Oracle Security in the Cloud

A step-by-step approach to building strong security architecture during Oracle ERP Cloud implementation and redesign projects

Powerful Insights. Proven Delivery.®
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 white paper, we discuss the steps to achieve a secure cloud system and avoid some of the common pitfalls in the process.
INTRODUCTION

Over the past few years, Oracle has been shifting its software solutions portfolio to the cloud to allow organizations to focus on business operations, with less time spent on back-end management of the supporting applications and infrastructure. As a result, organizations are increasingly transitioning off the standard on-premise, internally managed technologies in favor of a model that migrates 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 centers.

Company board members and chief executives are becoming better educated about 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, and customer resource 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 SoD and appropriate sensitive access levels. Leading practices indicate that access should be granted based on users’ job duties as well as management’s risk tolerance for performing conflicting functions (“Create a Supplier” and “Issue Payment to a Supplier,” for example).

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 CLOUD ERP SECURITY MODEL

The security model within Oracle ERP Cloud is very different from that of 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 application security architecture consists of six main components, discussed in detail below:

1. Privileges
2. Duty roles
3. Job roles
4. Data security policies
5. Data roles
6. Provisioning rules

Privileges are an attribute of duty roles. The privileges assigned to a duty role determine what functionality a user is able to access on his or her screen – all the available buttons, tabs, editable fields and reports capable of being generated by a particular user. Privileges are the old “Function” concept within Oracle EBS. Privileges are very specific to the capabilities within a form or menu – for example, Create Payables Invoice, Validate Payables Invoice, or Initiate Payables Invoice Approval task flows.

Duty roles are made up of different privileges within Oracle ERP Cloud. The duty role is a collection of privileges aggregated to perform specific actions; 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, including through mass updates, updates through uploads, or direct modifications within the invoice form. The duty roles are the fundamental building blocks of Oracle ERP Cloud and are assigned directly to job roles. They are not assigned directly to a user.

Job roles, which should represent 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. The job role can be assigned directly to the user.
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 security policies define on which data sets a user can perform his or her job. For example, the data role U.S. AP Clerk would allow the user to perform all the functions of the job role AP Clerk within the U.S. operating unit.

Data roles should be established according to the structure of the enterprise. In Oracle EBS, data security was managed through “Profile Options,” and access was granted based on “Ledgers,” “Operating Units” and “Inventory Organizations.” This data model still applies, but instead of assigning data access to a responsibility, the data access is restricted through data security policies. The combination of job role and a data security policy creates the data role that is assigned to the user.

Key Point: Data roles inherit job roles that give them access to specific functionalities (through duty roles) and provide access to specific data sets on which to perform those functionalities. It is recommended that users are provisioned through data roles and not job roles.

Data roles should be created based on the various transactional needs of the organization and should consider the business units, warehouses, distribution centers and shared services that will be supporting each transaction. Management should take data integrity into account when designing and assigning the data roles by restricting data access to the business units in which the ERP users transact.

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 processes 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

It is important that organizations 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 their key risks and define what sort of conflicts are acceptable and what roles must be segregated.

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

SoD and SA policies, the foundations of a security model, define what functionality applications are acceptable and what actions should occur when a potential 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 the 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 below:
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 the organization’s risk tolerance.

With an SA framework in place to support decision-making, the organization must define its specific 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 be vetted with all key business process owners and functional leads.

Note: “N/A” is acceptable as a ranking if it is determined that the access does not align with any of the organization’s risk rankings or if the organization believes the risk does not require specific attention. For example, the organization’s business process may allow everyone with Oracle ERP Cloud access to create purchase orders, because all purchase orders must be approved prior to being fulfilled. Thus, creating a purchase order may not be a significant business activity that requires monitoring and may not be included in the organization’s SoD or SA policies.

Once an organization has defined its SA policies, it can leverage that list of business activities to identify conflicting activities, which 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.

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.
Once the business activities and the conflicting activities among them have been defined, associated privileges should be mapped to those activities. 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.

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 for the Oracle EBS environment. However, these are not currently compatible with Oracle ERP Cloud software. Oracle will provide this capability with its soon-to-be-released Advanced Access Control Cloud Service offering, which integrates with the security administration module to support the ongoing monitoring process. Until then, leveraging third-party snapshot tools, such as Protiviti’s Assure for Oracle ERP Cloud, can help support the assessment process to ensure an appropriate design when developing the organization’s job and data roles.

While third-party tools can help in the short term, a longer-term solution such as the always-on Oracle Advanced Access Control Cloud Service should be considered once the organization goes live with Oracle ERP Cloud.

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 tasks that will be performed once the new system goes live. At this point, the Oracle application security team will group privileges on the basis of duty roles. Duty roles will then be combined to create roles specific to the job or position of users in the organization.

Job roles can be refined further by restricting their access to a subset of data specific to a business unit. This is done by creating a data role that inherits the job role and adding a data security policy to it that restricts data access to a specific business unit. A data role template simplifies this process. The template specifies the job roles and data dimensions that can be combined to arrive at a set of data roles for the organization.

Example: A data role template contains the job role Accounts Payable Manager, with the access and privileges appropriate for that role, and a dimension called Operating Unit. If there are two dimension values for each operating unit – U.S. Operating Unit (US OU) and Canada Operating Unit (CA OU) – this template would generate two data roles: Accounts Payable Manager-US OU and Accounts Payable Manager-CA OU. The template generates the data roles in accordance with a naming convention defined by a data role naming rule.
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 and data 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.

It is a good idea to incorporate the SA rankings within the roles’ names 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.

Key Point: Oracle comes with a set of pre-built, or “seeded,” duty and job 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. For organizations that choose to use the “seeded” roles, it is a leading practice to make a copy of them rather than use the originals. This way, when Oracle applies automatic patches, the organization will be protected from unwanted role updates that may unknowingly cause adjustments to the original security design. All patches that involve changes to security should be reviewed and validated to determine the impact of the patch on the roles’ design and identify which changes may require modifications to the security model.

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

- Maintain the convention of only assigning privileges to duty roles, duty roles to job roles, job roles to data roles and data 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 system.
- 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 either be addressed 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.
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 after go-live. Remember our security model from page 3:

- 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 rules and processes, the first line of defense for an organization’s security design, will dictate how individuals obtain access to the system. Key provisioning processes that should be implemented include:

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 control 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 70 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 57 on the 2016 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 ERP Solutions Practice

Protiviti’s ERP Solutions practice, and specifically Oracle Security and SoD professionals, provide access control and 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

Carol Raimo
+1.212.603.8371
carol.raimo@protiviti.com

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

John Harrison
+1.713.314.4996
john.harrison@protiviti.com