



Leveraging Oracle Consulting to Implement Identity Management at Cisco

A Cisco and Oracle White Paper—March 2009

Table of Contents

Executive Overview	3
Cisco Background	3
Cisco's EIAM Vision	4
Cisco's Solution Requirements	5
Cisco and Oracle Team	6
Oracle Consulting Methodology	7
Cisco Project Timeline	8
Phase I: Inception (Oracle)/ID & Assess (Cisco IT)	9
Phase II: Elaboration (Oracle)/Analysis (Cisco IT)	9
Phase III: Construction (Oracle)/Iteration (Cisco IT)	9
Phase IV: Transition (Oracle)/Enterprise Test (Cisco IT)	9
Phase V: Production (Oracle)/Implement (Cisco IT)	10
Next Steps	10
Results	11
Best Practices	11
Conclusion	11

Executive Overview

In late 2006, Cisco IT executives, key stakeholders, and the Corporate Security Programs Organization made a strategic decision to adopt an Identity Management (IdM) solution to manage user identities and access to critical corporate resources. This decision was based on the company's increasing pace, size and IT complexity following numerous acquisitions and integration of systems.

Cisco initiated a comprehensive program, defined as Enterprise Identity and Access Management (EIAM). The program's charter was to integrate business processes, policies and technologies that collectively manage access to Cisco's corporate resources and identities.

The EIAM program had the following key business drivers:

- Simplified and Personalized End-User/Customer Experience
- Streamlined Operations and Growth Through Partners/Customers
- Enable Growth through Acquisitions
- Intellectual Property Protection and Security
- Risk Mitigation of Regulatory Non-compliance
- Improved Auditability
- Operational Efficiency & Cost Containment (e.g. reduce IT support costs)
- Fraud Detection and Prevention

“The mission for Cisco’s EIAM program was to establish an integrated system of business processes, policies and technologies that facilitate and control users’ access to Cisco’s managed resources, while protecting confidential personal and business information from unauthorized users and enabling collaboration. The scope included managing identities and access for approx. 70,000 employees and non-employee contract workers in addition to our ecosystem of partners, customers and suppliers.”

**—Brenda Hughes
EIAM Program Leader
Cisco, Inc.**

Through business value analysis and roadmap planning, the program plan called for the central management and automation of identities and access leveraging leading enterprise-caliber solutions from Oracle and Cisco. The solution focused on leading technologies and services to enable automated provisioning, identity administration, and access and compliance management. Cisco engaged Oracle Consulting to assist the EIAM program team in deploying this solution. Oracle Consulting worked within a blended team model alongside Cisco architects and project teams to provide a cohesive solution around user provisioning, reduced sign-on, and access management reporting.

The joint effort between Oracle Consulting and Cisco was successful. Cisco launched an enterprise-wide solution in September 2008 leveraging Oracle Identity Manager (OIM). The initial rollout of this solution was by the Commerce platform, which is a transformational program geared towards improving the commerce experience for Cisco's customers, partners, and its own employees by providing the most innovative and seamless commerce experience - anywhere.

Cisco Background

Cisco Systems, Inc., which was founded in 1984, designs, manufactures, and sells Internet Protocol-based networking and telephony solutions and other products relating to the communications and information technology industry worldwide. Headquartered in San Jose, California, the company offers routers that interconnect computer networks and enables the moving of information between networks; switching systems, which provide connectivity to end users, workstations, and servers; *application networking solutions* to deploy and deliver business applications; *home networking products*, such as voice and data modems, network cards, media adapters, Internet video cameras, network storage, and USB adapters; *hosted small-business systems*, including integrated voice and data products; and *Cisco security solutions* to protect information systems. Cisco also provides *storage area networking* products that deliver connectivity between servers and storage systems; *unified communication products*, which integrate voice, video, data, and mobile applications on fixed and mobile networks; *video systems*, including digital set-top boxes and digital media technology products; and in-building and outdoor *wireless networking products*. Furthermore, the company also offers *cable access*, *service provider VoIP services*, and *optical networking products*.

Cisco's EIAM Vision

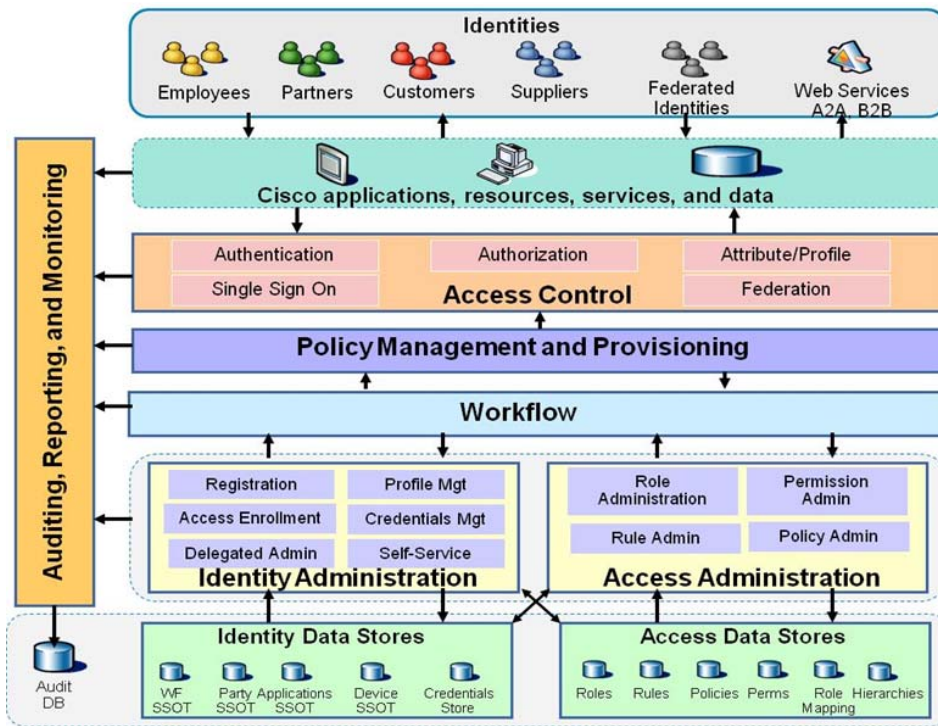
Cisco's EIAM program team performed an extensive analysis of the stakeholder requirements and the IAM technology market space. The thorough research enabled the team to define a standards-based, vendor-agnostic; data-driven modular architecture to enable centralized enterprise-wide access and compliance management capabilities.

The following were some of the key technical drivers that contributed to the decision-making process for designing Cisco's IAM end state architecture:

- Reduction of programmatic security in favor of declarative security
- Externalization and centralization of access management for applications, devices and resources
- Virtualization and controlled access to identity and policy data
- Centralization of auditing and reporting,
- Self-service and delegated administration of identities and access

The EIAM team worked more than 4 months on a comprehensive technology and integration proof of concept vetting the end state architecture and ensuring that selected vendor offerings meet not only Cisco's business and technology requirements but also its IT vision.

Figure 1.



Cisco's technology landscape already included a large number of applications, platforms, and solutions from Oracle and other vendors. In order to implement an end-to-end solution defined by the target state, Cisco needed to select a number of adjacent technologies in IAM space, such as an account provisioning system and Web access control technology to complement what it already had in-house. Access management, which is the cornerstone of Cisco's EIAM end state vision, is being implemented using Cisco's Enterprise Policy Manager (former SecureNet's Entitlements Management System). Cisco EPM provides centralized, policy-based access management. It is based on industry standards across heterogeneous systems and applications (Web, devices, network) and supports fine-grained access control for Cisco's myriads of custom applications and Web services. Cisco EPM enhances customer experience, reduces security risk and assists in meeting regulatory, legal and

corporate compliance requirements. The Cisco EPM solution also improves security posture through employing role and rule based policies and Segregation of Duty (SOD).

The Cisco team took the internal technology space into account as well as the state of the IAM market and selected Oracle Identity Manager (OIM) and Oracle Access Manager (OAM) to complete the EIAM foundation along with Cisco EPM.

Oracle Identity Manager (OIM) provides a centralized identity system to manage access to Oracle and other applications, provision user accounts, and manage user groups and responsibility memberships across various business communities, business platforms and enterprise directories. Oracle Access Manager (OAM) provides improved user experience and security through single-sign-on (SSO) and global logout functionality.

Together, Cisco's Enterprise Policy Manager and Oracle's Identity Management solutions offer a fully integrated and comprehensive enterprise IAM platform that contributes to business risk reduction; ensures regulatory, legal, and corporate policy compliance; streamlines customer experience; while providing alignment with enterprise level architecture, standards and platforms.

The result was a well-defined and integrated EIAM solution, which included the following Oracle IdM components:

- Oracle Identity Manager (OIM)
- Oracle Access Manager (OAM)

The complete technology stack for Cisco's EIAM platform included the following existing technologies:

- Oracle Identity Directory (OID)
- Oracle Application Server 10g (OAS)
- Oracle E-Business Suite (EBS) modules
- Tibco's MMX
- IBM WebSphere
- IBM WebSphere Portal
- Microsoft Lightweight Directory Services (MS LDS)
- Microsoft Active Directory (MS AD)

Cisco was looking for an implementation partner to realize its Enterprise Identity and Access Mgmt (EIAM) vision. It had an enormous scope, needing management of millions of users and their privileges across hundreds of different applications and platforms. After careful technical architecture vetting and resource expertise validation, Cisco selected Oracle Consulting as its trusted partner to implement one of the largest Oracle IdM deployments in the industry to date.

Cisco's Solution Requirements

Cisco has an aggressive list of IAM solution requirements. Some of the key access and provisioning requirements were as follows:

Oracle Identity Management Requirements

- **Management of the end-to-end lifecycle of user identities across all enterprise resources:** Manage a user identity by enabling timely identity attribute updates to ensure targets contain the most up to date user identity information regardless of the status of the user identity.
- **Centralized user provisioning/de-provisioning based on reconciled data from multiple Sources of Record (SORs):** Enable automated provisioning to targets from a central solution, which interfaces with the approved data sources for user identities.
- **Business rules driven auto-provisioning/de-provisioning:** Support event and business rules driven auto provisioning and de-provisioning; prevent unauthorized access to resources and provide support for a timely user on-boarding and off-boarding processes.

- **Logging and reporting of provisioning events:** Enable out-of-the-box logging and reporting functionality to track user identity changes and provisioning events in support of operations and compliance requirements.
- **Compliance monitoring:**
 - Enable the attestation functionality to support compliance requirements for periodic revalidation of a user’s access to targets.
 - Enable target reconciliation to detect rogue and orphaned accounts. As well as detect target administrator changes performed outside of the provisioning solution.

Oracle Access Management Requirements

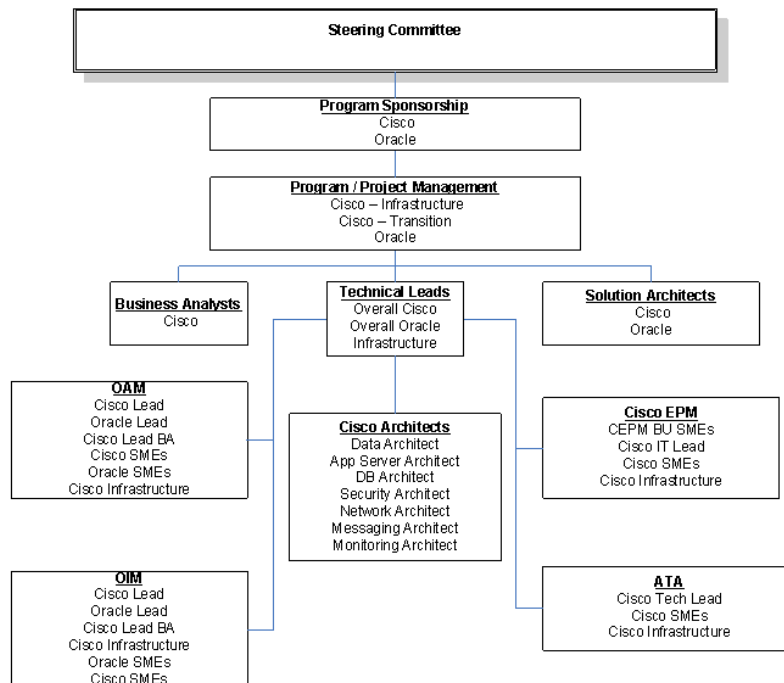
- **Web Single Sign On (SSO):** OAM will provide a seamless SSO experience for 2 million+ Cisco internal (Cisco workers) and external users (guests, customers, partners, and suppliers). In addition, the solution needs to ensure that SSO can be maintained between resources protected by legacy access control systems.
- **Global log out:** Improve customer experience by allowing a user to log out of one resource and log out of all other logged in resources at the same time.
- **Logging specific to access control:** Ensure access attempts and failures are logged in support of operations and compliance requirements.

Cisco and Oracle Team

Cisco chose Oracle Consulting to be their trusted advisor and lead implementation team across multiple System Integrators because of Oracle Consulting’s deep expertise in implementation of Oracle IdM products, breadth of best practices, as well as for direct access to Oracle support and Oracle product development teams.

The team consisted of an average of three (3) to as many as eighteen (18) Oracle Consulting consultants during the project. This number as well as the mix of onsite/offshore resources fluctuated with the phases of the release.

Phase 0 (Inception) Program Structure:



Post Phase 0 Program Structure:

In order to structure the team optimally to deliver on the end-to-end foundation, the implementation team was divided among several tracks:

- **Track 1** consisted of delivery of identity & account provisioning (leveraging OIM technology), as well as Web access control (leveraging OAM technology) components. This is where the team worked very closely with the Oracle Consulting and product management teams for successful execution.
- **Track 2** consisted of delivery of access and policy management as well as fine-grained access control (leveraging Cisco EPM technology). The team closely aligned with the Cisco product team to help incorporate requirements into product releases on the roadmap in alignment with Cisco IAM vision for this component.
- **Track 3** consisted of delivery of the Cisco IT custom-built Attribute Authority (AtA) component. AtA is a virtualization layer (virtual directory) for business attributes. Business attributes for requested identity (employee, partner, customer, guest etc.) are grouped as profile and available in various formats to the applications. The team worked across a number of Cisco organizations that manage the identity data sources in order to deliver on this virtualization layer for identity data.

Each of the tracks had a standard structure for an IT project and included a Cisco IT Project Manager, IT Technical Lead, IT Analyst and a number of IT Engineers. Depending on the Infrastructure requirements, appropriate Infrastructure teams (identity services, application server, networking, hosting, storage, DBAs, etc.) were involved in the deployment as well.

Oracle Consulting Methodology

Oracle Consulting, the primary professional services team partnering with Cisco, employed the Oracle Unified Method (OUM), Oracle's standards-based method that enables the full Information Technology (IT) lifecycle. OUM provides an implementation approach that is rapid, broadly adaptive, and business-focused. OUM includes a comprehensive project and program management framework and materials to support Oracle's growing focus on enterprise-level IT strategy, architecture, and governance. OUM supports Oracle-based business solutions including deep support for Identity Management (IdM) and Governance, Risk and Compliance (GRC).

OUM Project Phases

Workflows within an OUM project are categorized into five phases: Inception, Elaboration, Construction, Transition, and Production. These phases are described below:

Phase I: Inception

The overriding goal of the Inception phase is to achieve concurrence among all stakeholders on the lifecycle objectives for the project. This activity is most significant for new development efforts, in which important business and requirements risks must be addressed before the project can proceed. The Inception phase is used to kick off a solution development engagement; review the strategic direction of the client's business; and confirm, document, and prioritize the high-level business requirements for the implementation. It is also the time to begin assembling and integrating the project team, to scope the entire engagement, and develop the initial project plan.

Phase II: Elaboration

The goal of the Elaboration phase is to develop the detailed requirements models, partition the solution, develop functional prototyping, and baseline the architecture of the system. This effort results in a stable basis for the design and implementation effort in the Construction phase. The architecture evolves from the most significant requirements, those that have the greatest impact on the architecture of the system, and an assessment of risk. The stability of the architecture is evaluated through one or

OUM Overview

- **Business:** Focus on the business and assure stakeholder acceptance and delivery of the development's efforts.
- **Architecture:** Define architecture before resources are committed for development and implementation.
- **Adaptability:** Encourages adaptability for scalable delivery across small and large projects possessing disparate resources and skill levels.
- **Implementation:** Provides rapid implementation techniques to ensure business solutions in short timeframes
- **Standards:** Leverage the Unified Modeling Language and the Unified Software Development Process.

more architectural prototypes. During the Elaboration phase, the development team's understanding of the client's business requirements is verified to reduce development risk.

Phase III: Construction

The goal of the Construction phase is develop, test and integrate the components of the solution. This effort results in a first release, often called a beta release, of the solution. An iterative process is used to refine the data, detail the use cases, and develop the physical database and components. This process is repeated, within the constraints of the project timeboxes and priorities, until the business requirements are met.

Phase IV: Transition

The goal of the Transition phase is to install the solution onto the production system, perform acceptance testing, and launch the live application. During this phase, the new system is accepted by the client organization, the organization is made ready for the new system, and the system is put into production. If the new system replaces an old one, a smooth cutover to the new application is provided. The Transition phase can span several iterations and includes testing the product in preparation for release and making minor adjustments based on user feedback.

Phase V: Production

The goal of the Production phase is to operate the newly developed system, assess the success of the system, and support the users. This includes: monitoring the system; acting appropriately to ensure continued operation; measuring system performance; operating and maintaining supporting systems; responding to help requests, error reports and feature requests by users; and managing the applicable change control process so that defects and new features are prioritized and assigned to future releases.

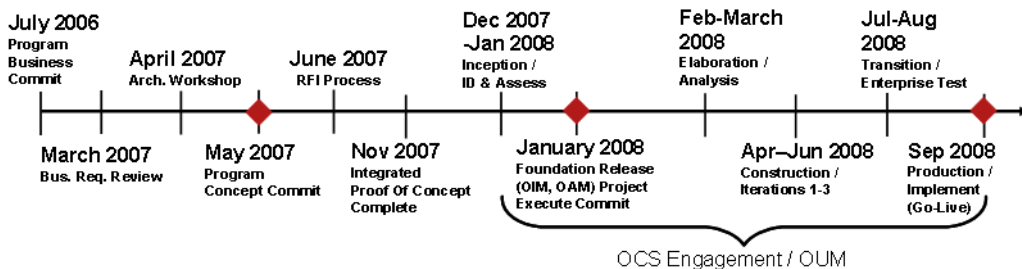
OUM Benefits

- **Improved Business – IT Alignment:** Improving enterprise business modeling efforts increases the chances that systems will be built to support business goals.
- **Reduced Project Risk:** Implementing an iterative, cross-functional method mitigates development over schedule and over-budget risks.
- **Reduce Costs:** Implementing a strategic, repeatable approach significantly reduces the cost of developing software.
- **Higher Quality Development:** Leveraging mature, iterative lifecycle management processes significantly reduces defects, misalignment with requirements, and other causes for project re-work.
- **Improved Planning:** Insight into overall business needs and vision; improved strategic tools for repeating project success allows IT management to more accurately forecast resource and budget needs.
- **Greater Adaptability:** Improvements to business and IT planning enable an enterprise to react more effectively to changes in the marketplace.

Cisco Project Timeline

Cisco follows an aggressive timeline mapped to each phase and identified key deliverables for each.

Figure 2. EIAM Program Timeline



Cisco IT follows the PLC (Project LifeCycle) methodology for project delivery to ensure a consistent operating model for all IT projects. This is especially important in cross-functional initiatives such as EIAM. In order to leverage best practices from the OUM methodology and the Cisco IT PLC practices, the Oracle and Cisco Program Managers mapped phases of the Cisco IT PLC (Iterative approach) to Oracle OUM and came up with a refined list of deliverables. This list was used to drive the project plan for the release. The mapping exercise also confirmed that the OUM model is consistent with the Cisco IT PLC (Iterative approach).

Phase I: Inception (Oracle)/ID & Assess (Cisco IT)

The Oracle Consulting team was initially engaged to provide advisory and implementation services to deliver the first phase of the foundation for the EIAM Platform of services. The Oracle Consulting team comprised of a Program Manager who was responsible for the overall success of the program deliverables. A Solution Architect offered the high-level architecture plan for the implementation and was responsible for putting together a team to deliver on this initiative. A Project Manager and an Enterprise Technical Lead were to carry out the initial Phase 0 of this project that included requirements gathering and initial technical design blueprints for the entirety of the project. This team was responsible for the overall delivery of the project working in tandem with the subject matter experts for each platform product i.e. track leads for OIM, OAM, etc. The Oracle Consulting team worked with Cisco to gather a clear understanding of the business drivers and worked on a detailed project scope to leverage the various EIAM capabilities. The defined scope helped put together a comprehensive project management plan and selection of the team for Phase 1 activities.

Phase II: Elaboration (Oracle)/Analysis (Cisco IT)

The team performed several critical tasks during the Elaboration phase that covered the traceability and validation of requirements against their defined use cases. This included the vetting and prioritization of use cases to maximize the business benefit for the initial foundational EIAM release; and to ensure that the solution was being developed and released in iterative time boxes and on time. Necessary development systems were built to ensure the teams could develop the solution

Key activities completed in this phase were:

- Defined the logical specification
- Prepared development and test environments
- Analyzed the impacts on boundary systems
- Developed high level schedules and resource requirements for the project

Phase III: Construction (Oracle)/Iteration (Cisco IT)

The custom development activity of the Cisco EIAM implementation leveraged the concept of a message-driven architecture, where all user-provisioning activities were initiated from a Cisco trusted source. Cisco leveraged Oracle Consulting's offshore (Global Services Delivery) teams to develop the necessary code around message beans, and all target provisioning related customizations. The on-site Oracle Consulting consultants designed and architected the system in close collaboration with the Cisco EIAM team, and offered necessary advice and assistance in deploying the code across environments to perform several rounds of testing. Comprehensive testing efforts include unit-testing limited to Oracle Consulting developers and consultants in both the Oracle offshore environment followed by deployment and then in the Cisco development environment. Finally Cisco QA team was responsible for all system integration and performance testing.

The Iteration phase was composed of multiple iteration cycles and the focus of each cycle was to deliver a functional increment of the final system (or the final system). At the end of each Iteration cycle a full set of unit and functional system tests were executed. Requests for additional functionality were also considered in subsequent iteration cycles as time allowed.

Phase IV: Transition (Oracle)/Enterprise Test (Cisco IT)

During the transition phase, the Cisco and Oracle Consulting teams ported the solution from development to the testing environment and finally to the production environment with necessary enterprise, user acceptance testing and final practice run. Several cut-over processes were executed in between these environment migrations to ensure that the actual go-live would be efficient and with minimal interruption to the business, with this integrated platform. Several cross-functional Cisco IT teams in addition to the core EIAM team were engaged to make necessary changes in the integrated systems getting deployed and to ensure acceptance testing was handled independently. All issues that appeared during these tests were remediated for management to make a positive go-live decision at the Readiness Review. This effort also included ensuring that the data acquired from a Cisco trusted identity source was cleansed before it was imported into OIM.

Phase V: Production (Oracle)/Implement (Cisco IT)

Before the actual production rollout, the management sign-off and change management processes were followed to adhere to Cisco's standard release cycles. The core EIAM team collaborated and coordinated with Cisco's business, infrastructure, applications and support teams to ensure smooth delivery and release. During the release period, the Oracle Consulting and EIAM core teams were available to address transitioning of the EIAM platform to the Environment Services - Directory Identity Services (DIS) team for long-term support and operations of the end-to-end solution. Appropriate individuals were identified to monitor the system performance in production and to resolve any unforeseen problems. Necessary SLAs (Service Level Agreements) were created to ensure timely resolution and response times were agreed upon by all of the Infrastructure and Application Service Provider teams. Finally, the team put in place a post-production support plan for continued management of the system - and an enhancement plan for the project's long-term success.

Next Steps

Cisco has defined a comprehensive long-term strategy that comprises of multiple initiatives to be completed over time. This phased approach enables Cisco to benefit from "quick wins" along the way to address the most critical challenges first while maximizing the business value.

The first phase, addressed by the initial production launch for access control and identity management, is aimed at user communities serving the commerce business processes, and the relevant key applications. This initial phase defined a comprehensive approach for on-boarding the remaining user communities and systems for adoption of the platform. The following phases will focus on extending the solution to manage access to other Cisco resources and platforms, and will be managed by a sustaining function within Cisco IT.

Oracle Consulting has provided Cisco with a recommendation around the deployment roadmap taking into consideration the existing systems landscape, active programs and upcoming initiatives. The adoption plan is in place for Cisco to continue to deploy the foundation solution by aggressively retiring legacy access applications.

Results

Below table represents the fulfilled goals with the initial release of the OIM Identity Provisioning Services (IPS) in production, with the corresponding release features and business value proposition.

Table 1.

Cisco Fulfilled Goals	OIM Foundation Feature	Cisco Value Proposition
Enhanced access to Oracle EBS for Commerce (initial client release) partners and work force users through improved on-boarding and off-boarding responsiveness	<ul style="list-style-type: none"> Streamlined and automated user account life cycle management for access management Near real-time business policy driven account provisioning management 	<ul style="list-style-type: none"> Reduce IT complexity and access control inefficiency by introducing policy driven access management Reduce IT costs by simplifying the maintenance effort for user account management Lower IT operating expenses by automating repeatable user administration tasks
Access management continuous improvement and operational excellence	<ul style="list-style-type: none"> Elimination of certain in-house custom script-based provisioning Vendor-based foundation for Identity and Provisioning Management 	<ul style="list-style-type: none"> Improve IT productivity by replacing manual in-house provisioning solution for Oracle EBS with an integrated IDM solution from Oracle Reduce risk of service degradation by shifting from in-house support of custom built scripts to premium support from a strategic vendor
Minimized SOX, IT, and regulatory compliance risk	<ul style="list-style-type: none"> Foundation for better auditing and account management with the automated identity life cycle management Identity reconciliation "policies" resulting in reported data integrity violations 	<ul style="list-style-type: none"> Reduce risk of unauthorized intrusion by detecting rogue/orphaned accounts that violate current policies Minimize SOX risk by maintaining user account access properly when user profile attribute changes occur Minimize SOX and regulatory compliance risks by decreasing the resolution time for out of compliance items
Streamlined solution deployment for implementing the OIM Identity Provisioning Services (IPS) in-production service quickly	<ul style="list-style-type: none"> Repeatable deployment process with OIM provisioning capability 	<ul style="list-style-type: none"> Reduce project costs and improve employee productivity by shortening implementation cycle for managing access control of Oracle EBS systems

Best Practices

- Deliver solution based on a proven methodology that is understood within the organization
- Develop a strong but pragmatic roadmap to deployment
- Document and thoroughly inspect the design before development of components
- Prototype the solution and demonstrate it to key stakeholders
- Plan for building of necessary tools to handle large data volume transfers i.e. bulk load techniques
- Implement and adhere to change management processes
- Develop best practices and processes around communications and management of the vendor product teams
- Ensure that the operations/support team is involved with and has inputs to the system design and requirements for operational considerations
- Ensure a plan for data clean-up and governance is in place
- Clear identification of roles and responsibilities across Oracle Consulting, System Integrators and internal teams
- Ensure configuration management is in place across all of the system lifecycles (sandbox, dev, stage, prod).

Conclusion

With a strong partnership, Oracle and Cisco successfully collaborated in meeting the key objectives of the program in addressing Cisco's key IdM challenges. As a result, Cisco has achieved its vision of IAM with a successful deployment of the largest, industry leading IdM solution anchored around providing business value with sound architectural design. Cisco anticipates this IdM solution to enable it to better serve both its internal and external customers.



Leveraging Oracle Consulting to Implement Identity Management at Cisco
March 2009
Contributing Authors: Manuel Fernandes, Amanda West, Thomas Burke, Tanu Sood, Ramki Pitchuiyer

Contributing Authors (Cisco Team): Sergei Rousakov, Brenda Hughes, Irene Sklyar, Charlene Wright

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



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA



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

Copyright © 2009, Oracle. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners

© 2009 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)
DM/LW15595 03/09