Introduction

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.¹

Synopsis

Remediation Approach

<table>
<thead>
<tr>
<th>Step</th>
<th>Remediation Approach</th>
<th>Key Lessons Learned</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Gain Visibility Into SAP</td>
<td>Project Management</td>
</tr>
<tr>
<td></td>
<td>• Determine the state of your security risks within SAP</td>
<td>• Treat security remediation projects as a system implementation</td>
</tr>
<tr>
<td>02</td>
<td>Form and Execute a Plan</td>
<td>Software Configuration</td>
</tr>
<tr>
<td></td>
<td>• Measuring exposures</td>
<td>• Tailor Compliance Calibrator rule sets for your business</td>
</tr>
<tr>
<td></td>
<td>• Determining project objectives and requirements</td>
<td>• Use FireFighter for business process-sensitive privileges</td>
</tr>
<tr>
<td></td>
<td>• Prioritizing and executing remediation</td>
<td>• Install software patches before implementing GRC tools</td>
</tr>
<tr>
<td>03</td>
<td>Enable Provisioning and Continuous Monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Implement procedures to protect your SAP environment against reintroduction of exposures</td>
<td></td>
</tr>
</tbody>
</table>

¹ 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).
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.

For Users of SAP® S/4HANA

With SAP® S/4HANA, apart from the general role-based security at the application layer (SAP® S/4HANA), security may also have to be defined at the HANA database layer, as well as the presentation layer if the new user interface, Fiori, is being used.

If using SAP Fiori as the user interface in addition to or instead of using the traditional SAP GUI, users may no longer require access to back-end transaction codes and instead will use Fiori apps to access different functionalities within the SAP® S/4HANA system. The SAP® S/4HANA roles will then have to be designed to include the additional authorizations and mapping required to access the specific apps on the Fiori UI by the end users.

For SAP® S/4HANA, access to the HANA database will be required by any individual working within the HANA database (admins, data modelers, developers, support staff, etc.) or any end users reading data directly from the database. For users who need direct access to critical data in SAP HANA®, a privilege-based role design will be required to secure the data and restrict access based on the type of user accessing the database. All these additional checks will have an impact on the design of the risk ruleset.

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).
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 rulesets 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.

<table>
<thead>
<tr>
<th>Method</th>
<th>Exposures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cleanup</td>
<td>30,000</td>
</tr>
<tr>
<td>Redesign</td>
<td>25,000</td>
</tr>
<tr>
<td>FireFighter</td>
<td>20,000</td>
</tr>
<tr>
<td></td>
<td>15,000</td>
</tr>
<tr>
<td></td>
<td>10,000</td>
</tr>
<tr>
<td></td>
<td>5,000</td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

Eliminating High-Risk Exposures
Key lessons learned from the project included the following:

- 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 the return on investment.
- Customize Compliance Calibrator rulesets to reflect the 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 the hardware and software meet the minimum requirements suggested for GRC software. SAP provides a “sizing guide” document that offers guidance on requirements for hardware and software needed for GRC tools.

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 is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About Protiviti’s Enterprise Resource Planning and SAP Technology Practice

We partner with chief information officers, chief financial officers and other executives to ensure their organizations maximize the return on information systems investments while minimizing their risks. Using strong IT governance to ensure alignment with business strategies, we drive excellence though the IT infrastructure and into the supporting applications, data analytics and security. We also facilitate the selection and development of software, implement configurable controls on large ERP installations, implement GRC software applications, and manage implementation risk throughout.

Protiviti is a premier provider of SAP consulting solutions and a long-standing SAP Gold partner. Given our risk and compliance background, we are in a unique position to help companies identify, address and mitigate risks around S/4HANA projects. We bring:

- Optimized S/4HANA business process templates and experienced resources to facilitate solution design
- Automated tools to assess application security, automated controls and data risks
- Predefined library of process and IT controls to consider as part of the S/4HANA solution design
- Expertise in GRC solution implementation related to S/4HANA’s impact on SoD rules and automated controls
- Proven methodology and approach to assess project readiness and risks throughout the implementation lifecycle

Contacts

John Harrison  
+1.713.314.4996  
john.harrison@protiviti.com

Carol Raimo  
+1.212.603.8371  
carol.raimo@protiviti.com

Aric Quinones  
+1.404.240.8376  
aric.quinones@protiviti.com

Thomas Luick  
+1.312.476.6342  
thomas.luick@protiviti.com

Ronan O’Shea  
+1.415.402.3639  
ronan.oshea@protiviti.com

Steve Cabello  
+1.213.327.1470  
steve.cabello@protiviti.com

Siamak Razmazma  
+1.408.808.3258  
siamak.razmazma@protiviti.com

John Livingood  
+1.415.402.3682  
john.livingood@protiviti.com

Toni Lastella  
+1.212.399.8602  
toni.lastella@protiviti.com

Martin Nash  
+1.813.348.3374  
martin.nash@protiviti.com

Kevin Erlandson  
+1.415.402.3682  
kevin.erlandson@protiviti.com

Mithilesh Kotwal  
+1.312.364.4912  
mithilesh.kotwal@protiviti.com

Kyle Wechsler  
+1.212.708.6369  
kyle.wechsler@protiviti.com