



# Keeping Track of System Security with SAP EarlyWatch Alert Workspace

Fritz Bauspiess  
Data Science, Automation & Technology, IDG, SAP SE

PUBLIC



SAP for Me



**SAP  
ONE  
Support  
Launchpad**

Your Personalized Digital  
Support Experience

**THE BEST RUN**



# Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, 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 presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document 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 presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation 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 presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP's intentional or gross negligence.

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.

# Before diving into the content ...

## This slide deck contains a combination of presentation and documentation

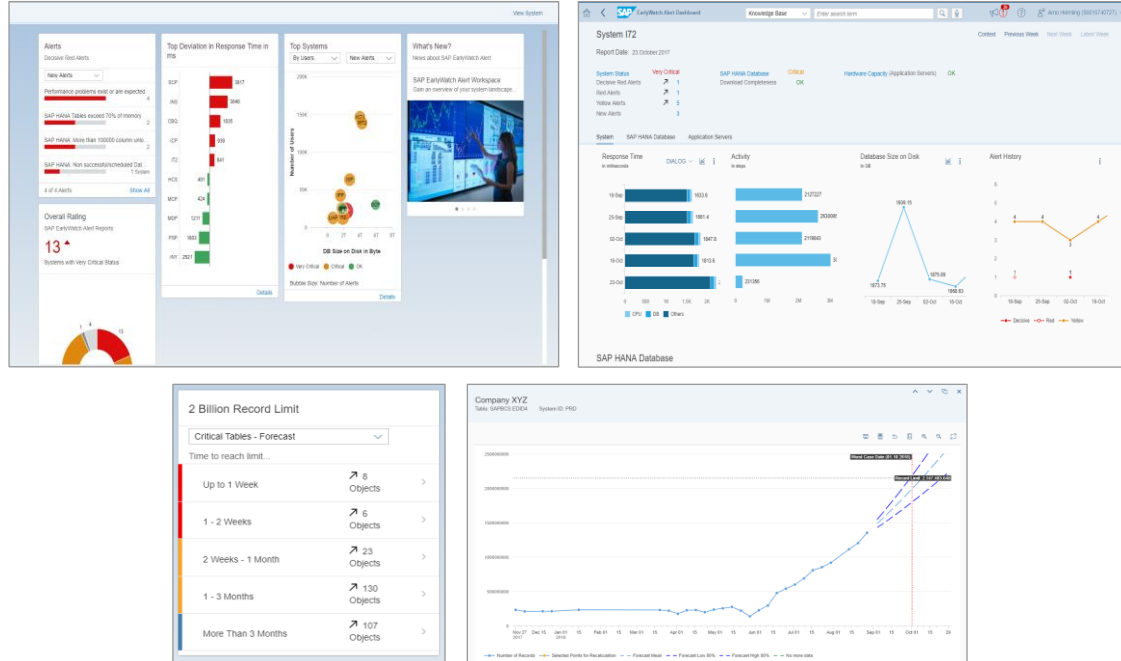
- Not every detail will get discussed in this Webinar. Instead, the slides will be used to give you a good overview and starting point. They will be made available to you afterwards also for reference purposes.

## Special S-User authorizations is required to view the 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.

# SAP EarlyWatch Alert Workspace

Get empowered to speak the same language across teams

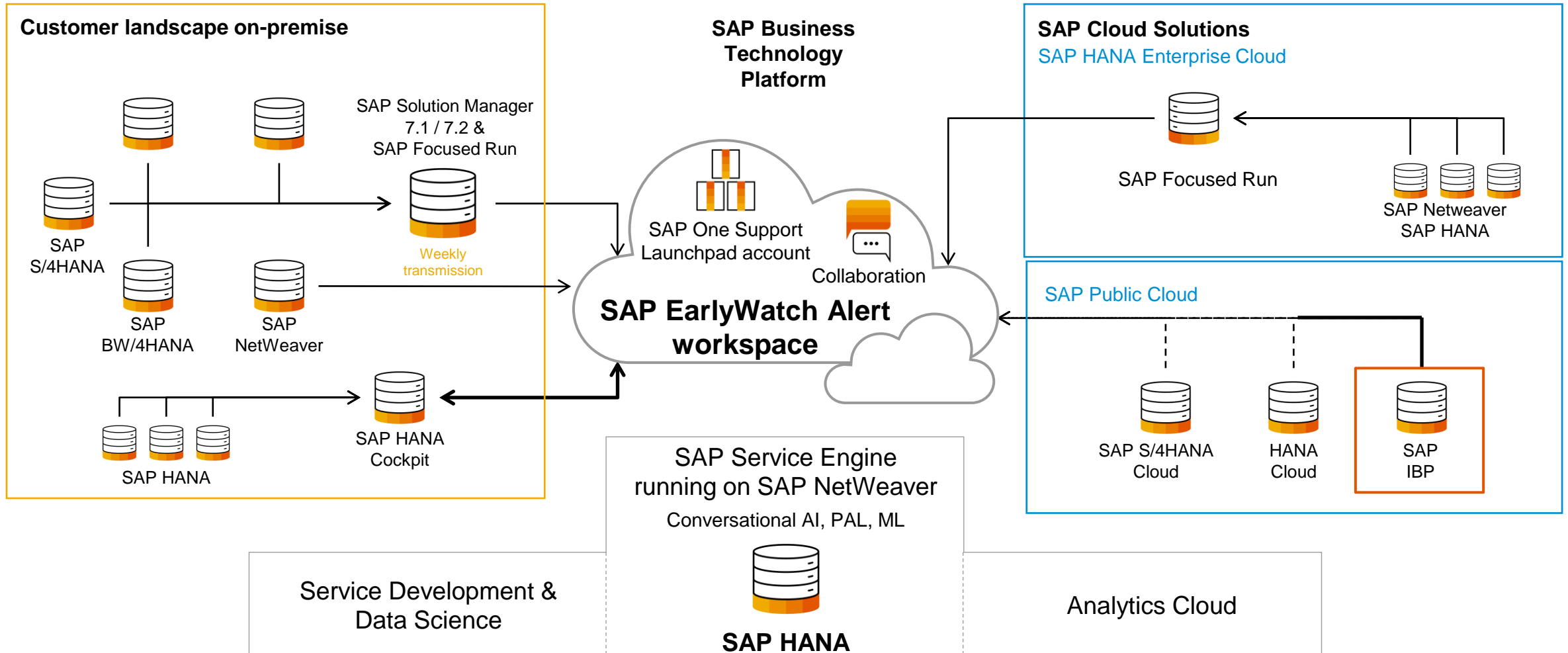


- One common view for all users
- Built for **simplicity** with Design Thinking
- One database with **years of history** of data
- One service engine using rules, predictions, and **Machine Learning**
- Transparency **at all times** for business continuity

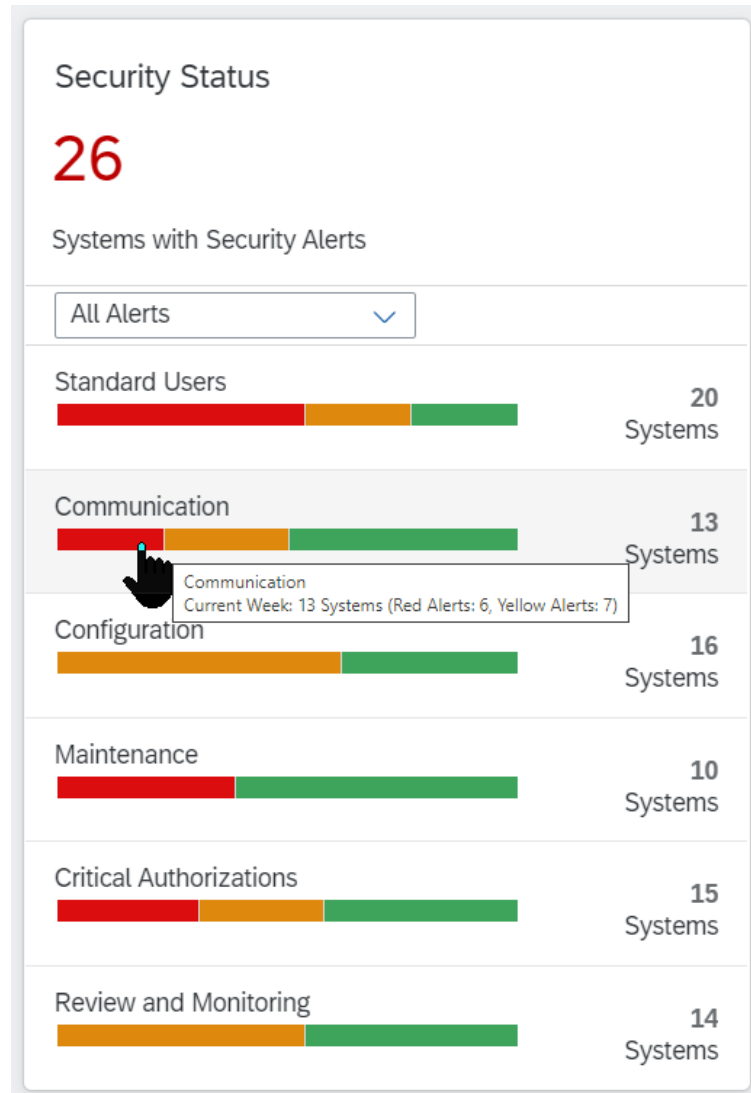
**Work with proven standards at any place and under all conditions.**

# SAP EarlyWatch Alert Workspace

## The Center of Data-Driven Collaboration



# 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

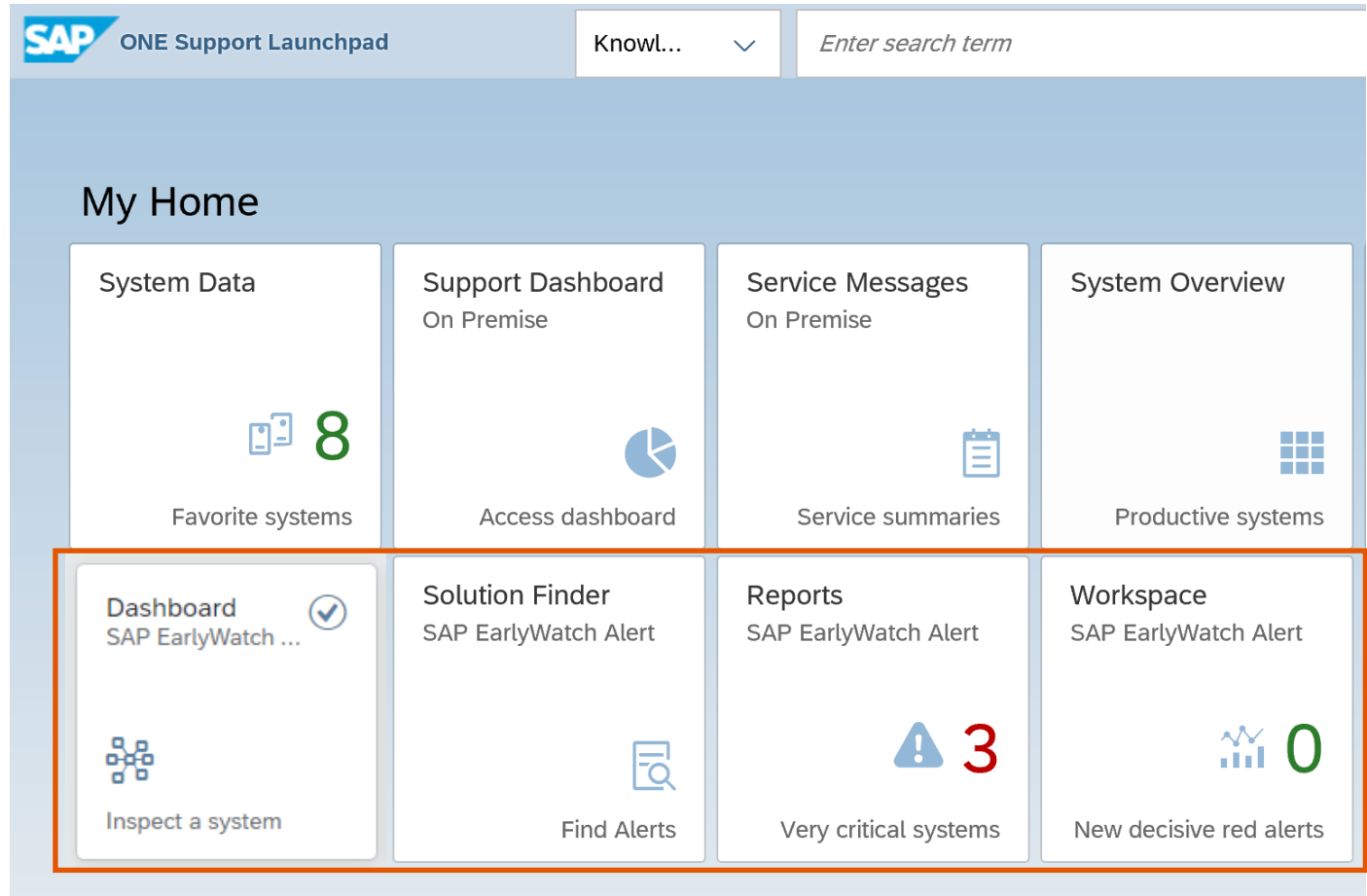
Available at <https://launchpad.support.sap.com/#ewaworkspace>

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

# Using the EWA Workspace

You can start the EWA Workspace and related functions

- via your One Support Launchpad



- via <http://launchpad.support.sap.com/#ewaworkspace>



# **Security Alerts** in the **SAP EarlyWatch Alert Solution Finder**



# Alert Category: Standard Users

## ABAP

Old



### Default Passwords of Standard Users (Security → ABAP Stack)

Standard users including SAP\* or DDIC have default password.



### Default Passwords of Standard Users (Security → ABAP Stack)

Standard users have default password.

This check triggers

With “red”

- if it is possible to logon with user SAP\* or DDIC with default password

With “yellow”

- if it is possible to logon with some other standard user besides SAP\* or DDIC with default password
- if user SAP\* does not exist in some client but cannot be immediately misused since profile parameter “login/no\_automatic\_user\_sapstar” is set to 1
- if user TMSADM exists in another client than 000

### Recommendation:

Standard users, including SAP\* and DDIC, have default passwords. Run report RSUSR003 to check the usage of default passwords by standard users. Ensure that:

- Profile parameter login/no\_automatic\_user\_sapstar is set to 1.
- **User SAP\* exists in all clients.**
- Users SAP\* , DDIC , and SAPCPIC have non-default passwords in all clients.
- User EARLYWATCH does not exist in any client and that the corresponding obsolete client 066 does not exist.
- User TMSADM exists only in client 000 but not in any other client and that this user has a non-default password.

For more information, see "Protecting Special Users" and "Profile Parameters for Logon and Password (Login Parameters)" either on SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide. SAP Note [1414256](#) describes a support tool to change the password of user TMSADM in all systems of the transport domain.

# Alert Category: Standard Users

## ABAP

New



### Default Passwords of Standard Users (Security → ABAP Stack)

Critical standard users have default passwords in client 000 / in other client(s) than 000



### Default Passwords of Standard Users (Security → ABAP Stack)

Standard users have default passwords in client 000 / in other client(s) than 000



### Control of the Automatic Login User SAP\* (Security → ABAP Stack)

User SAP\* does not exists in client 000, allowing critical logon to the system / in other client(s) than 000



### Control of the Automatic Login User SAP\* (Security → ABAP Stack)

User SAP\* does not exists in client 000, potentially allowing critical logon to the system / in other client(s) than 000



### Default Passwords of Standard Users (Security → ABAP Stack)

TMSADM exists in another client than 000

#### Recommendation:

Standard users, including SAP\* and DDIC, have default passwords. Run report RSUSR003 to check the usage of default passwords by standard users. Ensure that:

- Profile parameter login/no\_automatic\_user\_sapstar is set to 1.
- **User SAP\* exists in all clients.**
- Users SAP\* , DDIC , and SAPCPIC have non-default passwords in all clients.
- User EARLYWATCH does not exists in any client and that the corresponding obsolete client 066 does not exist.
- User TMSADM exists only in client 000 but not in any other client and that this user has a non-default password.

For more information, see "Protecting Special Users" and "Profile Parameters for Logon and Password (Login Parameters)" either on SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide. SAP Note [1414256](#) describes a support tool to change the password of user TMSADM in all systems of the transport domain.

# Alert Category: Standard Users

## HANA



### Activation Status and Validity of User SYSTEM (Security → SAP HANA Database)

SAP HANA database: User SYSTEM is active and valid.

#### Recommendation:

Review the current usage of user SYSTEM and set up and test a user and role concept, so that the use of user SYSTEM becomes obsolete. Deactivate the user account with the SQL statement: `ALTER USER SYSTEM DEACTIVATE USER NOW`. To prevent misuse of user SYSTEM, activate related audit policies in your SAP HANA system as described in the SAP HANA Administration Guide.

# Alert Category: Communication

## ABAP



### **RFC Gateway Access Control Lists (Security → ABAP Stack → RFC Gateway Security)**

Gateway Access Control List sec\_info is not effective. Well-known attacks may endanger your system.



### **RFC Gateway Access Control Lists (Security → ABAP Stack → RFC Gateway Security)**

Gateway Access Control List reg\_info is not effective.



### **RFC Gateway Security Properties (Security → ABAP Stack → RFC Gateway Security)**

RFC Gateway Access Control List may be bypassed. Programs that are not permitted may be able to communicate with the gateway.



### **Enabling an Initial Security Environment (Security → ABAP Stack → RFC Gateway Security)**

RFC Gateway default security behaviour is not activated. System may be at risk, when ACLs secinfo or reginfo are missing.

#### Recommendation:

The profile parameters gw/sec\_info and gw/reg\_info provide the file names of the corresponding access control lists. These access control lists are critical to controlling RFC access to your system, including connections to RFC servers. You should create and maintain both access control lists, which you can do using transaction SMGW. The files secinfo and reginfo, which are referenced by these profile parameters, should exist and should not contain trivial entries. The profile parameter gw/acl\_mode should be set to 1 to enable secure default rules if any of these files do not exist. The profile parameter gw/sim\_mode should be set to 0 to disable the simulation mode which would accept any connections. ...

# Alert Category: Communication

## ABAP



### Secure System Internal Communication (Security → ABAP Stack)

System-internal communication not protected.

#### Recommendation:

Activate authentication and encryption of system internal communication by setting profile parameter system/secure\_communication to ON. SAP recommends activating secure system internal communication on pure ABAP-based systems. For more information, see SAP Notes 2040644 , 2362078 , 2624688 , and 2778519.



### Message Server Access Control List (Security → ABAP Stack → Message Server Security)

Message Server Access Control List not effective. System not protected against access by rogue application servers.

#### Recommendation:

System-internal communication should be protected by setting profile parameter system/secure\_communication to ON. (see corresponding alert) If this is not the case, at least the profile parameter ms/acl\_info should be set to point to an ms\_acl\_info file with the message server's access control list...



### Message Server Administration Allowed for External Clients (Security → ABAP Stack → Message Server Security)

Message Server administration allowed for external clients.

#### Recommendation:

SAP recommends blocking external administration of the message server by setting the value of both of the profile parameters ms/monitor and ms/admin\_port to 0. For more information, see SAP Note [821875](#) ...

# Alert Category: Communication

## ABAP



### Protection of Passwords in Database Connections (Security → ABAP Stack)

#### Protection of Passwords in Database Connections

##### Recommendation:

Execute the valid manual postprocessing step described in SAP Security Note 1823566 . Note: This Note is valid for all ABAP installations that use database connections, including when the text focuses on SAP Solution Manager. The Note refers to SAP Solution Manager because typically, many DB connections are maintained. If this recommendation is displayed, there are DB connections with passwords on the analyzed system. Although transaction DBCO (which you use to maintain such DB connections) does not show the passwords, you can find the obfuscated passwords using transaction SE16 for table DBCON with the field value PASSWORD <> space.



### Kernel Patch Level (Security → ABAP Stack)

#### Insufficient Kernel Patch Level. Key security protection mechanisms missing.

##### Recommendation:

Update the kernel of your system to the newest kernel patch level available. Update to a kernel patch level equal to or higher than the minimum required kernel patch level specified above.

# Alert Category: Communication

## HANA



### SAP HANA Network Settings for Internal Services (Security → SAP HANA Database)

SAP HANA Internal Network Configuration is insecure.



SAP HANA Internal Network Configuration may lead to future security risks.

#### Recommendation:

Follow the instructions in SAP Note [2183363](#).



### SAP HANA Network Settings for System Replication Communication (listeninterface) (Security → SAP HANA Database)

SAP HANA network settings for System Replication is insecure.

#### Recommendation:

With current parameter settings, the default (public) network route is used for system replication communication or the system replication communication is not strictly restricted to the hosts of your scenario. This can be used to attack your SAP HANA system. Immediate action is recommended. Implement one of the best practices outlined below: Enable TLS encryption ...

If your system is already configured with separate networks for public, internal, and system replication communication, you can also choose an alternative approach. With such a network topology, you can ensure that hosts listen to system replication communication only on the dedicated ports of the separate network and reject incoming requests on other interfaces: ...If you choose this option, refer to the SAP HANA Security Guide on SAP Help Portal.



### SAP HANA Network Settings for System Replication Communication (listeninterface) (Security → SAP HANA Database)

SAP HANA network settings for System Replication may lead to future security risks.

#### Recommendation:

Some settings were detected in your configuration of system replication communication that are not according to SAP Best Practices, for example: 1. Parameter listeninterface ... is set to '.internal ', but the use of a dedicated non-public network for system replication communication could not be validated automatically. ... 2. Host-specific settings have been detected for some parameters. ...



# Alert Category: Configuration



## ABAP Password Policy (Security → ABAP Stack)

Secure password policy is not sufficiently enforced.

### Recommendation:

Assign a minimum value of 8 to the profile parameter login/min\_password\_lng.... <triggered by login/min\_password\_lng, login/password\_max\_idle\_initial>



## SAP HANA Password Policy (Security → SAP HANA Database)

SAP HANA database: Secure password policy is not sufficiently enforced.

### Recommendation:

Adapt all values to the recommended or stronger settings. <triggered by force\_first\_password\_change, maximum\_unused\_initial\_password\_lifetime, minimal\_password\_length>



## SAP HANA SSFS Master Encryption Key (Security → SAP HANA Database)

SAP HANA SSFS Master Encryption Key is not changed.

### Recommendation:

Change your SSFS master encryption key as described in SAP Security Note [2183624](#) and SAP HANA Administration Guide, section 'Change the SSFS Master Key'.



## SAP HANA SQL Trace Level (Security → SAP HANA Database)

SAP HANA database: SQL Trace is configured to write all result sets.

### Recommendation:

Use SQL trace with results in exceptional cases only. Change the trace level to ALL or a lower trace level. Even if the SQL trace is switched off (trace=off), the trace level should not be set to ALL\_WITH\_RESULTS because someone could activate this critical trace level unintentionally by switching on the SQL trace.

# Alert Category: Maintenance



## Age of Support Packages (Security → ABAP Stack)

SAP Software on this system is outdated. Support with SAP Security Notes is no longer ensured.



SAP Software on this system is about to be outdated. Support with SAP Security Notes is endangered.

### Recommendation:

Run support package updates at least once a year. In addition, evaluate SAP Security Notes once a month at the time of the monthly SAP Security Patch Day. SAP strongly recommends always performing support package updates for the complete support package stack and not just for the software components listed above. See <https://support.sap.com/en/my-support/software-downloads/support-package-stacks.html> for further information.




## Maintenance Status of current SAP HANA Database Revision (Security → SAP HANA Database)

SAP HANA database: Support Package has run out of security maintenance. Support with SAP Security Notes is no longer ensured.

### Recommendation:

Implement a clear SAP HANA maintenance strategy ensuring that the HANA software is kept up to date. As a general recommendation, an upgrade to the latest HANA revision of an SAP HANA major release should be performed at least once per year. For more information about the SAP HANA revision and maintenance strategy, see SAP Notes 2021789 - SAP HANA 1.0 Revision and Maintenance Strategy 2378962 - SAP HANA 2.0 Revision and Maintenance Strategy 1948334 - SAP HANA Database Update Paths for Maintenance Revisions for possible update paths...



when due within the next 6 months,  when overdue

# Regarding the Security Alert in SAP EarlyWatch Alert:

## Age of Support Packages: SAP Software on this system is outdated. Support with SAP Security Notes is no longer ensured.

### Official recommendation by SAP as given on the SAP Support Portal

<https://support.sap.com/en/my-support/software-downloads/support-package-stacks/support-package-stack-strategy.html>:

Most customers perform a planned maintenance for each productively used SAP application between once and four times a year ...

It is difficult to set up a general rule for defining the optimal time and frequency of a planned maintenance. You must decide what is best under the given circumstances; however, we recommend a planned maintenance at least once, or better yet, two to four times a year. ...

We assume that during the proactive planned maintenance the latest available support package stacks (SP stacks) are implemented and that the SP stacks used are not older than one year. ...

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


Starting June 11, 2019, for all new SAP Security Notes with high or very high severity we deliver fix for Support Packages shipped within the last 24 months\* for the versions under Mainstream Maintenance and Extended Maintenance.

\*See the following areas with an exception from the 24 months (starting June 11, 2019) with their general maintenance strategy


- Maintenance Strategy for SAP BW/4 HANA: see SAP Note [2347382](#)
- Maintenance Strategy for SAP Analytics BI Suite: see SAP Note [2771848](#)
- Maintenance Strategy for SAP GUI for Windows and SAP GUI for Java: see SAP Note [147519](#)
- Maintenance Strategy for SAP Kernel: see SAP Note [787302](#)
- Maintenance Strategy for SAP HANA: see documents for HANA1 and HANA2 or SAP Notes [2021789](#) and [2378962](#)
- Maintenance Strategy for SAP Business Client for Desktop: see SAP Note [2302074](#)


# Alert Category: Critical Authorizations


## ABAP

*Old*  **Users with Critical Authorizations (Security → ABAP Stack)**  
A high number of users has critical authorizations

## *New*

 **Critical authorizations, which should not be used in production (Security → ABAP Stack → Users with Critical Authorizations)**  
Users with critical authorizations, which should not be used in production in client 000 / in other client(s) than 000


 **Critical authorizations, which allow to do anything (Security → ABAP Stack → Users with Critical Authorizations)**  
Users with critical authorizations, which allow to do anything in client 000 / in other client(s) than 000

 **Critical authorizations, which should only see very limited use in production (Security → ABAP Stack → Users with Critical Authorizations)**  
Users with critical authorizations, which should not be used in production in other client(s) than 000 / in other client(s) than 000

### Recommendation:

Depending on your environment, review your authorization concept and use the Profile Generator (transaction PFCG) to correct roles and authorizations. You can use the User Information System (transaction SUIM) to check the results. For each check, you can review the roles or profiles that include the authorization objects listed in the corresponding section.

## HANA

 **SAP HANA System Privilege DATA ADMIN (Security → SAP HANA Database)**  
SAP HANA database: Users with critical privilege DATA ADMIN.

# Alert Category: Review and Monitoring



## SAP HANA Audit Trail (Security → SAP HANA Database)

SAP HANA database: Recommended Audit configuration is not applied.

### Recommendation:

Activate the SAP HANA audit trail and define appropriate audit policies.

Use the "Syslog" ("SYSLOGPROTOCOL") or the "Database Table" ("CSTABLE") target. Note: If you use the "Syslog" option, you also need to configure the operating system syslog accordingly so that you will not receive error messages in the event of issues with the OS syslog.

# FAQ

## ▪ Where can I find more information?

- SAP EarlyWatch Alert (EWA): <https://support.sap.com/ewa>
- SAP EWA Workspace: <https://launchpad.support.sap.com/#ewaworkspace>
- SAP Note [863362](#) - Security checks in SAP EarlyWatch Alert, EarlyWatch and GoingLive sessions
- SAP Security Optimization Services landing page: <https://support.sap.com/sos>

## ▪ I corrected the issue raised in an EWA Alert. Why does the EWA Workspace still show “red” / “yellow”?

- The EWA is an automated service available to all SAP customers with a maintenance contract, providing a common status view for joint work and collaboration. It evaluates the system data typically sent on a weekly basis. Thus, it will also only update typically weekly.
- The EWA is not intended to serve as live monitoring tool. Consider to use SAP Focused Run or the Configuration Validation in SAP Solution Manager in addition for such purpose.

## ▪ I am ok with some of the findings. Can I change the EWA Security Card and Checks to no longer raise an alert?

- The EWA provides SAP’s perspective onto your systems and thus compares against SAP recommendations. To compare against your specific Security Policy, consider to use SAP Focused Run or the Configuration Validation in SAP Solution Manager in addition. You may also be interested in the SAP Security Baseline Template (SAP Note [2253549](#)) in such context.

## ▪ Why can’t I see my Java systems in the EWA Security Card and Checks?

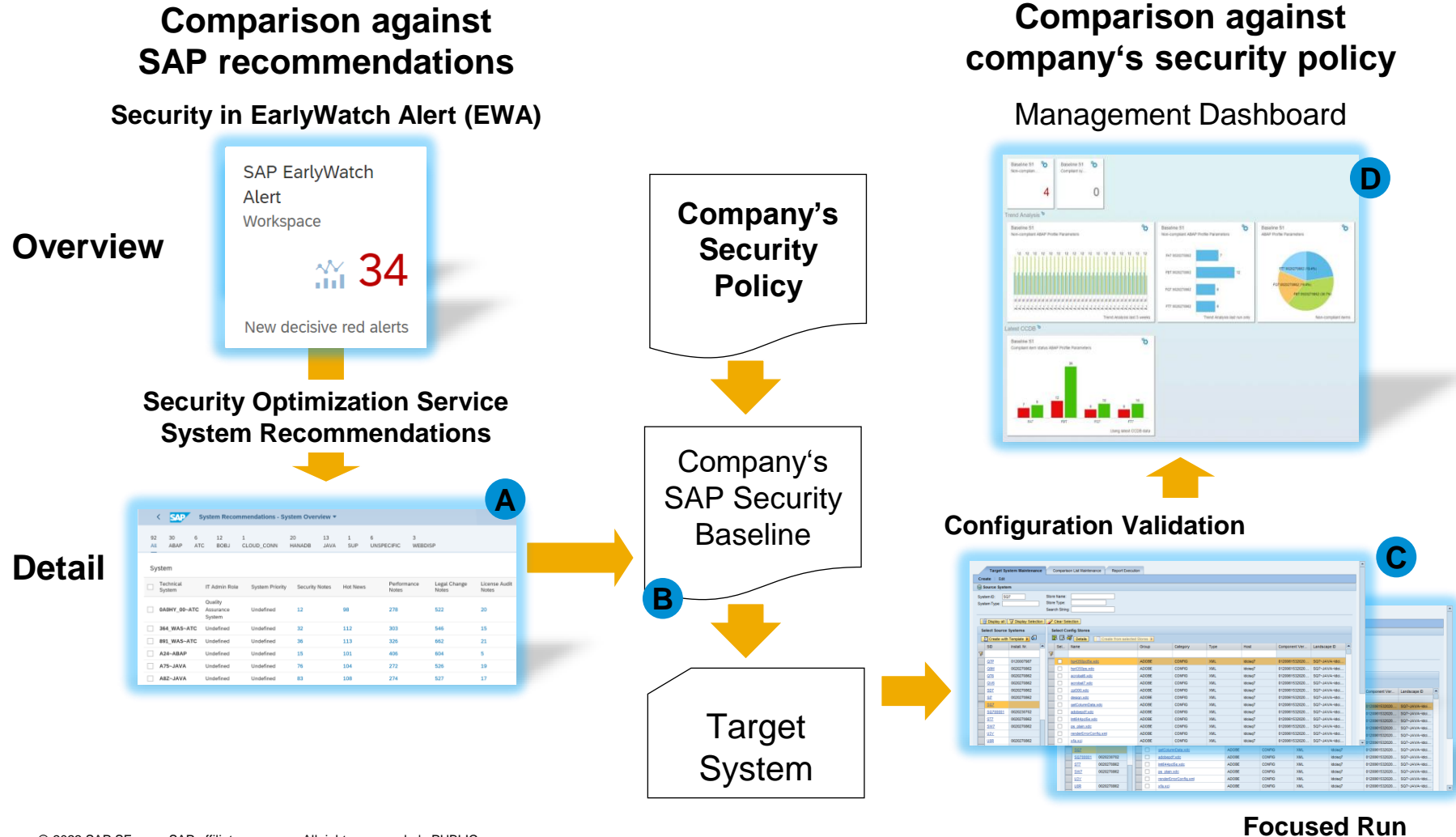
- Java systems currently do not provide data into the EarlyWatch Alert Workspace. However, you can review corresponding EarlyWatch Alert reports for Java systems in your local SAP Solution Manager

**How to continue on Security**



# Transparency for security and compliance

## Empowering on available tools and content



### Service delivery example:

**A** Automated services indicate security gaps

**Recommendation: Detailed look into gaps through experts**

**B** Service – Part 1:

- Root cause analysis for security gaps
- SAP Security Baseline maintenance

**C** Service – Part 2:

- Security patch deployment cycle
- Configuration setup
- Proactive threat identification

**D** Service – Part 3:

- Security control via dashboard

# Service Flow Cybersecurity & Compliance

Improvement Analysis and Roadmap Services (IAR)

Technical Security Check

Security Discovery

## Security Engagement

Level 3: Architecture – Architecting for security and compliance

Level 2: Engineering – Improvement for security and compliance

Level 1: Transparency – Empowerment for security and compliance

Security & Compliance Workshop

Contact &  
Touch Points

Impact  
Verification

Module FA08  
“Cybersecurity &  
Compliance”

Architecture Point of View  
Architecture Spotlight

## Deep Dive Packages

Patch Mgmt

Platform  
Security

DPP  
(GDPR)

Config  
Validation

...

from  
Catalog

Security Package  
Catalog

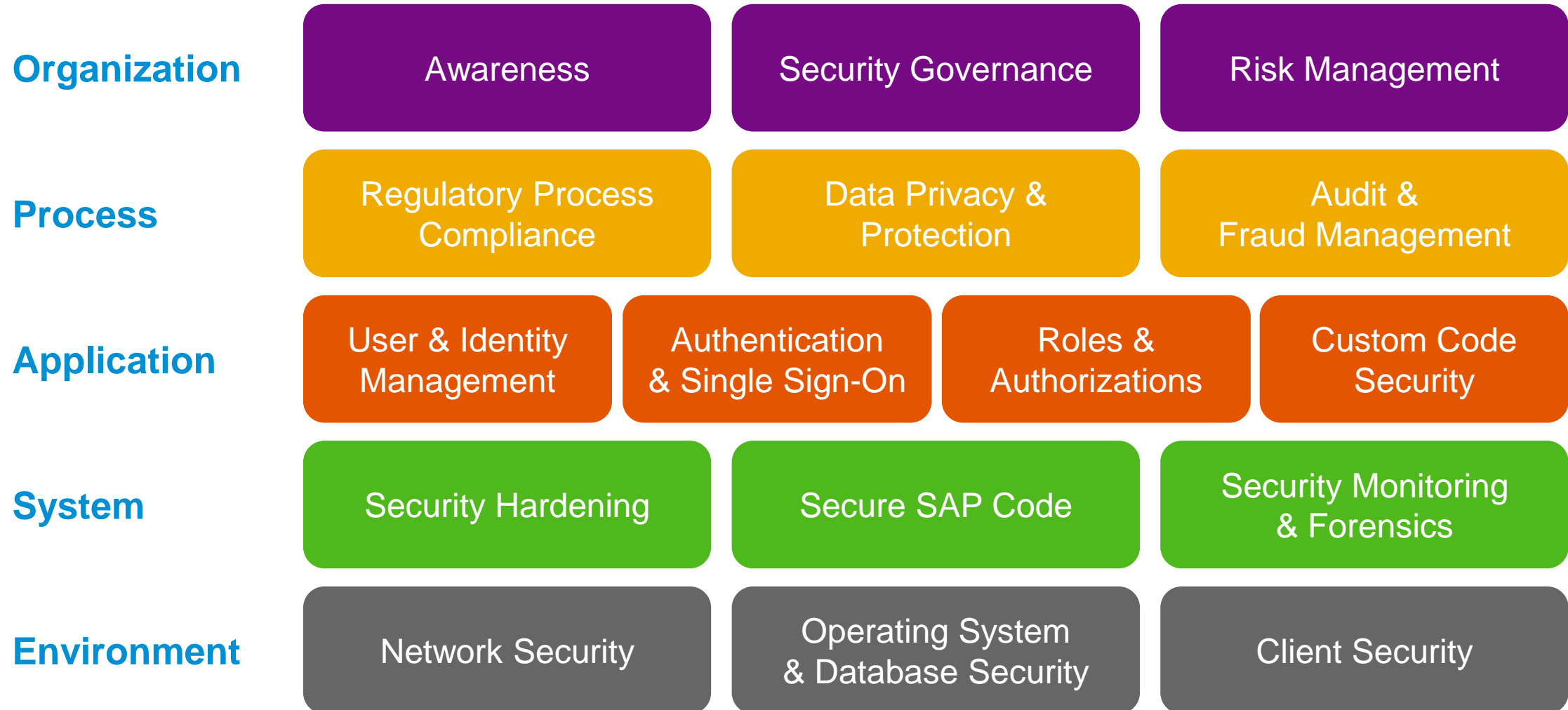


Immediate Action

Level 1: Transparency – Support for security and compliance  
Level 2: Engineering – Optimization for security and compliance  
Level 3: Architecture – Advisory for security and compliance

# Cybersecurity und Compliance Topic Areas

## The **Secure Operations Map**



# Thank you.

Contact information:

**Fritz Bauspiess, SAP SE**  
securitycheck@sap.com

Follow us



[www.sap.com/contactsap](https://www.sap.com/contactsap)

© 2022 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.

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

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

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

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. All other product and service names mentioned are the trademarks of their respective companies.

See [www.sap.com/trademark](https://www.sap.com/trademark) for additional trademark information and notices.