An Oracle White Paper
July 2012

Integrated Identity Governance

A Business Overview

ORACLE

Executive Overview

Enterprises need to ensure users have sufficient access privileges to perform their job functions, but for compliance and security reasons it's also important to constrain such access. Accordingly, enterprises must make it easy for users to acquire access, and also easy for managers, resource owners, and system administrators to review and revoke access. Oracle's governance products are designed to help enterprises balance these objectives of access, security, and compliance.

For large organizations, getting users the access they require can be a frustrating and time consuming task. New users have little exposure to IT jargon that would enable them to request privileges by name. New users often resort to requesting the same kinds of access as their peers, who may have privileges that new users shouldn't. And as employees and contractors work on a variety of projects, transfer departments and locations, change their job functions, and get promoted, their requirements for access change. At a deeper level, system administrators require access to privileged, shared accounts that allow them to perform business-critical and administrative functions. Often these accounts are "root-level" accounts that don't use administrators' named accounts, so it becomes critical to grant access to the right individuals in a timely manner. For all of these scenarios, Oracle provides identity governance solutions to simplify access grants by enabling users to request access in simple, web-based catalogs, and by routing these requests to appropriate approvers. The solution also provides privileged account management, which controls access to shared, root-level or admin accounts.

Similarly, access certification is an ongoing challenge for most enterprises, but necessary for compliance with regulations such as Sarbanes Oxley (SOX). The need to perform multiple, difficult tasks—such as certifying user access rights, enforcing security policies, and automatically revoking unnecessary access rights—is compounded by the reliance on slow, error-prone manual processes to handle them. These issues, coupled with the lack of a comprehensive, cohesive approach to compliance and auditing, make it nearly impossible to address the challenge in an effective and cost-efficient manner. As a result, enterprises are obliged to commit significant resources to compliance efforts. Oracle simplifies certification challenges by automating the review cycle. Oracle's access governance products automatically detect users' privileges and orphan accounts, notify the appropriate stakeholders of any action they need to take, apply risk scores to help stakeholders prioritize their certification tasks, and make changes to privileges and accounts once a decision is reached.

This white paper discusses how Oracle's identity governance products—Oracle Identity Manager, Oracle Identity Analytics, and Oracle Privileged Account Manager—work together to create an integrated identity governance process for the enterprise.

Oracle Identity Governance Suite – An Integrated Approach

Oracle Identity Governance Suite provides a modern, simplified, and integrated solution for managing accounts and access privileges across business applications and platforms. The solution supports a variety of popular administrative styles such as roles, rules, and policies to enable flexible and scalable administration. In addition, users can search an expressive catalog for requesting access to applications, data, and platforms. The system routes requests to the appropriate approvers before granting access. The access request catalog is available through a simple, self-service, web-based interface through which users can request access both for themselves and for others.

Stylistically, Oracle Identity Governance Suite offers enterprises an array of options for assigning access controls. For example, access rights can be issued automatically based on role assignments derived from a rule or policy governing how and when the role is applied to user accounts. Users can also request the capability of exclusively using a privileged account and, upon the grant, checkout the account to acquire exclusive privileged access to the underlying application or infrastructure component.

In order to continuously monitor and effectively enforce compliance controls, Oracle Identity Governance Suite provides automated periodic review of users' access rights as well as monitoring for exceptions to IT audit policies. These measures ensure employees aren't able to acquire a combination of access rights that would allow them (or an attacker who has hijacked the account) to perform fraudulent activities. Additionally, Oracle Identity Governance Suite continuously monitors for rogue access grants that originate outside the Identity Governance solution. Oracle Identity Governance Suite also provides rich audit and reporting that allows lines of business, IT administrators and auditors to review not only who has/had access to what but also how they acquired the access, in addition to when they used an exclusive privileged account.

Additionally, the Oracle Identity Governance Suite provides automated provisioning to managed applications and target systems upon access grant for both standard and privileged access, using a robust set of connectors. If these grants need to be revoked as a result of monitoring controls, they can be automatically de-provisioned using the same connectors, while providing a comprehensive audit trail.

Assembling the Blocks – Core Solution Components

The Oracle Identity Governance Suite consists of the following core components, with each component solving a unique governance challenge faced by enterprises.

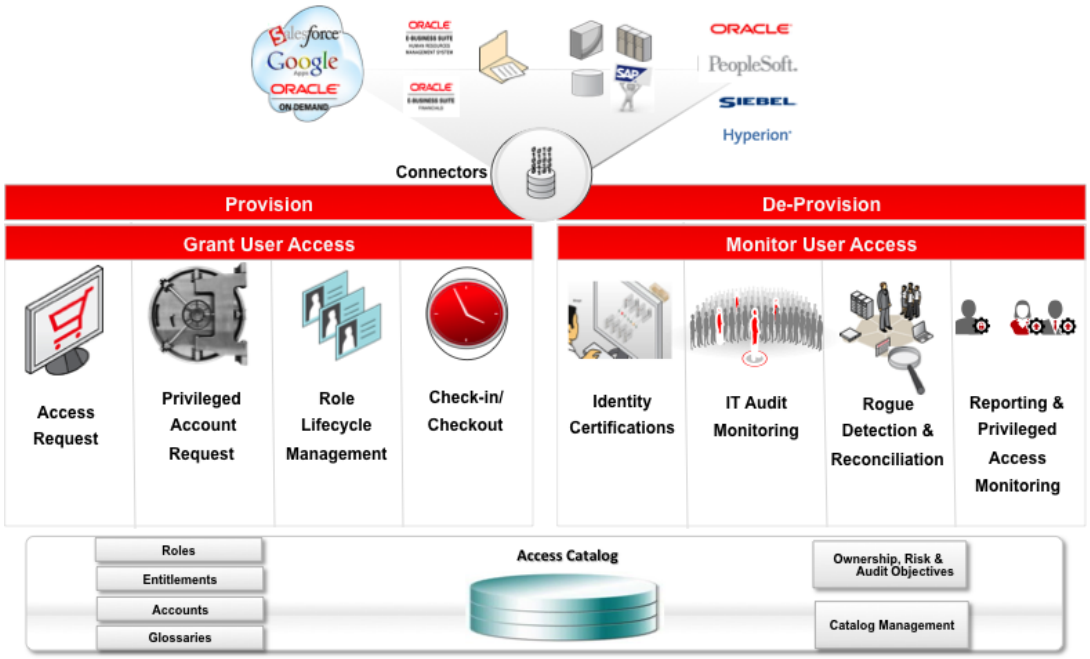

Figure 1. Oracle Identity Governance Suite – Core Solution Components

As shown in the figure 1, the Access Catalog is at the heart of the Oracle Identity Governance Suite, which provides a robust and intelligent storage solution for various access rights across applications and platforms, in addition to comprehensive catalog management capabilities. Using this catalog, organizations can grant access rights to their employees and workers by taking advantage of rich features such as Access Request, Privileged Account Management via Check-in and Checkout capabilities, Role Lifecycle Management along with a comprehensive Identity Connectors Framework. In addition, organizations can also monitor access rights assigned to users to enforce compliance via Identity Certifications, IT Audit Monitoring, Rogue Access Detection and Audit and Reporting capabilities. These components are now described in detail in sections below.

The Access Catalog

As shown in figure 2, the Oracle Identity Governance Suite provides a catalog of access rights, including enterprise and application roles, application accounts, and entitlements. The catalog automatically *harvests* privileges when new definitions of entitlements are detected in a target application or when the roles are defined or modified using the role administration features built in the solution. Catalog administrators, along with application administrators, then enrich the harvested data to make it friendly for the business users. In particular, for each role, application and entitlement in the catalog, administrators can author business friendly descriptions, list the audit objectives, and set risk levels. While the catalog management system automatically populates a set of search tags based on names and descriptions of the catalog entities, catalog administrators can also seed keyword tags by which business users may find the roles and entitlements in various

search results. Additionally, administrators can provide metadata for the catalog items. For example, they can specify the users or roles that will be involved in approval, certification or manual provisioning fulfillment activities related to the corresponding roles, accounts or entitlements. Once configured, catalog information is available across the identity governance functions including request creation, request tracking, approval, request history, manual provisioning, and certification.

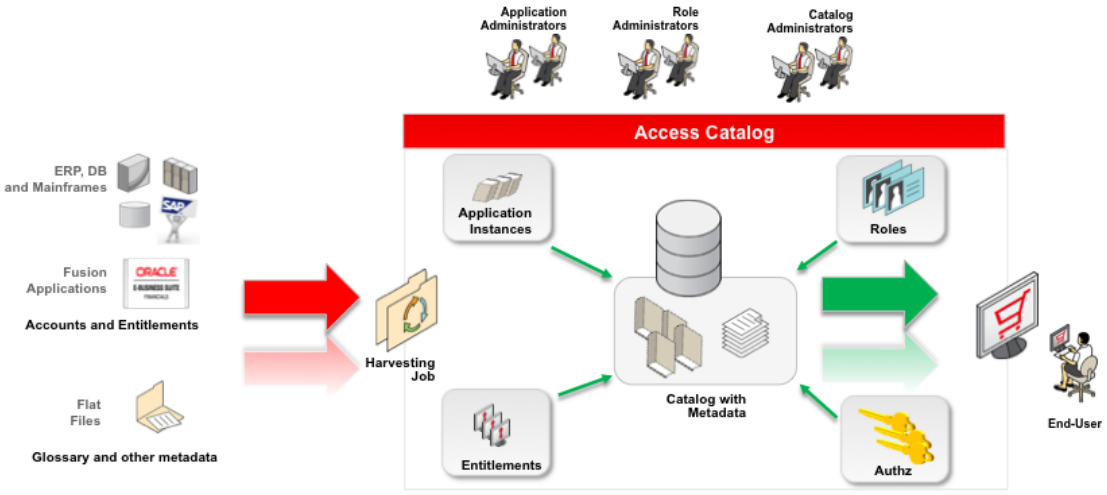

Figure 2. Oracle Identity Governance Suite – Access Catalog

Access Request

The Oracle Identity Governance Suite provides a browser-based tool to request access. The access request experience is similar to the "shopping cart" metaphor used in many e-commerce websites, so users are able to request access without the need for thorough training and require only a basic understanding of the organization's roles applications, and entitlements. Users simply search for the roles and entitlements they require by entering keywords they are familiar with. They can further refine and filter search results by using the tool's automated suggestions. Once users find the entitlements they need, they simply place the appropriate entitlements in a cart and submit the request.

Access Request provides a robust set of capabilities around business user friendliness, monitoring and UI customization, as described below.

Business User Friendliness of the Access Catalog

The Access Catalog makes it easier for requestors to quickly request the access rights they need across a variety of applications and target resources. These access rights can be granted via Roles, Entitlements or accounts in various applications. In addition to these, end users can save search results in a saved request cart and share these carts with other users. These "request profiles" can be used as a template for requesting a *basket* of frequently requested privileges.

The Access Catalog itself features robust search capabilities that follow the semantics of a web engine based search. End users are not required to know the cryptic names of accounts and entitlements or complex search operators, but can rely

on a business friendly search keywords or partial words (e.g. "pay" will return "payroll") that quickly allow them to search, find and request the access rights they need, in order to perform their job responsibilities.

The Roles, Entitlements and Applications residing in the Access Catalog feature an extensible metadata, with the ability for administrators to create business level glossary descriptions such as creating high level categories to organize access rights, providing multiple search tags for these access rights as well as defining user friendly descriptions, defining risk levels and setting audit objectives. Each Role, Entitlement and Application can also be assigned owners for approvals as well as certification. Once this catalog metadata is configured, it is consistently available across the various identity governance functions including access request, request tracking, approval, request history, manual provisioning, and certification.

Preventative IT Audit Policy Analysis during Access Request

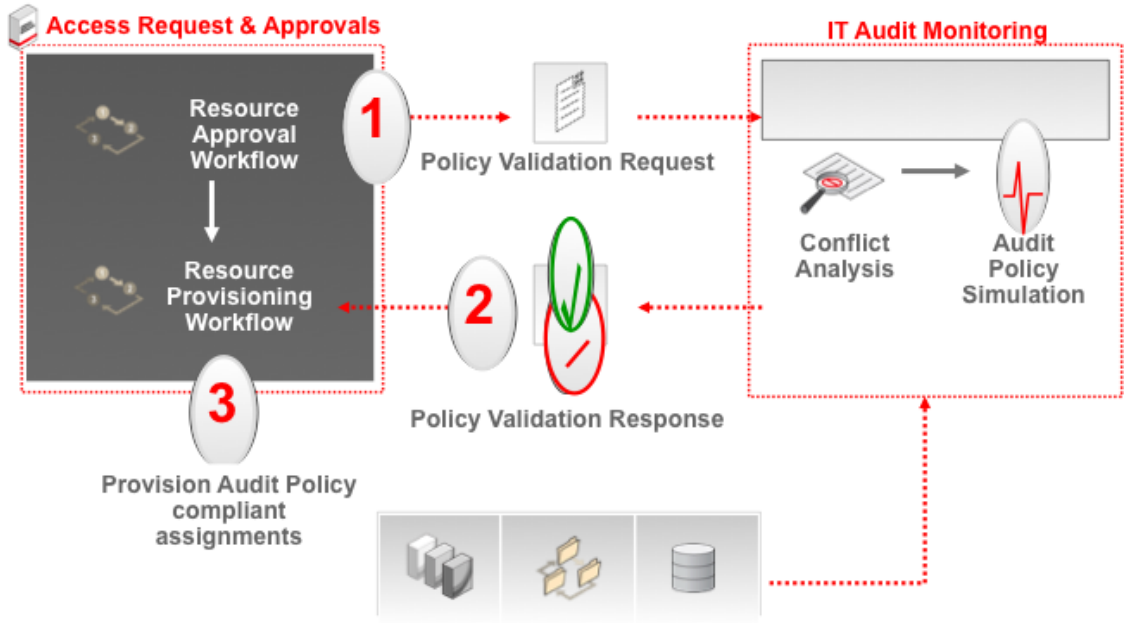

Figure 3. Oracle Identity Governance Suite – Preventative IT Audit Analysis & Simulation

As shown in figure 3, the Oracle Identity Governance Suite provides a comprehensive solution for automating and enforcing preventative IT Audit policies. During access request, a "what if" policy validation request is initiated from the provisioning process and run through a preventative simulation to determine if undesired access rights are being requested. This ensures that undesired access is not granted to a user and enforces compliant provisioning practices.

Tracking a Request

Users and help-desk administrators can track the progress of their requests online through the solution's comprehensive tracking tool. The tracking tool graphically displays the current state of the request approval in the provisioning workflow with a business friendly image that displays what steps are complete and what steps remain to fulfill the request. Using this tool, users can then help ensure their requests are handled in a timely fashion.

UI Customization & Durability

UI customizations, using the Oracle Identity Governance Suite, can be performed by drag-and-drop editing in a web browser, without any complex programming or proprietary scripting. The UI customizations are stored in a specialized and reserved namespace in the solution's metadata repository to ensure that they are durable and that they survive patching and upgrades. After patching and upgrades, customers are not required to reapply their customizations, eliminating the expensive customization merge and testing cycles and making it easier for customers keep their deployments current.

Privileged Account Management

Organizations have sensitive systems and applications with highly privileged accounts or shared schemas whose passwords are shared by multiple administrators. These accounts are powerful by nature, which can prove disruptive to the business if not managed and monitored appropriately. Privileged users perform sensitive activities that involve extended access to corporate resources. In most companies, privileged accounts are not clearly defined, and different individuals often share some of these accounts. When privileged accounts are not tightly managed, they present a high security risk for the enterprise. In addition, regulations typically require enterprises to be able to trace, authorize, track and audit all shared privileged account usage.

The number of privileged accounts grows with the number of servers, devices, and applications to manage. In most large enterprises, there are hundreds, sometimes thousands of privileged accounts for which multiple individuals know the username / password combination without a way to track who actually used a password at a specific time. Because an inflation of privileged accounts is hard to manage, passwords are rarely changed thus compromising overall security and violating corporate password policies.

To address these challenges, Oracle Privileged Account Manager, an integral part of Oracle's Identity Governance platform, enables the separation of privileges, self-service requests to privileged accounts, and provides password usage auditing and reporting. From a compliance perspective, the solution contributes to securing Global Trade Management (GTM) strategies in particular as they relate to compliance with regulations such as the Sarbanes-Oxley Act.

The solution is a server-based password repository designed to generate, provision, and manage passwords for privileged users accessing specific resources. It is a bona fide Fusion application running in Oracle WebLogic Server and leveraging the Oracle Platform Security Services (OPSS) framework including the credential store, policy store, wallet, authentication, authorization, and audit application programming interfaces (APIs).

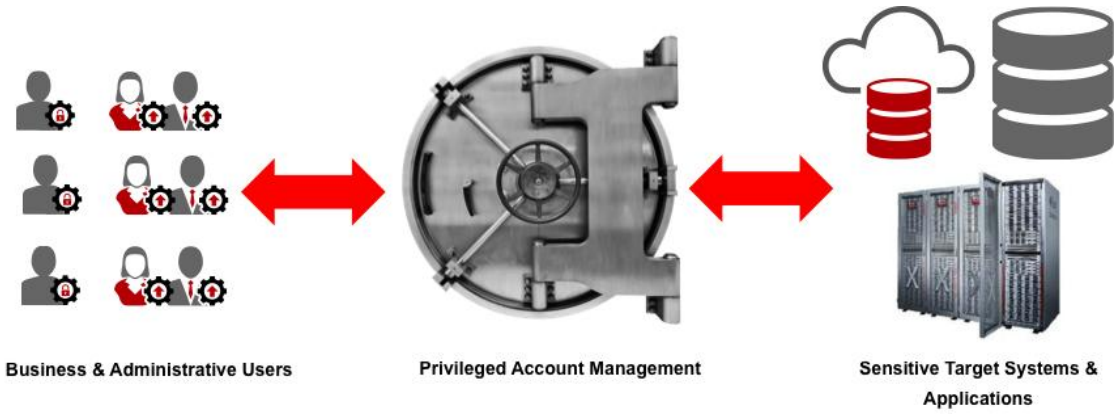

Figure 4. Oracle Identity Governance Suite – Privileged Account Management

As show in figure 4, the solution allows a privileged user, for example a system administrator or an application developer, to use a privileged account by "checking out" a password for a particular application, operating system, or database server. Once the solution gets the necessary approval, a password is issued to the administrator. The administrator uses the password, then "checks-in" the password, indicating that the administrative task is complete. The system can be configured to automatically change the password on check-in, thereby precluding the administrator from reusing the same password again.

Also, *Break-glass* access enables administrators to request emergency access to privileged accounts they are not normally entitled to (the break-glass metaphor comes from breaking the glass to pull a fire alarm). Such a situation may occur when a critical server is down and the designated server administrator is not available. In this case, the administrator goes through the request process indicating a break-glass emergency request. Submission of the request kicks off a break-glass workflow with minimal or automatic approval (based on the customer's processes and policies). The administrator is provisioned to the solution's LDAP group and can access privileged credentials. A special alert is generated for the event and is sent to security administrators. The access is automatically de-provisioned based on the security policies defined by the customer.

Every action of request, approval, check-in, checkout, who used it, when it was used, etc. are audited from a monitoring perspective. Privileged account information is also made available for identity certification, by allowing Risk to be calculated on privileged accounts and how it was provisioned. Finally, the solution also provides out-of-box integration with Oracle Enterprise Single Sign On to eliminate manual credential handling where secure passage of a token is not possible.

Role Lifecycle Management

Role lifecycle management is the process of defining and assigning roles to individuals who require access to organizational resources and of then managing their access according to those roles. Creating roles based on usage and enterprise policies enables greater visibility and better control. A limited number of appropriate roles make access much more manageable than dealing with a large number of individuals and infinite number of permutations of access rights. Role lifecycle management is therefore an efficient and effective way to address the challenges of access control for a large and constantly changing universe of users.

As shown in figure 5, it all begins with the definition of Roles, and Oracle Identity Governance Suite provides a unique combination of tools and methodology to allow organizations to define enterprise Roles, in addition to combining them with a robust Role based access control and role governance process. Role Discovery is a comprehensive set of market-leading role mining and analytics features that utilize a *hybrid approach* to discovering roles in the enterprise. This hybrid approach leverages the combination of bottom-up (or user entitlements) and top-down (user HR attributes) access rights and business descriptions of users as part of its robust clustering algorithms, to design suggested roles. Advanced analytics capabilities that showcase popularity of users in entitlements, role similarity comparisons, IT Audit violations within role definitions, percentage of users in engineered roles, and so on provide role engineers with comprehensive information to further refine role definitions.

Figure 5. Oracle Identity Governance Suite – Role Discovery

Coupled with the industry leading *wave methodology*, which is a practical approach to Role Definition, Oracle Identity Governance Suite provides a robust set of capabilities for organizations to solve their access control challenges.

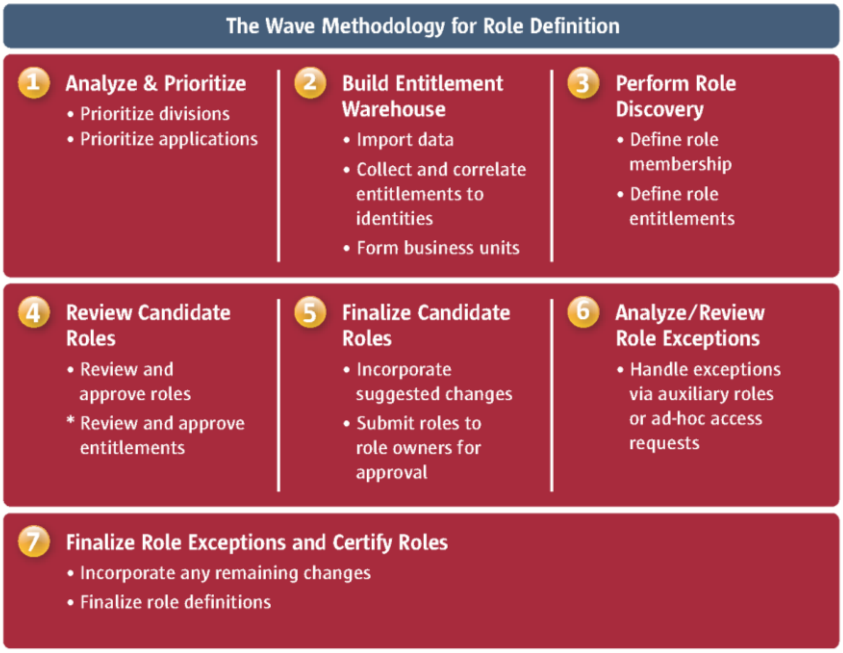

Figure 6. Oracle Identity Governance Suite – Wave Methodology for Role Definition

Based on years of experience in helping companies to adopt a role-based model for access control, Oracle's wave methodology for role definition, shown in figure 6, has proven to be an effective method for engineering roles. This seven-step process walks administrators through 1) analyzing and prioritizing the divisions and applications most urgently requiring access controls, 2) building a warehouse to store data critical to effective role definitions, 3) performing role discovery, 4) defining policies for candidate roles, 5) finalizing candidate roles, 6) analyzing and reviewing exceptions to the roles, and 7) finalizing role exceptions and certifying the roles defined.

The solution also offers incremental role mining capabilities to take into account new applications being on-boarded or applications being phased out, allowing existing role definitions to be dynamically modified and to automatically update the role definitions. This ensures that the underlying role content always stays current and is available for assignment, provisioning and compliance.

Enterprise roles, once defined, continue to evolve over time, and thus require a robust administration and audit process. The Oracle Identity Governance Suite provides role approvals upon detection of associated entitlement updates and performs real time impact analysis for role consolidation before changes are applied in a live environment. Role change approval process combined with role versioning, role change "what if" simulations and rollback features, provides a complete role change and lifecycle management solution. As part of its role lifecycle management features, the solution fully audits all the changes made to role definitions including role assignment rules and entitlement mapping policies.

From a governance perspective, the Oracle Identity Governance Suite provides role content certifications upon detection of entitlement updates and also performs impact analysis prior to initiating changes to live environments with respect to Roles. It also provides a complete audit trail around Role changes and role memberships. The solution enables role versioning, which creates an offline copy of a Role without disturbing the "live" version of a Role and provides capabilities to revert to any Role version recorded in the Warehouse. This improves the overall organizational flexibility by making it

fast and easy to change access based on business needs and also improves the alignment between IT and business organizations.

Identity Certifications

As shown in the figure 7, most organizations today, struggle with satisfying stringent compliance mandates to perform access reviews (or certifications) of users with access rights to thousands of business applications and target platforms, let alone making the process a sustainable and repeatable exercise. In addition to meeting the challenge of scale, automation is the key to increasing the effectiveness and reducing the cost of compliance. Automation streamlines and accelerates the processes, by reducing the need to rely on help-desk and administrative resources and at the same time lowering the risk of manual errors that can lead to audit failure. Most importantly, automation makes it possible to create sustainable, repeatable audit processes that enable the enterprise to address compliance in an ongoing manner without starting from scratch to address every new regulation or prepare for every audit.

Figure 7. Dealing with the Challenge of Scale

With highly advanced identity intelligence capabilities, in-depth risk analytics, persona-specific, business user friendly certifications and actionable dashboards, the Oracle Identity Governance Suite offers a robust set of Identity Certification features that provide a dramatic time and cost savings in access certification processes, and provide valuable insight to support business decisions. By automating access review and revocation processes, the solution helps control the overall

cost of complying with regulations that mandate access controls, at the same time, reducing the need for resources devoted to performing compliance and audit activities.

The certification solution provides capabilities to automatically collect, correlate and audit identity data from multiple enterprise resources and applications and dynamically generates risk-based certification campaigns presented to business (i.e. managers) and IT reviewers (such as application owners, data owners and role owners), with their own personalized, business friendly UIs. Spreadsheet-like views, advanced sorting and filtering capabilities and auto-certify options provide reviewers with the interactive tools they need to sustain potentially large volumes of user access information in their attestation reviews.

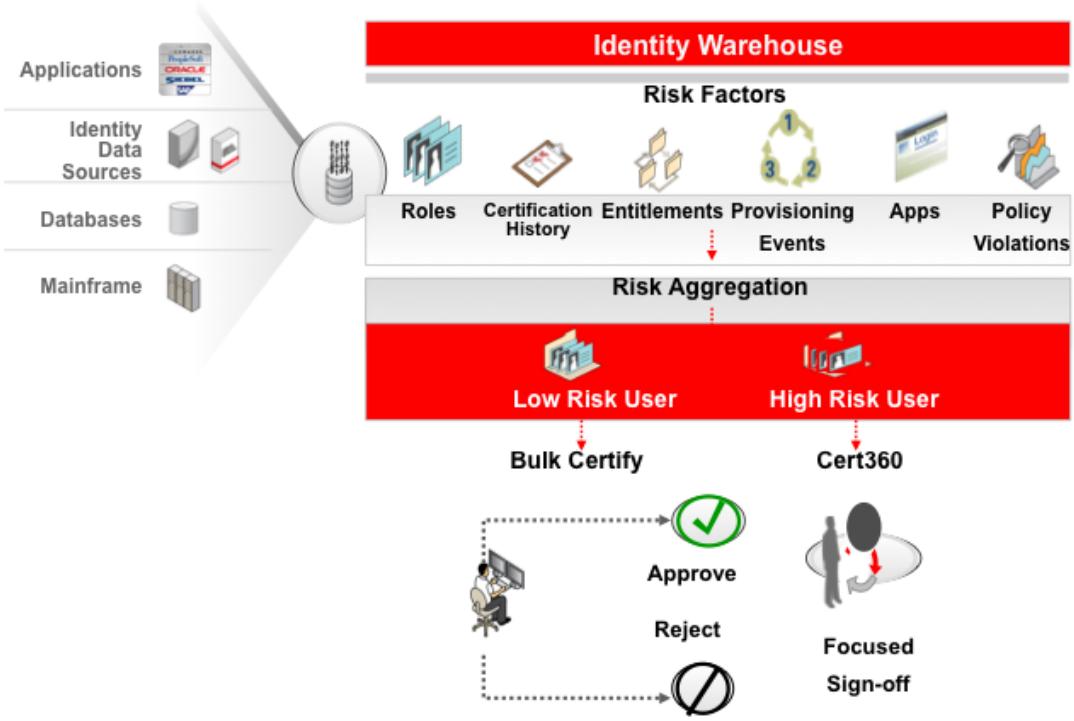

Figure 8. Oracle Identity Governance Suite – Risk Based Certifications

As shown in figure 8, the solution provides a business-centric certification user interface and certification campaign generation tools, which coupled with the introduction of rich Identity Risk Analytics, provides reviewers with the tools and contextual information they need to complete their certifications quickly. Risk aggregation and presentation across the user's identity lifecycle provides the core foundation of performing certification reviews in an efficient and sustainable manner. An end user's risk profile is determined with a clear High/Medium/Low Score associated to user roles, resources, entitlements and to events such as last attestation decisions, open audit violations and provisioning events. This allows reviewers to focus on "what matters most" to quickly prioritize and recognize high-risk user access, thus enabling smoother certification sign-off processes and improves user satisfaction.

In addition, the solution reduces operational risk exposure by providing reviewers with a *360-degree view* of users' access – not just "who has access to what", but whether access was appropriately assigned and how it is being used. The 360-degree view provides a holistic view of useful audit information such as previous certification decisions, rules or access policies used for assignment, role and entitlement metadata such as business glossaries and entitlement hierarchies, role usage

analysis, IT Audit violations and so on, providing comprehensive forensics capabilities to reviewers to make intelligent certification decisions.

As part of the robust integration between certification and provisioning, reviewers can determine *how* the access was assigned to a user and using visual risk indicators, determine high risk provisioning events. For example, if access rights were provisioned to a user using access request, the reviewers can view in the certification, any associated approval trails, and qualify it to be a lower risk event. However, if access rights were assigned to users directly in the target platform or application, as part of provisioning reconciliation, those access rights are monitored and flagged as high risk provisioning events, given that they might be rogue assignments. All high risk events are immediately flagged in certifications to allow reviewers to make intelligent decisions concerning user access and significantly reduce costs associated with existing manual controls and enhance audit effectiveness, resulting in enforcement of *"least privilege"* across the enterprise.

The use of roles lowers costs by simply reducing the number of objects that have to be managed for certification reviews and provides business reviewers with a better understanding of what they are attesting to. The solution provides *Role Vs. Actual* review capabilities that allow reviewers to quickly and efficiently attest to roles that users have access to, as well as the exception access rights, or the access rights that lie outside of the role assignments. Another feature that offers sustainability when automating certification reviews is the notion of *incremental* certifications, which allow reviewers to certify only the access rights that have been modified since the previous certification cycle, thus saving time and cost, while increasing efficiency.

Events such as employee transfers are common within an enterprise and the certification solution adapts to these events by dynamically generating event based certification reviews, allowing lines of business to monitor new access assigned to transferred users, while ensuring unwanted access is automatically remediated, thus enforcing compliant provisioning activities.

Finally, the solution offers *closed loop remediation*, which provides an automated, end-to-end solution for reviewing and revoking access across target systems and business applications and automatically verifies remediation and sends alerts if remediation does not take place. This helps control the cost of compliance by automating remediation processes and reduces the risk of policy violations and compliance failures.

IT Audit Monitoring

It is well known fact that majority of the computer-related criminal activity is a result of malicious activities performed by insiders. One of the most prominent threats is fraud that is particularly difficult to detect in computerized environments as automated through workflow systems. Therefore, it is of great importance to implement mechanisms to prevent such illegal activities. IT Audit policies then ensure that conflicting combinations or roles, entitlements and responsibilities of these smaller steps are not assigned to the same user. With the ability to define and enforce a security policy both within and across applications, Oracle Identity Governance Suite delivers a comprehensive solution for enforcing these policies, with continuous IT Audit Policy Monitoring. Policies may be defined at fine-grained entitlement or coarse-grained role

levels within an application or across applications, leveraging the complete set of identity and access data in the identity warehouse, collected from across the enterprise, and the enforcement process may be scheduled or executed on-demand. The IT Audit Monitoring engine can automatically identify imminent violations when users are provisioned especially after job changes that may affect their duties and maintains an ongoing record of activities with the potential impact of audit conflicts such as job changes, password resets, and so on.

Account Reconciliation & Rogue Detection

Account reconciliation is a key control objective for regulatory compliance, as it allows administrators to detect changes in access privileges originating outside the identity management system. These account changes are potentially rogue activities, and therefore trigger various remediation activities through the solution including exception approvals, certification cycles, and de-provisioning of entitlements or disabling accounts.

Accounts are linked to users' identities based on the correlation rules defined in the solution. If the correlation rules are unable to link an account to an existing identity, administrators can map accounts manually. Typically, this happens for some of the older accounts that were created before a strict user ID generation policy was in place. After manual linking there may still be accounts that may not be linkable to any user identities. These accounts are typically either recognized as specialized privileged or service accounts or orphaned accounts. Accounts may become orphaned because they were created at a given point of time for some special purpose and may not be required anymore. Orphaned accounts can be de-provisioned directly from the solution. The process of automatic and manual linking, identifying accounts, and remediating orphaned accounts is typically part of data cleansing that is performed as the first phase of on-boarding a new application using the Oracle Identity Governance Suite. However, periodic reconciliation can also help with detecting any orphaned accounts created.

Audit & Reporting

Oracle Identity Governance Suite provides comprehensive actionable dashboards and advanced analytics capabilities based on user identity, access and audit data residing in the Identity Warehouse of the solution. The solution provides various compliance and operational dashboards for a quick review of compliance and operational status in context of roles, segregation of duty policies, audit policies, remediation tracking and other controls. While compliance dashboards are typically used for executive level compliance monitoring, detailed out of box reports using BI technology enable IT staff, business users and auditors to structurally analyze the available wealth of identity data within their organization. The dashboards can further be customized for business users, compliance and audit officers and other end users on need basis. The solutions data dictionary is also published to allow customers to extend these reports and dashboards, and build their own.

From a certification perspective, all completed certification data is archived for audit purposes. This provides details information to auditors regarding *who has and who had access to what* rights, and whether revoked access rights were actually remediation from target systems and applications. A robust certification history of every action taken on user access rights is also available, thus providing crucial information to organizations to successfully pass their audits.

Some of the reports provided out of box with the solution include:

- Roles assigned to Users within each business unit in the enterprise
- Accounts associated to Users within each business unit in the enterprise
- Roles and associated policies within each unit in the enterprise
- Lists of all entitlements, roles, applications and their owners
- High privileged entitlements associated to users in the enterprise
- Operational exception reports classifying any missing data required for important correlations such roles without any policies, users with no roles, users with no entitlements, business unit with no associated users and so on
- Expiration forecast reports specifying user expiration, role expiration and role to user expiration
- Terminated user reports displaying terminated users in the enterprise for historical reporting
- Assigned vs. actual reports displaying users with access outside their roles
- Orphan Account dashboards providing the ability to accurately determine rogue accounts or assign accounts to their rightful owners
- Remediation Tracking Dashboards providing a comprehensive audit trail of revoked access (during certification reviews) and their remediation status
- Identity Audit Violations with a comprehensive exception management audit trail displaying action taken by remediators to correct IT Audit exceptions caused due to toxic combinations of user access
- Reports detailing who checked out privileged account passwords over a given period of time

Conclusion

Organizations today, face multiple challenges when balancing the need for users to require sufficient access rights to perform their job functions but at the same time, enforcing stringent governance processes to meet their compliance mandates. Oracle Identity Governance Suite solves these governance challenges by providing a unique focus in Identity Governance by amalgamating access grants and access monitoring to ensure that while users are able to procure access when they need it, there are sufficient preventative and monitoring controls in place to ensure that they have no more access than they need in order to fulfill their job responsibilities. This type of closed loop governance requires an integrated platform approach to governance problems and Oracle Identity Governance Suite uniquely distinguishes itself in its tight integration, common data model and platform based architecture.

Integraed Identity Governance - Business Whitepaper
July 2012

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

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together