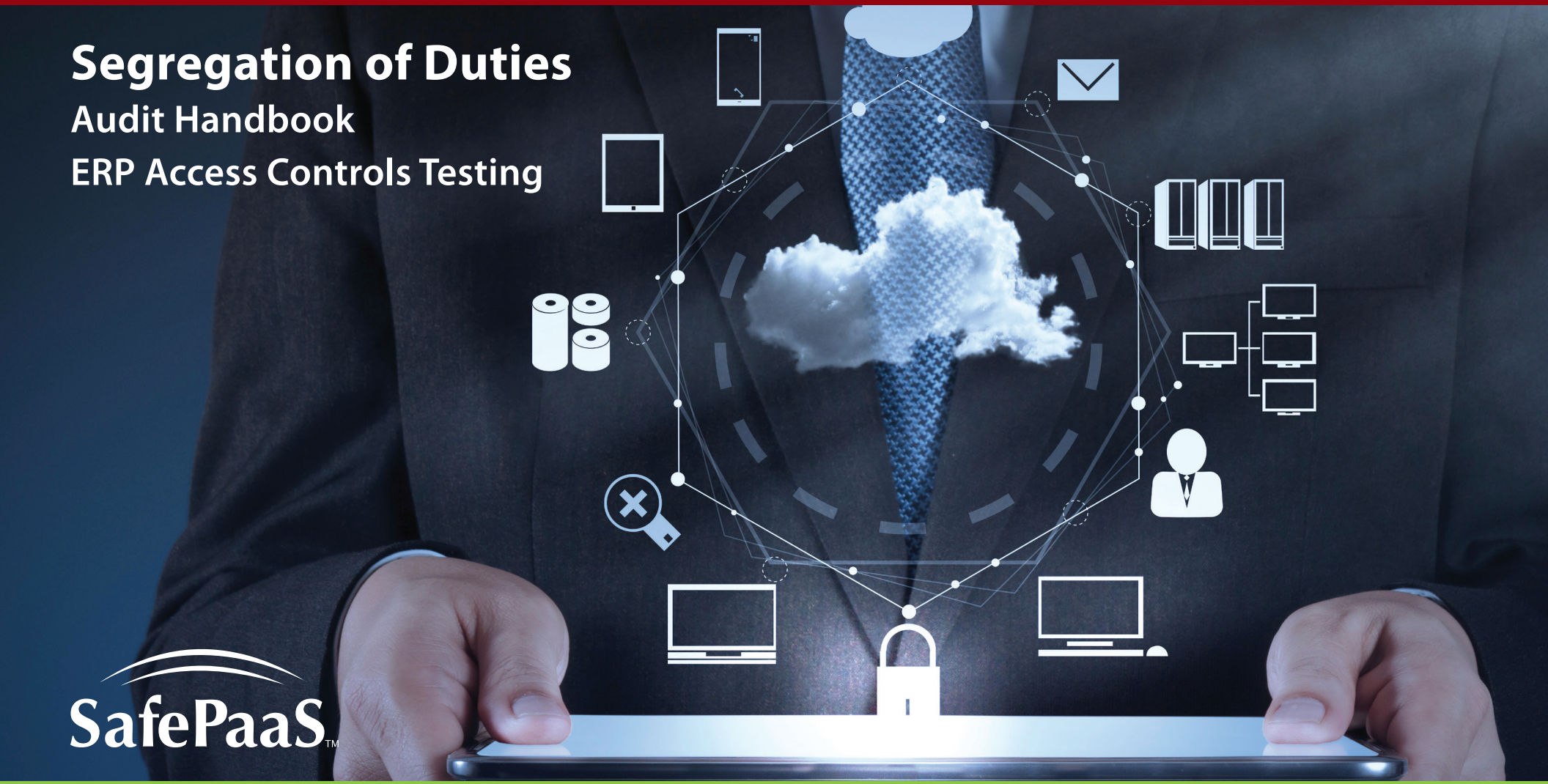
Segregation of Duties

Audit Handbook

ERP Access Controls Testing



SafePaaS™

Auditing Enterprise Applications for Segregation of Duties Risks

Enterprise applications enable organizations to better engage and empower employees in the workplace, improve collaboration with business partners, and effectively manage customer relationships. However, ineffective Segregation of Duty (SoD) access control within enterprise applications can result in operational losses, financial misstatements, and fraud.

Segregation of Duties risk is growing as organizations are rapidly adding users to their enterprise applications to execute all major business processes. Default roles in enterprise applications present inherent risks because the "seeded" role configurations are not well-designed to prevent segregation of duty violations. This risk is further increased as multiple application roles are assigned to users, creating cross-application SoD control violations. Business managers responsible for SoD controls, often cannot obtain accurate security privilege-mapped entitlement listings from enterprise applications and, thus, have difficulty enforcing segregation of duty policies. The lack of standard enterprise application security reports to detect Segregation of Duties control violations in user assignment to roles and privilege entitlements can impede the benefits of enterprise applications.

The user access provisioning process further increases the SoD risks in enterprise applications. IT Service Management (ITSM) tools, e.g., ServiceNow, BMC Remedy, etc. and Identity Management (IDM) tools, e.g., Microsoft Azure, Okta, OneLogin, SailPoint, etc., do not control SoD risks. These systems operate at such a high level that they cannot see what is going on in an enterprise application at the privilege level. In addition, these tools do not detect or prevent SoD violations in user access requests workflows, which are critical for compliance reporting, auditing, and forensics.

Therefore, Auditors must provide independent assurance of Segregation of Duties controls, which requires fine-grained access rules and advanced analytics to test thousands of access points to application entitlements, functionality, transaction data in complex ERP security models.

In this handbook, you will learn to audit segregation of duties controls in popular enterprise applications using a top-down risk-based approach for testing SoD controls in widely used ERP systems. In summary, we will cover the following topics in this handbook:

1. Segregation of Duties Controls
2. Risk-based Access Controls Design Matrix
3. Audit Approach for Testing Access Controls
4. Violation Analysis and Remediation Techniques
5. Security Model Reference Guide

SafePaaS™

Segregation of Duties Controls

Segregation of Duties (SoD) (also known as "Separation of Duties") is an internal control that prevents a single person from completing two or more tasks in a business process. Organizations require SoD controls to separate duties among more than one individual to complete tasks in a business process to mitigate the risk of fraud, waste, and error.

Actual job titles and organizational structure may vary greatly from one organization to another, depending on the size and nature of the business. Therefore, it's important to analyze the skillset and capabilities of the individuals involved based on the risk likely and impact to business processes. Critical job duties can be categorized into four types of functions: authorization, custody, record keeping, and reconciliation. In a perfect system, no one person should handle more than one type of function.

You can apply the following options to segregate job duties:

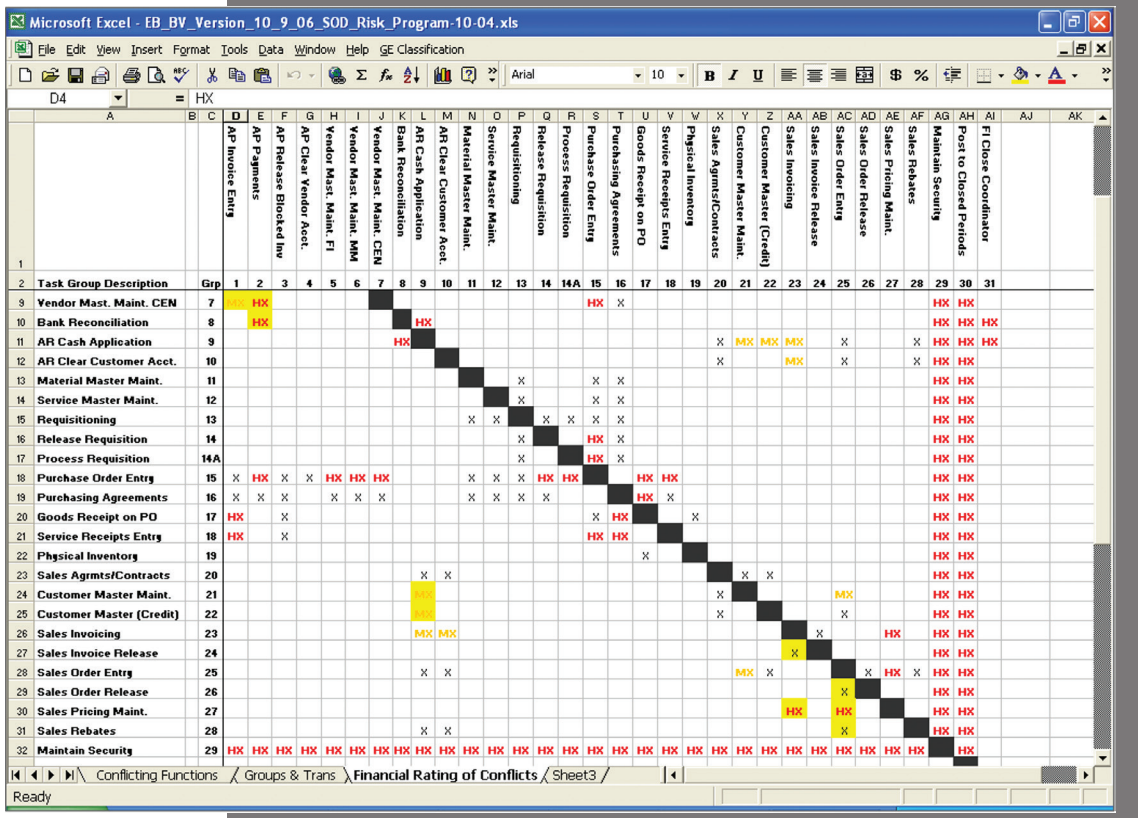
- Sequential separation (two signatures principle)
- Individual separation (four-eyes principle)
- Spatial separation (separate action in separate locations)
- Factorial separation (several factors contribute to completion)

Many companies find it challenging to implement effective SoD controls in their ERP systems, even though the concept of SoD is simple as described above. To a large extent, this is due to the complexity and variety of the applications that automate key business processes, and the ownership and accountability for controlling those processes require a complete analysis of thousands of functions available across roles and responsibilities assigned to users. For example, to assess SoD risk in an Account Payable application that a user, assigned the Payables Manager role has access to create a supplier and approve a payment requires completed analysis of all functions that constitute the entitlements granted through the role while excluding any false positives that may occur as a result of overriding attributes, profiles, page-level configurations or customizations that prevent such access.

SafePaaS™

Risk-based Access Controls Design Matrix

SoD controls for an enterprise application can be designed using a matrix to assess the risk that lists potential conflicts to determine what risk level (e.g., High, Medium, Low) would be realized should a user have access or authorizations to a combination of entitlements. For example, what is the likelihood, that a user can create a fictitious supplier and make a payment to that supplier? The risk likelihood and impact vary based on industry, business model, and even individual business unit. It is not uncommon for a large global company to have more than one matrix due to differences in the business processes by location or business unit. For example, a company may have a manufacturing business unit with a large amount of inventory, requiring an SoD matrix that focuses on specific inventory transactions. They may also have a service-based business unit necessitating a focus on project accounting, requiring a different SoD matrix. Though knowledge of similar businesses and industries can help to establish the conflict matrix, each business unit must perform a customized analysis of its conflicting transactions to capture the real risk for that particular business model.



The matrix provides a financial risk rating of access entitlement that is assigned to a user. The SoD Controls should be designed to mitigate access control violation risks. An access role contains one or more entitlement that consists of menus, functions, and transactions a user can access through the assignment of that role to perform a task to record an entry, change a setup, or update a data object.

The SoD Matrix enables the auditor to test the SoD Control design effectiveness, based on the risk level identified in the matrix. To ensure that the SoD matrix is accurate and complete, the auditor must obtain a complete snapshot of all user access points within the enterprise application to ensure that the SoD control design includes a level of granularity in the enterprise security model that grants user access as per the job role assignment for all the users.

The application mapping is the rule-set by which sensitive transactions are tested in the relevant systems. For example, vendor-update rights may be executed through a series of menus within a given application. The presence of these menus assigned to specific users should be mapped, walked-through, and documented for the company to accurately test for a particular conflict. The challenge is that in most modern applications there is more than one way to execute the same transaction. For example, there may be five ways to pay a vendor in an application, but the company may use only two of them. Moreover, the company is typically not aware of the other three ways and usually does not restrict access to or control these other methods to execute a vendor payment. The risk-based SoD process requires a company to discover all the potential methods for executing a transaction to understand the full potential for fraud, not just the limited view of the known methods. Mapping all the ways a user could potentially execute a transaction is critical to accurately depicting SoD.

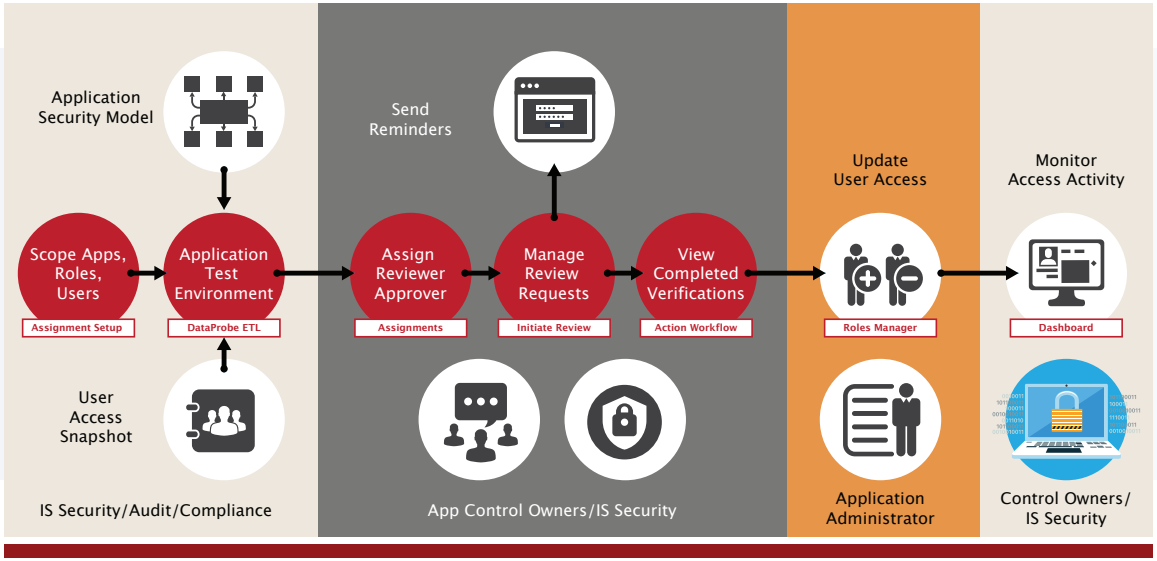
SafePaaS™

Audit Approach for Testing Access Controls

The audit approach for testing access controls starts by preparing a test plan to detect violations of SoD policies based on the access control design matrix approved by management. The following ten test steps should be considered to complete the SoD control assessment:

1. Prepare an access rule report from the access controls design matrix
2. Scope and add "sensitive" access rules to detect user access to restricted data
3. Gather a list of active application users and role entitlements including privileges and data access
4. Create a list of exceptions by analyzing the security object items that prevent user access violations
5. Identify application configurations that mitigate the inherent SOD risk
6. Detect access rule violations by applying security object items rule logic to filter the user access report in step 3 above
7. Finalize the access violations report by excluding exceptions, and mitigated risks
8. Perform look-back transaction analysis to detect materialized risks
9. Create a remediation plan with corrective actions to update the user assignments and role configurations.
10. Provide an access violation scorecard as evidence of control effectiveness

The following diagram provides an overview of the assessment approach:



SafePaaS™

The first swim-lane shows the steps to prepare the "test" environment that includes the rules in scope, configuration of the application security model, and the security configuration data extracted (snapshot) so that the rules logic can be applied to the user-role assignments and role entitlements at the privilege level.

The second swim-lane shows the steps to detect, analyze, and correct access control violations. The access control violations must be analyzed to eliminate false positives and identify any exceptions where ERP configurations mitigate the SoD risks. After the analysis is completed, an SoD violations report is prepared for review with the application control owner. This is an important step to ensure that the managers closest to the business process can confirm the results and provide valuable feedback that may not be available in the ERP system or supporting documentation.

The third swim-lane shows the steps to implement the remediation plan. Once the SoD violations report is confirmed, the auditor can ask the management to provide a remediation plan that includes changes to application security and configurations as well as the implementation of preventive controls such as continuous controls monitoring and workflow approvals in the enterprise application. At this stage, it is also important to create a project plan that ensures management sponsorship for adequate internal and external resources required for remediation and controls implementation.

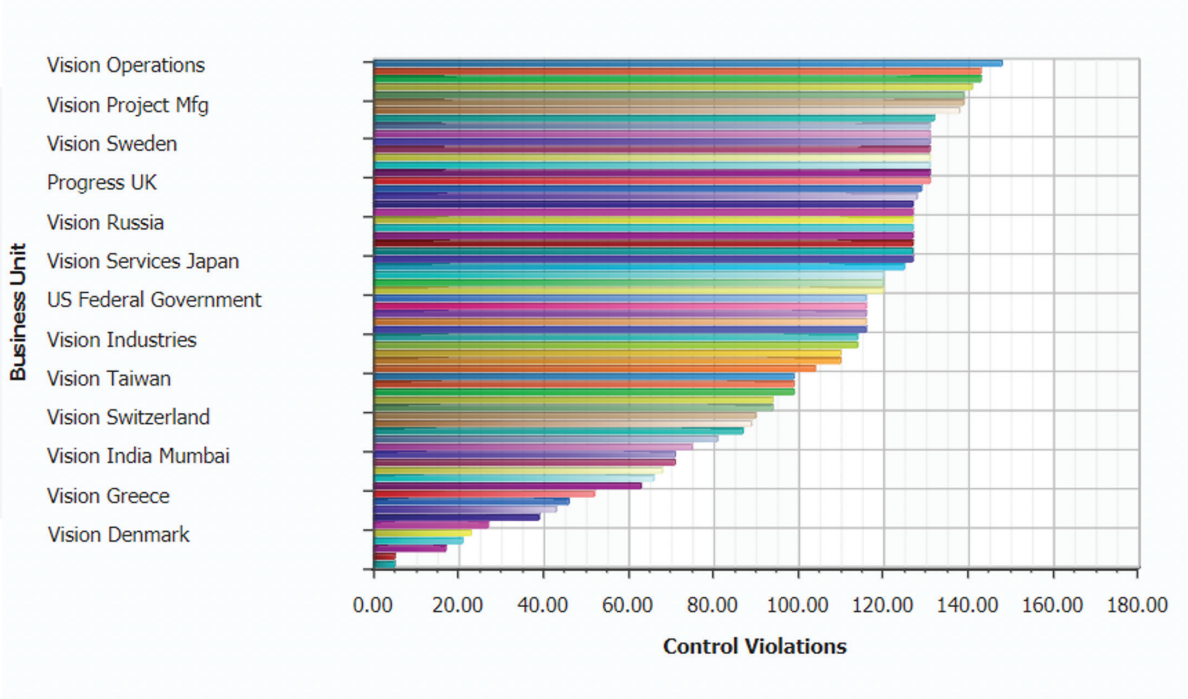
The fourth and final swim-lane shows the steps for control owners to monitor unmitigated access risks as well as new risks that that may be detected when new user requests are provisioned, or existing user access has changed.

SafePaaS™

Violation Analysis and Remediation Techniques

Violation analysis can be a time-consuming effort because thousands of incidents, including false positives, are generated due to the large number of users that have access to hundreds of access privileges in enterprise applications. The remediation effort can fail if the corrections to the security configuration disable the users' ability to performing business process activities.

You can streamline the violation analysis by creating a "Violation Scorecard" that shows the total user and role violations summarized by access control, risk level, and business units as shown below:

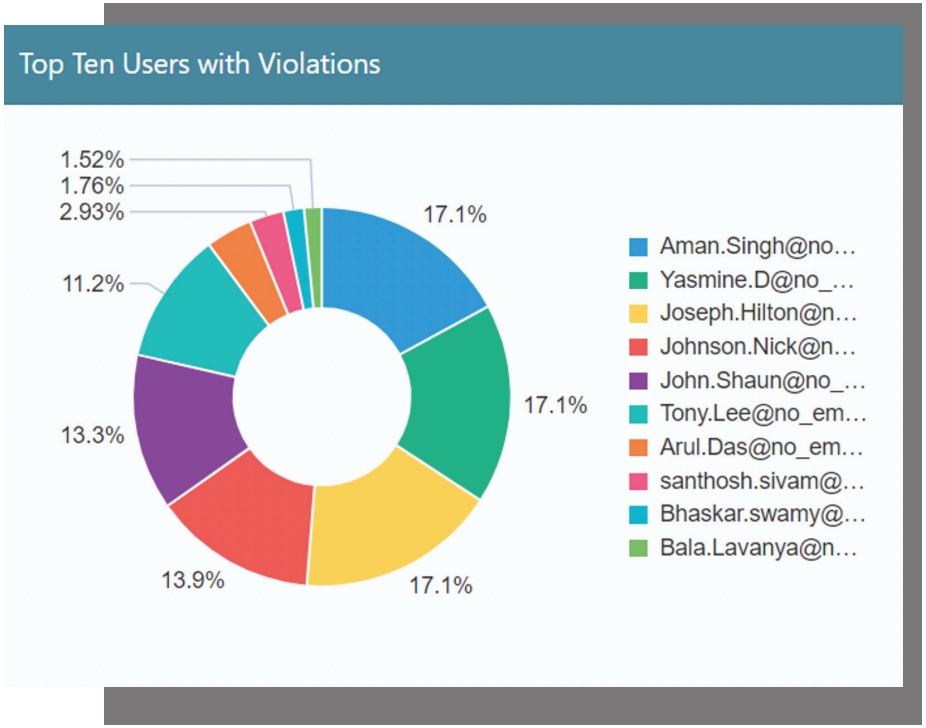


SafePaaS™

The scorecard provides the "big-picture" on "big-data" to gain necessary management sponsorship, allocate sufficient resources, prioritize the effort, and communicate progress to complete the analysis and remediation. For example, you may use the scorecard to start the analysis of the top twenty-five access controls in business units with the highest number of SoD violations to rapidly remediate enterprise risk where likelihood and impact are the greatest.

Next, you can drill down to the users with the highest violations to validate the violations against the enterprise application security model to ensure that only active users with access to active role-permission combinations are reported in the violation report. See sample chart to the right:

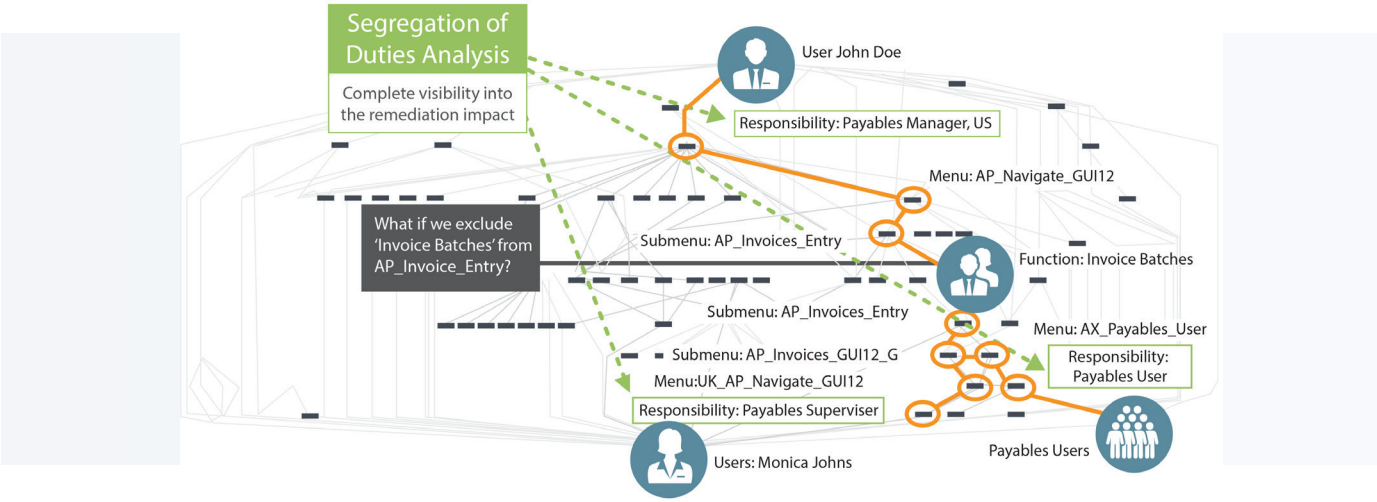
Once you have confirmed the users with control violations, you can start to analyze the role-privilege configurations to validate the violations within the security model. You will need a guide of the enterprise application security model to validate the SoD violations and eliminate false positives based on the security objects available to control user access. Please refer to section five for security models of the most widely used enterprise applications. The complexity of the enterprise application security model impacts the effort required to analyze violations, eliminate false positives, mark exceptions where risk is mitigated by security objects. For example, user profiles, application customizations, and data extensions should be analyzed to assess the residual risks.



SafePaaS™

If the enterprise application you are auditing does not follow the NIST Role-Based Access Controls (RBAC) to control data access within the role, you would need to perform an additional step to verify the violation by data sets assigned to roles using security attributes. Many widely used, mature ERP applications will require this step in your analysis. For such applications, you will need to analyze violations in each business unit because there may be variations of the role-permission manually created by the IT security team from a global template. Over time, business needs require a variation of these standard role configurations. Such variations cannot only increase the SoD violations, but also the time needed to correct the access control defects.

The final step is to create corrective actions to remediate the SoD violations. Effective remediation techniques require a root-cause analysis of the security defects and the ability to simulate the corrections to test user access before the changes are deployed in the production system. It is important to minimize the business process disruption by assessing the impact of security configuration changes on all users with access to the targeted roles and privileges. See the example below:

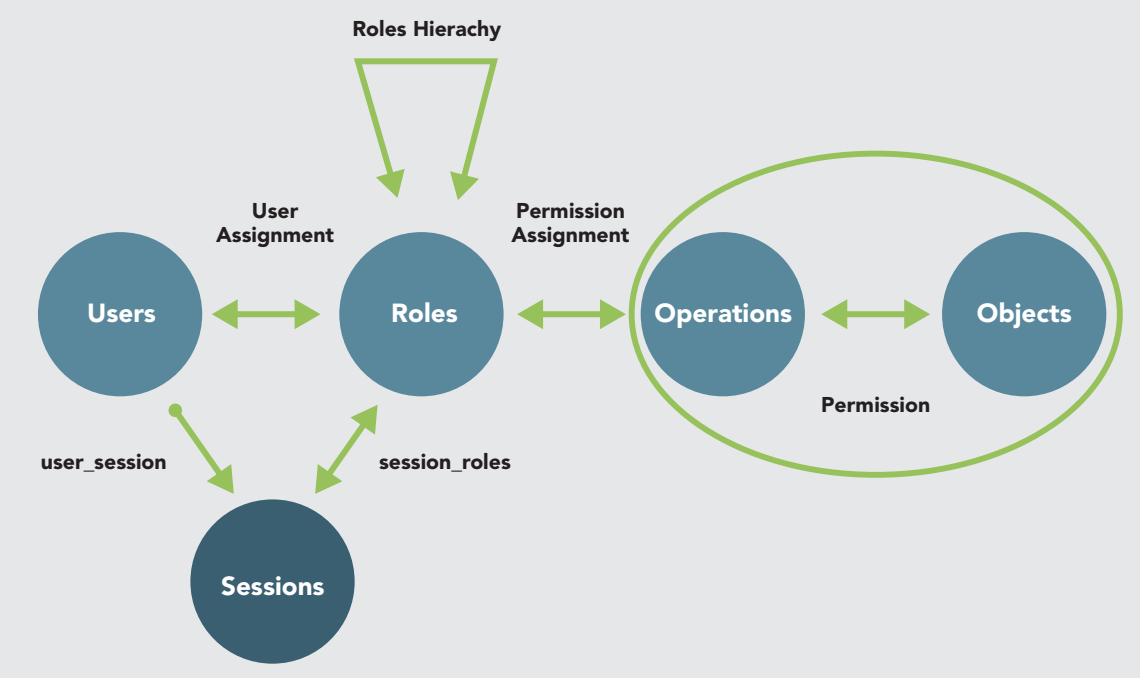


Access control remediation often requires role redesign that not only mitigates business risks but also improves user productivity. Roles included in enterprise applications grant users "keys to the kingdom" to execute all business activities such as master data maintenance, system configuration changes, and transactions that impact financial statements. These roles require significant configuration effort to match organizations business roles and segregation of duty policies. You can use the "out-of-the-box" roles as a source of templates to create target roles that match your user role requirements. Each target role can then be configured by assigning limited privileges. It is important to maintain change controls over the application security model to ensure that the control owners can review and approve role changes base on business needs, organization structure, and user access requirements.

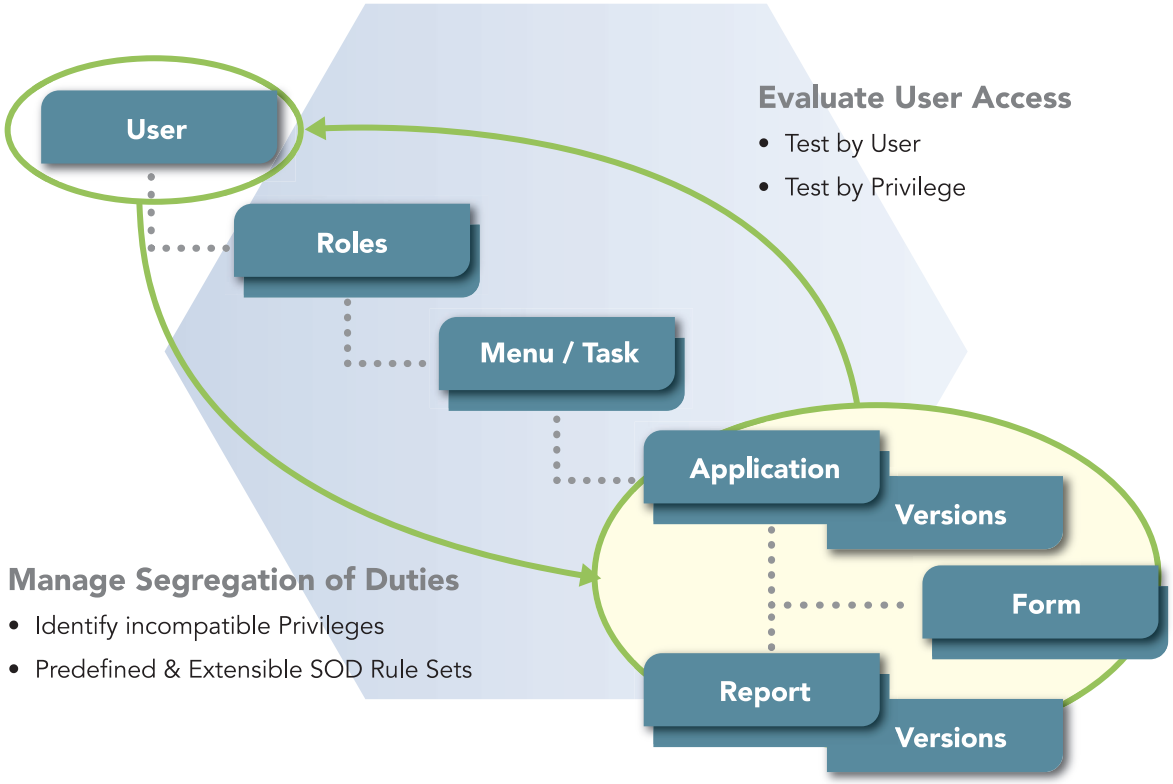
SafePaaS™

Security Model Reference Guide

In this section, we describe the security model of widely used enterprise applications to help you understand the security models to prepare your audit plan. All security models follow a hierarchy of security objects starting with the user. However, not all applications follow the US Department of Commerce National Institute of Standards and Technology (NIST) Role-Based Access Controls (RBAC) model which was adopted as American National Standard 359-2004 by the American National Standards Institute, International Committee for Information Technology Standards (ANSI/INCITS) on February 11, 2004. Application vendors that follow the RBAC model implement the security objects also have many different implementation options. The following section shows security models by enterprise application (alphabetical order), starting with the RBAC model as the meta-data template:

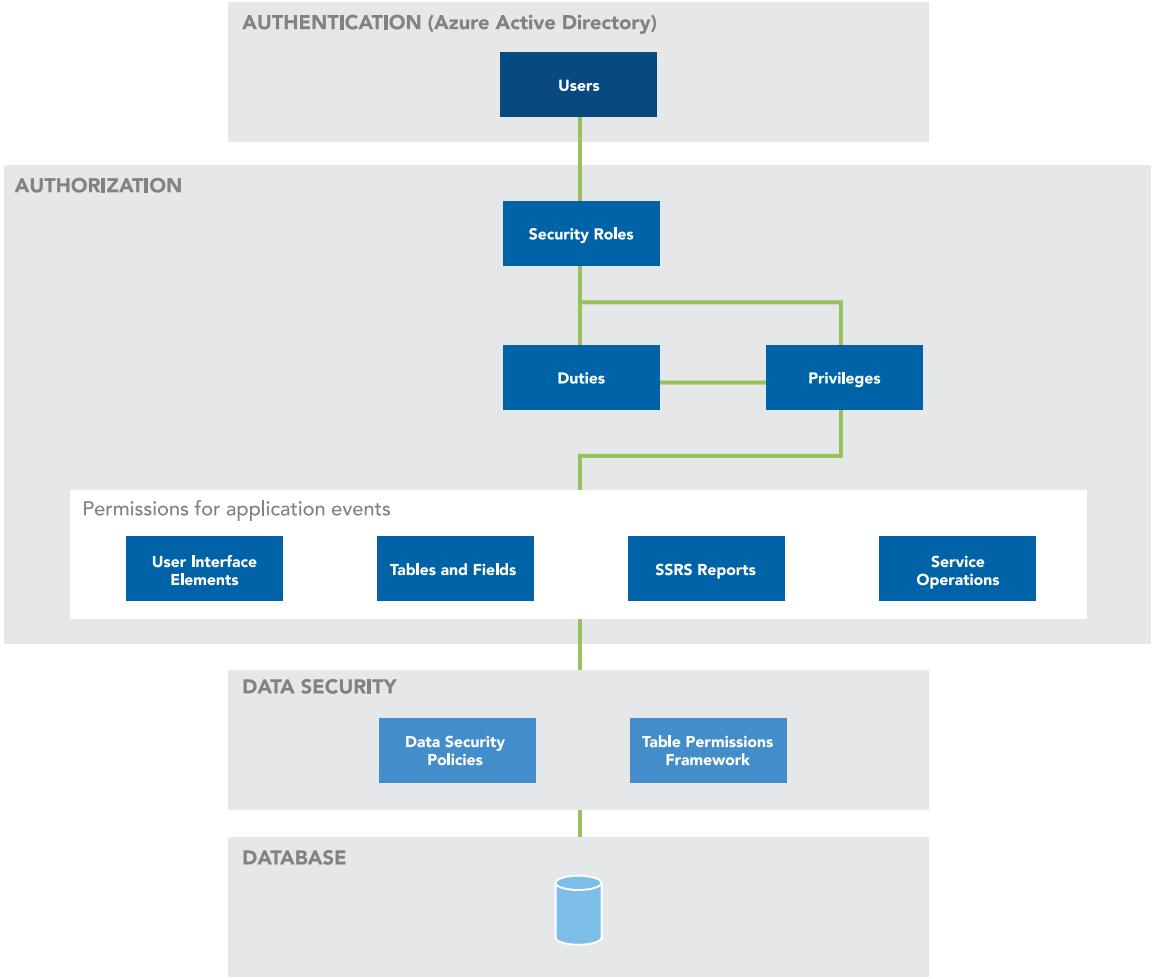


JDEdwards®
Enterprise Software



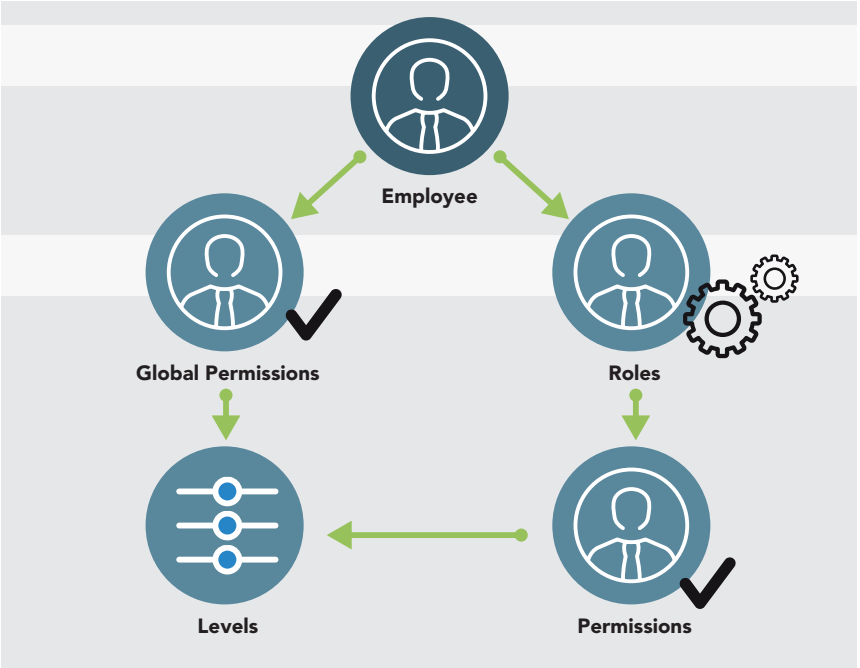
SafePaaS™

Microsoft Dynamics™



SafePaaS™

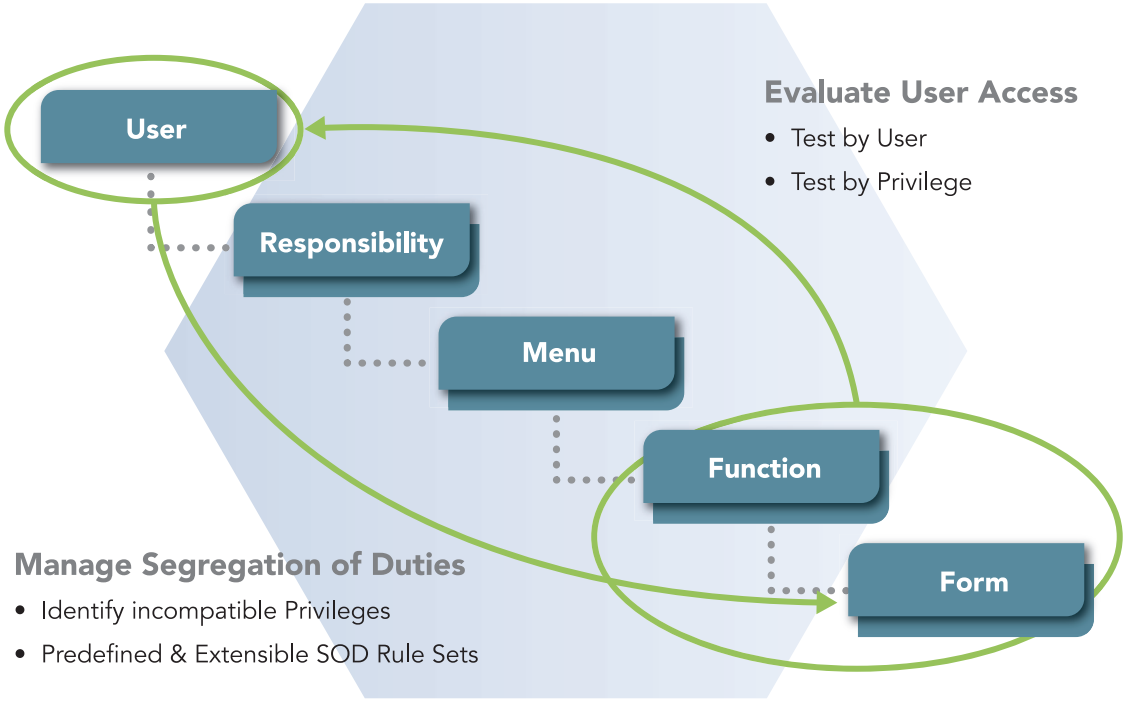
NETSUITE



SafePaaS™

ORACLE®

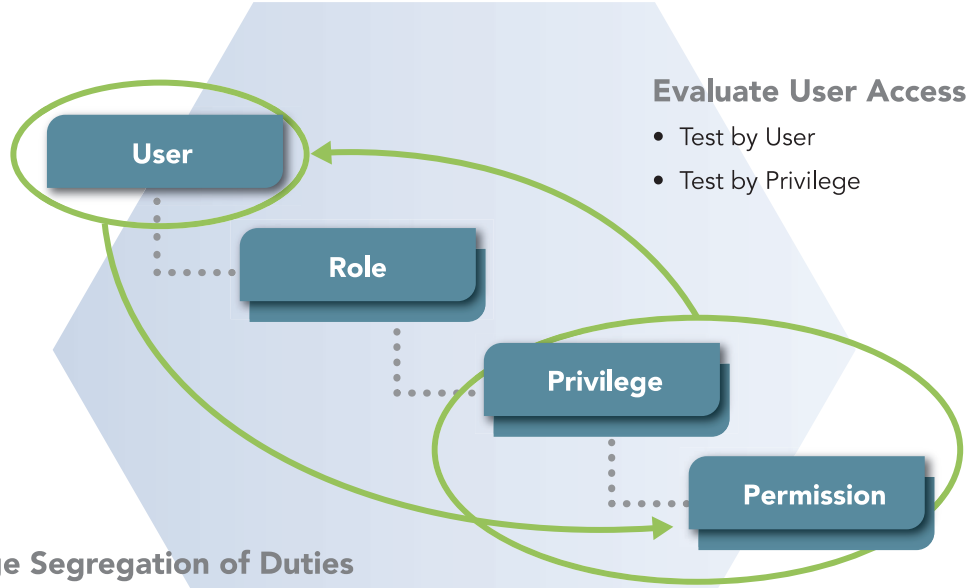
E-BUSINESS SUITE



SafePaaS™

ORACLE

ERP CLOUD



Evaluate User Access

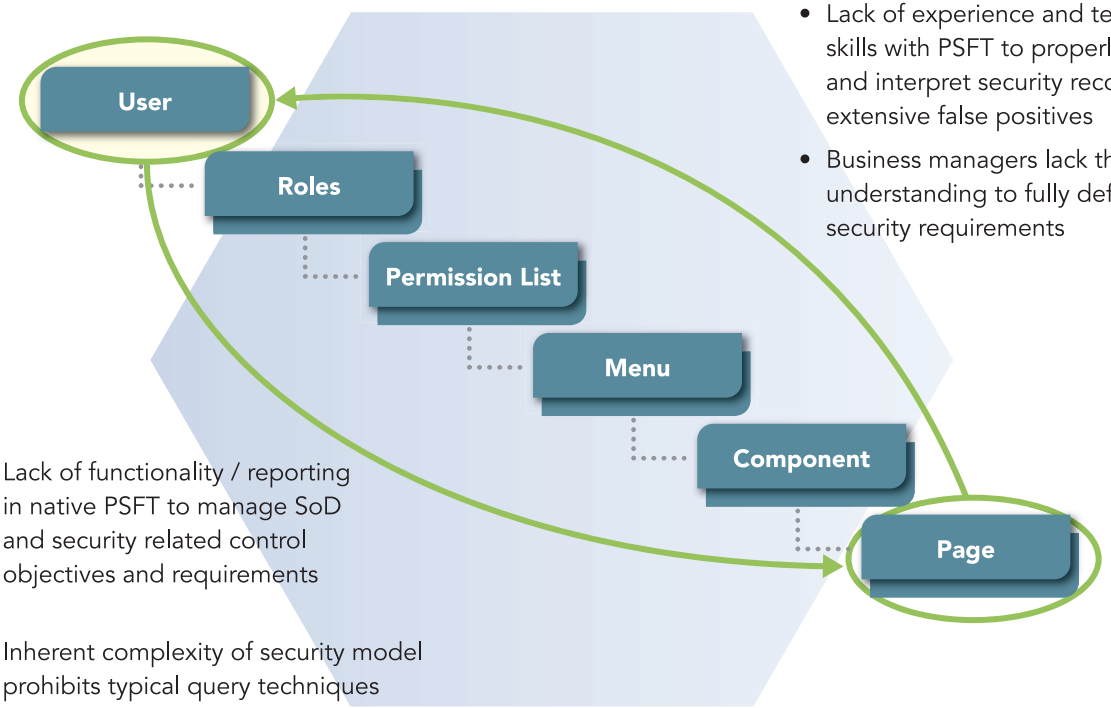
- Test by User
- Test by Privilege

Manage Segregation of Duties

- Identify incompatible Privileges
- Predefined & Extensible SOD Rule Sets

SafePaaS™

PeopleSoft



- Lack of experience and technical skills with PSFT to properly organize and interpret security records without extensive false positives
- Business managers lack the technical understanding to fully define compliant security requirements

- Lack of functionality / reporting in native PSFT to manage SoD and security related control objectives and requirements
- Inherent complexity of security model prohibits typical query techniques

SafePaaS™

Org Access

IP Ranges,
Login Hours

Object Access

Profiles

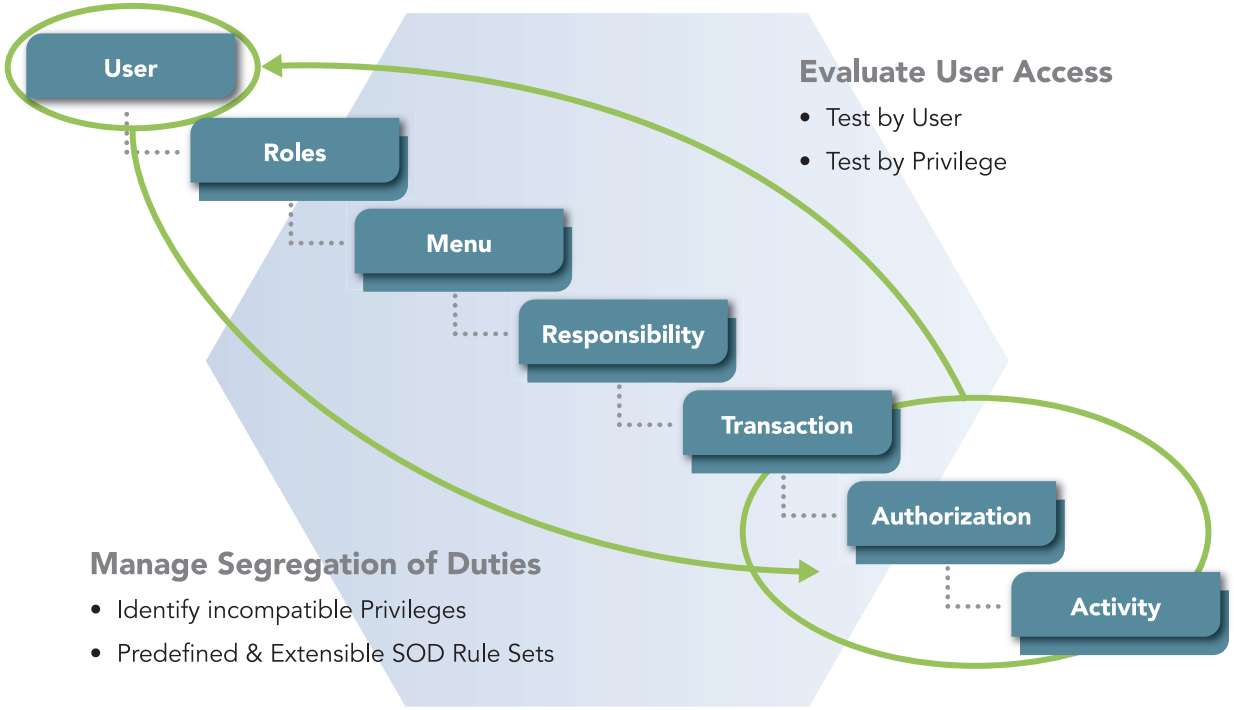
RecordAccess

Role Hierarchy

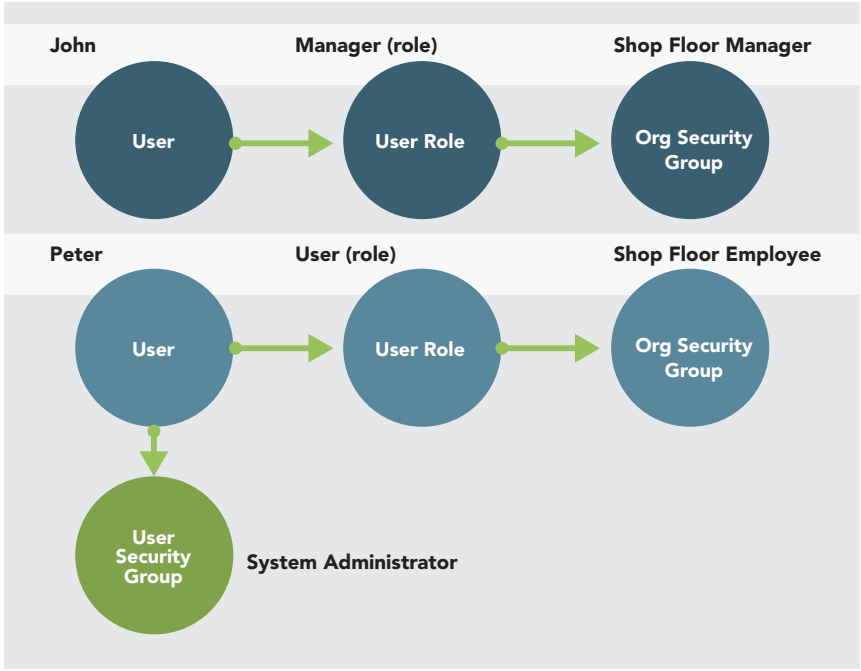
Field Access

Field Level
Security

SafePaaS™


User
Roles
Menu
Responsibility
Transaction
Authorization
Activity
Evaluate User Access
• Test by User
• Test by Privilege
Manage Segregation of Duties
• Identify incompatible Privileges
• Predefined & Extensible SOD Rule Sets

workday.



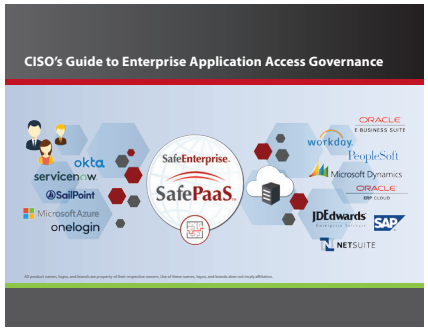
SafePaaS™

To learn more contact:

Emma.kelly@safepaas.com
https://www.safepaas.com/contact
https://www.safepaas.com/

You may be interested in our other ebooks:

Protect Your Business and Reputation by Securing ERP Application Access



CISO's Guide to Enterprise Application Access Governance

Transaction Monitoring with Machine Learning

Watch Demo