protiviti®

Face the Future with Confidence

Oracle Security in the Cloud

A Step-By-Step Approach to Building Strong Security Architecture During Oracle ERP Cloud Implementation and Redesign Projects

Internal Audit, Risk, Business & Technology Consulting

Executive Summary

Organizations are becoming more accepting of moving their key business applications to the cloud, including their enterprise resource planning (ERP) systems. For companies looking to move to Oracle ERP Cloud, the advantages are many — high scalability, consistent processes, real-time financial reporting and, not the least of all, cost savings from a hosted solution. Focusing on these benefits, however, should not obscure the need for a strong application security design aimed to deter fraud and ensure that transactions performed in the cloud are appropriate and authorized.

As auditors and the Public Company Accounting Oversight Board (PCAOB) continue to increase scrutiny of Segregation of Duties (SoD), it is important that organizations planning to implement Oracle ERP Cloud include a strong security design within their requirements and project plans.

In this paper, we discuss the steps to achieve a secure Oracle ERP Cloud system and avoid some of the common pitfalls in the process.

Introduction

Over the past few years, Oracle has been firmly shifting its software solutions portfolio model to the cloud, allowing organizations to focus more on business operations and less on back-end management of the supporting applications and infrastructure. As a result, organizations are rapidly transitioning off the standard on-premise, internally managed technologies in favor of a model that integrates key financial applications onto Oracle's cloud infrastructure stack, which requires only a browser and an internet connection to access.

The idea of the cloud has existed since the 1960s but has become more popular in recent years as computer processing power and bandwidth have made cloud-based services more accessible. Cloud computing leverages shared, elastic resources that can be delivered to users through self-service web technologies. This allows companies to use only what they need instead of purchasing resources and creating redundancies within their own data center.

Company board members and chief executives are becoming better educated in cloud capabilities and the potential cost savings, and chief information officers (CIOs) are increasingly asked to have a strategy for moving resources to the cloud. This strategy may include data center services, email, VOIP and phone services, Microsoft Office products, customer relationship management (CRM), and enterprise resource planning (ERP) solutions.

As more organizations begin developing their ERP cloud strategy, a number of considerations will drive executive decision-making, including compliance requirements and the impact that a cloud solution will have on the organization's internal control structure. Most notably, management will have to be proactive in planning for application-specific security to support strong segregation-of-duties (SoD) and appropriate sensitive access levels. Leading practices indicate that access should be granted based on a user's job duties as well as management's risk tolerance for performing conflicting functions (e.g., "Create a Supplier" and "Issue Payment to a Supplier").

A well thought-out and implemented ERP security design is the foundation for how the company's employees will interact with the application for years to come, allowing them to appropriately enter business transactions and interpret information used to manage the business. An effective design also scales with the growth of the organization without creating unexpected security gaps.

Companies that do not maintain consistency with a well-designed security model may face challenges during upgrades, acquisitions, employee hiring or termination, and other changes to the business. Consequences of a poorly executed security design include, but are not limited to:

- Errors stemming from entries by unauthorized personnel
- Unauthorized visibility into corporate information
- Fraudulent manipulation of financial information
- Theft of assets
- Inefficient access provisioning
- Regulatory and compliance issues

In the sections below, we explain key concepts and provide recommendations to achieve a robust security model and avoid these problems.

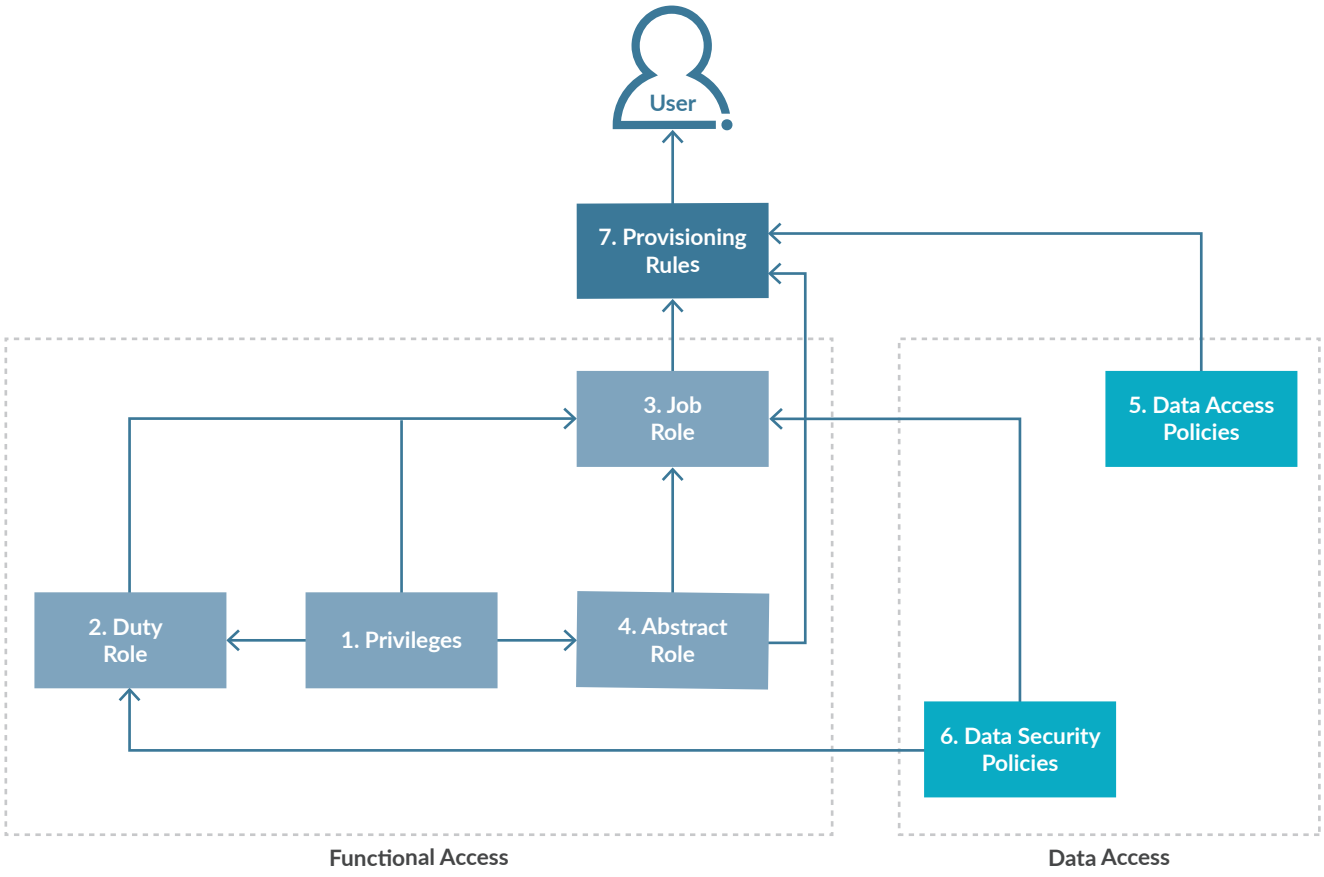
The Oracle ERP Cloud Security Model

The security model within Oracle ERP Cloud is very different from that of the traditional Oracle E-Business Suite (EBS) versions. Oracle has replaced the "responsibility" and "menu" containers with a role-based model that allows for a more robust and scalable approach to user administration.

The security models for Oracle ERP Cloud (Financials) and Oracle's other cloud applications (HCM, CX, SCM, EPM, etc.) are slightly different, and as such, our focus for this paper will be on Oracle ERP Cloud. However, the concepts for building and evaluating security can be applied toward the other applications.

Although the security design of the Oracle ERP Cloud applications can vary slightly for different offerings such as Financials and Human Capital Management, generally, the application security architecture can be separated into two considerations — functional access and data access. The different components of the Oracle ERP Cloud security model are discussed in detail below:

1. Privileges
2. Duty Role
3. Job Role
4. Abstract Role
5. Data Access Policies
6. Data Security Policies
7. Provisioning Rules



Functional Access

01 **Privileges** are the basic building blocks of functional access. Privileges determine what functionality a user is able to access and execute on his or her screen — all the available buttons, tabs, editable fields and reports able to be generated by a particular user. Privileges are the old "Function" concept within Oracle EBS and are very specific to the capabilities within a page. Examples of privileges include Create Payables Invoice, Validate Payables Invoice and Initiate Payables Invoice Approval Task Flow.

02 **Duty Roles** are made up of different privileges within Oracle ERP Cloud to perform specific actions with specific data; typically, they are very specific task-based activities within the business process. An example of a duty role is "Payables Invoice Creation Duty." The collection of privileges within this duty role would enable one to create and update an invoice, either through mass updates, updates through uploads or direct modifications within the invoice form. The duty roles are assigned directly to job roles. They are not assigned directly to a user. (Note: While duty roles can be assigned to other duty roles, it is not recommended to take this approach except when strictly copying an out-of-the-box role provided by Oracle.)

03 **Job Roles**, which should represent the specific jobs or positions within an organization, are a collection of duty roles that allow a person to perform specific job functions. For example, the job role "AP Clerk" would allow the user to perform those functions an accounts payable clerk should be able to complete as part of his or her job requirements. (Note: While job roles can be assigned directly to other job roles, it is not recommended to take this approach except when strictly copying an out-of-the-box role provided by Oracle.)

04 **Abstract Roles** are similar to job roles but define required tasks based on level of employment rather than job title. A simple example of this would be a role assigned to all employees for the intention of timecard entry, selecting benefits and reporting expenses. This role would be defined as the abstract role "Employee." Another example of an abstract role is "Line Manager," which, when assigned to managers, provides them the ability to perform certain tasks they would be expected to perform, such as approving time entries, managing goals for the team, etc.

Key point: *The key to taking a proactive security approach is establishing strong policies governing security design and a solid foundation of job roles that are conflict-free.*

Data Access

Prior to Release 12, data access was managed by data roles and data security policies. A security model introduced by Oracle for new users of Release 11 and all users of Release 12 eliminated the need for data roles. Data access is now managed by a combination of data security policies and data access policies. This new access functionality exists within ERP Cloud and Supply Chain Management (SCM) Cloud.

In EBS Financials, data security was managed through "Profile Options" and access was granted based on "Ledgers," "Operating Units" and "Inventory Orgs." This data model still applies, but instead of assigning data access to a responsibility, the data access is restricted through data security policies and data access assigned to users in Oracle ERP Cloud.

05 **Data Access Policies** are specific values of database resources. These resource values need to be assigned to each user and to each role that is provisioned to it.

For example, the job role "U.S. AP Clerk" would allow the user to perform all the functions of a payables clerk, but only within the U.S. business unit. The privileges inherited by the job role will allow the user to view and transact within all the appropriate business objects such as invoice and payment terms. The data security policy will restrict the access to only the specific business units assigned through the data access policies, in this case, the U.S. operating unit. This becomes very useful when larger companies have several employees with the same job title, but with each employee needing to work within a different set of data.

06 **Data Security Policies** define the permissible level of data access allowed in reference to a specific database resource, such as business unit, ledger and asset book, and are assigned to a job role. They act as the WHERE clauses to limit what data can be accessed by those database resources. Due to this, in order for a job role to reach the desired level of access, it may take several data security policies.

07 **Provisioning Rules** are the rules that define how access will be granted to users. They ensure that the integrity of the Oracle security model is maintained by laying down specific rules for maintaining user access requests. We discuss provisioning rules in more detail in Steps 4 and 5 in the next section.

Building Security Within Oracle ERP Cloud

Key point: *Managing security in Oracle ERP Cloud is a two-part process requiring configuration at the role level as well as the user level. Job roles inherit one or more data security policies along with privileges, which define the level of access the role has in regard to business objects. However, when this job role is assigned to a user on its own, it does not provide the user with access to the data. The data access and data security policies need to be defined in order for them to be able to access data and perform transactions.*

The Oracle ERP Cloud security model is very flexible. It allows customization of all the components mentioned above and allows these components to be used in various combinations in order to meet the security needs of an organization. However, that can lead to a complex and inconsistent security design. In this section, we will walk you through our recommendation about how to design and build security within Oracle ERP Cloud that is consistent and scalable.

It is important for organizations to take a proactive approach to designing their security models. Security requirements should be built into the blueprinting phase of the implementation to ensure that appropriate SoD is considered before the processes are implemented. In order to determine an organization's SoD requirements, management should identify business risks and define which risks are acceptable and what roles must be segregated.

Step 1: Define SoD and Sensitive Access (SA) Policies

SoD and SA policies, the foundation of a security model, define what functionality applications are acceptable and what actions should occur when a violation is identified. Before an organization defines its SoD and SA policies, it should develop a risk-ranking framework to ensure that all stakeholders are on the same page with regard to risk levels and definitions. This step is often overlooked or marginalized but is key to applying decisions consistently based on common business objectives.

A risk framework should define and rank the risks, and describe the action required for each risk. A risk ranking scale typically uses levels such as "High," "Medium" and "Low." The risk description should outline certain risk qualifiers that help determine the risk rating, and the required action should define whether remediation or mitigation is required. An example of a risk framework is outlined on the next page.

STANDARD SoD RISK CRITICALITY DEFINITIONS		
RISK RANKING	**RISK DESCRIPTION**	**REQUIRED ACTION**
CRITICAL	Access granted to multiple critical areas related to user management, table access, program access, batch processing, system change management functions, approval authority and other management override activities. Authority given to individuals who are part of senior management or are core transactional users. (Examples: "Create or Post Journals" and "Create or Modify Users")	Remediation Required
HIGH	Access granted to multiple business-sensitive areas directly relevant to financial reporting, such as financial close, procure-to-pay and order-to-cash processes. This could result in financial reporting errors or misstatements. (Examples: "Create or Post Journals" and "General Ledger Setups")	Remediation Preferred, Mitigation Required
MEDIUM	Access granted to allow users the ability to execute day-to-day transactions that involve creation, change and reporting on operational information. Conflicting access could result in data integrity and availability issues. (Examples: "Create Invoices" and "Open and Close Purchasing Module Periods")	Mitigation Preferred, No Required Action
LOW	Access granted to allow users to display operational information that may contain confidential or sensitive data that allows them to adjust transactions as necessary. (Examples: "View Item Costing" and "Create Sales Orders")	No Required Action

After an organization has defined its SoD framework, it must also define an SA framework. This framework will use the same concepts as the SoD framework, but the definitions and expected actions will be slightly different. For "Required Action," the expectation regarding monitoring frequency (quarterly, biannually, annually, ad hoc, etc.) should be defined. Organizations may also choose to include certain provisioning approval requirements based on their risk tolerance.

With a SA framework in place to support decision-making, the organization must define its SA policies and the associated risk rankings. When establishing policies, it helps to develop a comprehensive list of business activities (e.g., "Create a Supplier") that can be prioritized for items that are relatively sensitive to the organization's business processes. This list should include all standard and custom functionalities within the system and should be vetted thoroughly with all key business process owners as well as functional and compliance leads. Once an organization has defined its SA policies, it is able to leverage the list of sensitive business activities to identify the conflicting potential functionalities that will be the basis for its SoD policies. Organizations should identify those key business activities that, when in conflict, create a violation that aligns with the definitions within the SoD framework, and assign a risk ranking to these activities based on the descriptions within its SoD framework. Finally, policies and risk rankings must be documented, as they form the basis for the organization's SoD and SA rulesets.

Once the business activities and conflicting functionalities among them have been defined or identified, associated privileges should be mapped to those activities and functionalities. The privilege assignment is a prerequisite for the assessment of the organization's role design. Remember to include any custom privileges (privileges specific to the organization) in the organization's ruleset to ensure that it is comprehensive.

Key point: *Key business process owners, functional leads, and risk and compliance leads should be involved in developing the list of key business activities, conflicting activities and risk rankings to ensure that the list addresses comprehensively the risks of the entire organization. In some cases, the sign-off of this step is a critical audit artifact that should be documented and retained as audit evidence.*

Step 2: Identify and Implement a Security Assessment Tool

To ensure appropriately designed and conflict-free roles, organizations should use a security assessment tool to help shape their security design and build. There are a few tools on the market that provide this capability, including Saviynt, Fastpath and Oracle. (Oracle recently released Advance Access Control Cloud Service only for Oracle ERP Cloud Release 13.) If, during design, the organization is not prepared to invest in a software solution, organizations can leverage third-party snapshot tools such as Protiviti's Assure for Oracle ERP Cloud. These snapshot tools support the assessment process to ensure an appropriate design when developing the organization's job roles. While third-party tools can help in the short term, a longer-term solution such as one of the tools described above should be considered to ensure that the organization's investment in security design is protected.

Step 3: Design and Build Conflict-Free Roles

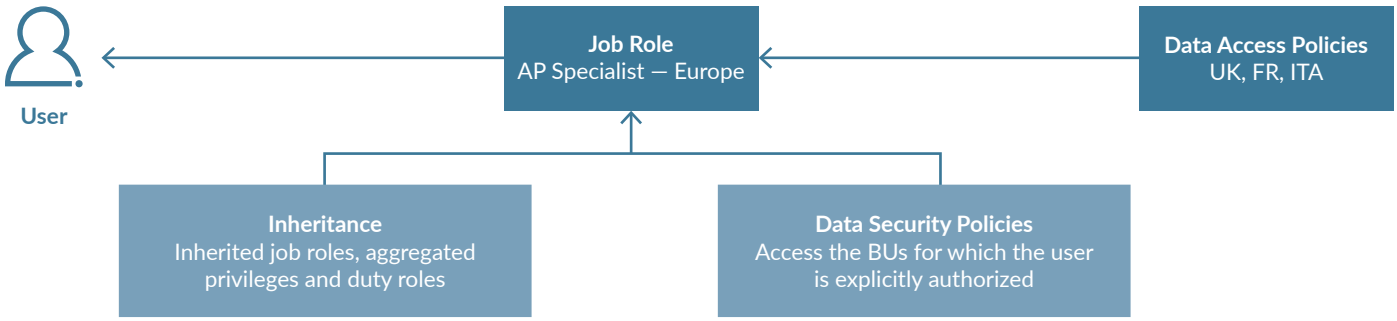
Designing roles that are free from SoD conflicts early in the Oracle ERP Cloud project can lead to increased granularity and more restrictive access, as well as increased transparency related to the access given to a user.

In addition, conflict-free roles can reduce ongoing security maintenance, because user access can easily be modified to accommodate changes in a user's job responsibilities resulting from the implementation of new Oracle functionality and/or organizational realignment.

The initial role design starts by reviewing the future-state business processes and conducting a preliminary analysis of the user access requirements as well as the individual functional tasks that will be performed once the new system goes live. At this point, the Oracle application security team will begin to group privileges and data security policies into the basis of duty roles. Duty roles will then be combined to create job roles that are specific to the job requirements of the user in the organization, and abstract roles will be assigned based on the position of the user within the organization. Job roles can then be restricted to access only a subset of data specific to a business object by creating a data access policy.

Key point: *The security console is an administrative interface used for security management that was released as part of Oracle ERP Cloud Release 9 and has since become a very user-friendly way to manage application security. Using the console, a user can create custom job, abstract and duty roles; compare all role types; review role assignments and hierarchies; and perform several user management tasks.*

Data access policies are particularly useful in shared services environments. Take, for example, an organization where the same team manages payables activities for all of Europe. A user could be provisioned with the "AP Specialist" job role and multiple business units could be assigned to this job role through the data access policies. The data access policies, along with the data security policies, will allow the user access to the data for all of Europe.



Below are some examples of how data security policies and data access policies can be configured to provide a robust and secure data access framework.

USER	JOB ROLE ASSIGNED TO USER	DATA SECURITY POLICY APPLIED TO JOB ROLE	DATA ACCESS POLICY APPLIED TO USER	DATA ACCESS
JOHN DOE	Accounts Payable Manager	Access the **Business Unit** for which the user is explicitly authorized.	**None**	No Access Granted
ALLEN JONES	Accounts Payable Manager	Access the **Business Unit** for which the user is explicitly authorized.	Business Units Associated with User: **Detroit**	Allen granted access to data only in the Detroit Business Unit.
JANE SMITH	Accounts Payable Manager	Access the **Business Unit** for which the user is explicitly authorized.	Business Units Associated with User: **All Business Units**	Jane granted access to data in all Business Units.
ORLANDO RODRIGUEZ	Accounts Receivable Manager	Access the **Ledger** for which the user is explicitly authorized.	**None**	No Access Granted
SUSAN HAWTHORNE	Accounts Receivable Manager	Access the **Ledger** for which the user is explicitly authorized.	Ledgers Associated with User: **US Ledger**	Susan granted access to data only in the US Ledger.
MIKE RAWLINS	Accounts Receivable Manager	Access the **Ledger** for which the user is explicitly authorized.	Ledgers Associated with User: **All Ledgers**	Mike granted access to data in all ledgers

Some examples of Oracle seeded roles with inherent conflicts are as follows:

JOB ROLE	# OF HIGH RISK CONFLICTS	CONFLICTS
ACCOUNTS PAYABLE MANAGER	9	AP Invoice Entry & AP Release Payables Invoice Hold AP Release Payables Invoice Hold & AP Payments AP Setup & AP Invoice Entry AP Setup & AP Payments AP Supplier Master & AP Invoice Entry AP Supplier Master & AP Payments GL Journal Entry & GL Journal Post GL Open and Close Periods & AP Payments GL Open and Close Periods & GL Enter OR Post Journals
ACCOUNTS RECEIVABLE MANAGER	8	AP Supplier Master & AP Invoice Entry AR Customer Master & AR Cash Receipts AR Customer Master & AR Transactions AR Open and Close Periods & AR Cash Receipts AR Open and Close Periods & AR Transactions AR Setup & AR Transactions GL Journal Entry & GL Journal Post GL Open and Close Periods & GL Enter OR Post Journals
ASSET ACCOUNTING MANAGER	2	FA Setup & FA Depreciation GL Journal Entry & GL Journal Post
GENERAL ACCOUNTING MANAGER	5	AR Customer Master & AR Transactions AR Open and Close Periods & AR Transactions GL Accounting Setup & GL Enter OR Post Journals GL Journal Entry & GL Journal Post GL Open and Close Periods & GL Enter OR Post Journals

Following the initial grouping of privileges and duty roles, business process owners (BPOs) should validate, through a series of workshops, that the respective Oracle ERP Cloud job roles are aligned with the future business processes and organizational structure (or, in the case of security redesign projects, existing business processes). A naming convention should be established that helps articulate the level of access each role is granting as well as the privileges that have been assigned to each role.

Key point: *Oracle comes with a set of pre-built, or "seeded," duty roles that have inherent conflicts to accommodate a goal toward user convenience. Oracle explicitly advises that the roles should be customized to align with each organization's functional user needs and risk tolerance.*

It is a good idea to incorporate the SA rankings within the role's name to clearly identify which roles require additional levels of approval. The roles will then be documented and will consist of the role's technical name along with its underlying privileges and assigned data security policies.

When designing role security for an organization, keep these recommendations in mind:

- Maintain the convention of only assigning privileges to duty roles, duty roles and abstract roles to job roles, and job roles to users, in order to ensure a well-structured, consistent and scalable role design.
- Develop a strong naming convention that clearly articulates the role's purpose to ensure that end users, management and system administrators are all aware of that role's capabilities.
- Limit the duplication of key functions across multiple job roles as much as possible.
- Incorporate an SoD tool into the design process to ensure that roles are developed free of conflicts.

Step 4: Assign Roles, Test and Implement

There are a number of steps that need to be performed before an organization's security design is considered complete and can be implemented along with Oracle ERP Cloud.

User Mapping – Based on organizational structures and process owner input, roles should be mapped to each system user. This is typically done in a spreadsheet or simple database used by the security team.

User Assignment – After approvals are received, the final mappings are translated to assign the actual Cloud ERP roles to the users within the test systems.

User Assessment – After assignments, it is highly recommended to run the SoD and SA assessment tool again to determine if the combination of roles has created any new conflicts within a user's assigned security. If conflicts are identified, they should be addressed either by assigning that responsibility to someone else, or through the identification of mitigating/compensating controls. This may be an iterative cycle until risks are brought to an acceptable level prior to going live.

User Acceptance Testing (UAT) – Ideally, roles and user assignments are tested as early as possible, but this formal step is an absolute requirement. It validates that users have the ability to accomplish all tasks they will be expected to perform at go-live.

Go-Live – At this point, all roles have been designed and assigned and are ready to be used by the user population. Security personnel should be on hand for at least two weeks after go-live to respond to the need for tuning during the early use stage.

Key point: *Oracle ERP Cloud provides a security feature called role provisioning rules that determines which roles can be assigned to a user. These rules are defined for the roles on the user-role mapping list and have a specific set of conditions, such as the business unit or department, which the user must satisfy in order to be provisioned the role. This provides a strong line of defense for incorrect assignment of roles to users and the subsequent potential for fraud. This feature is particularly useful for provisioning birthright roles that all employees within an organization are assigned. However, applying this feature for all roles can create a very rigid role provisioning process that does not consider scenarios the business may encounter, such as emergency access for issue resolution or backup access provisioning for employees on vacation.*

Step 5: Implement Ongoing Maintenance and Proactive Security Design Management

In order to maintain the integrity and conflict-free design of an organization's security, organizations should establish provisioning rules and role maintenance processes to guide how users gain access to the Oracle ERP Cloud environment. These will serve as the first line of defense for an organization's security design and will dictate how individuals obtain access to the system. Key provisioning processes that should be implemented include:

- Integrated SoD checks when granting users access to the different job roles
- Regular SoD reviews and validations
- Identification and assignment of mitigating controls for authorized conflicts
- Escalated approvals for individuals requiring elevated levels of access — for example, for system administration or organizational setups
- Granting of temporary access to IT individuals who need it to support a production issue or implement a change

Provisioning processes will proactively manage who has access to the ERP system and each person's level of access. However, the business needs of all organizations evolve, and security changes may need to be made to accommodate them. To ensure the continuity of the ERP security design, organizations must develop proactive processes that maintain the integrity of the current role design and continue to validate that access is appropriate. These key processes include:

- Strong role change management processes to ensure that changes to the current role design are necessary, redundant security roles are avoided and the roles remain free of SoD conflicts
- Regular user access reviews to validate that the granted access is still appropriate
- Ruleset review and process updates to ensure that the ruleset is still relevant and that it applies to the current business processes being performed within the system

If thorough controls processes are not in place, updates and changes made to the organization's environment over time are likely to cause conflicts, which can pose varying levels of risk to the business and may ultimately force the organization to revisit its security design.

Conclusion

Designing, configuring and implementing Oracle ERP Cloud application security is a complex and resource-intensive endeavor. However, the long-term benefits of fraud prevention, scalability and compliance efficiency are worth the effort, particularly if security can be a robust focus in the early stages of Oracle implementation projects. Further, access risk is not managed by the service provider and, as such, organizations should take ownership of security requirements in alignment with their risk tolerance.

By following the five stages outlined in this paper, companies can achieve scalable, highly effective control over user access while avoiding the unnecessary costs related to compliance issues and the need for redesigning their Oracle security in the future.

ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 75 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Ranked 46 on the 2018 *Fortune* 100 Best Companies to Work For® list, 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 ORACLE APPLICATION SECURITY AND SOD PRACTICE

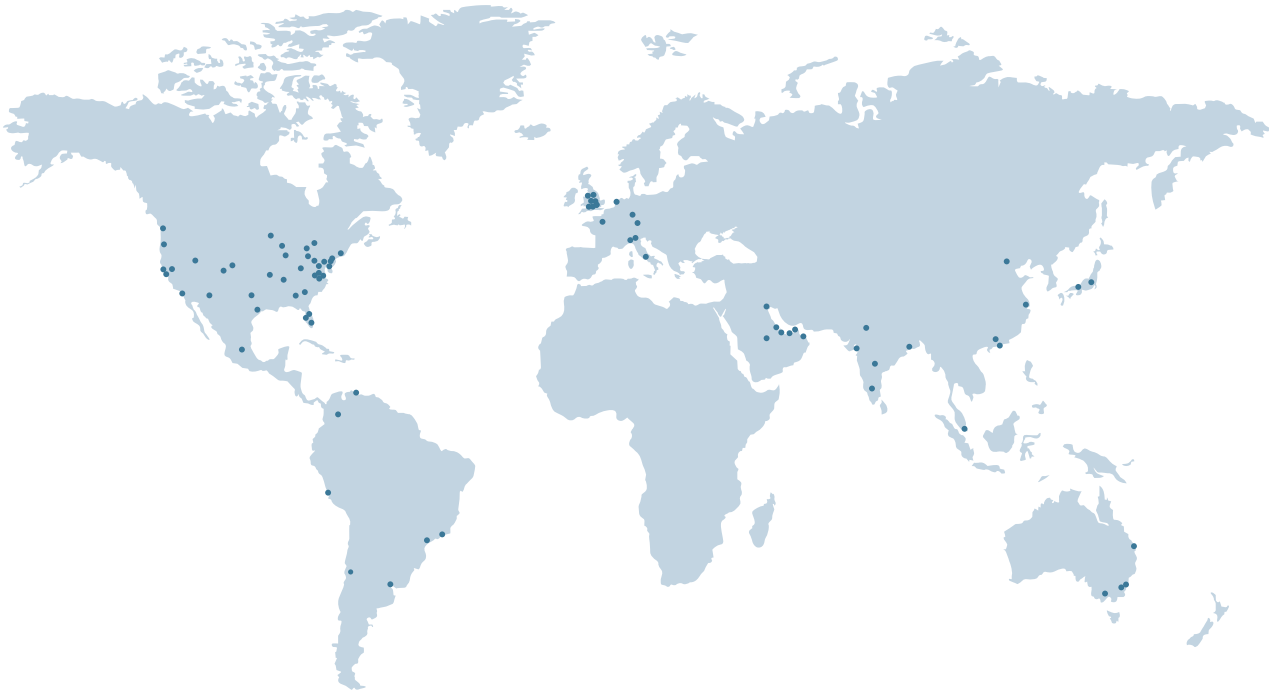
Protiviti's Application Security and SoD professionals provide Oracle Access Control and Oracle Security guidance and implementation support to ensure that organizations better understand and manage risks around their ERP applications and supporting systems. We assist with the identification and effective management of security and application access risks across the organization's enterprise architecture to help organizations realize their desired business efficiencies while protecting their information from unauthorized access.

In addition, Protiviti provides ERP services to clients such as solution design, control optimization, Advanced Access Control implementation and ERP audits.

CONTACTS

Martin Nash
+1.813.348.3374
martin.nash@protiviti.com

Kevin McCreary
+1.404.926.4322
kevin.mccreary@protiviti.com



THE AMERICAS

UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
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

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE & MIDDLE EAST

FRANCE
Paris

GERMANY
Frankfurt
Munich

ITALY
Milan
Rome
Turin

NETHERLANDS
Amsterdam

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®