

SAP Security Remediation: Three Steps for Success Using SAP GRC

All companies need strong application security environments as part of a successful overall risk management strategy. Strong risk-oriented security environments rely on internal application security features, drawing upon entity and process controls only as a last resort when mitigating security risk exposures. Many companies have turned to governance, risk and compliance (GRC) software to help them remediate and manage their complex security environments. This paper discusses one such endeavor using SAP's GRC Access Control suite.*

Synopsis

Remediation Approach	Key Lessons Learned
<p>Step 1 – Gain Visibility Into SAP</p> <ul style="list-style-type: none"> Determine the state of your security risks within SAP <p>Step 2 – Form and Execute a Plan</p> <p>Build a remediation plan by:</p> <ul style="list-style-type: none"> Measuring exposures Determining project objectives and requirements Prioritizing and executing remediation <p>Step 3 – Enable Provisioning and Continuous Monitoring</p> <ul style="list-style-type: none"> Implement procedures to protect your SAP environment against reintroduction of exposures 	<p>Project Management</p> <ul style="list-style-type: none"> Treat security remediation projects as a system implementation Obtain stakeholder buy-in early, including external audit's input Prioritize remediation activities to achieve “quick wins” <p>Software Configuration</p> <ul style="list-style-type: none"> Tailor Compliance Calibrator rule sets for your business Use Firefighter for business process-sensitive privileges Install software patches before implementing GRC tools

Defining Concepts: Security Areas Within SAP

SAP has several layers of security or privileges: profiles, roles, transaction codes, authorization objects, fields and infotypes. From a compliance perspective, risks are analyzed across each of these layers. Risks typically addressed include Segregation of Duties (SoD), Sensitive Access (SA) and User Provisioning. An SoD risk is present when an employee possesses two incompatible functions, such as “creation of vendors” and “processing of invoices.” SA risks occur when users have critical privileges such as the maintenance of bank details within a vendor master record. User provisioning involves the granting, changing and removing of employee privileges to a system.

Distilling Complexity: A Three-Step Remediation Approach

Several approaches may be used to remediate security exposures. Protiviti has found that the following approach effectively integrates traditional remediation steps with automation provided by SAP's GRC Access Control suite, quickly yielding substantial results.

Step 1 – Gain Visibility Into SAP

First, companies need to gain visibility into their security environment within SAP. This process involves running queries within SAP or using commercially available tools to extract and compile the data. However, because of SAP's multiple layers of security, these manual techniques create numerous false positives, reporting exposures that do not truly exist. SoD Assessment tools such as SAP's Compliance Calibrator automate data extraction. Configured to scrutinize all layers of security, Compliance Calibrator significantly reduces false positives (though some may still occur).

*SAP Access Controls components have been recently renamed, although they are still commonly known by their old names. They are now called Risk Analysis and Remediation (formerly known as Compliance Calibrator and Risk Terminator), Superuser Privilege Management (formerly known as Firefighter), Compliant User Provisioning (formerly known as Access Enforcer) and Enterprise Role Management (formerly known as Role Expert).

Step 2 – Form and Execute a Plan

Once the data is obtained in Step 1, a plan may be built to address identified exposures. Key activities include:

Measure exposure: Results should be evaluated and quantified in terms of the number of potential security exposures. Known false positives should be removed, and the remaining issues should be assessed to determine root causes. Reducing false positives reported by a tool such as Compliance Calibrator entails refining the SA and SoD rule sets within the tool. Once rule sets are refined, Compliance Calibrator provides an insightful summary and detailed reporting that enables companies to focus their efforts on their greatest areas of risk.

Determine requirements: As part of any remediation effort, it is important to establish the goals of the project and determine what exposures and remediation techniques are acceptable to management. External audit may also provide valuable guidance as to what should be expected through remediation efforts. Project options for resolving security exposures should be considered in terms of cost vs. benefit so that the sponsors are able to make an informed decision as to how the project should proceed.

Prioritize and execute remediation: Once the exposures are quantified and requirements determined, a plan may be formed that prioritizes remediation efforts in terms of the greatest exposures combined with the cost/benefit of remediation activities. For example, removing “SAP_All” from user privileges may reduce SoD exposures exponentially without requiring much effort. After prioritizing remediation areas, the following activities may be undertaken:

- **Clean up** – Cleanup efforts primarily entail the removal of unnecessary access. Users often have SAP privileges that relate to a past project, not their current function. For example, a system administrator responsible for implementing the finance module during an implementation should be restricted to system administration functions after the application is implemented.
- **Assess and restrict sensitive access** – Business owners should determine who should have access to sensitive functions and data, such as banking information. If an analysis indicates that 20 people have access but only five need that access, the remaining 15 users should have the privilege removed. Conducting this analysis before focusing on SoD reduces the number of SoD conflicts up front. If it is determined that users should retain some sensitive access, SAP’s GRC component, Firefighter, may be considered to manage sensitive access. (Users with these privileges are often referred to as “super users” or “power users.”) Alternatively, a manual, or “library,” process of checking sensitive privileges in and out may be used.
- **Assess and restrict segregation of duties** – In this phase, companies may consider removing privileges from users or redesigning privileges and/or employee functions. If it is determined that several SAP privileges need to be redesigned, Role Expert is an effective tool to model and analyze privileges.
- **Apply mitigating controls** – Despite best efforts to remediate SA and SoD, security exposures will persist. SAP has over 500 automated controls that may be configured to mitigate remaining security exposures. In the past, several companies have documented these controls in Risk and Control Matrices, as well as Compliance Calibrator. SAP’s latest GRC solution, Process Controls, is designed to improve on those methods, helping companies centralize their compliance documentation and testing efforts.

Step 3 – Enable Provisioning and Continuous Monitoring

Once security is remediated, provisioning and continuous monitoring processes and procedures should be enabled. Periodic security reviews, which are necessary, may be facilitated with Compliance Calibrator. Utilization of sensitive access and its approvals should be reviewed, a process enabled by Firefighter and its associated logs. User provisioning, whether it entails granting, changing and/or removing access, should be established or enhanced depending on the circumstances.

SAP’s Access Enforcer can automate this process and prevent exposures from being introduced into a clean environment. Any changes to procedures should be documented, formalized and approved by appropriate management. Moreover, ownership must be defined for each step in provisioning and monitoring, as well as for GRC software maintenance and operation.

Case Study: Global Pharmaceutical Company

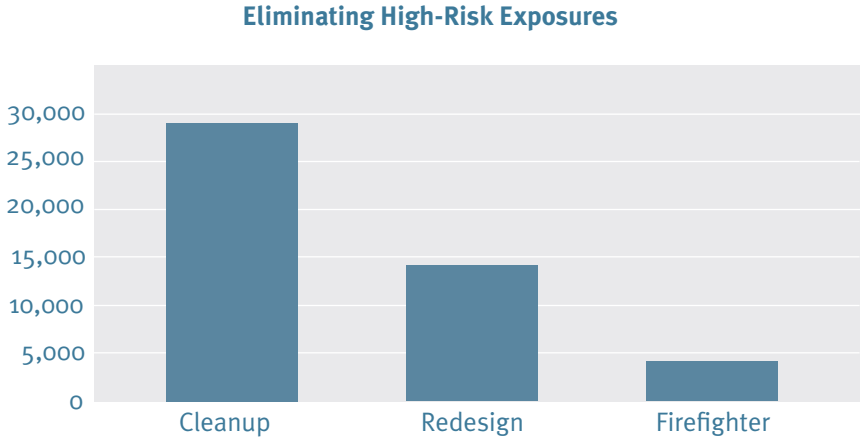
A global pharmaceutical company acquired a leading European generic drug manufacturer. The company’s internal audit team worked closely with Protiviti to conduct a “due diligence” security assessment of the acquisition’s SAP environments. Concurrently, the company acquired SAP’s GRC Access Control and Process Control solutions.

Remediation Assessment and Approach: Initial assessments quantified over 200,000 potential SoD exposures across three SAP instances and six countries. Given the nature of the exposures, the company’s finance, audit and IT departments partnered with Protiviti to form a steering committee and develop an action plan similar to the one described previously.

As the team gained more visibility into the SAP environments and measured the results, 50,000 exposures were classified as high risk and 40,000 as medium risk. The remainder were considered low risk based on the company’s business environment, industry benchmarks and external audit input.

Remediation Results and Lessons Learned: Within six months, about 60 percent (nearly 30,000) of the high-risk conflicts were eliminated through cleanup, 30 percent (nearly 15,000) through redesign, and the remaining 10 percent (about 5,000) with a Firefighter process. Medium-risk exposures were resolved in a similar manner, while low-risk exposures were mitigated by business process controls.

The chart below illustrates the number of high-risk exposures and how they were remediated.



Key lessons learned from the project included the following imperatives:

- Treat security remediation projects as system implementations that require executive sponsorship, change control (including unit testing and user acceptance testing), regular status meetings and training.
- Obtain stakeholder buy-in early, including external audit’s input. Stakeholders may include key leads from finance, operations, IT and audit functions.
- Prioritize remediation activities to achieve “quick wins” that build project momentum while maximizing your return on investment.
- Customize Compliance Calibrator rule sets to reflect your business environment.
- Use Firefighter for business process-sensitive privileges, not just for IT. Business functions that involve maintaining payroll or bank master data should be considered for Firefighter roles.
- Ensure that supporting systems have up-to-date software patches before implementing GRC tools and that your hardware and software meets minimum requirements suggested for GRC software. SAP provides a “Sizing Guide” document that provides guidance as to requirements for hardware and software needed for GRC software.

Summary

Security remediation projects can be large and complex undertakings. One key factor for success is the use of a proven method such as the three-step remediation approach described in this paper.

When implemented correctly, GRC solutions, such as SAP's Access Control suite, may enhance remediation efforts and reduce the time and costs required to complete the project.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting and internal audit firm composed of experts specializing in risk and advisory services. We help our clients solve problems in finance, operations, technology, litigation and GRC. Our highly trained, results-oriented professionals serve clients in the Americas, Asia-Pacific, Europe and the Middle East and provide a unique perspective on a wide range of critical business issues.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

For more information regarding our Enterprise Application Solutions (EAS) or the topics discussed in this white paper, please contact:

Paul Shultz
Managing Director, EAS
972.788.8521
paul.shultz@protiviti.com

Carol Raimo
Managing Director, EAS-SAP
212.603.8371
carol.raimo@protiviti.com

Cary Haggard
Director, EAS-SAP
212.399.8663
cary.haggard@protiviti.com

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.