Benefits and Challenges of Implementing Cross-System SoD Monitoring Using SAP GRC

A leading development bank with operations across multiple countries had a mandate to improve the lives of its customers. An exercise was initiated to identify the extent of segregation of duties (SoD) conflicts for the same users of different applications and systems across the bank, the embedded risk those conflicts may pose to financial reporting, and ways and means to mitigate the risk. One option was procuring and implementing third-party systems that can integrate with SAP or non-SAP enterprise resource planning (ERP) systems; however, the cost factor made it prohibitive. The next best option was to implement SAP governance, risk and compliance (GRC); however, there was no internal expertise around SAP GRC to move forward in such a complex and uncharted territory.

Since its introduction, SAP GRC has continually been at the forefront of technology solutions for SoD analysis of roles and users. The primary target of such analysis is an SAP system such as ERP central component (ECC) or supplier relationship management (SRM). This is because of the underlying capabilities of a rule set, which provides a predefined set of rules to determine what constitutes an SoD conflict. The rule set includes access risk, which is made up of two conflicting functions. Each of these functions contains an associated action, underlying permissions and their field values. In fact, the creation or maintenance of such SoD rules makes SAP GRC a system of choice for applications that identify and monitor for SoD conflicts.

SAP GRC is useful for monitoring and controlling SoD conflicts for customers with large user bases. It is able to identify and mitigate SoD risk with its flexibility to define customer-specific SoD rules, either by way of modifying SAP rules or developing specific rules for individual clients' business processes, defined business or operational risk, and associated mitigation controls.

Hidden inside SAP's own documentation and its support portal Service Market Place is a powerful capability: SAP GRC has a built-in mechanism designed to monitor SoD conflicts for systems not connected to SAP. This capability can be leveraged to deploy organizationwide systems and processes to identify, mitigate and monitor cross-system SoD conflicts involving SAP ECC and SRM with other non-SAP systems—as is the case in the example of a development bank, which will be examined here.

This case study specifically covers the implementation of cross-system SoD analysis across heterogeneous systems, such as SAP, and other non-SAP systems, such as treasury management (TMS), loan funds management (LFM), currency chest management (quantum), and the Society for Worldwide Interbank Financial Telecommunications (SWIFT), a global payment system. Currently, the bank's operational risk management function monitors business risk from a fraud or manipulation perspective based on access all users have across different systems. The function also monitors

SNEHAL D. PANDYA | CRISC, CISM

Is a director of consulting at ERP Infosys Inc. and has more than two decades of experience in SAP consulting around security, authorizations, access control, and governance, risk and compliance (GRC), focusing on SAP GRC, and segregation of duties and risk management. He has worked with many large SAP implementations in organizations across industry verticals such as telecommunications, banking, finance, pharmaceutical, engineering, energy and government.

cross-system access risk when it affects multiple systems to ensure that appropriate controls are in place to mitigate risk. This is the primary objective of implementing the solution described in this case study. It took approximately 10 months' worth of effort to fully implement the solution.

Project Scope

A project team consisting of a risk management manager and analyst, a SAP security and GRC expert, and financial application access administrators at the bank evaluated various technology options to address the stated objectives of implementing SoD monitoring across different systems, including:

1. Procuring and implementing third-party software that would allow full integration between SAP and non-SAP systems
2. Leveraging existing systems and exploring the possibility of implementing the cross-system monitoring of SoD using SAP GRC

A cost-benefit analysis determined that one of the most important factors that had a direct impact on the overall cost of assessing risk related to SoD conflicts was evaluating the SoD risk manually. This was done by using reports of user access from all the financial application systems and then comparing each individual user's access manually to determine if it was creating any SoD conflict. Since this was all expected to be manual, the other factors that would have impacted the cost indirectly would have been related to the accuracy of the analysis.

Once the analysis was completed, the second option was selected.

The scope of the project included:

- Configuring cross-system connectors in SAP GRC with LFM, quantum, TMS and SWIFT systems and other parameters related to the cross-system SoD requirements
- Creating an SoD rule set for non-SAP systems
- Defining the extraction, transformation and loading (ETL) mechanism of user and permissions data from in-scope systems
- Developing an Advanced Business Application Programming (ABAP) program in SAP GRC for data loading
- Designing and testing the solution
- Defining the operational process and sustainment documentation

These steps were necessary to successfully implement the proposed design of the system. The scope was validated by the technical team for ensuring the implementation requirements.

The cost of external third-party software to manage cross-system SoD conflict is a significant factor in the overall budget to manage access risk.

Benefits of Implementing Cross-System SoD Monitoring

There are several benefits of creating organizationwide systems and processes to identify, mitigate and monitor SoD risk across different systems, including:

- **No cost of third-party software to manage cross-system SoD conflicts**—The cost of external third-party software to manage cross-system SoD conflict is a significant factor in the overall budget to manage access risk. In this example, the bank was able to significantly reduce the cost of compliance and manage access risk across the landscape of various heterogeneous systems because it did not use a third-party solution. Additional dependent costs that were avoided were related to infrastructure, dedicated resources, team member training and other significant sustainment costs.
- **Cross-system SoD risk monitoring**—Monitoring of cross-system SoD conflicts across different non-SAP systems was important to the client organization—a development bank—because its banks are spread across multiple locations globally and operate in different time zones.
- **Compliance with enterprise access control policies**—The technical solution aids in compliance with some enterprise access control policies, especially those related to granting SoD free access to all users.

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

- **Reduced cost of access control compliance**—The cost of managing access control compliance was significantly reduced, which improved efficiency within the overall compliance initiatives as SoD reports across different systems for the same user were created. Previously, the monitoring was completely manual, which was cumbersome, inefficient and prone to human error.

A custom program is required to load the files into appropriate GRC system folders so that they are accessible when updating SAP GRC-specific data tables in the future.

Overcoming the Challenges

Before the start of the project, the project team brainstormed to find ways to address the challenges and design sustainable processes. The project faced numerous challenges including unavailability of a cross-system SoD rule set and lack of an automated system to manage the ETL of the user and permissions data on SAP GRC.

Challenge 1: Unavailability of a Cross-System SoD Rule Set

By default, SAP GRC comes with prepopulated SoD rules consisting of actions and permissions for all SoD combinations—the SAP SoD Rule Set. However, this prepopulated SAP SoD rule set available in SAP GRC is limited to SAP financial and procurement systems. If there is a requirement of using SAP GRC for non-SAP systems, the project team is then faced with building a set of rules for actions and permissions across different systems.

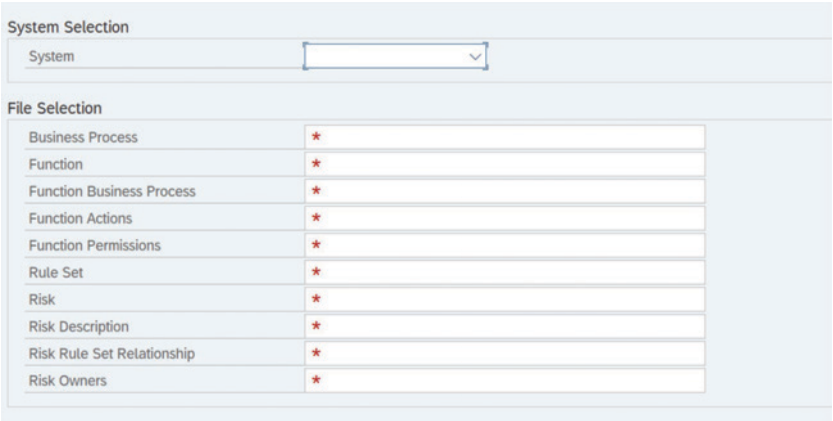
SAP GRC's delivered rule set for a SAP financial and procurement system can be used as a guide for all non-SAP systems and can help address the rule set building challenge. Because rule set building is not a recurring exercise, for this project significant efforts were expended during the design phase to create the rule set. The client had an existing change management process; therefore, it could be leveraged for making changes to the rule set once defined and in production. The SAP GRC rule set was downloaded using the program GRAC_DOWNLOAD_RULES and the format was used to populate the various rule set files (**figure 1**). In the project scope, the team decided to use a permission-only rule set and no actions. Under this rule set, SAP allows rules to be defined involving various permissions associated with system access. Accordingly, all the function actions and function permissions files were populated with permission-only functions and were required to be defined as ^!ZZZZ (Online System Support [OSS] as per SAP GRC requirements.[1, 2]

The approach to building a custom rule set includes:

1. As required in SAP GRC, any rule set needs to have actions and associated permissions. Accordingly, a full inventory of permissions was documented for each system in the project.
2. Once the list of all possible permissions is created, each distinct function in a system is documented. Examples of functions include processing a payment and creating a vendor.
3. The final step in the process is building a master list of all access risk based on possible combinations of functions. For example, SoD access risk can be processing a fraudulent payment, which consists of two conflicting functions: creating a vendor and processing a payment.

FIGURE 1

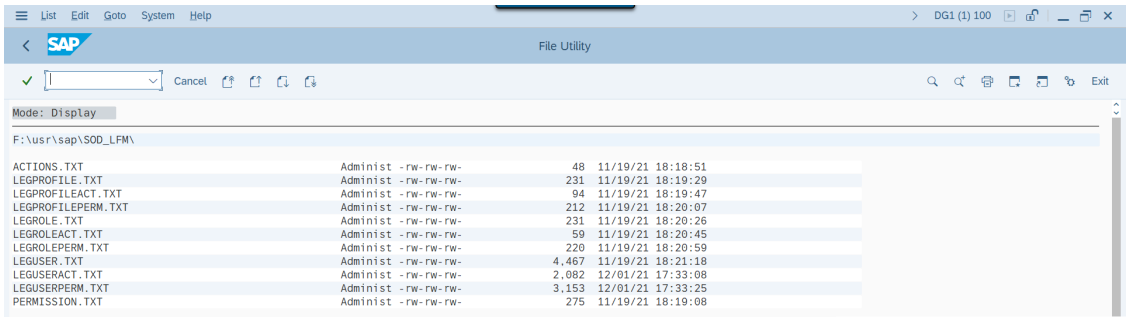
Files Required to be Populated for a Custom Rule Set of the Non-SAP System



Source: SAP Community Blog, "Download, Modify and Upload the Access Risk Analysis Rule Set in SAP Access Control 10.x.," 21 April 2014, *https://blogs.sap.com/2014/04/21/download-modify-and-upload-the-access-risk-analysis-rule-set-in-sap-access-control-10x/.* Reprinted with permission.

FIGURE 2

Permissions Files to Be Loaded Into SAP GRC System



Challenge 2: No Automated System to Manage the ETL Data Into SAP GRC

Solving the previous challenge involved managing the interface with standard text file transfer (upload and download) functionality available in SAP GRC. This strategy involved creating all the available user and permissions data in text file formats and uploading them to SAP GRC using standard functionality and the transaction code FILE. The extraction and transformation process involved manually creating all the files in the required format per SAP GRC. In total, 11 files were created and uploaded to SAP GRC (**figure 2**).

As part of data loading, the project team decided to develop a custom program to load the files in the specific directories (**figure 3**). A custom program is required to load the files into appropriate GRC system folders so that they are accessible when updating SAP GRC-specific data tables in the future.

Challenge 3: Design and Deployment Issues

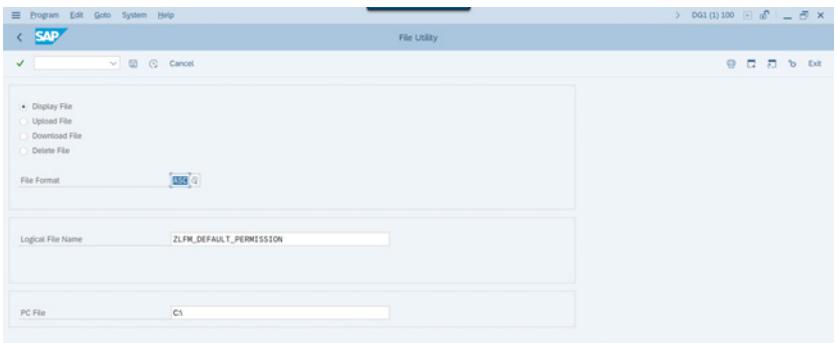
The project team faced some unexpected issues during the design prototype testing, including:

- **Inconsistent user IDs**—Some of the user IDs defined on the non-SAP system were not defined as per enterprise unique user ID requirements or were not based on the active directory. This resulted in some user IDs not being recognized during the loading phase and led to data loading errors. This was corrected manually in the data load file and reuploaded. To avoid this issue in the future, the appropriate project support teams should be notified.
- **Incorrect entries during data transformation**—The data transformation stage was manual and resulted in some incorrect entries in the data load files. The errors were corrected as each issue was identified.
- **Undocumented configuration requirements**—Some configuration requirements, especially for configuring the connector group for non-SAP systems, required the connection type to remain blank. This was not mentioned in any configuration documents, so the project team raised the issue via OSS message to SAP support, and the solution was provided.[3]

Once the solutions were applied, the issues were resolved.

FIGURE 3

Key Functionalities of the File Upload Utility



Addressing Risk

Key SoD risk was identified and added to the risk and control matrix (RACM), which is a powerful tool that can help an organization identify, rank and implement control measures to mitigate risk. A RACM is a repository of risk that poses a threat to an organization's operations and to the controls in place to mitigate the risk. Put simply, a RACM serves as a snapshot of an organization's risk profile, measuring risk against the formalized actions taken to prevent negative events from occurring.

Examples of SoD risk that were identified as part of this project include:

- Under/overstatement of loan transaction may occur due to misappropriation.
- Fraudulent/incorrect cash transfer may occur due to a user's inappropriate access.

Business managers were required to identify appropriate mitigation controls to remediate the SoD risk identified. Those controls were added to the RACM and also became part of the control library. The analysis provided useful insight into the users who had such conflicting access, so the risk management group at the bank could monitor those users' access and the activities they performed on the systems.

Conclusion

When organizations attempt to set up cross-system processes, they must understand that there are many challenges and unknown variables to address and overcome. However, with meticulous planning and execution, organizations can be successful without any major time or cost overruns. The execution of the cross-system user-level SoD risk analysis between SAP ECC and non-SAP systems provides insight into the access risk that prevails in the user base and helps remediate it through appropriate mitigation controls or through the removal of conflicting access.

Author's Note

All references to SAP's Online Support System notes for providing guidance to implementors, consultants and project managers can be found at *https://launchpad.support.sap.com/*.

Endnotes

1 SAP One Support Launchpad, Note # 2130951—Explanation of ^! characters in permission-only rules, *https://launchpad.support.sap.com/*

2 SAP One Support Launchpad, OSS Note #1736661—How to upload transaction object description for non-SAP systems in Access Control 10.x was referenced, *https://launchpad.support.sap.com/*

3 SAP One Support Launchpad, Referencing to OSS Note #1696581—Cross system SoD analysis in AC 10.0 and OSS Note #2596198—Cross system risk analysis: Feature explanation and example scenario, *https://launchpad.support.sap.com/*