



# SAP EarlyWatch Alert Security Workshop

SAP SE – Intelligent Technology & Digital Platform – Global CoE Technology – Security Services  
[securitycheck@sap.com](mailto:securitycheck@sap.com)

July 2020

PUBLIC



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.

# Preliminary Remarks

- **This session will NOT be recorded.**

Security is a sensitive topic! At the same time, this is a workshop and we are very interested in an open and interactive exchange and discussion. Thus, we decided not to record this session to lower the barrier for open communication.

- **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:

- The already existing authorization **Service Reports and Feedback** (section Reports) to view SAP EarlyWatch Alert reports and apps.

- The new 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>)

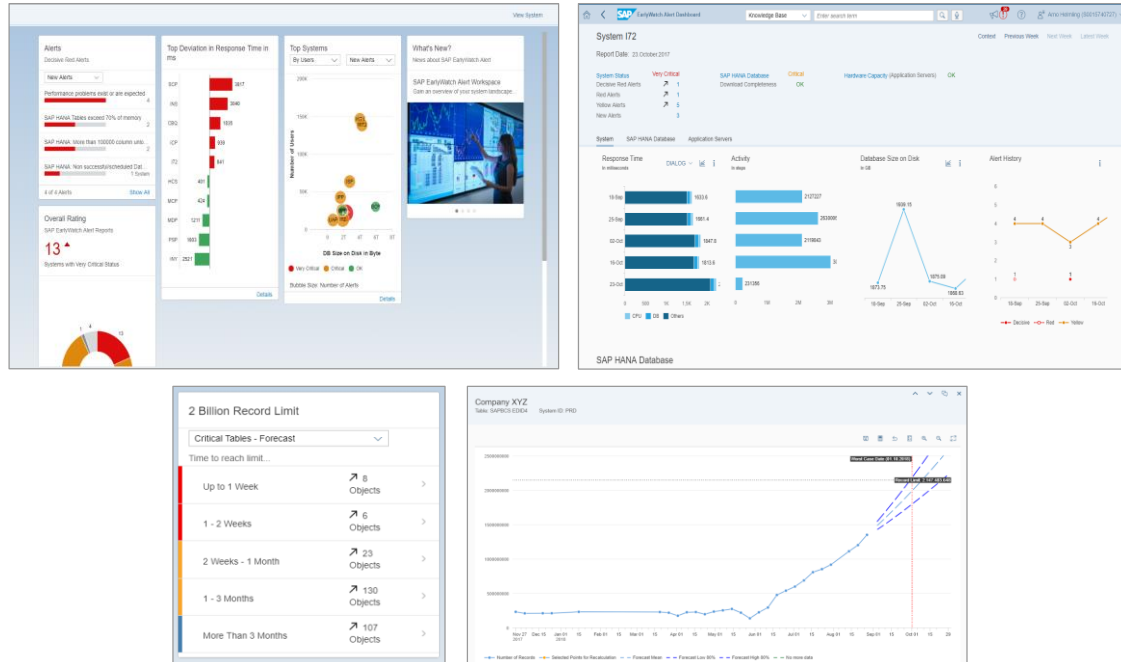
- If you don’t see it, ask your S-User Super Admin to grant the above authorizations to you.

**Security Card**

**in the SAP EarlyWatch Alert Workspace**

# SAP EarlyWatch Alert Workspace

Get empowered to speak the same language across teams

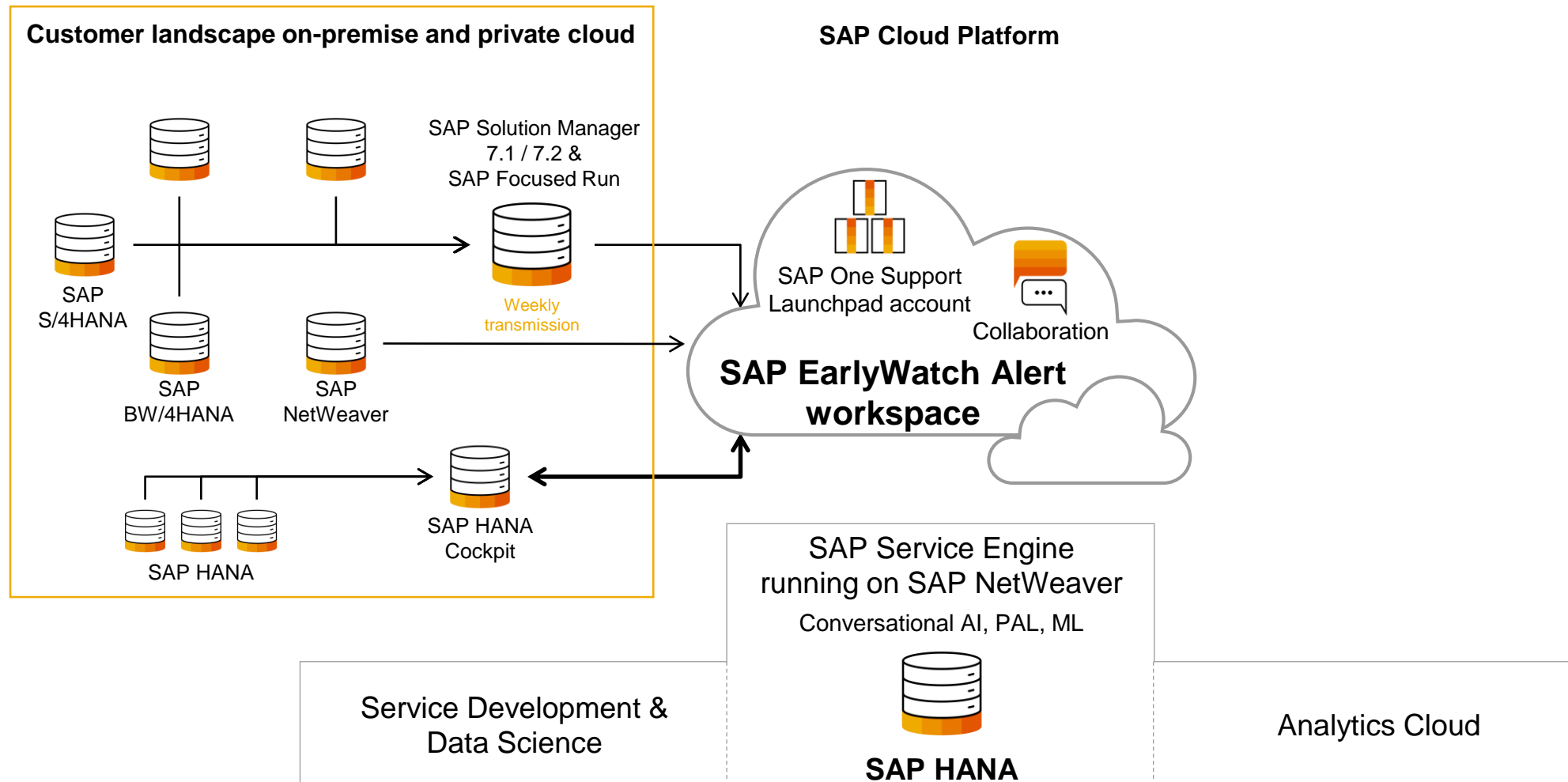


- One common view for all users
- Built for **simplicity** with Design Thinking
- One database with **3+ years history** of data
- One service engine using rules, predictions, and **Machine Learning**
- Transparency **at all times** for business continuity

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

# SAP EarlyWatch Alert Workspace

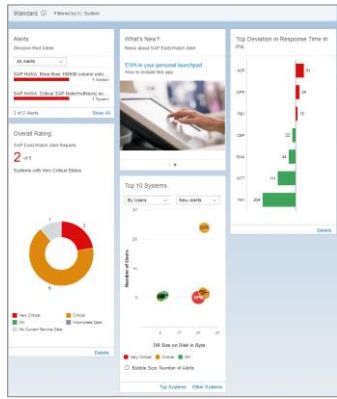
The center of data-driven collaboration



# Key Collaboration Views and Benefits

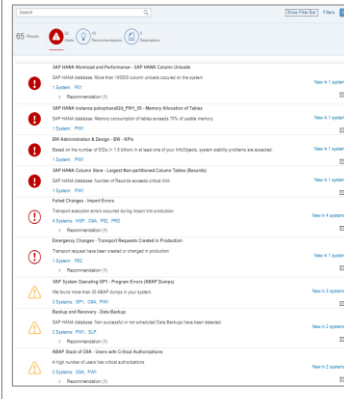
## Powered by SAP EarlyWatch Alert Workspace

### Landscape summary



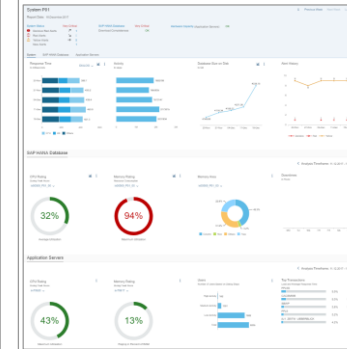
- Find top risks for business continuity
  - Easily identify top improvement actions
- Fiori Overview Page**

### Alert list per landscape



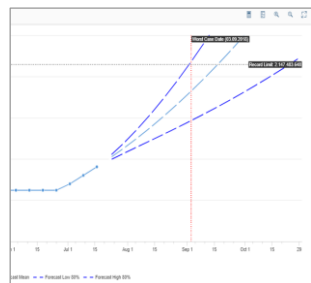
- Aggregated and prioritized alert view
  - Get best practices for mitigation
- Powered by SAP HANA Text Search**

### Dashboard per system



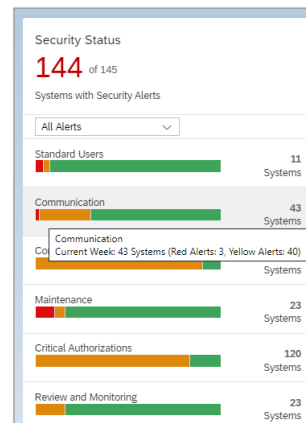
- Identify serious bottlenecks
  - Find critical trends in KPIs
- Embedded Analytics via CDS views**

### Predictive alerts



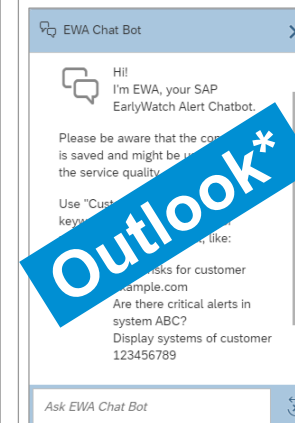
- Timely forecasts of critical situations
  - Avoid business downtimes well in advance
- Powered by SAP HANA Predictive Analytics Library (PAL)**

### Security risks per landscape



- Get secure and stay secure
  - Hardening of security settings
  - Perform easy security scans
- Fiori Overview Page**

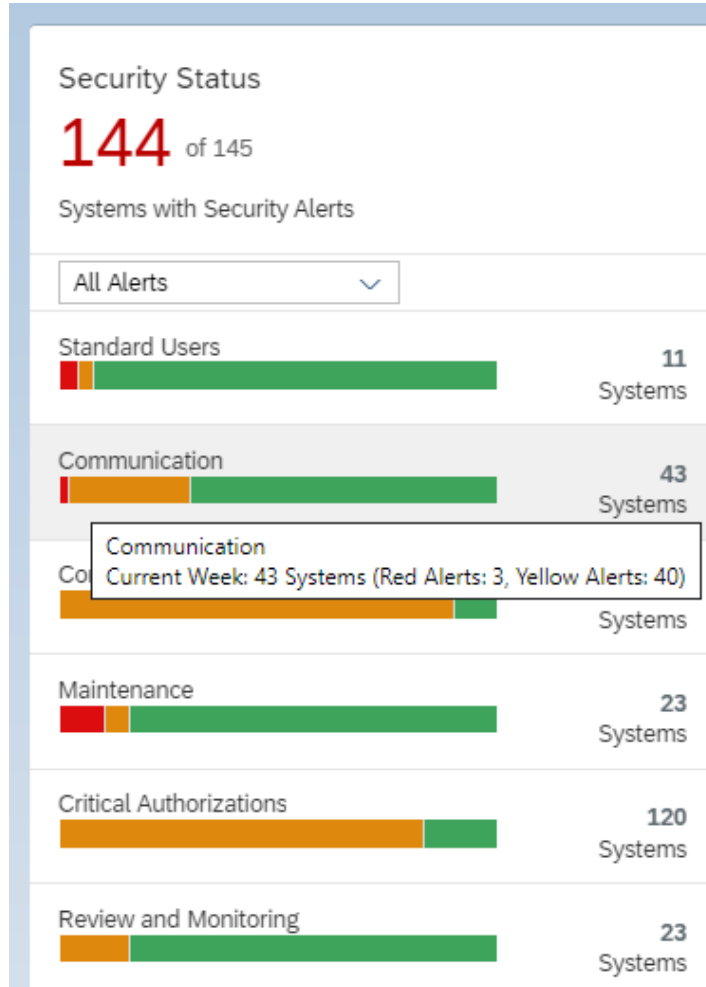
### Active collaboration at all times



- Get informed about alerts
  - Get embedded support
  - Searchability
- Powered by Conversational AI**



# 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*”



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

# Security Alerts in the SAP EarlyWatch Alert Solution Finder

## Most Critical Alerts – Default Passwords of Standard Users

- **Default Passwords of Standard Users (Security → ABAP Stack)**
  - Standard users including SAP\* or DDIC have default password. 
  - Standard users have default password.  (i.e. neither SAP\* nor DDIC)

Standard users, including SAP\* and DDIC, have default passwords.

Run report RSUSR003 to check the usage of default passwords by standard users. Ensure that:

- User SAP\* exists in all clients
- Users SAP\* , DDIC , SAPCPIC , and EARLYWATCH have non-default passwords in all clients
- Profile parameter login/no\_automatic\_user\_sapstar is set to 1.

For more information, see "Protecting Standard Users" and "Profile Parameters for Logon and Password (Login Parameters)" either on SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide.


Make sure that the standard password for user TMSADM has been changed. SAP Note [1414256](#) describes a support tool to change the password of user TMSADM in all systems of the transport domain. SAP Note [1552894](#) shows how to update the report RSUSR003 to show the status of user TMSADM.


# Security Alerts in the SAP EarlyWatch Alert Solution Finder

## Most Critical Alerts – RFC Gateway Security

- **RFC Gateway Security (Security → ABAP Stack → RFC Gateway and Message Server Security)**

- Gateway Access Control List (reg\_info/sec\_info) contains trivial entries / does not exist

- “sec\_info” affected 

- “reg\_info” affected 

- 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/sim\_mode should be set to 0 to disable the simulation mode which would accept any connections.
- Enable the missing property by adding the bitmask value to the current value of profile parameter gw/reg\_no\_conn\_info. For more information about profile parameter gw/reg\_no\_conn\_info, see SAP Note [1444282](#).
- The profile parameter gw/acl\_mode should be set to 1 to enable secure default rules if any of these files do not exist.



SAP recommends defining and properly maintaining these access control lists to prevent rogue servers from accessing the system. For more information, see the following SAP Notes:

SAP Note [[1305851](#)] - Overview note: "reg\_info" and "sec\_info" / SAP Note [[1408081](#)] - Basic settings for reg\_info and sec\_info

For more information, see "Configuring Connections between SAP Gateway and External Programs Securely" on SAP Help Portal and the SAP Gateway wiki on the SAP Community Network. See also the white paper on SAP Security Recommendations: Securing Remote Function Calls (RFC) available at [https://support.sap.com/content/dam/support/en\\_us/library/ssp/security-whitepapers/securing\\_remote-function-calls.pdf](https://support.sap.com/content/dam/support/en_us/library/ssp/security-whitepapers/securing_remote-function-calls.pdf).

# Security Alerts in the SAP EarlyWatch Alert Solution Finder

## Most Critical Alerts – Security Maintenance Status

- **Age of Support Packages (Security → ABAP Stack)**
    - SAP Software on this system is outdated. Support with SAP Security Notes is no longer ensured.
  - **Maintenance Status of current SAP HANA Database Revision (Security → SAP HANA Database)**
    - SAP HANA database: Support Package will run out of security maintenance. Support with SAP Security Notes is endangered.
- 
- overdue 
  - due within the next 6 months 

# Security Alerts in the SAP EarlyWatch Alert Solution Finder

## Most Critical Alerts – Security Maintenance – Guidance by SAP

### 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, better twice 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 priority we deliver fix for Support Packages shipped within the last 24 months\* ...

\*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](#)”

# Security Alerts in the SAP EarlyWatch Alert Solution Finder




## SAP HANA Configuration-Related Alerts

- **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. 
- **SAP HANA Network Settings for System Replication Communication (listeninterface) (Security → SAP HANA Database)**
  - SAP HANA network settings for System Replication is insecure. 
  - SAP HANA network settings for System Replication may lead to future security risks. 
- **SAP HANA Audit Trail (Security → SAP HANA Database)**
  - SAP HANA database: Recommended Audit configuration is not applied. 
- **SAP HANA SQL Trace Level (Security → SAP HANA Database)**
  - SAP HANA database: SQL Trace is configured to write all result sets. 
- **SAP HANA SSFS Master Encryption Key (Security → SAP HANA Database)**
  - SAP HANA SSFS Master Encryption Key is not changed. 




# Security Alerts in the SAP EarlyWatch Alert Solution Finder

## User-Related Alerts

### SAP ABAP AS

- **Users with Critical Authorizations (Security → ABAP Stack)** 
  - A high number of users has critical authorizations
- **Protection of Passwords in Database Connections (Security → ABAP Stack)** 
  - Protection of Passwords in Database Connections
- **ABAP Password Policy (Security → ABAP Stack)** 
  - Secure password policy is not sufficiently enforced.

### SAP HANA

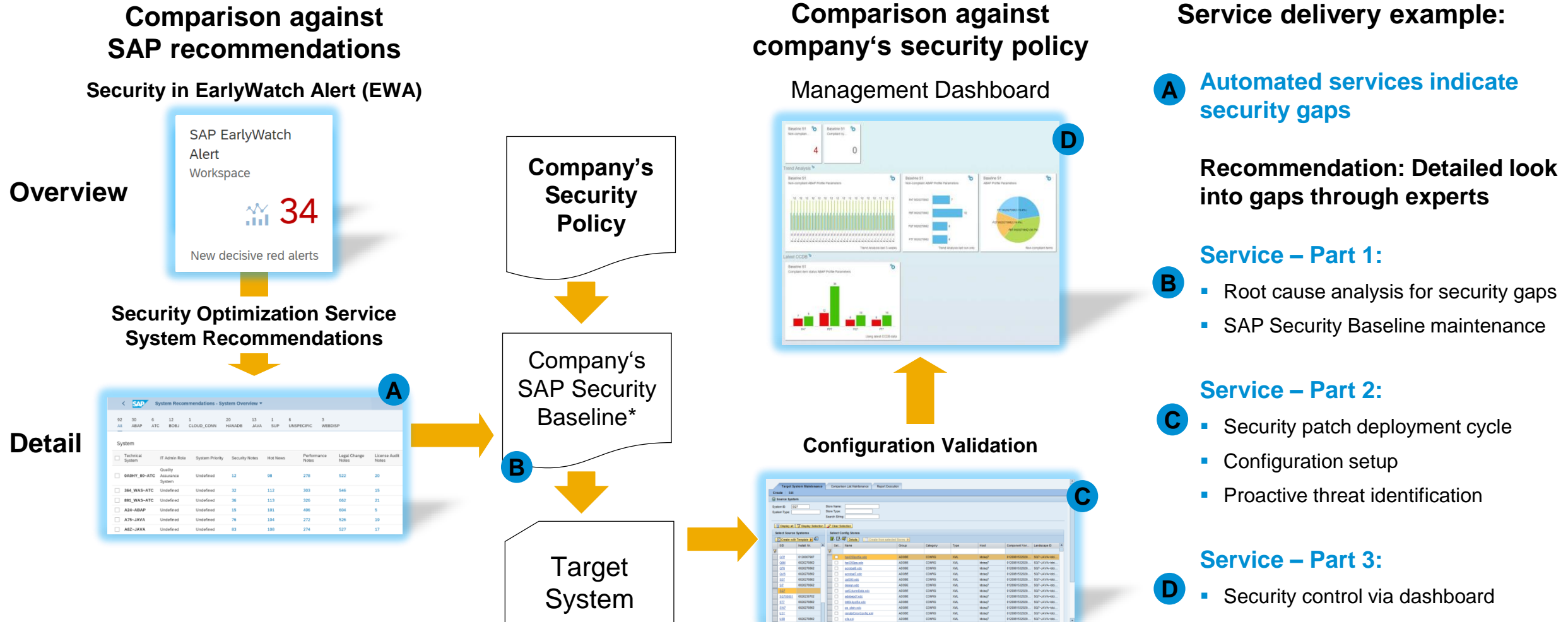
- **Activation Status and Validity of User SYSTEM (Security → SAP HANA Database)** 
  - SAP HANA database: User SYSTEM is active and valid.
- **SAP HANA System Privilege DATA ADMIN (Security → SAP HANA Database)** 
  - SAP HANA database: Users with critical privilege DATA ADMIN.
- **SAP HANA Password Policy (Security → SAP HANA Database)** 
  - SAP HANA database: Secure password policy is not sufficiently enforced.



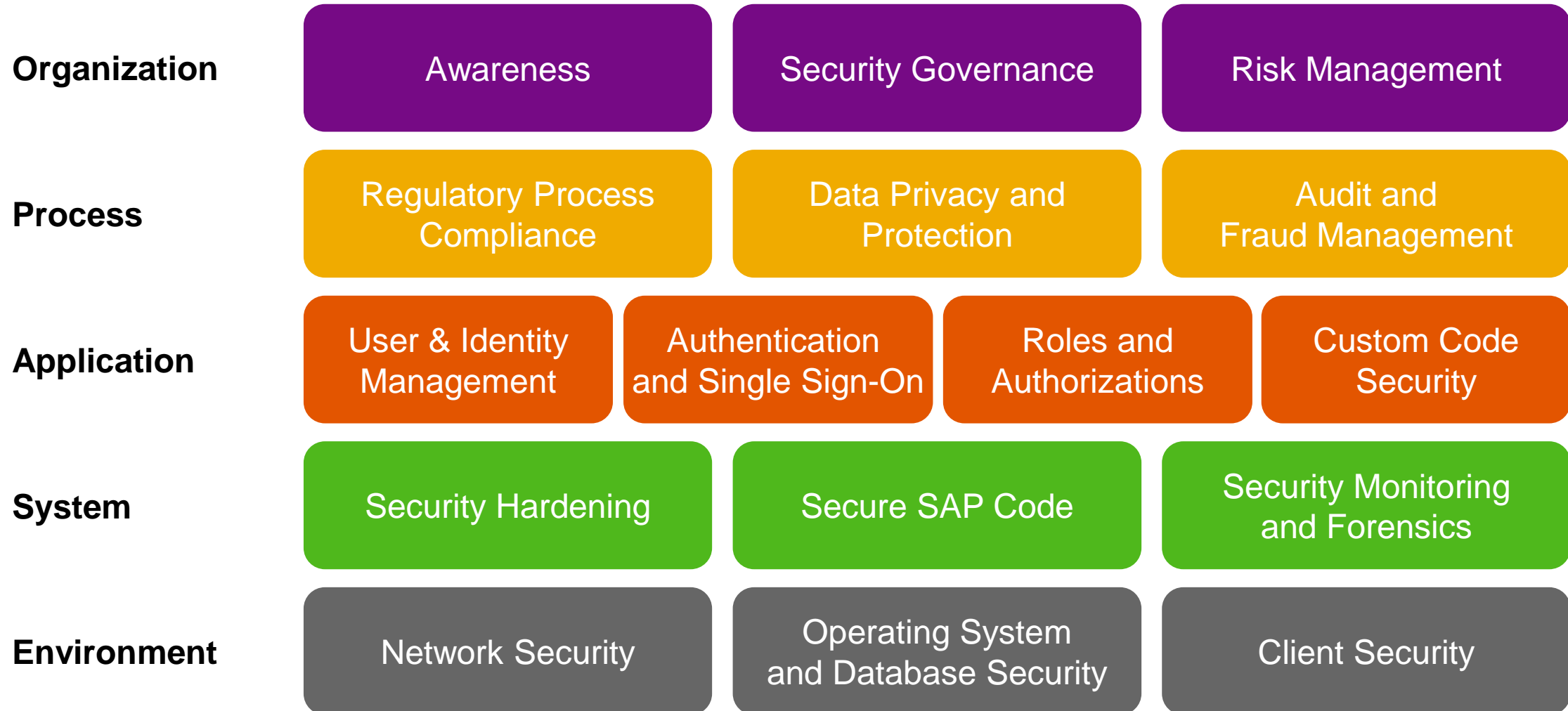
**How to continue on Security**

# Transparency and Mitigation

Empowering on available tools and content

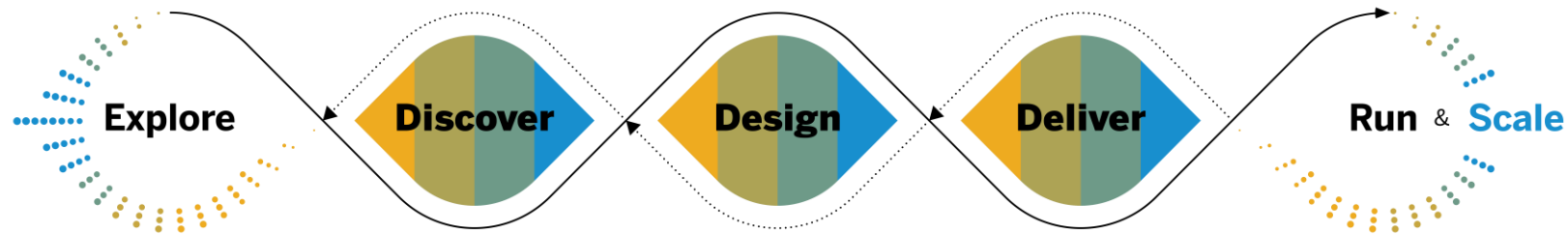


# Cybersecurity and Compliance – Secure Operations Map



# Cybersecurity and Compliance – Project-related Services

Bridge the gap between business and IT to drive innovation and run SAP best and ensure security and compliance to safeguard your investments in innovations



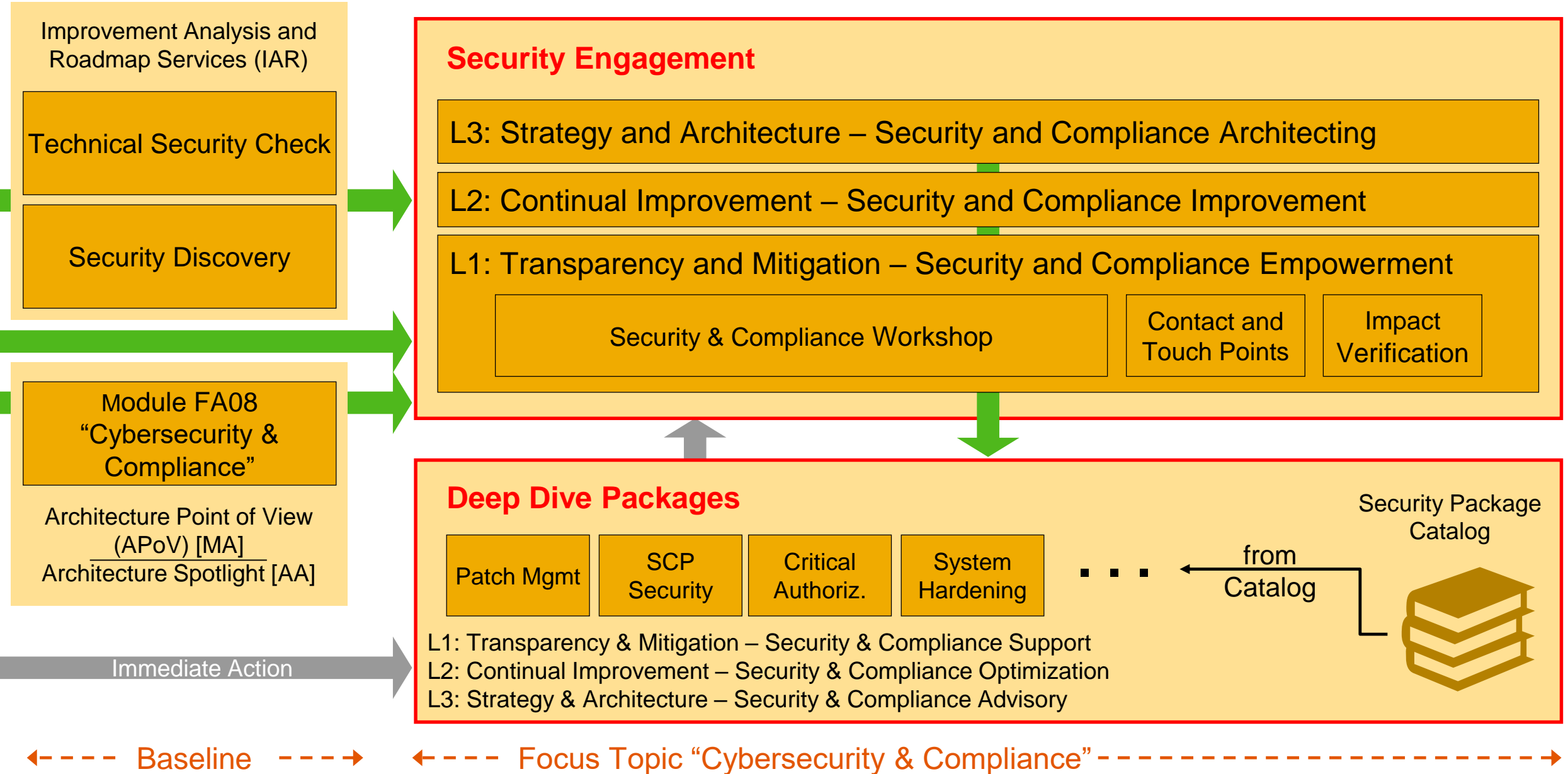
## Architecture and Planning service for cybersecurity and compliance

- Information Security Compliance Review
- Identity Access Management
- Infrastructure Security
- Data Protection and Privacy
- Cybersecurity Reference Architecture
- Technical Security Review

## Execution and Implementation service for cybersecurity and compliance

- Cloud Identity Services – Quick Start
- Cloud Identity Access Governance – Quick Start
- Re-Platforming for Identity Access Management
- SAP Access Control Implementation
- SAP Identity Management – Business Extensions
- Risk Compliance and Assurance Implementation
- Automated Implementation of Role Concepts

# Cybersecurity and Compliance – Engagement-related Services



Follow us



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

© 2020 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/copyright](http://www.sap.com/copyright) for additional trademark information and notices.