Buyer's Guide for Identity Administration

An Oracle White Paper
March 2009

ORACLE

Note:

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Buyer's Guide for Identity Administration

INTRODUCTION

Front-page headlines describing security and privacy breaches are daily reminders of the elevated threat environment facing businesses today. Governmental and regulatory compliance also demand that today's corporations carefully manage and control user access to sensitive data, satisfy audit requirements and enforce tight control over system resources. With such intense external pressure, today's corporations are carefully examining their information systems security implementations. But what tools exist to help manage these diverse identity and access management problems?

Many corporations are turning to identity administration software solutions to address information security concerns. Identity administration refers to software solutions that manage and maintain identity data for a variety of tasks such as single sign on, provisioning and consolidation of accounts across multiple systems. Although there are many software components that make up identity administration, this white paper will focus on how two components, enterprise role management and user provisioning, address critical business needs and also describe the business benefits to implementing this combination of solutions.

User provisioning systems help automate the creation and management of user accounts and entitlements to information systems, For example, when bringing a new employee on board, a provisioning solution can ensure that a new employee automatically gets the access he or she needs on day one. User provisioning provides a cost-effective way to deliver vital security controls over information systems while also automating tasks that can take much longer when done manually.

However, many businesses with a pure provisioning strategy are running into trouble when significant business events, such as a re-organization, occur. Provisioning systems are not "business smart" and cannot fully model and react to significant business events that demand automated changes to user access.

Additionally, provisioning systems encourage access decisions where user access is modeled after existing users – rather than determined by a specific business attribute or relationship that could change, such as being a member of a project team. The end result is that access to systems and information can quickly go against corporate policy, or worse, violate governmental regulations.

Provisioning is clearly a key component to an identity management enterprise strategy, but today's complex corporations are demanding more than just automation. Role based access control or RBAC systems can provide additional capabilities to help organize and control user access to critical business systems based on unique business data, such as the location the employee is in or the relationship a person has to a project. Role based access control systems provide the extra "business smarts" to determine user access, taking a traditional provisioning solution to the next level. Some of the factors driving this interest in role based access control include:

- Provisioning deployments without enterprise role management cannot manage and drive provisioning based on complex business relationships or organizational information.
- Organizational demands to strengthen regulatory compliance through detailed audits on who should have access to what, and why a user was given access.
- Business demands to ensure that user access changes when business events, such as re-organizations or mergers occur.
- Requirements to have an authoritative model of business and operational data for analysis and compliance reporting.

Enterprise role management systems can augment existing user provisioning solutions and provide the necessary tools to drive provisioning events based on policies or rules that are sensitive to business context. Organizations have found that by implementing an enterprise role management system in combination with a user provisioning system they are able to ensure that as the business changes, access and privilege changes are automated as well.

This paper will provide a detailed list of product features and vendor capabilities that many customers consider when evaluating these components of an identity administration solution.

IDENTITY ADMINISTRATION OVERVIEW

Enterprise security architectures are integrated, coherent sets of services for securing applications and data throughout the

organization. As opposed to a security infrastructure, enterprise security architecture reflects the strategic decisions on the part of an organization's management that guide application development, procurement and deployment decisions. Some of the advantages of adopting and deploying enterprise security architectures include:

- Enabling enterprises to deliver a consistent level of application security across all of the applications deployed in the enterprise.
- Reducing the cost of securing and managing applications by allowing all applications to leverage a common set of services and interfaces.
- Permitting application developers and administrators to more easily leverage best practices for securing and managing applications.
- Providing a framework for application-level interaction with other organizations doing business with the enterprise.
- Providing a basis for better application procurement and deployment decisions.

Role management and user provisioning solutions are two key components of an identity administration solution.

Identity administration systems are essential components of enterprise security architecture. Figure 1 provides an overview of the identity administration components of enterprise security architecture. These include:

- Access control services, for securing access to web-based, legacy and web services applications, both within and across the extended enterprise.
- Authorization and entitlement services, including authorization of users at defined policy decision points as well as the management of entitlement data across multiple resources.
- Identity administration services, including administration of users, role-based access control, automatic provisioning of users to applications, and automation of periodic compliance-driven processes such as attestation.
- Directory services, including repositories for storing and managing identity information, as well as integrating identity information from across the organization.
- Audit and compliance services for recording information on changes in the identities and privileges managed in the

environment, and enforcing key administrative controls such as separation of duties.

- Management services, which ensure that the other services within the architecture are deployable, manageable, and deliver the required service levels.

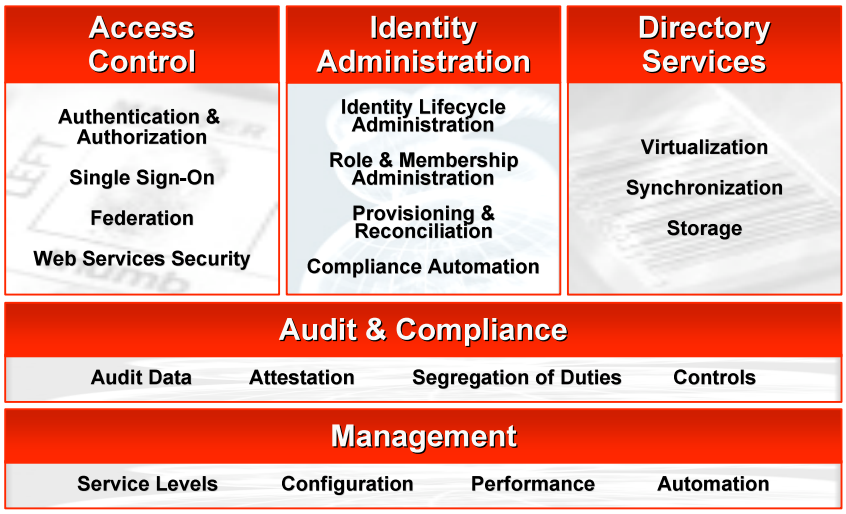

Figure 1: Identity administration components of enterprise security architecture.

When combined with a user provisioning solution, enterprise role management systems can address the identity administration functionalities highlighted in figure 1.

Examining Enterprise Role Management

Enterprise role management systems provide a comprehensive feature set for role lifecycle management as well as business and organizational relationships and resources. Most businesses today manage a complex ecosystem including vendors, partners, and professional services teams in addition to full time employees. However, most businesses today need to find a "smart" way to grant access to different resources in order to ensure that business can run smoothly. Enterprise role management solutions define user access by abstracting different resources and entitlements as roles. These solutions offer the ability to model business data such as organizations, locations and reporting structures that can be used to drive role membership according to rules or policies. When combined with a provisioning system,

these automated rules ensure that user access will change when the business changes, providing a level of flexibility that adapts well to complex and dynamic relationships in today's organizations.

The ideal enterprise role management solution also offers critical functionality to address compliance concerns, such as providing reports on role membership, auditing historical role membership, providing periodic review of role membership and role definitions. Another feature of an enterprise role management solution is the ability to seamlessly integrate with a provisioning product to ensure that roles and role membership changes drive automated provisioning events.

The next section of the whitepaper examines the standards that exist for identity administration solutions.

Standards for Role Based Access Control

In 2000, the U.S. Department of Commerce's National Institute of Standards and Technology proposed a unified model for RBAC, which was adopted by the International Committee for Information Technology Standards (INCITS) in 2004. The standard for RBAC, known as INCITS 359-2004, describes a common model and vocabulary of terms to define RBAC features. Long recognized as way to organize privileges and responsibilities, the key feature of the RBAC standard defines all access through roles. A user's role in an organization for example determines what access he or she is authorized for. Roles provide a meaningful way to organize and simplify the management of user access.

Many industries and governments have decided to manage user access using the benefits of a role-based solution. Both the US Health Insurance Portability and Accountability Act of 1996 (HIPPA) and the US Federal Aviation Administration (in specifications for the National Airspace Systems security) cite RBAC requirements as the secure approach to user access control.[1] The general nature of the RBAC specification allows IT systems to be built in a variety of ways that address the requirements of the specification, including the following three rules:

- Role Assignment – All active users must be assigned to a role before access is granted.

[1] *Role-Based Access Control, Second Edition,* Ferraiolo, Kuhn, Chandramouli, 2007

- **Role Authorization –** Each role assignment to an active user must be authorized by an authoritative source before the assignment is considered valid.
- **Transaction Authorization –** Active users can only execute transactions for which their assigned roles permit.

The RBAC specification provides a clear path to implementing a core tenet of access control administration: the principal of least privilege. This principal simply states that users should be assigned the least amount of permissions necessary for the user to perform his or her job.

When considering an enterprise role management solution, it is important to find a solution that has been engineered to support the ANSI INCITS 359-2004 RBAC specification.

Evaluating Identity Administration Solutions

Candidate enterprise role management solutions should be evaluated for functionality, deployability, scalability, auditing and vendor capabilities.

At a high level, requirements for identity administration solutions can be considered in four categories:

- **Functionality –** Does the system deliver the key functionalities the organization requires to administer user access according to roles? These include comprehensive features for role lifecycle management, seamless integration with a provisioning system, tools to model organizations and business relationships and support for complex role membership policies.
- **Deployability and Supportability –** Does the system include the tools and interfaces for managing deployments, migrations and ongoing system administration? Does the system support the various application infrastructures deployed in the organization? Can it meet the scalability and availability requirements of the organization, and are the user interfaces customizable and easy to deploy?
- **Auditability** – Does the system support the organization's audit and reporting processes? Does it provide the ability to generate role membership and audit reports as well as support role membership attestation processes?
- **Vendor capabilities –** Does the vendor have the demonstrated ability to provide global support for the product? Does the vendor demonstrate technology leadership and continued investment in the product area?

More detailed requirements associated with these high-level categories are provided in the next section. This white paper will

next consider some of the benefits of deploying an identity administration solution.

Addressing Security Risk with Identity Administration

Role management systems address the three aspects of CIA: confidentiality, integrity, and availability.

Security risks to information systems can be broadly categorized into three categories. Known as "CIA" to cue the memory, "C" stands for the need to maintain confidentiality of the information managed by the system, "I" stands for the integrity of that information, and "A" stands for the availability of the systems or information under management. To analyze how identity administration systems address information security risks, it is helpful to review each category with a focus on RBAC:

- Confidentiality – RBAC impacts the confidentiality of systems' data by ensuring that authorized role assignments dictate which users can access applications and data on various enterprise systems. It also promotes the confidentiality of identity, organization and role information by leveraging RBAC principals for the internal system security of the enterprise role management solution.
- Integrity – RBAC impacts systems integrity by enforcing a least-privilege model for user access governed by role assignment. As role assignments change, users' privileges change to ensure that they no longer have permissions on systems they are no longer authorized to access. Combining an enterprise role management system with a provisioning solution ensures that role assignment changes result in automated user access changes. This combination promotes integrity by preventing modifications to application data by unauthorized users.
- Availability –When combined with a provisioning system, an enterprise role management system accelerates the process whereby authorized users are granted access to applications through role assignments, speeding the organization's response to events such as new hires and employee job changes.

A well-designed, well-implemented identity administration solution provides essential information system security controls and represents a key component of an information security program.

ORACLE'S ENTERPRISE ROLE MANAGEMENT SOLUTION: ORACLE ROLE MANAGER

Oracle Role Manager, part of Oracle's Identity and Access Management offering, is Oracle's solution for role based access control and role lifecycle management. This section provides a high-level description of the functional components of Oracle Role Manager.

Solution overview

A functional overview of Oracle Role Manager is shown in Figure 2. As shown, the solution embodies nine major functionalities to provide role based access control. These are:

- Contextual Role Resolution functionalities include roles that can calculate membership automatically based on business relationships (e.g. who reports to whom, what organization a person is member of)
- Polyarchy and Relationship Management functionalities allow users to model and define relationships that exist between multiple hierarchies and objects, relationships common to today's organizations. This unique capability allows role membership to be based on up to date business information to ensure that user access is secure.
- Business Role Management allows users to manage the lifecycle of a type of role known as a Business Role that can collect groups of users that share a common business function. Providing an out of the box role model that includes Business Roles is a widely recognized successful strategy for enterprise role engineering.
- Hierarchy Management functionalities allow users to model multiple business hierarchies such as locations, cost centers and reporting organizations. The attributes and relationships contained within these hierarchies can then be used in role membership rules.
- IT Role Management allows users to manage the lifecycle of a type of role known as an IT Role that can collect groups of entitlements or permissions. Providing an out of the box role model that includes IT Roles is a widely recognized successful strategy for enterprise role engineering.
- Role Mining functionalities provide a bottom-up approach to role engineering. This process helps to accelerate role engineering and data cleanup in preparation for an enterprise role management deployment.

- **HR and LDAP Organization Hierarchies** allow users to model HR and LDAP hierarchies that are already present in the corporate IT infrastructure. The attributes and relationships contained within these hierarchies can then be used in role membership rules.
- **Application Entitlements** allow users to map the appropriate application entitlements or permissions to roles. This data, provided by a provisioning system, helps role engineers clearly define "who should have access to what?"
- **Reporting, audit and compliance** describe the framework and tools necessary to track, report and verify all of the significant events performed by the enterprise role management solution.

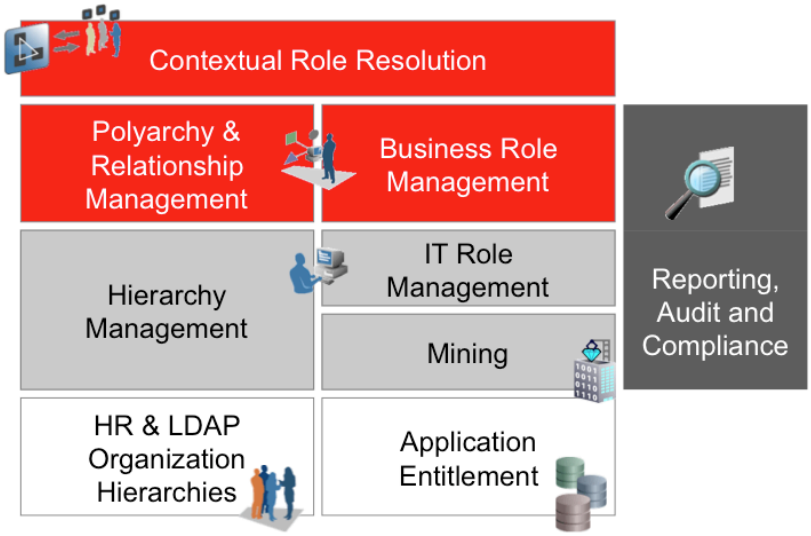

Figure 2: Functional overview of Oracle Role Manager

This white paper will next consider the features and functionality provided by Oracle's user provisioning solution, Oracle Identity Manager. Because Oracle Role Manager works so closely with a provisioning system to automate RBAC, it is important to highlight the synergies that both products play in a complete identity administration architecture. Together, these two products form the basis for scalable, reliable and standards-based enterprise security architecture.

ORACLE'S USER PROVISIONING SOLUTION: ORACLE IDENTITY MANAGER

Oracle Identity Manager, part of Oracle Identity and Access Management, is Oracle's solution for identity administration and user provisioning. This section provides a high-level description of the functional components of Oracle Identity Manager.

Solution overview

A functional overview of Oracle Identity Manager is shown in Figure 3. As shown, the solution embodies seven major functionalities to provide identity administration and user provisioning. These are:

- **Identity and role administration** functionalities include self-service and delegated administration interfaces for managing user identities, attributes and roles.
- **Request administration and approval workflows** describe services for processing user requests for changes to identity profile information and access privileges. These are routed through a flexible approval process defined to model the business requirements, with information automatically updated at completion.
- **Rules and polices** embody the business requirements for automating updates to identity information and approval processes. They also include enforcement of policies for password management and role membership.
- **Provisioning workflow and attestation** provide the capability to provision IT and non-IT resources, sequentially or in parallel, according to a logical flow. Attestation allows users of the system to certify access to users and resources for audit and compliance.
- **Integration framework** provides the interfaces and services required to integrate with target applications and identity repositories. The adapter factory, part of the integration framework, is a unique capability that makes it possible to build and maintain custom application connectors without coding.
- **Deployment, diagnostic and management tools** include the wizards and management applications required to effectively install, deploy and manage the identity management solution and migrate data and configurations between systems.
- **Reporting, audit and compliance** describe the framework and tools necessary to track, report and verify all

of the significant events performed by the identity management solution.

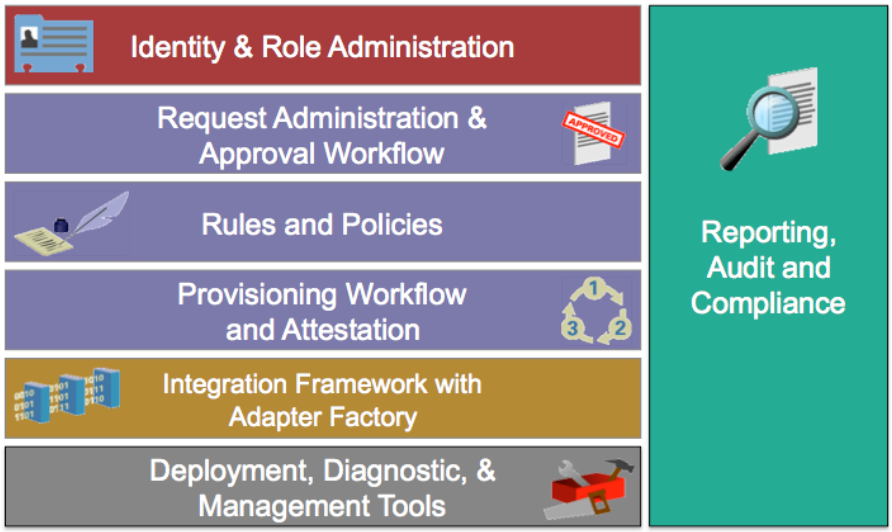

Figure 3: Functional overview of Oracle Identity Manager

The Oracle Identity and Access Management suite provides an integrated set of best-in-breed identity management solutions.

ORACLE IDENTITY AND ACCESS MANAGEMENT SOLUTIONS

Oracle Role Manager and Oracle Identity Manager are key components of the Oracle Identity and Access Management suite. Oracle offers a comprehensive set of Identity Management solutions as illustrated in Figure 4. In addition to these two products, Oracle offers the following Identity Management solutions:

- **Oracle Access Manager** delivers critical functionality for access control, single sign-on, and user profile management in the heterogeneous application environment.
- **Oracle Adaptive Access Manager** delivers real-time fraud prevention, multifactor authentication and protection mechanisms for sensitive information to complement identity and access management solutions for single sign on, federation and fine-grained authorization.
- **Oracle Entitlements Server** provides a fine-grained authorization engine to simplify the management of complex entitlement policies on user interfaces, business logic and databases.

- **Oracle Enterprise Single Sign-on** provides password management and user single sign-on to "fat client" and legacy applications.
- **Oracle Identity Federation** enables cross-domain single sign-on with the industry's only identity federation server that is completely self-contained and ready to run out-of-the-box.
- **Oracle Web Services Manager** is a comprehensive solution for adding policy-driven security and management capabilities to existing or new web services.
- **Oracle Virtual Directory** provides Internet and industry standard LDAP and XML views of existing enterprise identity information, without synchronizing or moving data from its native locations.
- **Oracle Internet Directory** is a robust and scalable LDAP V3-compliant directory service that leverages the high availability capabilities of the Oracle Database platform.
- **Audit and Compliance** includes the framework and services for recording, auditing and reporting on identity and access management activities.
- **Management** of Oracle Identity and Access Management is provided through Oracle Enterprise Manager for Identity Management. Built on Oracle Enterprise Manager's framework for enterprise system management, it provides an integrated platform for controlling and monitoring the processes and services in the suite.

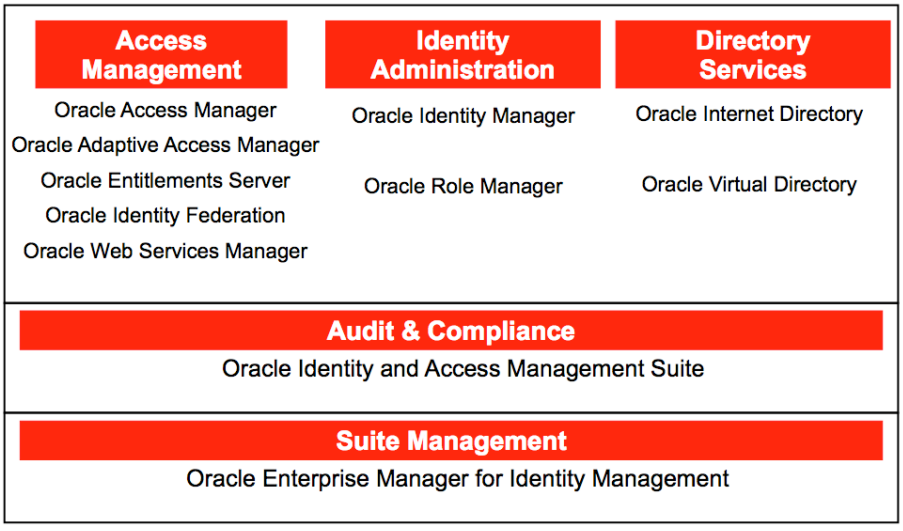

Figure 4: Oracle Identity and Access Management Solution Set

Oracle Identity and Access Management is an integrated suite of best-of-breed components. While the components of Oracle Identity and Access Management function efficiently together, they are designed to be "hot pluggable." This means that organizations deploying components of the suite can select which services they deploy, and in which order. Individual suite components embrace open standards and function well when merged with existing infrastructures. When deployed together, these components form the basis of cohesive and effective enterprise security architecture.

ENTERPRISE ROLE MANAGEMENT AND USER PROVISIONING CHECKLISTS

This section presents a baseline list of requirements for an enterprise role management and user provisioning solution. In each of the tables presented, the left column describes a requirement, and the right column describes how Oracle Role Manager or Oracle Identity Manager meets that requirement. At the highest level, these requirements can be grouped into four categories including functionality, deployability and manageability, enterprise audit, and vendor capabilities. Each of these categories of requirements is considered in turn.

Functionality for Enterprise Role Management Systems

Functional considerations when evaluating enterprise role management solutions include contextual role resolution, polyarchy and relationship management, Business Role and IT Role management, hierarchy management and role mining.

System functionality considerations for an enterprise role management system include comprehensive features for role lifecycle management, seamless integration with a provisioning system, tools to model organizations and business relationships and support for complex role membership policies.

The functionalities covered in this section follow the structures that were described in Figure 2.

Contextual Role Resolution

Contextual role resolution represents a key ability to calculate role membership based on how each user relates to organizations, locations and other users. Contextual role resolution must be powerful enough to calculate complex relationships between entities to resolve role membership.

☑	**GUI-based role membership policies**	Easy-to-use GUI allows users to define policies that dynamically calculate role membership.
☑	**Powerful role membership policy and resolution engine**	Supports complex logic for role membership policies that trigger role assignment. Complex role membership policies can be rapidly resolved to support large scale deployments.
☑	**Dynamic role resolution**	Ability to calculate automatically the members of a role when either a policy change occurs or a user's attributes or relationships change. (e.g. Sam moves from job code 123 to 678)
☑	**Polyarchy-aware role membership policies**	Allows role membership rules to be based on complex relationships between hierarchies, e.g. the cost center that is based in Atlanta or the manager of the security project team.
☑	**Configurable role resolution**	Ensures that role resolution can be configured to occur more frequently (or less) to accommodate different deployment scenarios.

☑	**Integration to HR source data**	Integrates with a provisioning system to ensure that as HR data changes, role membership is update to reflect changes in attributes or relationships in the business.

Polyarchy, Hierarchy and Relationship Management

Users should easily be able to model and manage relationships across multiple hierarchies. This modeling should be efficient, flexible and easy to define and manage.

☑	**Supports multiple intersecting hierarchies (aka polyarchies)**	Users can create as many hierarchies as needed to model common business structures such as reporting organizations, locations and cost centers.
☑	**Manage and maintain custom relationships across hierarchies**	Allows users to define and configure custom relationships across hierarchies and users.
☑	**Use relationship and polyarchy data for role membership policies**	Allow role membership policies to use relationships from the multiple intersecting hierarchies to drive role assignments.
☑	**Provide a visual representation of each hierarchy**	Display a visual representation of each hierarchy in the user interface to aid in role engineering.

☑	**Supports the addition of custom hierarchies**	Allows users to add custom hierarchies to the out of the box model shipped with the product.

Business Role and IT Role Management

An out of the box role governance model should provide Business Roles and IT Roles to streamline role engineering. The management of the role lifecycle should be easy to use and customize.

☑	**Support for Business Roles**	Provides out of the box support and definition of business roles to group users according to common business functions or responsibilities.
☑	**Support for IT Roles**	Provides out of the box support and definition of IT roles to group common sets of entitlements and permissions.
☑	**Support for role mapping**	Allows users to map Business Roles to IT Roles to ensure that roles clearly associate with permissions.
☑	**Supports customizations to roles**	Supports customized attributes or relationships to roles to aid in role lifecycle management.
☑	**User friendly GUI for role lifecycle management**	Provides a best of breed user interface for managing the lifecycles of roles.

Mining

Provides methodology for role mining and supports the import of mining results to become managed roles within the enterprise role management system. Mining should be supported for customers with or without a provisioning system in place.

☑	Import of data from a provisioning system	Allows users to leverage data from an existing provisioning system to mine for roles.
☑	Import of data from a flat file or other external source	Allows users to import data from external sources using flat files.
☑	Supports a process to mine for and analyze roles.	Provides users multiple ways to mine and analyze the results of mining.
☑	Exports roles to an enterprise role management system	Supports the export of mined roles to an enterprise role management system.

Functionality for User Provisioning Systems

System functionality considerations for a user provisioning system include how end users and administrators interact with the system, how they manage their authentication credentials throughout the user identity lifecycle, and the ways the system can automate the process of account provisioning to the various systems under management.

The functionalities covered in this section follow the structures that were described in Figure 3.

Identity Administration

Identity administration represents the user-facing function of the user provisioning solution. This must be intuitive and easy-to-use.

☑	Self-service	Allows end-users to view,

	administration	manage and update their own profile data across all managed resources.
☑	Delegated administration	Ability to delegate administration of groups, organizations and resources to groups and users within and beyond the enterprise.
☑	Integrated interface	Common interface for approvals, notifications, self-service and delegated administration.
☑	Recovery from lost passwords	Presents customizable challenge questions to enable identity verification for password reset.
☑	Password synchronization	Ability to synchronize changed and updated passwords with connected systems.
☑	Integration with role management products	Integrates with enterprise role management solutions for organizations with heavy requirements around role discovery, management and definition.

Request administration and approval workflow

Request administration and approval workflows process requests on behalf of users according to defined policies. They should be efficient, flexible and easy to define and manage.

☑	Self-service provisioning requests	Users can create provisioning requests for resources and

		fine-grained entitlements.
☑	**Requests to provision multiple users**	Allows generation of requests to process multiple users at once.
☑	**Request monitoring**	Requestors view status of workflows.
☑	**Request escalations**	Automatically escalates requests in the event of approver non-response.
☑	**Request-driven workflow**	Workflows can be initiated in response to user or administrator requests.
☑	**Event-driven workflows**	Workflows can be initiated by an event such as creation of a user in an authoritative directory.
☑	**Serial processing**	Ability to process workflows through a complex sequence of steps.
☑	**Parallel processing**	Ability to manage multiple workflow events simultaneously.
☑	**Flexible approval routing**	Ability to route request to named individuals, group members, users with a particular role, or via dynamic lookup of a supervisor.

☑	**Dynamic re-routing**	Able to change approval path based on the outcome of intermediate steps within the process.
☑	**Route requests to multiple reviewers**	Allows approval contingent on approval of a subset of approvers.
☑	**Additional input needed**	Supports the ability of a reviewer to request additional input from requestor or third party.
☑	**Approver proxy**	Allows users to define other users as proxies for approvals.
☑	**Addition and removal of approval workflow to provisioning policy**	System allows easy addition/deletion of approval workflows to provisioning policies
☑	**Integration of manual and automated tasks**	Allows easy integration of manual and automated administrative tasks into workflows.
☑	**E-mail notifications**	E-mail notifications of workflow events and final user creation step.
☑	**Workflow design tools**	Interface provides an easy way to build provisioning workflows without coding or custom scripting.

Rules and policies

Rules and policies describe the ability of the system to represent and enforce organizational policies over the provisioning process. They need to be manageable and support the real-world business requirements of the organization.

☑	**GUI-based rules specification**	Easy-to-use GUI allows users to define rules using a compilation of complex Boolean logic.
☑	**Flexible rules engine**	Highly configurable, integrated rules engine for functions such as group assignments, workflow policy decisions and target provisioning criteria.
☑	**Configurable password policies**	Ability to specify centralized policies for password generation and enforcement.
☑	**Event-driven processing**	Rules can be defined to initiate processing based on events such as identity attribute changes.
☑	**Time-based processing**	Rules can be defined to initiate processing based on time or time intervals.
☑	**Rule re-use**	Defined rules can be re-used for a variety of specific applications.

Provisioning workflows

Provisioning workflows orchestrate the creation and management of user accounts within the managed applications once the proper

approvals are granted. Backend provisioning can be a complex process with many moving parts, and the provisioning workflow functionality must be capable of processing multiple tasks in sequence and in parallel.

☑	**User account management**	System manages native user accounts in the resources under management.
☑	**Service account management**	System manages privileged application service accounts in the systems under management.
☑	**Rule-based provisioning**	Rule-based criteria for execution of provisioning connectors to relevant target systems.
☑	**Workflow task library**	Includes pre-defined set of commonly used provisioning workflow tasks.
☑	**Workflow extensions**	Ability to extend workflows via programmatic interfaces to external systems.
☑	**Provisioning of non-IT resources**	Ability to track provisioning of non-IT resources such as mobile phones, laptops, company credit cards, etc.
☑	**Separation of workflow from integration layer**	Allows changes to integration components without impacting implemented workflows.

☑	**Separation of workflow from approval layer**	Allows changes to approval policies without impacting implemented workflows.
☑	**Workflow design tools**	Interface provides an easy way to build provisioning workflows without coding or custom scripting.

Integration framework

The integration framework facilitates the implementation of manageable connectors for supporting all of the applications deployed in the enterprise. The integration framework should support a variety of connectors to popular systems as well as the rapid deployment and easy maintenance of customized connectors without coding or scripting.

☑	**Application specific connectors**	Connectors for commercial applications deployed in the enterprise including ERP, CRM and e-mail system using application-specific APIs.
☑	**Generic technology connectors**	Connectors for generic resource targets such as flat file systems, databases, LDAP directories and SPML-enabled/web services applications.
☑	**Custom connector development support**	Adapter Factory provides graphical environment for rapid development and maintenance of custom connectors without programming or scripting.

☑	**Trusted identity source**	Ability to designate a target system as trusted source for enterprise identities, and synchronize identity records from the trusted identity source.
☑	**Account reconciliation**	Ability to extract account data from target systems and match extracted accounts to new and existing users using configurable matching rules.
☑	**Reconciliation history**	Ability to track full history of all reconciliation events. Allow changes to be made and re-execute any reconciliation.
☑	**Integration with Microsoft Active Directory passwords**	Ability to capture password changes made in Microsoft Active Directory and apply them to other managed resources.
☑	**Integration with ERP application passwords**	Ability to capture password changes made in connected ERP systems and apply them to other managed resources.
☑	**Connector partner validation programs**	Established program for validating commercially available third party connectors.

Important factors when evaluating identity management solutions include ease of deployment, diagnostic and management tools, solution architecture, enterprise scalability, high availability, user interfaces and vertical industry solutions.

Managing and Deploying Identity Administration

The ease with which the user provisioning or enterprise role management solution can be rolled out to the organization, and the solutions ability to be managed over time impact the total cost of ownership of the solution. Major considerations here include the ease of use and ease of management of the user interfaces, the ability of the solution to support the various application infrastructures in use in the environment, and how well the solution fits into an overall enterprise security architecture. This category also considers factors such as the need for the solution to provide high availability and scale to meet the demands of the organization.

Deployment, diagnostic and management tools

Deployment, diagnostic and management tools address the needs for product installation, account migration, configuration management and ongoing system administration. These should be intuitive and easy to use.

☑	Installation ease	Wizards and consoles provided for installation and configuration.
☑	Identity migration tools	Tools for automatically migrating and reconciling identities from target systems.
☑	Configuration migration tools	Tools for automatically migrating system configurations between test, pilot and production implementations.
☑	Configuration merge tools	Tools for automatically merging system configurations made by different administrators.

☑	**Diagnostic tools**	Diagnostic tools for pre- and post-installation testing and diagnosis of technology platform and system connectivity.
☑	**Integrated system management platform**	Provides automatic discovery, monitoring, service level management and configuration management of enterprise security architecture services through an integrated enterprise application management platform.
☑	**Integration with SNMP**	Integration with SNMP-based system management platforms.

Solution architecture

The architecture of the enterprise role management and user provisioning solution is a top-level concern when evaluating its deployability and manageability. The architecture should support the various infrastructure components deployed in the enterprise and reflect the best practices for modern, application server-based architectures.

☑	**Modern platform architecture**	J2EE-based, N-tier deployment architecture.
☑	**Secure implementation**	Architecture utilizes technologies such as SSL and JAAS (Java Authentication and Authorization Services) to protect sensitive data.

☑	**Operating system support**	Heterogeneous support for popular operating systems including AIX, RedHat AS, Solaris and Windows 2003/8.
☑	**Application server support**	Heterogeneous support for multiple application servers, including Oracle WebLogic, JBoss, and IBM WebSphere.
☑	**Database support**	Supports Oracle and Microsoft SQL Server as backend databases
☑	**Centralized single sign-on support**	Administration clients support third-party web access management solutions.
☑	**Integrated auditing**	Out-of-the-box integration of user provisioning, audit and compliance functionalities.

Enterprise scalability

Enterprise scalability is the ability of the enterprise role management and user provisioning solution to scale to meet the requirements of the organization, and beyond. Scalability should be considered in two dimensions: 1) the total number of users managed by the system, and 2) the total number of resources under management by the system. A useful metric for evaluating the scalability of the user provisioning system is provided by the product of these two quantities, and is referred to here as the "user-resource product."

☑	**Demonstrated "user-resource product" scalability**	Demonstrated ability to manage large number of users across large numbers of applications in a single customer deployment expressed as the product of users and managed resources.
☑	**Separate reporting database**	Supports deployment of a separate reporting database to meet enterprise scalability requirements.
☑	**Data archiving tools**	Provides automated tools for managing high volumes of audit data and archiving data into an archiving database.
☑	**Reports generated from local audit data**	Locally stores audit data so that reports do not require frequent target resource accesses.

High availability

High availability of the enterprise role management and user provisioning solution is a critical requirement for most organizations. The solution should be capable of supporting high availability deployment features to meet any uptime requirement.

☑	**Built-in application server clustering support**	Supports application server clustering for virtually automatic failover in mission-critical computing environments (without deployment of a third-party message bus.)

☑	**Database clustering support**	Can leverage Oracle Database's Real Application Clustering (RAC) capabilities to provide data tier high availability.
☑	**Offline reporting**	Ability to generate reports without all of the target resources being available.

User interfaces

The architecture and design of the user interface components are a major factor in evaluating the ease of deployment and ongoing system management. User interfaces should be easy to deploy and maintain on user's desktops, and should support customizations that can be tailored to the organization's needs.

☑	**Web-based user administration interface**	Self-service and delegated administration features accessed through web-based, thin client.
☑	**Ready-to-deploy clients**	Clients ready to deploy in standard configuration without coding or scripting.
☑	**Feature-rich design console**	Design console environment for designing forms, workflows and custom connectors.
☑	**Administration client customization support**	Look and feel of web client can be customized via cascading style sheets and open source J2EE framework.

☑	Client extensibility	Support for extensions to client functionalities through documented client integration interfaces.

Vertical industry solutions

Many vertical industries have special needs with respect to user provisioning and compliance management. Available industry-focused configuration solutions can help speed the process of system deployment.

☑	Custom solutions	Out-of-the-box support for customized solutions for specific industries.

Compliance

Compliance considerations when evaluating identity management solutions include audit data capture, audit data reporting and policy compliance monitoring.

Compliance capabilities refer to the ability of the solution to support the key audit and attestation processes employed by the organization. These are supported by the "Reporting, Audit and Compliance" functionalities presented in Figure 2 and 3 and are a vital consideration for organizations seeking to satisfy regulatory requirements. Additional information about compliance capabilities can be found in the Buyers Guide for Compliance Solutions in Identity Management.

Audit data capture

Audit data capture refers to the types of audit data collected by the system, and how that data is retained, managed, and made available for reporting.

☑	Out-of-the-box audit data collection	Collects audit data related to user profile, enterprise roles and managed applications without customization or changes to the application.
☑	Central storage of historical data	System is not dependent on the target system to store historical data.

☑	**Snapshot and temporal audit data**	Retains both “point-in-time” and temporal information related to auditable events.
☑	**Storage of audit data in a database**	Retaining audit data in a database management system with backup and recovery capabilities helps ensure safety of the data.

Audit data reporting

Audit data reporting refers to the report generation functionalities supported by the user provisioning system on captured audit data. These include the ability to generate static reports on the state of user entitlements, as well as reports based on historical data.

☑	**Suite integrated reporting**	Single console integrates audit reporting across the entire identity and access management suite.
☑	**User entitlement reporting**	Supports automated reporting of operational and historical user access privileges as well as workflow events.
☑	**Answers to “who, what, when, how and why” questions**	Generates reports to respond to complex questions such as “Who had access to what resources over what period of time, how did they gain access to those resources, and what was the business need for granting them access?”

☑	**Preconfigured reports**	Large collection of preconfigured reports to show operational and historical information including role assignments, user resource access privileges, and attestation events.
☑	**Historical reports**	Create and run historical reports on transactions that have occurred over time, including but not limited to role assignments, user resource access privileges, and attestation events.

Policy compliance monitoring

Policy compliance monitoring functionalities support monitoring compliance with corporate policies on an ongoing basis. These include processes to monitor user entitlements, track periodic entitlement attestations, and enforce separation of duties policies.

☑	**Entitlement profile compliance reporting**	Ability to compare user and role-based entitlement profiles to actual resource entitlements.
☑	**Out-of-the-box integration of provisioning and audit features**	Provisioning and audit features integrated to enable "actionable auditing" (where the provisioning system can automatically respond to issues discovered during an audit) and compliance automation.

☑	**Attestation support**	Automates the process of generation, delivery, review, sign-off, delegation, tracking and archiving of user access rights reports for reviewers on a scheduled or ad-hoc basis.
☑	**Separation of duties (SoD) support**	Implements policies to allow or deny actions based on separation of duties requirements.

Vendor capabilities

Vendor considerations when evaluating identity management solutions include product support, industry leadership, and vendor portfolio.

The ability of the vendor to deliver design, deployment and product support whenever and wherever it is needed is critical. The vendor should demonstrate the technology leadership and level of investment necessary to ensure that solutions remain state-of-the art. Finally, enterprise role management and user provisioning solutions should be available as part of a comprehensive and integrated enterprise security product portfolio, allowing customers to maximize their returns on investment.

Product support

Product support speaks to the ability of the vendor to provide pre- and post-sales support, including deployment help and professional product training.

☑	**Customer support**	Global services providing 24x7 support.
☑	**Education services**	Product training available through instructor-led classroom events and online courses.

☑	Implementation partners	Implementation partners can help customers deploy the product and maximize the value of their investments. Recommended partners should comprise of both global and regional choices to suit customer and project needs. In addition, the vendor should also offer consulting services.

Industry leadership

Industry leadership describes how the vendor demonstrates technology leadership and the degree to which the vendor's solution is adopted in key vertical markets.

☑	Technology standards leadership	Active involvement in major identity management standards forums such as Liberty, OASIS, The Open Group, and the Identity Governance Framework.
☑	Vertical market adoption	Adoption of solution by major vertical market segments, including (a) financial services, (b) hospitality, retail, and services, (c) manufacturing and transportation, (d) technology and communications, (e) healthcare, and (f) government, education and public sector.
☑	Industry recognition	Recognized as a leader in identity management by top-tier analyst firms.

Vendor portfolio

Vendor portfolio addresses the reputation, capabilities and complementary products offered by the vendor.

☑	Complete identity management portfolio	Vendor offers a complementary portfolio of identity management capabilities including LDAP directory, virtual directory, web access management, enterprise single sign-on, and web server policy management.
☑	Complete middleware suite	Oracle Identity Management and Oracle Role Manager are part of Oracle Fusion Middleware. With over 35,000 customers globally, 870 of the Global 1000 and 39 of the world's largest 50 companies rely on Oracle Fusion Middleware for business critical applications.
☑	Identity-enabled applications	Offers a full portfolio of Oracle Fusion-ready applications that can leverage common identity services, including Oracle E-Business Suite, PeopleSoft Enterprise, Siebel, JD Edwards EnterpriseOne, and JD Edwards World.
☑	Vendor stability and reputation	Public company with over 60,000 employees worldwide and annual revenues of over $22.6 billion.

CONCLUSION

Together, Oracle Role Manager and Oracle Identity Manager form a powerful and flexible identity management solution. For more information, go to http://www.oracle.com/identity.

Forward-thinking organizations everywhere are deploying identity administration solutions to improve security, control costs, and address compliance regulations. User provisioning helps organizations achieve these goals by centralizing and automating the management of user accounts and entitlements in organizations' information resources such as databases, directories, business applications and e-mail systems. Enterprise role management help organizations achieve these goals by providing a single authoritative source for roles that determine user access to drive provisioning events based on RBAC. Increasingly, industry best practices recommend the use of an enterprise role management solution to simplify and organize user access control more effectively. When implemented correctly, enterprise role management and user provisioning solutions collectively deliver positive benefits to all three principles (confidentiality, integrity and availability) of an information security program.

The best way to leverage the benefits of an enterprise role management solution is to consider it as a component of an enterprise security architecture that includes complementary services such as access control, identity administration, directory, audit and compliance, and system management. By adding role based access control to the enterprise security architecture, organizations can quickly reap several benefits including consistent security across applications, implementation of the least privilege principle, and overall improved interoperability and manageability to control user access.

Together, Oracle Identity Manager and Oracle Role Manager provide the complete functionalities for identity and role administration. This includes role lifecycle management, contextual role resolution, polyarchy and relationship management, request administration and approval workflows, provisioning orchestration, integration framework with adapter factory, deployment, diagnostic and management tools, and reporting, audit and compliance services. Oracle Role Manager and Oracle Identity Manager are part of the Oracle Identity and Access Management suite, which provides functionalities for application access management, directory services, audit and compliance services, and management tools. Each component of Oracle Identity and Access Management is "hot pluggable," a quality which allows organizations to deploy components individually, when it makes sense, and with existing infrastructures. As a

whole, the Oracle Identity and Access Management suite provides a complete and integrated infrastructure for enterprise security architecture.

When considering identity administration solutions, enterprises should carefully evaluate product and vendor qualities that impact functionality, deployability and supportability of the solution. The selected solution should meet the needs of the organization from a functionality perspective, providing the necessary role lifecycle management, role engineering and automated user access through provisioning integrations. Next, the solution should provide the tools and architecture that allows rollout of a scalable, dependable and manageable system. Finally, consideration should be given to the strength, reputation and support capabilities of the vendor and its partner network to ensure that the system will continue to deliver business benefits in the years to come. When these factors are considered, you will find that Oracle is a strong partner who can meet your identity administration needs.

Buyer's Guide for Identity Administration
March 2009

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com