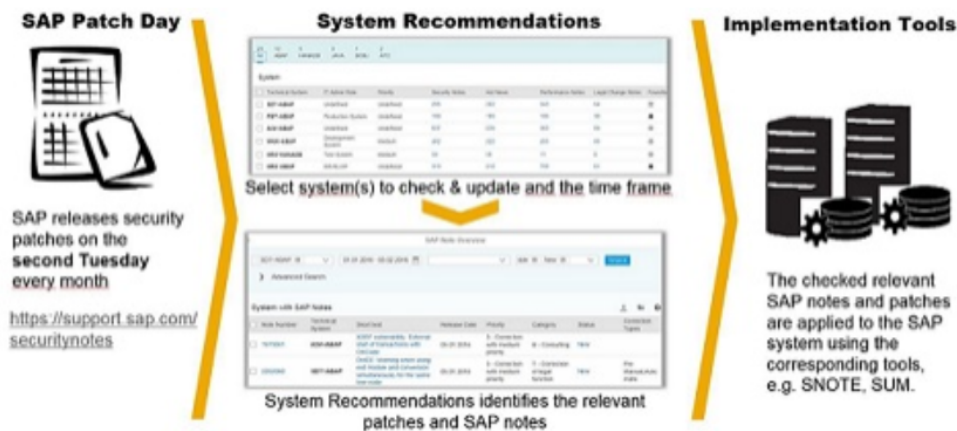
System Recommendations

Overview Resources

System Recommendations

Tailored Automated Recommendations for SAP Notes

System Recommendations provides a detailed recommendation of ABAP and non-ABAP SAP Notes which should be implemented, based on the actual status of the system and already implemented SAP Notes.



Important SAP Notes

- ✓ Note [3058231](#) - SysRec: Job downloads notes only once a day
- ✓ KBA [3105490](#) - Recommendation of job frequency of Job SM:SYSTEM RECOMMENDATIONS
- ✓ Note [3134903](#) - SysRec 7.2: Enhance system authorization check in Note Overview Page
- ✓ Note [3191942](#) - SysRec: Updated flag of note is back after clicking the Refresh button
- ✓ Note [3196680](#) - The release of kernel component is missing in configuration validation report

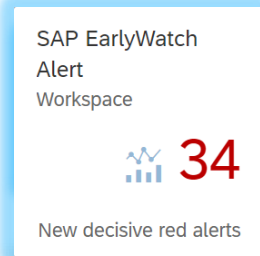
The role of the Security Baseline Template

Template for a “Company’s SAP Security Baseline”

Comparison against SAP recommendations

Security in EarlyWatch Alert (EWA)

Overview



Security Optimization Service System Recommendations

Detail

System	IT Admin Role	System Priority	Security Notes	Hot News	Performance Notes	Legal Change Notes	License Audit Notes
069VY-00-ATC	Quality Assurance System	Undefined	12	98	278	522	20
384-WAS-ATC	Undefined	Undefined	32	113	303	846	15
891-WAS-ATC	Undefined	Undefined	36	113	326	862	21
A24-ABAP	Undefined	Undefined	15	101	406	804	5
A7S-JAVA	Undefined	Undefined	76	104	272	526	19
ABZ-JAVA	Undefined	Undefined	83	108	274	527	17

Company's Security Policy

Company's SAP Security Baseline

Target System

Comparison against company's security policy

Management Dashboard



Configuration Validation

ID	Name	Category	Type	Inst.	Component Ver.	Licensekey ID
027	ABAPSYS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
028	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
029	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
030	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
031	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
032	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
033	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
034	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
035	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
036	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
037	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
038	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
039	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
040	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
041	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
042	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
043	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
044	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
045	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
046	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
047	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
048	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
049	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...
050	ASCS	ABAP	COMP	Inst.	6.20.00010000	SAP-JAVA-MS...

SAP Solution Manager

SAP Focused Run

The SAP Security Baseline Template Package

- Explained and referenced via SAP Note [2253549](#) “The SAP Security Baseline Template”
(This note can also be used to get alerted on new versions)
- Consisting of
 - The SAP Security Baseline Template in MS Word format to serve as an easy starting point for a customer-specific SAP Security Policy
 - Prepared modules for automated checking of landscapes via the “Configuration Validation” functionality in SAP Solution Manager
 - Prepared policies for automated checking of landscapes via SAP Focused Run

SAP Security Baseline Template

TABLE OF CONTENTS

1	Overview, Requirements and Guidelines	9
1.1	Purpose of this template	9
1.2	Structure	9
2	Regulations	11
2.1	Environment	12
2.1.1	Network Security	12
2.1.2	Operating System and Database Security	12
2.1.3	Client Security	12
2.2	System	12
2.2.1	Security Hardening.....	12
2.2.1.1	<i>CHANGE: Protect Production System against changes</i>	12
2.2.1.1.1	CHANGE-A: Protect Production System against changes – ABAP	12
2.2.1.2	<i>DISCL: Information Disclosure</i>	13
2.2.1.2.1	DISCL-A: Information Disclosure – ABAP	13
2.2.1.2.2	DISCL-J: Information Disclosure – Java	13
2.2.1.2.3	DISCL-O: Information Disclosure – Web Dispatcher.....	13

The Security Value Map in SAP Enterprise Support

See blog [“Get more from our reimagined SAP Enterprise Support value map for Security”](#)

Security Value Map - SAP Enterprise Support ☆ Public
548 Members

This value map guides you through the different sources of information, tools and services available from SAP Enterprise Support to help you to efficiently build and run your SAP systems. We are utilizing the SAP Secure Operations Map as a foundation to share our content:

Overview

Security Overview

Overview Content
Feed Updates Forums
Members Events
Trash

Learning Programs What's New Events Ask Questions About Us

SAP Enterprise Support Security Value Map

Organization

- Awareness
- Security Governance
- Risk Management

Process

- Regulatory Process Compliance
- Data Privacy & Compliance
- Audit & Fraud Management
- User & Identity
- Authentication & Authorization
- Roles & Permissions
- Custom Code

Welcome to the SAP Enterprise Support Security Value Map

This value map guides you through the different sources of information, tools and services available from SAP Enterprise Support to help you to efficiently build and run your SAP systems. We are utilizing the SAP Secure Operations Map as a foundation to share our content:

Agenda

■ Introduction

- Why Security Services
- The Secure Operations Map
- Security Services for SAP Cloud Solutions

■ Information

- Our Security Optimization Services Landing Page
- The Security Notes Webinar
- Additional interesting information sources on SAP Security

■ Content & Services

- The EarlyWatch Alert Workspace
- Security Optimization (Self) Service
- System Recommendations
- The Security Baseline Template Package
- Security Value Map

■ Premium Engagement (MaxAttention, ActiveAttention, ValueAssurance)

- Security Engagement
- Deep Dive Components

Premium Engagement Services: Cybersecurity and Compliance

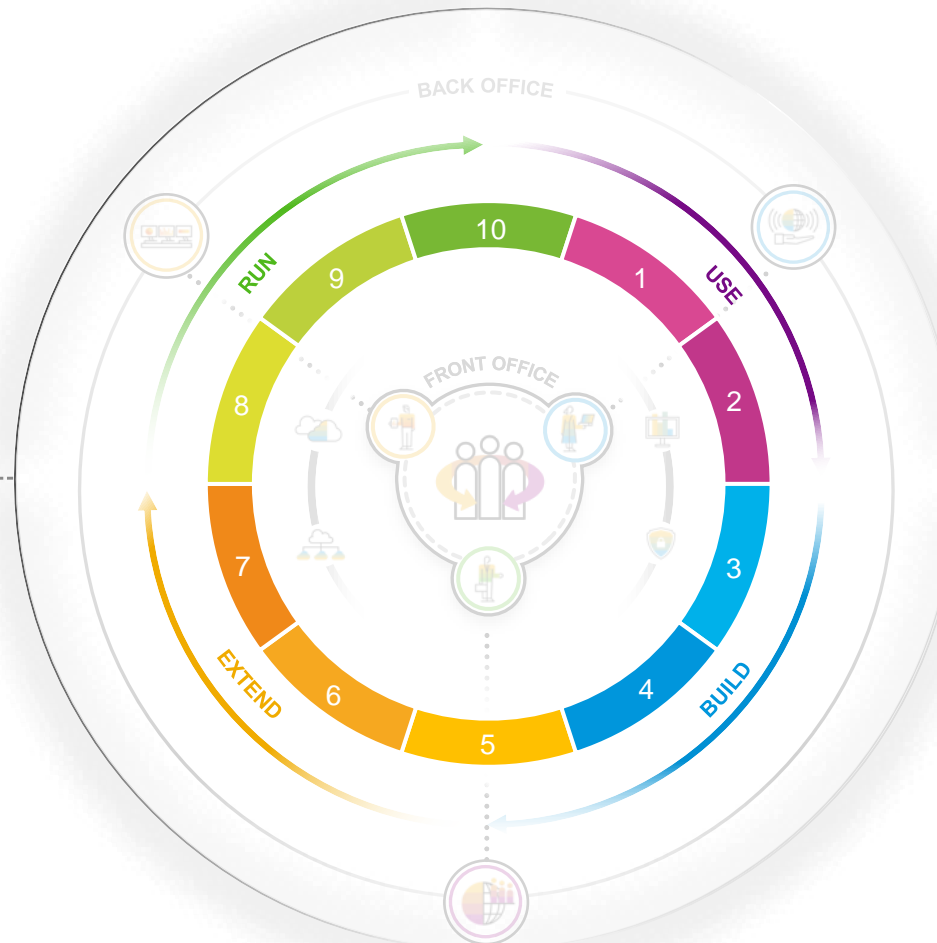
We deliver predictable outcomes through services we adapt to your specific needs. As a result, you will be able to tap into the full potential of your SAP solutions and cloud opportunities and unlock unprecedented value with your operational excellence.

Run Better

- Cybersecurity and Compliance
- Safeguarding
- End-to-end Hybrid Operations
- Accelerated Support

Extend Use

- Co-/Design
- Architecture Planning
- Implementation Support



Use Better

- Co-/Design
- Architecture Planning
- Analytics and Data Management
- Cybersecurity and Compliance
- PaaS and DevOps

Build New

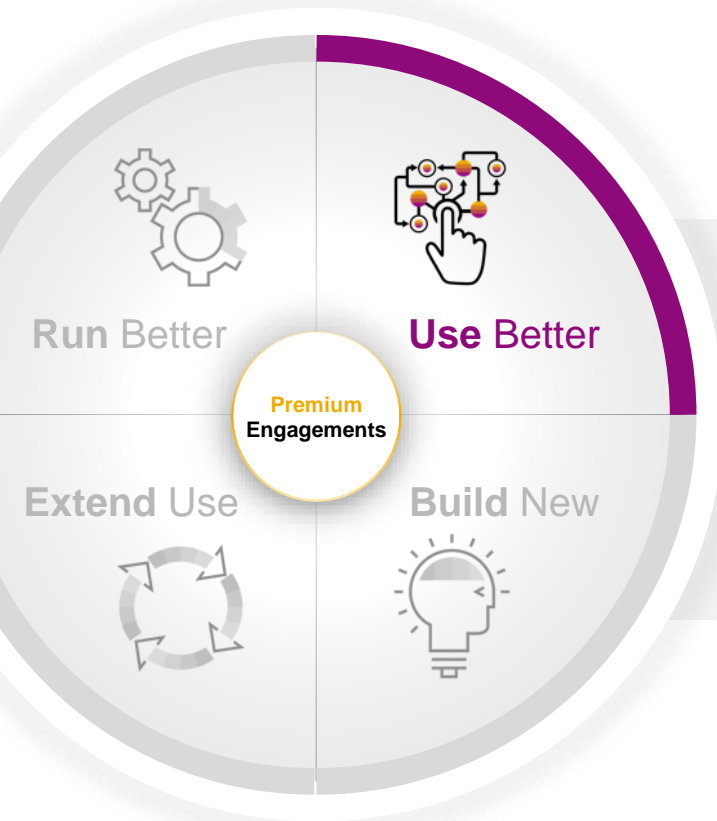
- Innovation Services
- Architecture Planning
- Implementation Support
- PaaS and DevOps

Potential Benefits of the Premium Engagement Services



Focus Topic:

Cybersecurity and Compliance

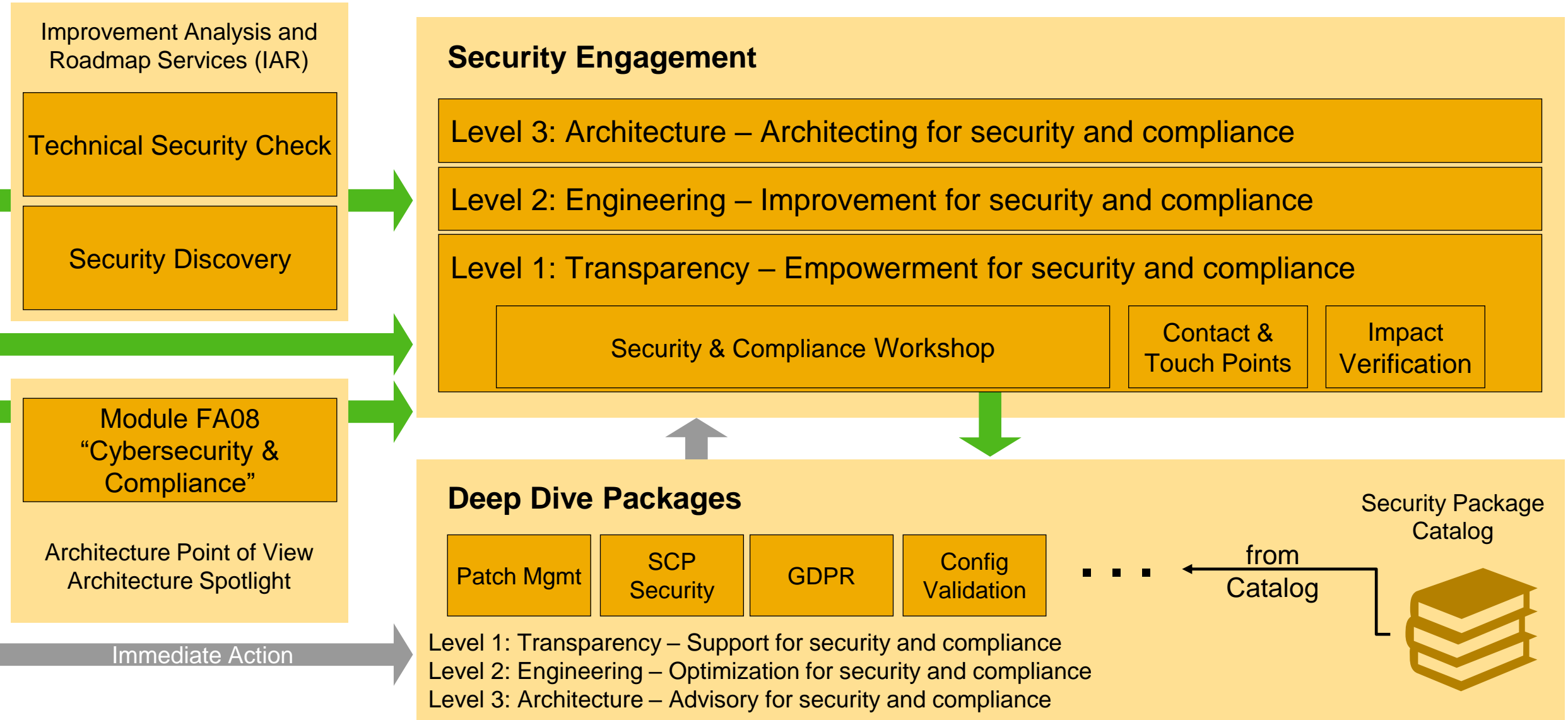


“I want to **increase security levels** and reduced effort for compliance.”

Tool-enabled transparency on missing security measures.
Risk-based mitigation plan for security improvement.
Best practice approach for compliance related procedures and security architecture

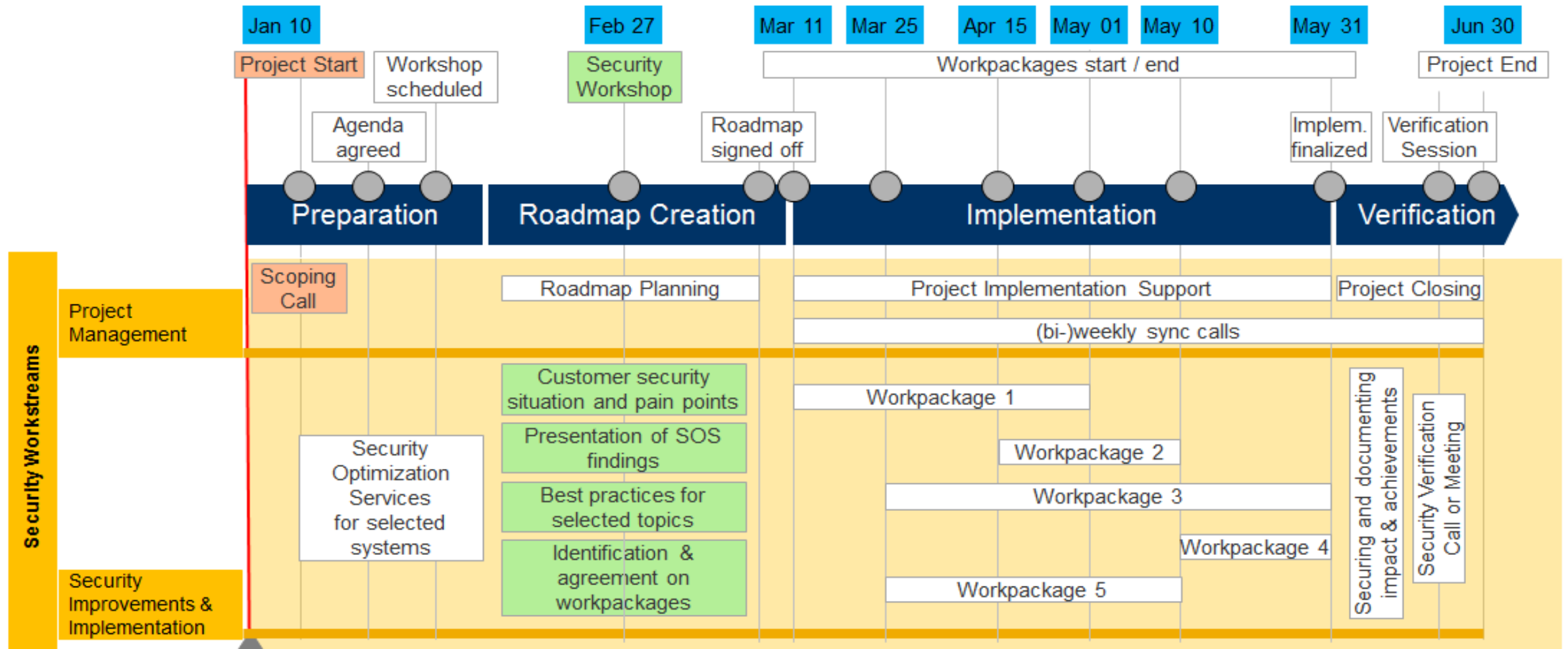
* Benefits assume the team (consisting of customer, partner and SAP) strictly follow the SAP service delivery approach and timeline

Service Flow Cybersecurity & Compliance



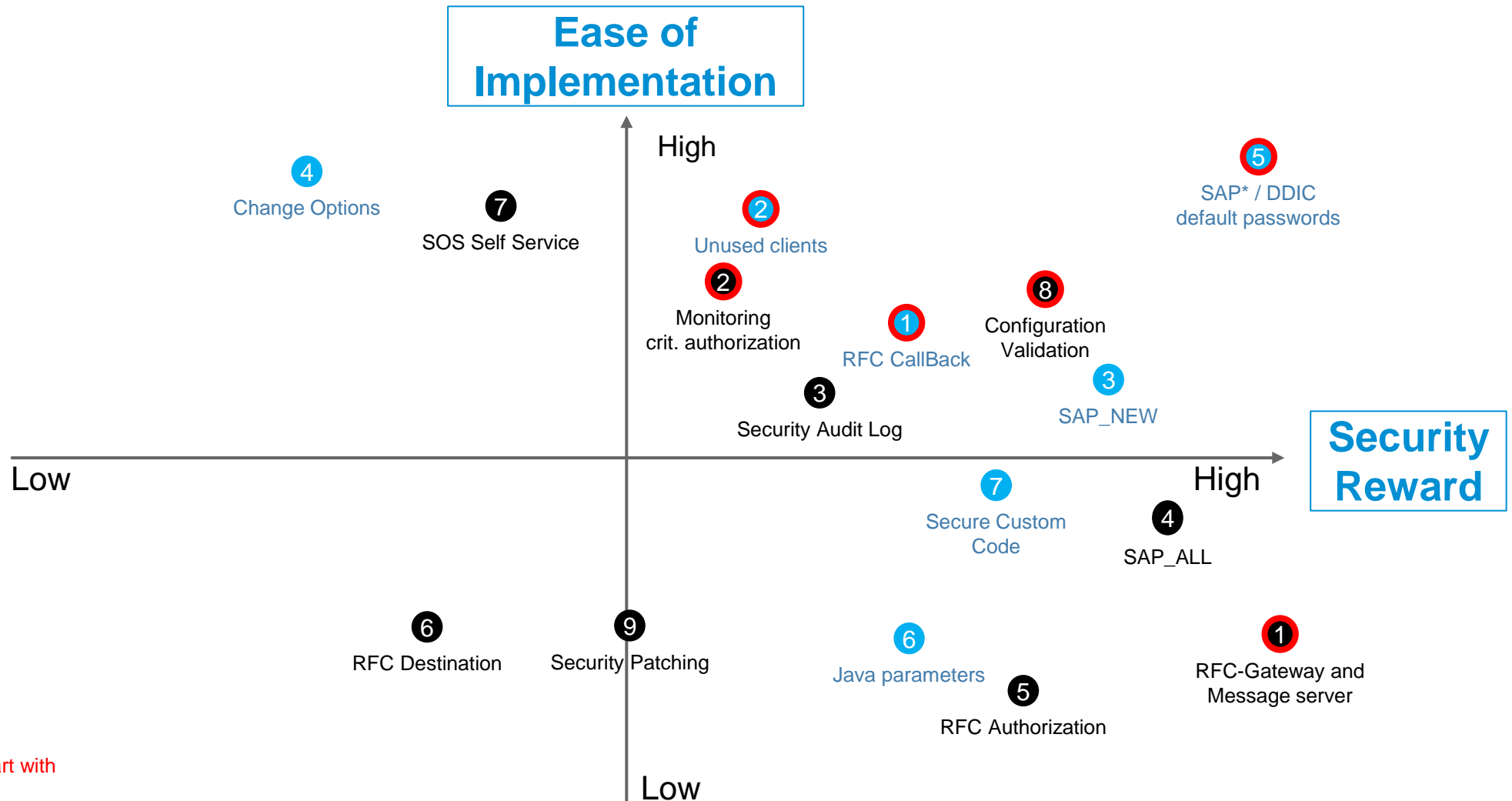
Transparency for security and compliance

Security road map creation as part of SAP MaxAttention engagements



Sample Result

Work Packages and Action Items – Risk Heatmap



- Work Packages
- Action Items
- Top Activities to start with

Thank you.

Contact information:

Fritz Bauspiess
securitycheck@sap.com

