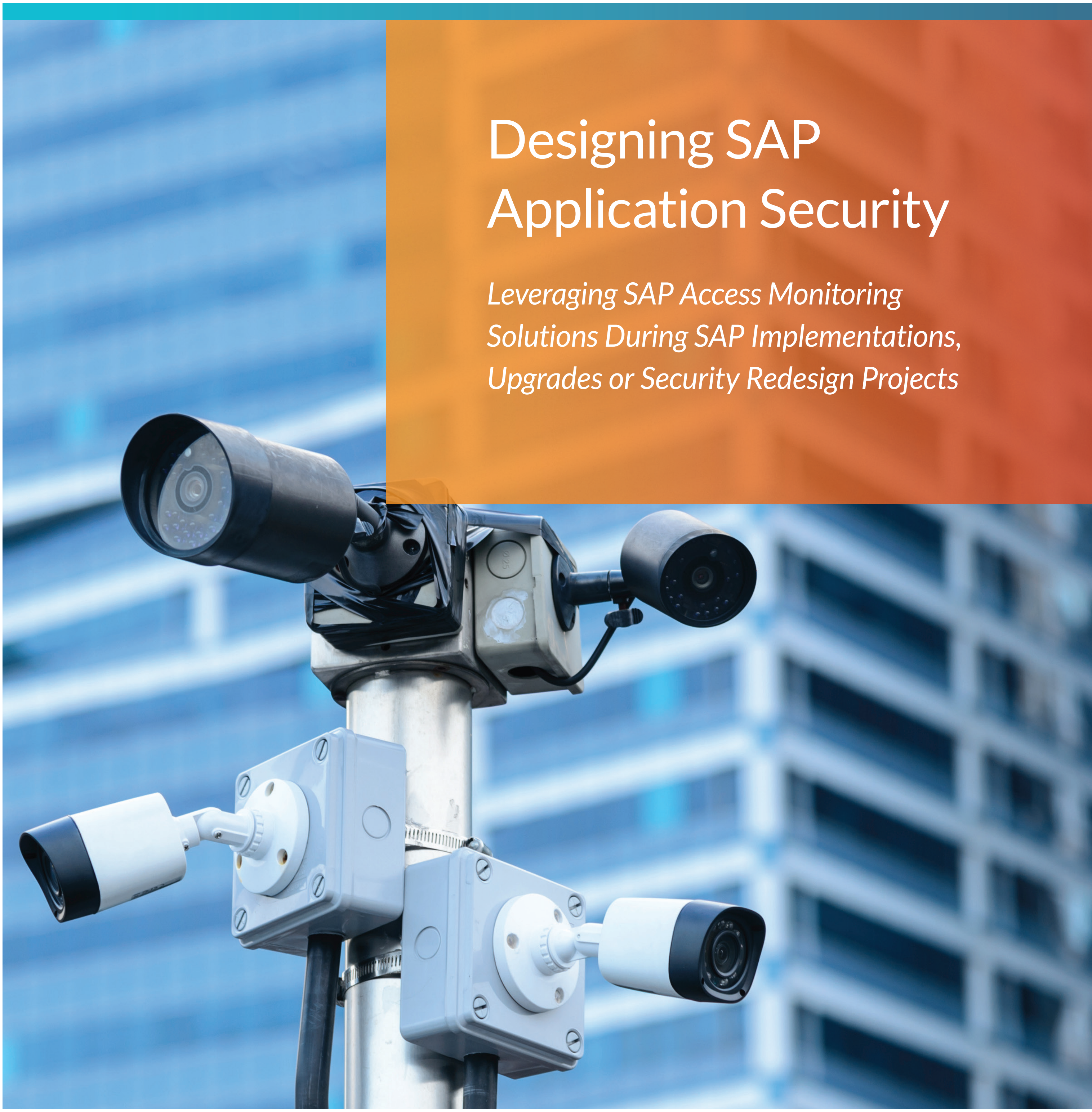
protiviti®

Face the Future with Confidence

Designing SAP Application Security

Leveraging SAP Access Monitoring Solutions During SAP Implementations, Upgrades or Security Redesign Projects



Internal Audit, Risk, Business & Technology Consulting

Introduction

The results of a poorly executed SAP security design process are many: unauthorized access, increased potential for fraud, inefficient access provisioning for end users, and numerous audit issues. All too frequently, companies that have not proactively identified and addressed potential security issues face expensive and challenging redesign projects within one to two years of the initial SAP rollout. This also applies to organizations that have integrated systems due to mergers or acquisitions or otherwise performed SAP integrations without an overall SAP security strategy. The pitfalls of a bad security design not only include frequent projects to mitigate security exposures, but also loss of productivity due to delays in granting access.

"Defining SAP security requirements in the early phase of an SAP implementation, upgrade or re-implementation project can help ensure efficiency and achievement of a 'clean slate' with regard to mitigation of security risks prior to go-live."

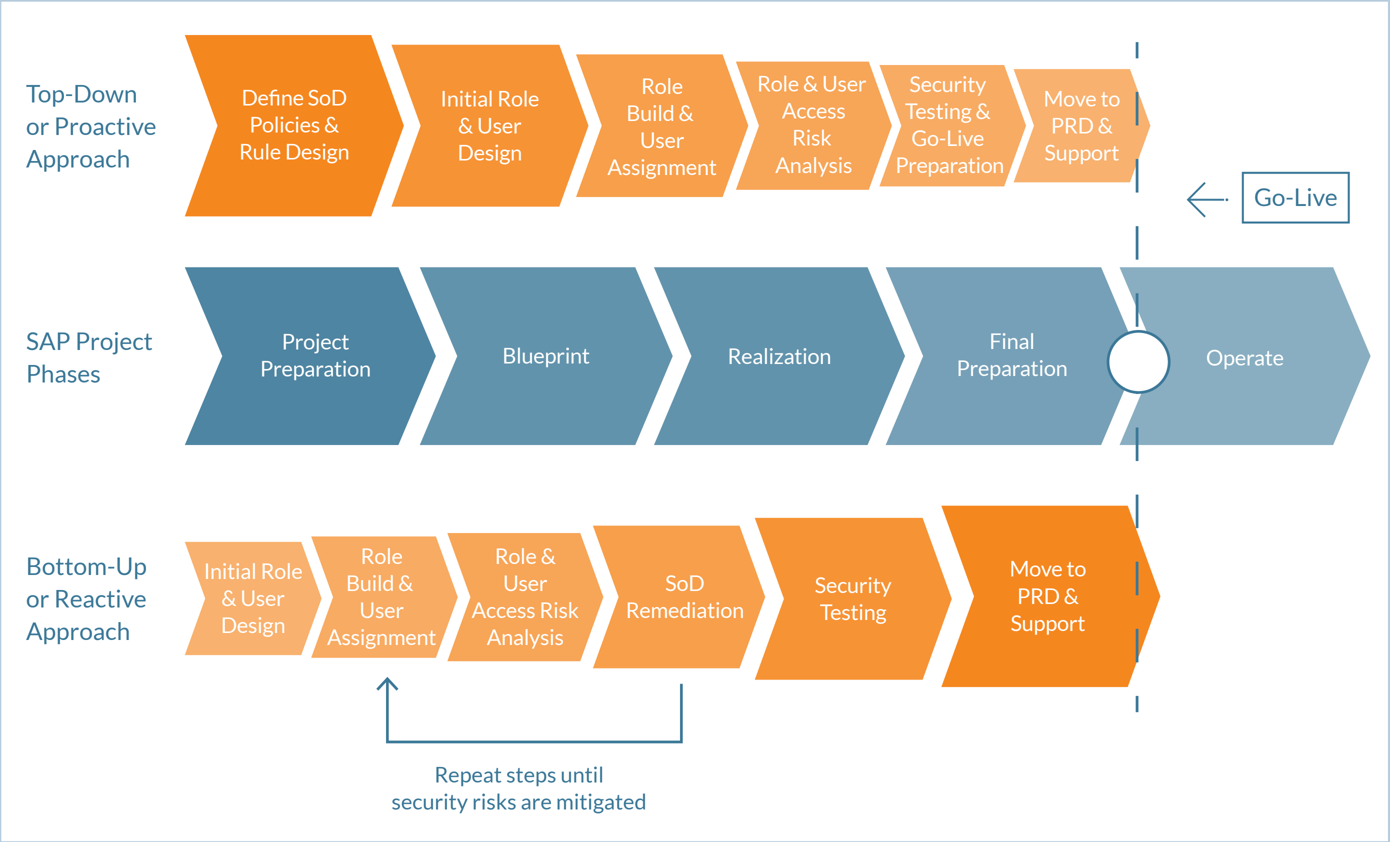
There are two main approaches when building application security in SAP. The first approach is the "top-down" or "proactive" approach described in detail in this white paper. It starts by defining security requirements up front during the blueprint phase. The second approach, the "bottom-up" or "reactive" approach, starts with developing SAP roles based on available transactions and job functions and considering security requirements and restrictions as a subsequent step, after roles have been set up in the system.

Organizations that use the second method, the bottom-up approach, do not address security risks or compliance requirements during the initial design of their SAP systems. Instead, they assess security risks and requirements after roles have been built and access has been granted to users, or after go-live. This approach is commonly used by companies implementing SAP for the first time. However, while this method appears time-efficient in the shorter term, it ultimately may prove more time-consuming because security design has to be re-evaluated — and very likely rebuilt — over time due to excessive access and a large number of segregation of duty (SoD) conflicts.

The bottom-up approach is also particularly inefficient when a high number of SoD conflicts must be resolved or SAP roles need to be changed to comply with financial regulations and audit requirements. In addition, this method runs the risk of allowing a high and unnecessary number of SAP roles to be built (i.e., new roles may be created to solve existing SoD conflicts, which often fails to address the root causes for SoD conflicts).

Defining SAP security requirements in the early phase of an SAP implementation, upgrade or reimplementation project ("SAP project") can help ensure efficiency and achievement of a "clean slate" with regard to mitigation of security risks prior to go-live. It is also important to leverage access management technology, such as SAP Access Control or similar solutions, to monitor whether security design requirements and SoD restrictions are properly maintained throughout the system build, deployment and go-live phases.

Approaches to Building SAP Application Security


Top-Down or Proactive Approach
Define SoD Policies & Rule Design
Initial Role & User Design
Role Build & User Assignment
Role & User Access Risk Analysis
Security Testing & Go-Live Preparation
Move to PRD & Support
Go-Live
SAP Project Phases
Project Preparation
Blueprint
Realization
Final Preparation
Operate
Bottom-Up or Reactive Approach
Initial Role & User Design
Role Build & User Assignment
Role & User Access Risk Analysis
SoD Remediation
Security Testing
Move to PRD & Support
Repeat steps until security risks are mitigated

Top-Down Approach for SAP Security Design

1. Define SoD Policies and Ruleset Design

The first step in implementing SAP application security using the top-down approach is to work with business process owners (BPOs), SAP functional leads, and compliance organizations to identify business processes and applications in-scope of the SAP project and determine how the different SAP modules (e.g., Financials and Controlling, Materials Management) and SAP applications (e.g., Supply Chain Management, Human Capital Management) would be utilized for each business process. A series of meetings and validation workshops should be conducted to establish an agreed-upon and written SoD management framework, including SoD policies with respective risk descriptions, risk ratings, and compliance and audit requirements.

• • • Key Components of an SoD Management Framework

	Definition	Example
In-Scope SAP Applications	Systems, modules, or applications where information related to the risk is entered or processed	SAP accounts payable module, supply relationship management (SRM) application, etc.
Business Risk	Definition of overall risk that drives the SoD rule and security controls	Fraud: acts committed by internal or external sources, intentional & concealed, causing loss of funds, value and reputation, or unauthorized benefit
Risk Description	Definition of what a user could do if allowed certain access in the SAP system	Cut fraudulent or unauthorized checks
SoD and Sensitive Access Policies	Job functions that represent or increase risk if provided to a user without proper monitoring	Access to create or change transactions for procure-to-pay and master data maintenance
Job Function	Tasks assigned to a specific user	Create a vendor master account, post payments, etc.
SoD Rule	SAP transactions and respective authorization objects related to the conflicting job functions	Change vendor master (e.g., XK02) vs. execute payment run (e.g., F110)

As part of this framework definition process, SoD policies should be outlined and classified into risk levels such as critical, high, medium, and low risk, as described in the example below. This will help management prioritize areas of focus during role build or security remediation phases:

- **Critical risk:**
  - Represents significant impact to company operations or company value
  - Risk cannot be mitigated, it requires remediation
- **High risk:**
  - Represents a direct financial misstatement risk or significant profit and loss (P&L) impact
  - Affects corporate image
  - Represents a deviation on standard best-practice processes or noncompliance with laws and regulations
  - Generates inconsistencies on master data governance or transactional data
  - Causes loss or theft
  - May be mitigated with an effective management-level report, or may require remediation
- **Medium risk:**
  - Causes a financial statement reclassification risk
  - Represents medium P&L impact (e.g., percent of revenue, materiality, potential loss)
  - Disrupts an operational process (no impact to financial statements)
  - Causes noncompliance with internal policies
  - Can be mitigated with a management-level report
- **Low risk:**
  - Costs more to mitigate than the cost of the risk to the business

These definitions vary from company to company based on the organization and industry-specific criteria. After these SoD policies and risks are defined, SAP standard and custom transactions should be evaluated to identify those that provide the ability to create, modify, post or delete data related to any of the identified risks. Ultimately, these SAP transactions are grouped into job functions (e.g., Create a GL Account, Post Payments) and should be configured in an automated SAP security monitoring solution (such as SAP Access Control or a similar solution) as "rulesets,"[1] which are used to analyze SoD conflicts at the role or user level.

In addition to SoD policies and risk definitions, companies also should define, group and classify sensitive SAP transactions to enable monitoring and reporting on SAP roles and users who have add, modify or even display access to the company's sensitive information, such as vendor pricing lists, customer lists, bills of materials (BOMs), sensitive SAP tables, financial data, and human resources (HR) information.

For Users of SAP S/4HANA Systems

With the introduction of SAP S/4HANA, the SoD ruleset will have to be reassessed to incorporate changes due to the introduction of new security layers, including over 200 new transactions, and the consolidation/replacement of old transactions and checks (e.g., Simplified Finance & Logistics and Business Partner). Additionally, security at the new presentation layer (SAP Fiori) and database layer (SAP HANA) may also have to be taken into account when designing the new ruleset.

[1] Most SAP Access Management solutions include a standard/predefined set of SoD rules; however, these rules, along with the risk ranking (critical, high, medium, low), need to be adjusted to reflect the company's risk profile. In addition, it is important to note that these standard rulesets may report on false positives if the security parameters (i.e., authorization objects) are not adjusted to reflect the company's security design.

2. Initial Role and User Design

The next step after establishing the SoD policies and rulesets in SAP Access Control, or a similar solution, includes the initial design of SAP roles. This step starts by reviewing "to-be" business processes and conducting a preliminary analysis of individual tasks and SAP transactions that will be performed once the new system goes live. At this point, the SAP application security team will group transactions into the beginning stages of SAP roles. This step could be challenging without predefined role templates due to the lack of available documentation to perform the role design related to transaction functionality.

Another approach for defining the set of SAP transactions to include in the updated SAP roles is to review the SAP transaction history. This method is applicable to SAP upgrade or security redesign projects only, since no transactional history will be available for new SAP implementations. In this approach, transaction logs are analyzed to determine the set of monthly, quarterly and year-end transactions that should be included in the newly designed SAP roles.

The next step after the initial transaction grouping is to conduct workshops with BPOs to validate that the respective SAP transaction groups are aligned with the "to-be" business processes in case of new SAP implementations or existing business processes in case of security redesign projects. At this stage, the "role templates" will be documented. These consist of the role's technical name and the underlining transaction codes. They also may include key information related to security restrictions, such as company codes, cost centers or document types. (Note: These parameters may vary over the course of the SAP project, as "to-be" processes are adjusted throughout the implementation.)

• • • Example of an SAP Role Template

Role Name	Transaction Code*	Transaction Code Description
Billing Role Z:US_SD_BLLNG	FBL5	Display Customer Line Items
	VF01	Create Billing Document
	VF02	Change Billing Document
	VF04	Maintain Billing Due List
	VF11	Cancel Billing Document
	VF31	Output from Billing Documents
	Z038	Delivery Related on the Billing Due
SD Customer Master View Z:US_SD_CUSTMST_SLSVIEW	VD01	Create Customer (Sales)
	VD02	Change Customer (Sales)
	VD03	Display Customer (Sales)
	VD04	Customer Changes (SD)
Blocked Billing Role Z:US_SD_BLCKD_BLLNG	VF02	Change Billing Document
	V.23	Release Sales Order for Billing

*Some of these transaction codes are disabled in SAP S/4HANA.

The next key step within the role and user design phase is to define "role owners" for each role template. Role owners are typically part of the functional implementation, or business teams, and usually "own" or are responsible for managing and reporting on the data being updated by the SAP transactions and roles they own. For instance, a corporate controller would own finance-related roles. Responsibilities for role owners include review and approval of SAP transactions to be included in the role and ongoing maintenance of the role (e.g., transaction additions, deletions, and approval of mitigating controls if conflicts occur).

SAP Security Design Considerations

"Job-based" vs. "task-based" roles

The first key decision to make during the actual design of SAP security is whether to use "job-based" or "task-based" roles. The intention of job-based roles is to give each user one role (e.g., Accounts Payable Manager) that encompasses all of that person's job activities. This approach utilizes fewer roles, but also gives users access to transaction codes they might not need. Also, the roles themselves may have SoD conflicts due to the large number of transactions assigned. The intention of task-based roles is to give each user multiple roles, each representing one job task (e.g., Release Purchase Requisition). This approach utilizes more roles, but will limit user access to the respective tasks performed. The decision around using a job-based or task-based approach will depend on the overall consistency of job positions, and the maturity of HR departments in relation to the integration between SAP access requests and employee hiring, transfer and termination processes.

Single vs. composite roles

Another decision to make is whether to use composite roles, which are a grouping of roles held within another role. It is common for job-based roles to consist of several task-based roles (composite roles). The main advantage in composite roles is that they provide a simpler user provisioning process since the user will receive one role. The main disadvantage of composite roles is that users may be granted more access than required due to additional tasks or backup responsibilities being included in the composite role.

Custom or pre-delivered SAP roles

It is also important to note that each SAP system comes pre-delivered with out-of-the-box roles, and an organization can decide to implement those instead of tailoring their security design. However, it is not recommended that out-of-the-box roles be used as a long-term strategy to maintain SAP security. These roles are designed as one-size-fits-all roles, meaning they have such a wide range of job activities combined in a single role that it will be nearly impossible to provision these roles to a user without granting excessive access. Also, out-of-the-box roles may not meet all business access requirements and control restrictions.

HR or position-based design vs. functional design

Another consideration when designing SAP security is the level of integration with HR processes (e.g., hiring, termination) and overall consistency with job descriptions and positions. In an ideal scenario, SAP roles should reflect job responsibilities, but if HR departments and positions are not mature or consistent, an independent security design based purely on job functions may be the best option. For organizations to apply a position-based design, HR job descriptions would have to be well-defined and consistent across the company. Also, "hire-to-retire" processes would need to be in a mature stage to enable integrated provisioning.

For Users of SAP S/4HANA Systems

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 S/4HANA roles will have to be designed to include the additional authorizations and mapping required to access the specific apps on 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.) as well as by end users reading data directly from the database. If users need to have 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.

3. Role Build and User Assignment

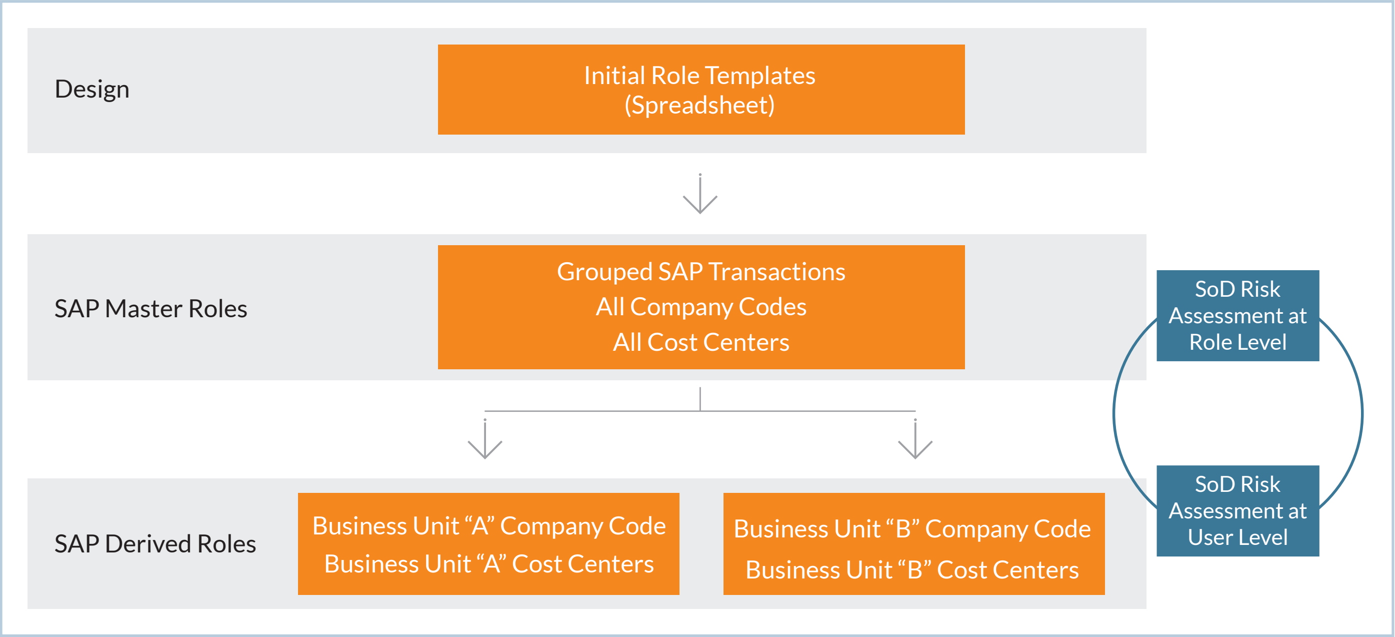
Once the initial SAP role templates have been designed and approved, the roles can be built in SAP and subsequently assigned to end users. The technical design phase starts with building "master roles" or "template roles" including the grouped transactions. Building master roles requires close coordination with the systems integrator and BPOs so that all standard and custom SAP transactions and objects being used as part of the role design are understood in terms of functionality (e.g., create master data, update financial statements) and are also properly incorporated in the template roles. The second step in designing SAP roles is to create "derived" or "child" roles, which is where security restrictions are applied (e.g., company code and cost center limitations).

Designing roles that are free from SoD conflicts early in the SAP project can lead to increased granularity and more restrictive access, as well as increased transparency related to the authorizations given to a user. In addition, it can reduce ongoing security maintenance because it makes it easier to respond to changes in user responsibilities resulting from the implementation of new SAP functionality and/or organizational realignment.

End user role assignment is a critical step when designing SAP application security, due to the different restrictions that must be applied to users (e.g., some users may need access to one, multiple or all company codes or cost centers, in case of shared services departments).

During these steps, it is also important to leverage SAP Access Control, or another SAP security monitoring solution, to confirm that roles are SoD-conflict-free before assigning them to end users. If master roles have inherent SoD conflicts, all derived roles and subsequently assigned users also will have conflicts.

• • • SAP Role Build and User Assignment Process


Design
Initial Role Templates (Spreadsheet)
SAP Master Roles
Grouped SAP Transactions
All Company Codes
All Cost Centers
SAP Derived Roles
Business Unit "A" Company Code
Business Unit "A" Cost Centers
Business Unit "B" Company Code
Business Unit "B" Cost Centers
SoD Risk Assessment at Role Level
SoD Risk Assessment at User Level

4. Role and User Access Risk Analysis

At this stage, SAP Access Control, or another SAP security monitoring solution, should be leveraged to perform periodic role and user analyses to determine if the newly designed SAP roles are in compliance with SoD policies. This is done by simulating and monitoring changes affecting SAP security design, and providing timely feedback to BPOs in case potential conflicts arise. Risk analyses should be run on a periodic basis, especially after unit and integration testing, which is when the SAP system design will be updated to accommodate process improvements. It is important to note that the defined SAP ruleset in SAP Access Control also may change during the course of the SAP project, given that new SAP transactions may be added to "to-be" processes or new custom transactions may be developed.

To ensure an SAP environment is "clean" or "conflict-free" post-go-live, a sound SAP security provisioning process must be designed and implemented. This includes procedures that require SAP security teams to perform a risk simulation in SAP Access Control prior to granting user access or modifying a role. This simulation will determine if role or user changes are posing SoD or excessive access security risks. In addition, continuous monitoring procedures must be established and followed as the project go-live date approaches. Detective SAP security monitoring processes also should be established, including generating periodic SoD violation reports reviewed by BPOs and role owners to validate security changes. For SAP upgrade or security redesign projects, post-go-live activities may also include additional change management processes to assign and manage new roles and, over time, to discontinue the use of legacy roles.

For Users of SAP S/4HANA Systems

The SAP Access Control functionality will have to be expanded across the S/4HANA landscape to address the access risks arising with the introduction of new security layers. Changes may need to be made at both the system architecture level (configuring additional connectors) and the Access Control tool functionality level (workflow changes) if users are provided access to Fiori and the HANA database.

5. Security Testing and Go-Live Preparation

SAP security Unit Testing (UT) and User Acceptance Testing (UAT) are critical steps to ensure users experience minimal access issues prior to go-live. SAP security testing includes executing all SAP transactions within a role to confirm that the role has required transactions and authorization objects to complete the process (e.g., display, update and post a financial transaction). These steps should be performed in conjunction with project functional testing (during SAP implementations or upgrades) or before assigning the new roles in the production environment (during security redesign projects). Security testing also should include formal SoD and sensitive access reviews to confirm the newly created or updated SAP roles are as SoD conflict-free as possible, and that access to key functions (e.g., update vendor master, update chart of accounts) is properly restricted.

Involving SAP security teams in early stages of the functional testing phase allows the discovery of potential security issues before it is too late — or costly — to modify roles. It is also very important for the final UAT process to create test users in the Quality Assurance environment with the SAP roles to be used in the production environment (i.e., users with accurate SAP role assignments). This will allow proper identification and remediation of security changes, including verification of "authorized conflicts" and resolution of "unauthorized conflicts" prior to going live with the SAP project.

Be sure to work closely with BPOs, role owners and the SAP security team to remediate unauthorized conflicts by regrouping the transaction codes within the conflicting role(s) or reassigning the roles for the conflicting user. For SoD conflicts that cannot be resolved for a business-approved reason, such as limited headcount, mitigating controls should be identified and documented.

For Users of SAP S/4HANA Systems

With SAP S/4HANA, testing steps will require some updates to account for the additional security levels introduced at the presentation (Fiori) and database (HANA) levels. At the application level (SAP S/4HANA), the testing procedures will have to take into account the transactions that have been consolidated, simplified or removed.

6. Move to Production and Support

Once testing is complete, the newly designed SAP roles can be migrated to the production environment according to the organization's change management policy and users can be assigned. No matter how well UT and UAT are performed, it is very likely that access issues will be encountered during go-live, stabilization, and the post-go-live period due to the overall complexity of implementing or changing ERP systems and processes in an organization.

It is critical to establish a support team specifically assigned to address any SAP access issues during go-live and stabilization activities. This team not only can help resolve access issues on a timely basis, but also run access risk reports to determine if security changes will result in SoD or other access risks. Also, a communication plan should be established to ensure affected users are aware of any changes and support protocols related to go-live of the SAP system.

A common practice during SAP implementation and upgrade projects is to allow for temporary broader access for "power users" during the go-live and stabilization period. This is done to help with stabilization of the new system, to ensure users are capable of performing job functions during and after go-live, and often is performed using SAP Access Control to review transaction and super-user action logs. It is important to review and remove this temporary broader access after the new implementation is stable.

It is recommended to leverage SAP provisioning solutions to automate user provisioning processes. For instance, SAP Access Control can enable "paperless" SAP security provisioning by automating the assignment and approval of roles. User provisioning and approvals can be accomplished through a few clicks on a webpage. If an issue is detected during the user assignment process, the approval path is automatically redirected so the appropriate role owner can resolve the SoD conflict before access is granted.

Conclusion

Designing, configuring and implementing SAP security is a complex and resource-intensive endeavor. Companies should consider their approach to building SAP Application Security in the early stages of SAP projects. Embedding proper security requirements during the system build process helps to avoid the need for a redesign later. Using automated security monitoring solutions such as SAP Access Control and applying best practices can increase efficiency and acceleration of the security design and the implementation of conflict-free SAP roles, and dramatically reduce the possibility of having to redesign SAP security in the future.

Organizations that meet any of the following criteria should consider assessing their SAP security design and the implementation or optimization of SAP security monitoring solutions in order to "clean" and "maintain" their SAP security environment:

- Organization-specific SoD policies have not been defined, approved by the business, or are outdated
- Creation of new roles and/or new role assignments generates new SoD conflicts requiring remediation or mitigation
- A significant number of SoD conflicts exist within roles
- The SAP environment consists of more roles than users
- SoD checks are performed manually
- Automated security monitoring solutions, such as SAP Access Control, are not in place to support provisioning processes or ongoing monitoring of the environment
- Lack of business involvement in the SoD risk management process

For Users of SAP S/4HANA Systems

When moving to S/4HANA, keep in the mind the changes and additional layers introduced with the new data model to develop a cost-effective and compliant security architecture.

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 your 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 your 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 your 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

THE AMERICAS

UNITED STATES

Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*

Buenos Aires

BRAZIL*

Rio de Janeiro
Sao Paulo

CANADA

Kitchener-Waterloo
Toronto

CHILE*

Santiago

MEXICO*

Mexico City

PERU*

Lima

VENEZUELA*

Caracas

EUROPE MIDDLE EAST AFRICA

FRANCE

Paris

GERMANY

Frankfurt
Munich

ITALY

Milan
Rome
Turin

NETHERLANDS

Amsterdam

UNITED KINGDOM

London

BAHRAIN*

Manama

KUWAIT*

Kuwait City

OMAN*

Muscat

QATAR*

Doha

SAUDI ARABIA*

Riyadh

SOUTH AFRICA*

Johannesburg

UNITED ARAB EMIRATES*

Abu Dhabi
Dubai

ASIA-PACIFIC

CHINA

Beijing
Hong Kong
Shanghai
Shenzhen

JAPAN

Osaka
Tokyo

SINGAPORE

Singapore

INDIA*

Bangalore
Hyderabad
Kolkata
Mumbai
New Delhi

AUSTRALIA

Brisbane
Canberra
Melbourne
Sydney

*MEMBER FIRM

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