SAP Security Engagement Service Package

SAP CoE Security Services
October, 2017

CUSTOMER
Agenda

Why Security Engagement?

SAP Secure Operations Map

SAP Security Engagement Service Package
Why SAP Security Engagement
Why Security Engagement?
Security in the Digital Business Framework

SAP business software provide built-in security features to protect your business critical information.

SAP security software can help you shield your business from attacks and protect your information assets with secure solutions.

DBS Security Engagement services offer support to implement security best practices, product security features and cybersecurity for SAP solutions.

Security is an essential part
Why Security Engagement?
Challenges during Transition to S/4HANA and Cloud

Digital Transformation

SAP Business Suite
- ABAP Programs
- Database
  - Any RDBMS

SAP S/4HANA Back-End System
- Gateway Back-End Enablement
- Application Services
  - Business Functionality
- ESH

SAP HANA Platform
- CDS

Reverse Proxy
- Web ports & forwarding rules

Front-End Server (SAP Gateway)
- SAPUI5 (incl. SAP Fiori Launchpad)
- Application UIs

Browser
SAP GUI
Mobile

SAP Mobile Platform

SAP Cloud Platform
SAP Secure Operations Map
The 16 Secure Operation Tracks cover the following topics:

**Security Governance:** Adopt security policies for your SAP landscape, create and implement an SAP Security Baseline

**Audit:** Ensure and verify the compliance of a company’s IT infrastructure and operation with internal and external guidelines

**Cloud Security:** Ensure secure operation in cloud and outsourcing scenarios

**Emergency Concept:** Prepare for and react to emergency situations

**Users and Authorizations:** Manage IT users and authorizations including special users like administrators

**Authentication and Single Sign-On:** Authenticate users properly – but only as often as really required

**Support Security:** Resolve software incidents in a secure manner

**Security Review and Monitoring:** Review and monitor the security of your SAP systems on a regular basis

**Secure Configuration:** Establish and maintain a secure configuration of standard and custom business applications

**Communication Security:** Utilize communication security measures available in your SAP software

**Data Security:** Secure critical data beyond pure authorization protection

**Security Maintenance of SAP Code:** Establish an effective process to maintain the security of SAP delivered code

**Custom Code Security:** Develop secure custom code and maintain the security of it

**Network Security:** Ensure a secure network environment covering SAP requirements

**Operating System and Database Security:** Cover SAP requirements towards the OS and DB level

**Frontend Security:** Establish proper security on the frontend including workstations and mobile devices
SAP Security Engagement Service Package
The Security Engagement Service Package helps to efficiently design, build and run SAP on premise and cloud systems and landscapes in a secure manner.

**Coverage**
- Creation of customized SAP Security Roadmap which identifies security gaps and risks to be mitigated via continuous support and execution of the service package.
- Evaluate the security capabilities of SAP digital solutions to provide end to end security design recommendations.
- Security assessment and optimization focusing on system hardening and secure operations.
- Provide detail plan and support to implement security functionalities based on customer specific security policy, operation process, and system landscapes.
- Prototyping of SAP security products and continuous safeguarding service until Go-live.
- Foundation for accessing SAP security expertise by providing a Security Architect, on an advisory role as the single contact of all SAP security related questions.

**Project Involvement**
- SAP: security planning, design, prototyping and safeguarding during the project
- Partner-/customer-led: overall project responsibility and security functional implementation

**Your Benefits**
- Empowered by security features and best practices of SAP Digital Business Framework
- Accelerated security design and technical advisory for large, complex SAP digital solutions incl. but not limited to S/4HANA and SAP Cloud Platform
- Minimized security risks and vulnerabilities by implementing SAP security standards and best practices in the project and safeguarded/validated by SAP security experts
## Security Engagement Service Package

### Standard Services

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Planning Workshop</td>
<td>Planning activities to define the scope of Security Engagement based on overall assessment of different aspects of SAP Secure Operations Map across SAP landscapes. The workshop also provides an overview of best practices, standard security baseline template, security services and tools available from SAP for secure operation.</td>
</tr>
<tr>
<td>Security Optimization Service</td>
<td>Safeguard the security aspect of project implementation by providing a detailed technical analysis of the security of SAP solution in comparison to SAP recommendations and best practices.</td>
</tr>
<tr>
<td>Security Design Support</td>
<td>Core activities to provide a detailed concept of the technical security functionalities for the SAP S/4HANA or Cloud solutions based on the scope defined in the Security Planning Workshop. This service provides design and review of technical architecture related to SAP security products and solutions. Optionally it supports development of a customized security baseline document that includes communication and data security, front end/mobile security and other topics from SAP Secure Operations Map.</td>
</tr>
<tr>
<td>Prototyping</td>
<td>Conduct prototyping in an agile approach to ensure accelerated deployment of SAP security products in an innovative business scenario. Support for planning, safeguarding, technical and functional implementation of critical SAP security product components.</td>
</tr>
<tr>
<td>Security Architect</td>
<td>Single point of contact to discuss all topics related to your SAP security products, security service delivery and secure operations. Security Architect makes sure your team is empowered with the most up-to-date security information and knowledge from SAP. This person also helps ensure security design and build activities of the project are properly executed to avoid common security pitfalls in SAP projects. Via the Security Architect you get access to the security experts from different organizations within SAP.</td>
</tr>
</tbody>
</table>
Service Plan Options

**Planning First Variant**
- Start with Security Planning Workshop to define the scope of the engagement
- Use Security Design Support to provide guidance on product specific (such as S/4HANA or Cloud) security functionality implementation
- Security Optimization Service is delivered during Deploy phase for system hardening

**Value First Variant**
- Start with a more in-depth security analysis on the system to provide immediate action plan as the input for Security Planning Workshop
- Security Planning Workshop defines the scope of follow up services

**Variant for Security Product Implementation**
- Security Planning Workshop defines the effort and scope of the engagement
- Prototyping provides a quick PoC to show case basic configurations
- Implementation support for production environment and safeguarding of the project Golive

© 2017 SAP SE or an SAP affiliate company. All rights reserved. | CUSTOMER
SAP Security Engagement service package – service component description

Security Planning Workshop

BUSINESS NEEDS
• Support in identifying the security gaps in current SAP solution and landscapes
• Define a comprehensive security strategy and roadmap based on customer security policy, requirements, landscapes and operation processes
• In need of latest SAP security information and best practices
• Define the scope of security engagement for S/4HANA or SAP Cloud solutions
• Define the scope of project safeguarding for SAP security products

DELIVERY APPROACH AND SCOPE
• Provide an overview of best practices, services and tools available from SAP for secure operation of SAP systems and landscapes
• Get an overview on the specific customer’s situation regarding SAP security
• Identify needs, options and next steps – summarized in a Security Roadmap - to improve the security of the customer’s SAP environment.

SHORT DESCRIPTION
• The service offers a comprehensive analysis of SAP security at the customer taking into consideration of security policy, requirements, solution and processes. It also enables customer on SAP security best practices and various security features of SAP products. It acts as the leading service of most security engagements to define the scope and roadmap for execution.

VALUE AND BENEFITS
• Creation of customer specific roadmap to execute security strategy for S/4HANA or SAP Cloud projects
• Recommendations on selected security topics
• Plan and define security aspect of SAP project execution and product implementation
SAP Security Engagement service package – service component description

Security Design Support

BUSINESS NEEDS
- Incorporate security concept in the design phase of the project
- Minimize security risks of SAP system landscape
- Best practice of security design in SAP on premise or cloud solutions

DELIVERY APPROACH AND SCOPE
- Deep dive analysis of a component, product or procedure to assess the security of the respective object and provide design recommendations
- Support in designing solution for SAP IDM, GRC and SSO
- Support in designing authentication, authorization concept of S/4HANA, HANA DB, Analytics and applications running on SAP Cloud Platform
- Design high level security architecture for complex SAP landscape and infrastructure
- Support in developing custom security baseline document of communication and data security, mobile/front end security and other topics from SAP Secure Operations Map

VALUE AND BENEFITS
- Validation and assurance of security architecture for SAP cloud and on premise solutions
- Accelerated definition of security concepts and activities during the full project lifecycle
- Enforce best practice in security product implementation and designing security capabilities of SAP business and platform software

SHORT DESCRIPTION
- This service supports the customer in definition of a more detailed security concept and architecture for SAP solutions. Depending on the target solution this service supports solution design of SAP security products or security design of SAP business software on premise and on cloud.
Security Optimization

BUSINESS NEEDS
- Ensure smooth operation of your SAP solution by taking action proactively, before severe security problems occur
- End to end platform security analysis in a complex SAP digital solution landscape

DELIVERY APPROACH AND SCOPE
- Detailed technical analysis of the security of a system in comparison to SAP recommendations and best practices with focus on critical authorizations, secure configuration as well as process to manage of SAP Security Notes.
- Provide additional information on the security reason and relevance of each check, concrete findings and recommended resolution or mitigation steps.
- This session can be used for any SAP system based on either of these application servers. It is useful to check for the security configuration of the application server, like critical basis authorizations or settings of profile parameters. For analyzing application specific security objects like BW or CRM authorizations it is delivered via Security Design Support service.

VALUE AND BENEFITS
- Decrease the risk of a system intrusion and costly downtime due to wrong user interaction
- Ensure the confidentiality of your business data and authenticity of your users.

SHORT DESCRIPTION
- This service is designed to verify and improve the security of the SAP systems of customers by identifying potential security issues and giving recommendations on how to improve the security of the system.
SAP Security Engagement service package – service component description

Security Architect

BUSINESS NEEDS

- Advisory on all SAP security related questions during the whole project life cycle
- Alignment with different SAP teams (Product Security, Security Backoffice, Security Service Delivery) on particular issues and drive to a quick resolution

DELIVERY APPROACH AND SCOPE

Security Architect Tasks and Deliverables

- **Subject Matter Expert** on SAP security topics including but not limited to security of S/4HANA (OP/Cloud), SAP public cloud solutions and SAP Cloud Platform as well as SAP Secure Operation Roadmap.
- **Cybersecurity advisory** and guidance on **SAP Security Best Practice** based on the methodology of SAP Secure Operation Roadmap.
- **Service planning and scoping** to setup security services to address specific needs in certain areas with the right security expertise
- **Liaison** to SAP Security Backoffice and Product Security team for any issues related to SAP security products and secure cloud operation

VALUE AND BENEFITS

- Single point of contact of all SAP security issues
- SAP Security knowledge assurance
- Full project cycle safeguarding coverage on SAP security aspect

SHORT DESCRIPTION

- The Security Architect is your contact partner to discuss all topics related to your SAP security products, security service delivery and secure operations. This person makes sure your team is empowered with the most up-to-date security information and knowledge from SAP. Security Architect also helps ensure security design and build activities of the project are properly executed to avoid common security pitfalls in SAP projects. Via the Security Architect you get access to the security experts from different organizations within SAP.
SAP Security Engagement service package – service component description

Prototyping

BUSINESS NEEDS
- Showcase of critical functionalities of SAP security products
- Quick deployment of SAP security products in non-production environment

DELIVERY APPROACH AND SCOPE
- Rapid prototyping of SAP security products based on pre-defined scope of Proof-of-Concept project
- Configuration or implementation support of SAP security products to showcase the key capabilities
- Empowerment session to enable customer on product knowledge and best practices
- Support to fix product issues identified during prototyping phase with SAP development teams
- Handover documentation
- Basis installation is not included

VALUE AND BENEFITS
- Accelerated and worry-free deployment of SAP security products
- Faster enablement of project team to move towards full blown project

SHORT DESCRIPTION
- This service consists of activities to conduct prototyping in an agile approach to ensure accelerated deployment of SAP security products in an innovative business scenario. Support for planning, safeguarding, technical and functional implementation of critical SAP security product components.
SAP Security Engagement
Project timeline [template]

**Preparation**
- Project Start
  - Jan 10
  - Workshop scheduled
  - Agenda agreed

**Roadmap Creation**
- Roadmap Planning
  - Mar 11
- Security Workshop
  - Feb 27
- Roadmap signed off
  - Mar 25

**Implementation**
- Workpackages start / end
  - Apr 15
  - May 01
  - May 10
  - May 31

**Verification**
- Implem. finalized
  - Jun 30
- Verification Session

**Security Workstreams**
- Project Management
  - Scoping Call
- Security Workflows & Implementation
  - Security Optimization Services for selected systems
  - Customer security situation and pain points
  - Presentation of SOS findings
  - Best practices for selected topics
  - Identification & agreement on workpackages

**Agenda**
- Workpackage 1
- Workpackage 2
- Workpackage 3
- Workpackage 4
- Workpackage 5

**Roadmap**
- Roadmap Planning
- Security Workshop
- Roadmap signed off

**Workpackage Completion**
- Workpackage 1
- Workpackage 2
- Workpackage 3
- Workpackage 4
- Workpackage 5

**Verification**
- Implem. finalized
- Verification Session

**Project Closing**
- Project Closing
- (bi-)weekly sync calls

**Security Verification Call or Meeting**
- Securing and documenting impact & achievements

© 2017 SAP SE or an SAP affiliate company. All rights reserved. | CUSTOMER
Thank you.

Contact information:
SAP CoE Security Services
securitycheck@sap.com
The SAP security portfolio

Secure access
- SAP Single Sign-On
- SAP Cloud Platform Identity Authentication

Secure code
- SAP NetWeaver AS, add-on for code vulnerability analysis

Detect attacks
- SAP Enterprise Threat Detection

Manage users and permissions
- SAP Identity Management
- SAP Access Control
- SAP Cloud Platform Identity Provisioning
- SAP Cloud Identity Access Governance
The SAP 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 Systems,
although the model also could be applied to non-SAP realms.
The “Security Compliance” layer focuses on the governance and regulations around the SAP systems, to which the SAP systems have to adhere themselves – e.g. general or IT-specific Security Policies, Audit requirements or Emergency Plans.

The three middle layers of the Secure Operations Map directly apply to the operation of SAP systems themselves. The further discussion of the Secure Operations Map will focus on these three layers.

The “Infrastructure Security” layer focuses on SAP-specific requirements towards the non-SAP technical environment – e.g. network, operating systems, non-SAP databases, clients.
### Security Maintenance of SAP Code

- SAP is continuously doing a high investment to develop and deliver secure code to its customers. Nevertheless, security updates of already delivered code are required regularly due to new attacks and new vulnerabilities.
- Customers need to establish a corresponding Security Maintenance process to ensure a regular and suitable consumption of these security updates – code corrections as well as configuration recommendations.

### Custom Code Security

- The first step in Custom Code Security is proper Custom Code Management: Unnecessary custom code should be removed, required custom code should be maintained in a proper Custom Code Lifecycle Management.
- Custom Code Lifecycle Management should cover the whole lifecycle from secure architecture & design via secure development – including but not restricted to the use of code security scanners – up to secure deployment, security maintenance and finally custom code retirement.
Secure Configuration
– Secure Configuration foremost deals with suitable secure settings of relevant system parameters and other configuration settings. It also includes activation of security features and functionalities, which may be switched off initially for backward compatibility and migration purposes.

Communication Security
– This part deals with the security of communication connections – from connection lifecycle management via proper management of communication users and authorizations up to encryption of communication lines and the corresponding cryptographic key management.

Data Security
– Data Security deals with the security of data at rest – change and read access control and logging, purpose-driven encryption of sensitive or all data and additional protection mechanisms like data masking.
Secure Operation

Users and Authorizations
- This is often the most well-known area of operational security, since operation of a system does not work without. It includes the lifecycle management of users accounts in systems and landscapes, proper assignment, maintenance and revocation of authorizations and control of compliance and segregation of duties (SoD)

Authentication and Single Sign-On
- Authentication deals with the verification of the true identity of a claimed user. It may be as simple as a password, may include multi-factor mechanisms and may also deal with trusted system connections in which one systems relies on the correct authentication by another system.
- Single Sign-On establishes an infrastructure, in which a user authenticates himself once in a landscape to then get access to several systems without the need for repeated additional authentication.
Support Security
- The topic area of “Support Security” does not only deal with external support – as e.g. provided by SAP – but also includes internal support teams. Whoever is providing support often needs extended access and authorizations to be able to help. Such extended rights should be tightly controlled and properly maintained. Only such rights should be permanently assigned which are required on a regular basis. Others should be only assigned when needed, e.g. via an emergency process or user. Support activities should also be monitored and controlled to ensure security by limitation to the real need.

Security Review and Monitoring
- With todays powerfull attacks and complex landscapes, proactive security is absolutely required but not sufficient. It needs to be enhanced by reactive security mechanisms, which are able to identify security weaknesses and breaches and thus allow to properly counter them. This includes review and validation activities as well as life monitoring of system operations and triggering appropriate countermeasures in case of an attack or some suspicious system behaviour.
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.
How to use the Secure Operations Map

- Therefore use the Secure Operations Map as a structure to informally identify areas and topics which are most important to address.

- Do not try to cover at once every area in all details.

- Revisit security on a regular (e.g. yearly) basis. New functionality and new technologies require new security measures. New attack patterns arise and need to be countered.