Compliance & SAP Security

Secure SAP applications based on state-of-the-art user & system concepts
Secure IT systems and secure data are a must for the operation of any business-critical application. This is no more apparent than in the news on hacker attacks, data theft, or unauthorized disclosure of sensitive data due to inadequate access concepts.

Typically, IT security projects concentrate on PC software and networks. SAP is considered a stable backend application with its systems safely located in the data center and the user rights set up according to the classic SAP authorization concepts.

This approach, however, is not without shortcomings because it fails to acknowledge that SAP is a dynamic system: Users enter or leave the company, business processes are adopted, and code is customized. Considering the sensitivity of critical business data like payrolls, orders or production data, backdoors or fraud within the system has serious consequences. And so it is time to think about security!

More than ever, it is important to have a comprehensive and coherent security concept. Only the combination of the secure operation of SAP components with compliant access concepts mitigates risks and gives decision makers the security they need. Our consulting portfolio helps you implement SAP landscapes that comply with audit trail requirements, ease the burden on your IT staff, and protect your enterprise. Get maximum IT security with minimal cost and risk!
Why REALTECH?

REALTECH customers rely on our many years of expertise in Compliance & SAP Security, which has been repeatedly recognized by SAP with numerous Special Expertise Partnerships (SEP). We know how to handle regulatory compliance with the Federal Data Protection Act, COBIT, GoBS, EuroSOX, SOX, etc.

The sheer number of applications involved in SAP access and authorization projects make them very complex. This complexity is a result of the inclusion of necessary interfaces from within SAP and the integration with existing directory services (e.g. MS Active Directory, Novell eDirectory or OpenLDAP).

For this reason we have developed a comprehensive consulting approach:

“We combine our experience and technological expertise with your in-depth knowledge of your applications and processes.”

Compliance & SAP Security projects require an end-to-end overview of your users’ working environment. The combination and systematic application of knowledge will make your project a joint success. Therefore, we rely on a team of experts who can effectively navigate a complex (IT) environment.

Our comprehensive set of security measures includes:

- Authorization Concepts
- User Lifecycle Management
- Accessibility & Single Sign-On
- Technical Security
- Vulnerability Detection
- Fraud Detection

Increase value and minimize risks

Virtually every department and individual within the company benefits from our consulting services:

Management:
Data security and risk minimization through access concepts with complete audit trails.

Business departments:
Better process quality through defined access authorizations based on secure programs.

Users:
Easier access to applications using the required access rights to increase acceptance.

IT organization:
Benefits from secure applications and processes to become a business enabler. Also, the IT staff can control the quality of code programming, which is often changed by external partners.
SAP audits and authorization concepts with complete audit trails

The fulfillment of legal requirements and compliance with international guidelines and company policies are the key to successful SAP audits. This can be achieved with future-proof authorization concepts that avoid conflicts in the segregation of duties (SoD) and ensure traceability.

These are the key questions:

- How well prepared are you for an SAP audit?
- Do you have the understanding and expertise needed to work with auditors in order to move smoothly through the process?
- How secure and future-proof is the existing authorization concept?
- Do users have the exact authorizations they require, not more or less?
- How are the activities surrounding the assignment of authorizations documented?
- What access measures are established to deal with emergencies?

<table>
<thead>
<tr>
<th>What can be achieved:</th>
<th>Our consulting services:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Cut costs in the preparation and conduct of SAP audits.</td>
<td>- Preparation of SAP audits (audit self check).</td>
</tr>
<tr>
<td>- Minimize the findings of SAP audits through the implementation of authorization concepts that meet today’s requirements.</td>
<td>- Assistance in conducting and following up on SAP audits.</td>
</tr>
<tr>
<td>- Avoid conflicts in the segregation of duties and introduce mitigating controls.</td>
<td>- Creation and implementation of authorization concepts for your SAP applications that provide complete audit trails.</td>
</tr>
<tr>
<td>- Ensure traceability of all activities surrounding the management of authorizations.</td>
<td>- Support in the selection and implementation of tools (e.g. SAP Business Objects Access Control) needed to ensure fulfillment of compliance requirements and to review SoD conflicts.</td>
</tr>
<tr>
<td>- Establish emergency concepts with complete audit trails.</td>
<td>- Design and implementation of emergency user scenarios.</td>
</tr>
</tbody>
</table>
Employees typically hold several positions during their career within a company and each of them is associated with different roles. The right User Lifecycle Management strategy ensures that employees always have the appropriate authorizations to access all of the IT applications they need to accomplish their work – not more or less. Companies need an intelligent Identity Management strategy to centralize and automate this process.

Transparent authorization workflows ensure traceability and the fulfillment of compliance requirements while mitigating security risks.

Additionally, user self-services speed up the processes associated with assigning roles and authorizations, thereby reducing costs and improving employee productivity.

### What can be achieved:
- Improve security with consistent and transparent user lifecycle processes.
- Provide all employees with the necessary access rights when they need them.
- Implement authorization workflows that comply with audit requirements by ensuring traceability.
- Improve security with custom-tailored role authorizations (principle of least privilege).

### Our consulting services:
- Analysis and assessment of your user lifecycle processes.
- Support in devising an appropriate Identity Management strategy.
- Tool selection support.
- Design and implementation of SAP NetWeaver Identity Management.
- Migration from SAP Central User Administration to SAP NetWeaver Identity Management.
- Definition and implementation of user self-services and authorization workflows.
**User-friendly security concepts**

Concepts that are tailored to today's requirements ensure that users can securely access all applications they need in their daily routines.

Single Sign-On mechanisms improve user acceptance and make it more convenient for them to access information scattered across different systems or resources without having to sign on over and over again using different authorization procedures. As a consequence, the service desk has to spend less time dealing with password management issues. In addition, the encryption of data traffic makes it impossible to intercept data transferred through the network (e.g. between SAP client and SAP server).

### What can be achieved:

- Comply with regulations by encrypting your data traffic.
- Reduce service desk request associated with password resets.
- Drive user productivity with single sign-on.
- Improve security by preventing password abuse.

### Our consulting services:

- Design and implementation of central user and authentication mechanisms using single sign-on.
- Support in the selection and implementation of suitable solutions, e.g. SAP NetWeaver Single Sign-On.

**Secure operation of SAP systems**

The secure operation of SAP applications is a prerequisite for the provision of applications that provide detailed audit trails. To achieve this, a number of questions have to be asked, starting with those addressing the secure configuration of all components involved and concluding with questions related to the maintenance and daily operation of your SAP systems that take into account the necessary security aspects.

### What can be achieved:

- Protect your data by implementing secure SAP systems and securing your databases and platforms.
- Operate and maintain your SAP systems taking security aspects into account.

### Our consulting services:

- Definition and implementation of security concepts for the SAP components you use.
- Protection of your SAP data with suitable hardware concepts and database implementations (encryption, backup/recovery concepts, availability).
Identify and eliminate vulnerabilities in SAP applications

All SAP applications are open source code systems that often require modifications or in-house developments (performed by service providers or internal employees). Therefore, unsafe ABAP code that is vulnerable to attacks such as ABAP/SQL/OS command injections or executions can easily get into your system.

<table>
<thead>
<tr>
<th>What can be achieved:</th>
<th>Our consulting services:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure your applications based on secure source code – the first step towards better security.</td>
<td>Tool-based analysis of your SAP ABAP in-house developments to identify vulnerabilities with REALTECH theGuard! Smart Change. theGuard! SmartChange Application Security &amp; Performance Scans are based on the Virtual Forge CodeProfiler technology, which is used by SAP itself to secure the company’s product development.</td>
</tr>
<tr>
<td>Elimination of ABAP vulnerabilities with improved code.</td>
<td>Support in making SAP ABAP and JAVA programming more secure.</td>
</tr>
</tbody>
</table>

SAP Fraud Detection

Regardless of how much effort you put into securing your SAP applications and all related SAP systems, someone might still get into your system and try to steal or manipulate your business data.

<table>
<thead>
<tr>
<th>What can be achieved:</th>
<th>Our consulting services:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect intrusions and data theft by analyzing SAP user input and interactions to discover suspicious transactions and access.</td>
<td>Installation and configuration of REALTECH’s Fraud Detection Solution for SAP.</td>
</tr>
<tr>
<td>Cover all interactions from SAP users (SAP Gui, portal, webdynpro, webservices, remote programs-rfc) to identify vulnerabilities.</td>
<td>Support in making your systems secure.</td>
</tr>
<tr>
<td>Enable flexible configuration and reporting by including only selected data in the analysis and benefit from the possibility to include non-SAP systems.</td>
<td></td>
</tr>
</tbody>
</table>
## Consulting Units

<table>
<thead>
<tr>
<th>IT Management Consulting</th>
<th>User Productivity &amp; Integration</th>
<th>Compliance &amp; SAP Security</th>
<th>IT Technology Consulting</th>
<th>SAP Solution Manager Consulting</th>
<th>IT Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Quickscan</td>
<td>Enterprise Portals</td>
<td>SAP Audits and Authorization Concepts with Audit Trails</td>
<td>Making the Most of New IT Technologies</td>
<td>Solution Manager Strategy</td>
<td>SAP Operations</td>
</tr>
<tr>
<td>IT Sourcing</td>
<td>Mobility Solutions for SAP</td>
<td>User Lifecycle Management / Identity Management</td>
<td>Upgrades</td>
<td>Implementation of All Solution Manager Scenarios</td>
<td>Flexible IT Services</td>
</tr>
<tr>
<td>Project &amp; Risk Management</td>
<td>Usability</td>
<td>User-Friendly Security Concepts</td>
<td>Migrations</td>
<td>Solution Manager Upgrade to 7.1</td>
<td>SAP Sourcing Consulting</td>
</tr>
<tr>
<td>Infrastructure Management</td>
<td>SAP Knowledge Warehouse</td>
<td>Secure Operation of SAP Systems</td>
<td>Virtualization</td>
<td>End-to-End Monitoring and Error Analysis</td>
<td>ITIL-Compliant Operations</td>
</tr>
<tr>
<td>Cloud Strategy</td>
<td>Custom Development</td>
<td>Identify &amp; Eliminate Vulnerabilities in In-House Developments</td>
<td>SAP HANA</td>
<td>Software Enhancements Timekeeping in Incident and Change Management</td>
<td>Operational Concepts and Strategies</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Digital Signatures &amp; Document Management With SAP Solution Manager</td>
<td>SAP HANA Operations</td>
</tr>
</tbody>
</table>

REALTECH Consulting GmbH
Industriestraße 39c
69190 Walldorf · Germany
Tel. +49.6227.837.0
Fax. +49.6227.837.837
customer-services@realtech.com
www.realtech.com