Secure Operations Map v3
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 Systems,
although the model also could be applied to non-SAP realms.
The “Environment” layer looks at the non-SAP technical environment of SAP cloud offerings, solutions and systems.

- **Network Security**
  It is important to have additional protection and monitoring mechanisms embedded into the underlying network infrastructure. Potential attacks need to be countered already through zoning concepts and network components like routers, firewalls or web application filters. Security-critical activities need to be monitored and countered by intrusion detection and prevention systems.

  Note that communication security measures in SAP offerings and solutions as well as SAP infrastructure components like SAProuter or SAP Cloud Connector are not part of this block. They are handled in “Security Hardening” (e.g. SAP Cloud Connector, SAProuter), “Authentication & Single Sign-On” (e.g. RFC Gateway, SNC, TLS) or “Roles & Authorizations”.

- **Operating System & Database Security**
  When OS and DB are insufficiently configured or users are able to bypass access controls at that level, the protection of applications running on top is at risk. Corresponding security controls in focus include file system level permissions, database user security, tenant separation or data-at-rest encryption methods.

  Note that databases from SAP are not part of this building block. They are addressed as specific projections on the Secure Operations Map, as several buildings apply with more details and SAP-specific content.

- **Client Security**
  Adversaries may attack client systems to get an entry point, inject bogus data in the traffic or subject the client to weird behavior, if not properly protected. This building block is about client side controls such as secure maintenance, configuration, control and monitoring of the client or execution rules for browsers.

  SAP clients like SAPGUI or SAP Business Client are not considered here but in the “Security Hardening” building block.
The “System” layer addresses the SAP platform layer which provides the foundation for all applications operated upon it. The integrity and robustness of this platform is key to ensure that application layer controls (e.g. the authorization systems) cannot be circumvented by lower level vulnerabilities (e.g. SQL injections made possible via insecure code).

- **Security Hardening**
  - Security Hardening foremost deals with suitable secure settings of relevant system parameters and other configurations. It also includes activation of security features and functionalities, which may be switched off initially for backward compatibility and migration purposes or which need specific setup and configuration (e.g. UCON).
  - It also includes hardening of SAP frontend components like SAPGUI or SAP Business Client and of SAP infrastructure components like SAProuter or SAP Cloud Connector.

- **Secure SAP Code**
  - SAP is continuously doing a high investment to develop and deliver secure code to its customers. Nevertheless, security updates for already delivered code are required regularly due to new attacks and newly identified vulnerabilities. SAP provides these security updates to its customers via Support Packages / Releases and via SAP Security Notes – published monthly on the SAP Security Patch Day.
  - Customers need to establish a corresponding Security Maintenance process to ensure a regular and suitable consumption of these security updates.
Security Monitoring & Forensics

With today's powerful 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 of appropriate countermeasures in case of an attack or suspicious system behaviors.

Logs and support are also required for forensics in retrospect of identified or suspected attacks. Also this needs preparation. If one only starts to look for evidence, when something seems to have happened, it may be too late to activate what would have been required to have this evidence.
The “Application” layer is about controls that are available in SAP standard applications and non-standard applications built by customers. Here, protective measures are discussed on users and privileges level as well as proper application design.

- **User & Identity Management**
  - This building block includes the lifecycle management of user accounts in systems and landscapes, proper provisioning, maintenance and revocation, including the approval, assignment and revocation of authorizations to/from specific users. Technical and emergency users are handled here as well as the topic of federation in hybrid environments.
  - Authorization design, role building and handling of Segregation of Duties are not handled here but in “Roles & Authorizations”.

- **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.
  - As communication security mechanisms like TLS for http-based connections or SNC for RFC connections support the authentic communication between systems and with clients, these mechanisms are included here as well.
▪ **Roles & Authorizations**
  ▪ This building block is about everything around roles and authorizations, including the proper definition, distribution and maintenance of authorizations as well as the alignment and combination of roles to business roles across systems in hybrid landscapes. Control of compliance and Segregation of Duties is also covered here.
  ▪ The assignment and revocation of roles to/for specific users is not handled here but in “User & Identity Management”.

▪ **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.
The “Processes” layer extends the pure security view with compliance aspects. While security focuses on operating robust SAP applications preventing intentional and unintentional malfunctions and compromise of confidentiality, regulatory compliance deals with the correct behavior of applications with regards to policies and legal demands coming from the various jurisdictions SAP systems are operated in.

- **Regulatory Process Compliance**
  In this building block, application functions are considered for their potential capabilities to significantly violate legal requirements when not used properly. Additional controls are then investigated that help keep the risk of such violations under control – prominent examples are mechanisms such as double invoice checks or special tax statement control. Typical regulation that is addressed by such procedures is HIPAA, Basel II+III or SoX, just to name a few.

- **Data Privacy & Protection**
  The topics in this building block focus on proper handling and protection mechanisms applicable directly to data belonging to individuals that are specifically protected by newer DPP legislation such as the European GDPR and similar requirements that demand capabilities such as blocking & deletion, consent management, right of access and validation etc.

  Even though such mechanisms are not solely related to DPP demands, this building block also includes strong confidentiality measures like field tokenizing or encryption at rest.

- **Audit & Fraud Management**
  While regulation must be followed for legal reasons, company often require additional capabilities to detect fraudulent behavior and make sure the controls in place are working effectively. This building block discusses solutions that allow auditing and fraud detection to run smoothly and provide correct data on the covered applications.
Similar to the “Environment” layer, this “Organization” layer is also important to set the environment for SAP systems and SAP cloud solutions. It sets the stage and gives needs and requirements as input to be considered.

- **Awareness**
  General security awareness is an important pre-condition to achieve security. Not everyone has to be a security expert – but everyone needs to contribute on his part and also needs to identify when security expertise should be called. Ignoring or even countering or circumventing security regulations and mechanisms can endanger a whole landscape. “Awareness” thus also is directly linked to user-friendliness and ease of handling of any security mechanisms or configuration.

- **Security Governance**
  Security Governance addresses everything regarding general organization, procedures and regulations including those, which may directly or indirectly impact the setup, configuration, integration and operation of SAP cloud solutions, systems and landscapes.

- **Risk Management**
  This comprises all elements on identifying, handling, mitigating and resolving risks including services or SAP solutions in this area.
Projections in the Secure Operations Map

There are some topic areas which provide like a third dimension to the Secure Operations Map since they give a specific view onto several blocks.

The following projections are currently explicitly identified:

- SAP HANA
- Service Providers & Hyperscaler

Currently only block selections in the map are shown.
## Secure Operations Map Projection – blocks with specific information for SAP HANA

<table>
<thead>
<tr>
<th>Organization</th>
<th>Processes</th>
<th>Application</th>
<th>System</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness</td>
<td>Regulatory Process</td>
<td>User &amp; Identity Management</td>
<td>Security Hardening</td>
<td>Network Security</td>
</tr>
<tr>
<td></td>
<td>Compliance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Management</td>
<td>Audit &amp; Fraud Management</td>
<td>Roles &amp; Authorizations</td>
<td></td>
<td>Client Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Secure Operations Map Projection – blocks with specific information for Service Providers & Hyperscalers

<table>
<thead>
<tr>
<th>Organization</th>
<th>Processes</th>
<th>Application</th>
<th>System</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness</td>
<td>Regulatory Process Compliance</td>
<td>User &amp; Identity Management</td>
<td>Security Hardening</td>
<td>Network Security</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Audit &amp; Fraud Management</td>
<td>Roles &amp; Authorizations</td>
<td>Security Monitoring &amp; Forensics</td>
<td>Client Security</td>
</tr>
</tbody>
</table>
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.
Contact information:

SAP CoE Security Services
securitycheck@sap.com
List of Abbreviations

DB    Database
DPP   Data Privacy and Protection
GDPR  General Data Protection Regulation
HIPAA Health Insurance Portability and Accountability Act
OS    Operating System
RFC   Remote Function Call
SNC   Secure Network Communication
SoD   Segregation of Duties
SoX   Sarbanes-Oxley Act
SSO   Single Sign-On
TLS   Transport Layer Security
UCON  Unified Connectivity