
SAP security solutions
Is your business protected?



SAP security overview



Background

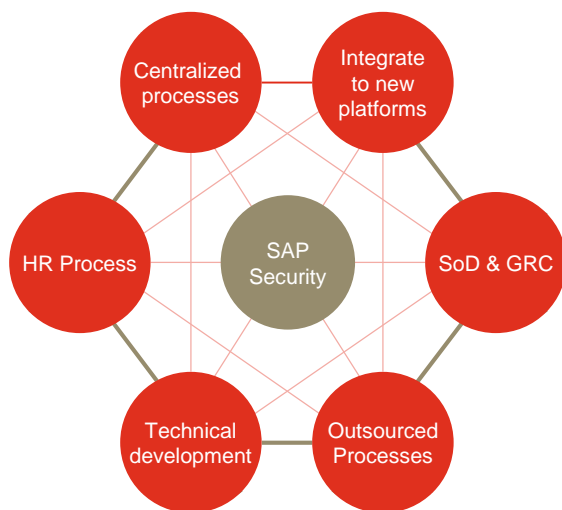
SAP Security is becoming more difficult to control due to a constantly evolving compliance landscape and increasingly complex business environments.

Restrictions required by legislation, upgrades to systems, centralization of functions within businesses, and continually changing role responsibilities increase the importance of having a well-designed security management process.

The increasing complexity of SAP's software applications, adds to the risk of security threats, with evolving technology, new functionality, and web-based solutions.

Ultimately how can you ensure that your users have the information they need in a timely manner yet comply with the challenges above in an efficient and optimal manner?

Opportunities and challenges



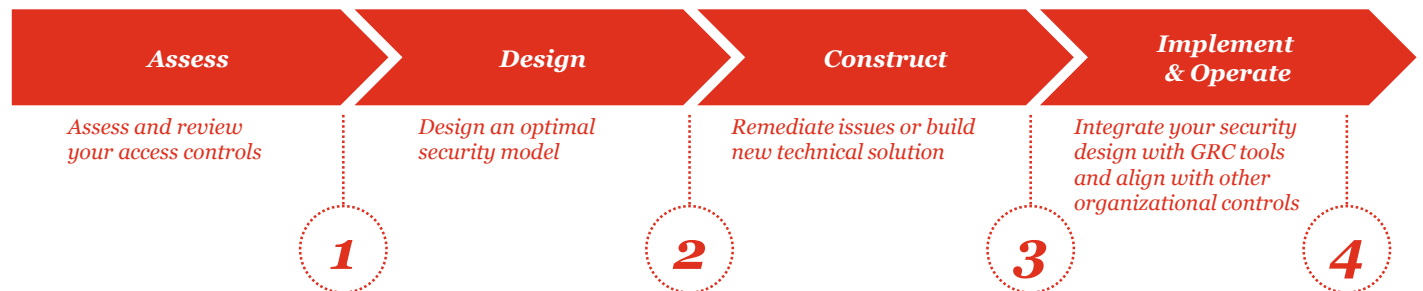
- Ensuring flexibility to accommodate organizational changes and underlying process variations
- Accommodating centralized functions within old security designs and processes
- Reducing the amount of time spent on technical administration and end-user security management by both IT and the wider business
- Integrating the SAP Security structure and controls into the day-to-day operations of the business
- Key enabler for leveraging GRC technologies
- Opportunities for delivering improvements and efficiencies through GRC or other tools
- Ensuring that the security controls are properly aligned with other configurable and manual controls in the SAP environment
- Remediating segregation of duty (SoD) issues in the most efficient manner
- Managing costs and commercial leakage from outsourced administrators
- Effectively transition to managing shared service center

Our approach

high-level overview

PwC Transform – Security Design and Remediation process						
Phases	Assess	Design	III. CONSTRUCT		IV. Implement Operate	
Task	Project Preparation	Design	Build	Test	Final Preparation	Go-Live & Support
Objective	The project is initiated and supporting infrastructure is established	Business Risks are Identified	Security requirements are translated	SOD Compliance	Deployment Package	Deployed Security
Deliverables	Project Plan	Business Risks	Rule set(s) Built	Finalized Initial Rule set(s)	End User Mapping	Cross-Application SOD Reports
	Systems, Business Processes, and Actions Analyses	Action Groupings	Updated Policies and Procedures	Rule set(s) Signoff	Security Admin Process	SOD Review and Action Plan
	Roles and Responsibilities	Risk Rankings	Tool Configured	Reports Material	Provisioning Process	Mitigated Conflicts
Interfaces						
Infrastructure						
ERP						

SAP security: Redesign to align



1 Assess and review access controls

During the assessment of the Security and SOD “as is” position we focus on the following areas:

- Assess and compare how your individual business units are adopting existing controls.
- Benchmark how your security issues measure against industry standards.
- Implement PwC’s User Activity Analysis tool to analyze your actual transactional usage.
- Map activity analysis output back to existing security design and pinpoint areas for design remediation.
- Map the Security Access controls design back to SAP Security governance design.

2 Design an optimal security operating model

Building on the assessment work, we can assist in your effort to transition to an optimized security design:

- Provide the strategy and approach to deliver a security model, where compliance objectives are embedded into the design.
- Develop a design that is flexible enough to accommodate likely changes to the organizational structure while integrating existing business controls.
- Devise a security blueprint that maximizes the sustainability of the future security model.
- Address root causes of specific control and access issues at the design phase to ensure a consistent and efficient “clean up” effort.
- Design and develop a process for using accelerators like SAP GRC in security build and maintenance phases to maximize efficiency.
- Underpin technical aspects of the design with a robust SAP security governance framework.

3

Remediate or rebuild

We can assist in managing the integration of the risk and controls elements of the security design and build throughout the life cycle of the engagement, from remediation of existing issues, to a complete rebuild of the technical platform.

The work focuses on ensuring your strategy design and build are aligned to the long-term organizational requirements.

We provide this service by:

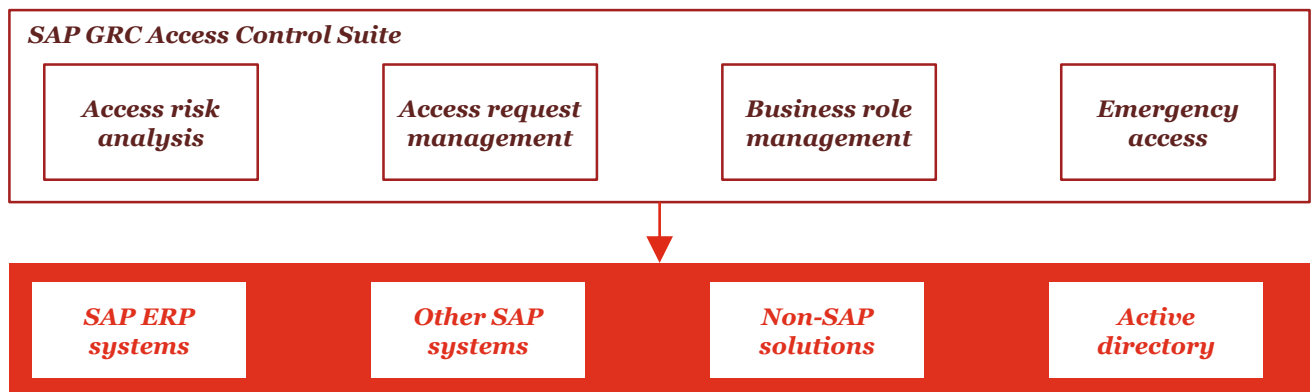
- Utilizing accelerators in the build phases to expedite technical role build activities
- Following a best practice iterative design/build/re-analyze process to ensure that technical solution is fit for purpose and SoD compliant
- Implementing PwC's enabler technology for rebuild activities
- Ensuring that security build at the template and local levels doesn't deviate from the overall strategy, reducing the risk of your security design regressing back to being localized or fragmented

4

Integrate your security design with GRC tools and organizational controls

PwC can work with you to:

- Utilize GRC technology for structured, compliant, and accelerated role design and build.
- Integrate with GRC tools for SoD compliance at a technical role and user provisioning level.
- Integrate the SAP security model with IDM tools to provide single sign-on capabilities and controls.
- Provide assistance to design an operating model that fully utilizes the controls potential available in GRC tools.



Benefits realized by our clients:

- Significantly improved governance and management of access risks
- Business-owned and standardized access management processes
- Reduced business time spent on access reviews by 60%
- Greater transparency into who has what access
- Reduced complexity of roles leads to sustainable, lower-cost SAP security processes
- Significant increase in business user support capabilities

Client citation leading automobile manufacturer

Background

This client was struggling to meet service level agreements related to SAP provisioning and user maintenance. Although the initial implementation of SAP GRC Access Controls suite was complete, the organization was using only a small subset of the suite's capabilities.



The PwC solution

The first phase of this project focused on assessing the current state and designing of the future state. In our design of the future state, we included the full deployment of the SAP GRC Access Controls suite to simplify and automate the user provisioning processes, while remaining compliant. We worked with the client to design and implement a new SAP security design following our tier 4 methodology. The implementation of the new SAP security design helped this client reduce the number of roles in the SAP environment, which, combined with the SAP GRC Access Controls application, facilitated the overall user provisioning processes.

What has the client achieved?

After the completion of the SAP security design and implementation of the SAP GRC Access Controls applications, this client was able to realize the following benefits:

- 75% reduction of SAP security roles in the SAP production environment
- 99% reduction of transaction code duplication in SAP security roles
- 0 SAP security roles with inherent segregation of duties conflicts
- Reduced user provisioning time from 21+ days to 2.3 days (average)

