

WE CAN HELP YOU SECURELY MANAGE YOUR RELATIONSHIPS WITH YOUR MOST VALUABLE ASSETS...



IDENTITY MANAGEMENT & SARBANES-OXLEY

October 4, 2004

Ehab Dawoud

Director, Advisory Practice



Table of Contents

- Identity Management
- Value of Identity Management
- Sarbanes Oxley
 - ✓ Overview
 - ✓ Section 302
 - ✓ Section 404
- Control Objectives of Sarbanes Oxley
- The Issue
- The Recommended Solution





IdM Identity Management is not a turnkey solution – it is a business strategy manifested in a comprehensive and evolving solution deployment that must ultimately involve the entire enterprise. IdM is a convergence of technologies and business processes. There is no single approach to IdM because the strategy must reflect specific requirements within the business and technology context of each organization.

Identity Management (IdM), its a business strategy affecting the entire organization.

The Solution



Identity Management (IdM), from



Key Drivers

Cost Reduction

Increased Security

Increased Compliance

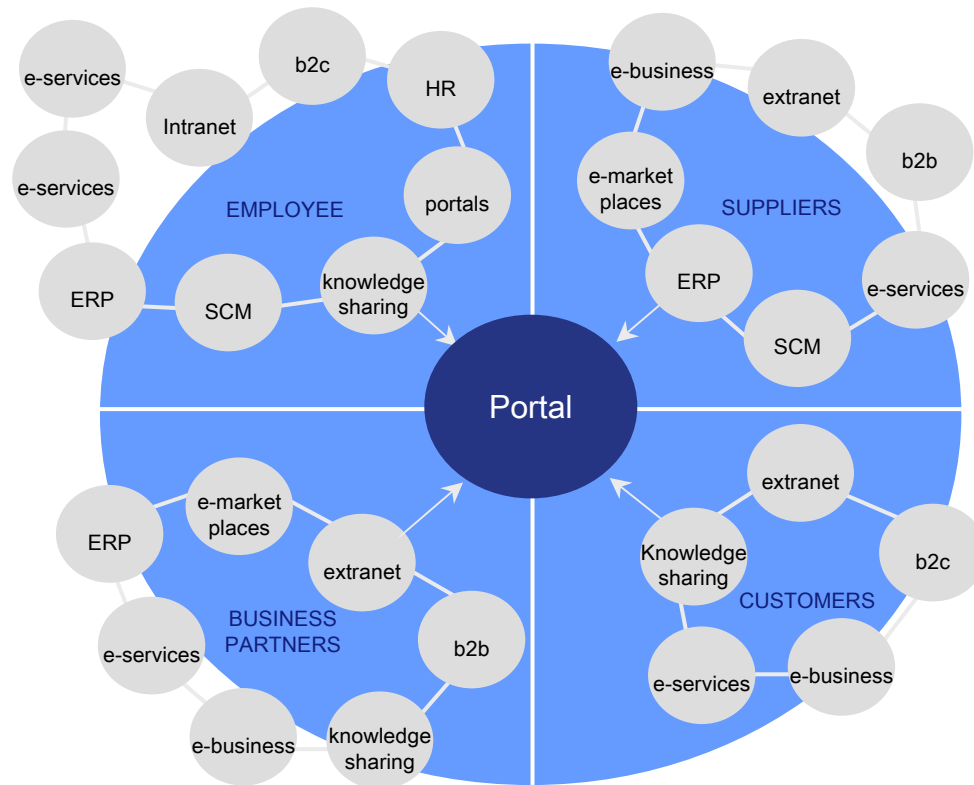
Enhanced User Experience

Centralised Policies

Delegated Administration



How do I manage all of the corporate user's identity and credentials across the enterprise application landscape?



Enterprise Security



Enterprise Security

- The strategy for securing information and enabling resources
- The security delivery model for the company
- The security framework that serves the extended enterprise
- Provides a common security services component framework

Identity Management

- The source of timely and trustworthy user management
- The place where user information is secured
- The vehicle for user enablement across the enterprise
- The focal point of securing the enterprise information
- The solution to effectively and efficiently be Sarbanes Oxley compliant



What is the IdM value?

Key IdM Business Drivers and Objectives – Gartner/PwC Market Study

Security

- ✓ Secure data and network access
- ✓ Increase ability to manage enterprise assets
- ✓ Assure authentication across platforms
- ✓ Centrally managed environment

Operations Management

- ✓ Decrease administrative/help desk overhead
- ✓ Reduce number of logins/passwords
- ✓ Efficiently and effectively support high-turnover, high-growth environments

Compliance

- ✓ Sarbanes Oxley
- ✓ HIPAA
- ✓ FDIC
- ✓ Gramm-Leach-Bliley
- ✓ Sarbanes-Oxley

Business Initiatives

- ✓ Support CRM, Portals, SCM, ERP, etc.

Strategic Initiatives	Regulatory Requirements
Increased Security	Operations Management



What is the IdM value?

Key IdM Business Drivers from a Sarbanes Oxley Point of View

Short Term

- ✓ User access control
- ✓ Enterprise role definition
- ✓ Segregation of duties
- ✓ Delegation of authority
- ✓ Adequate methods of de-provisioning user accounts
- ✓ Audit trail for system access.

Long Term

- ✓ Develop consistent, sustainable, reusable method of managing user access controls including:
 - ✓ Addressing open audit issues
 - ✓ Internal/external employees, non-employees, contractors, consultants, partners, and vendors
 - ✓ The entire lifecycle from submission of an application to termination of employment or contract including job transfers



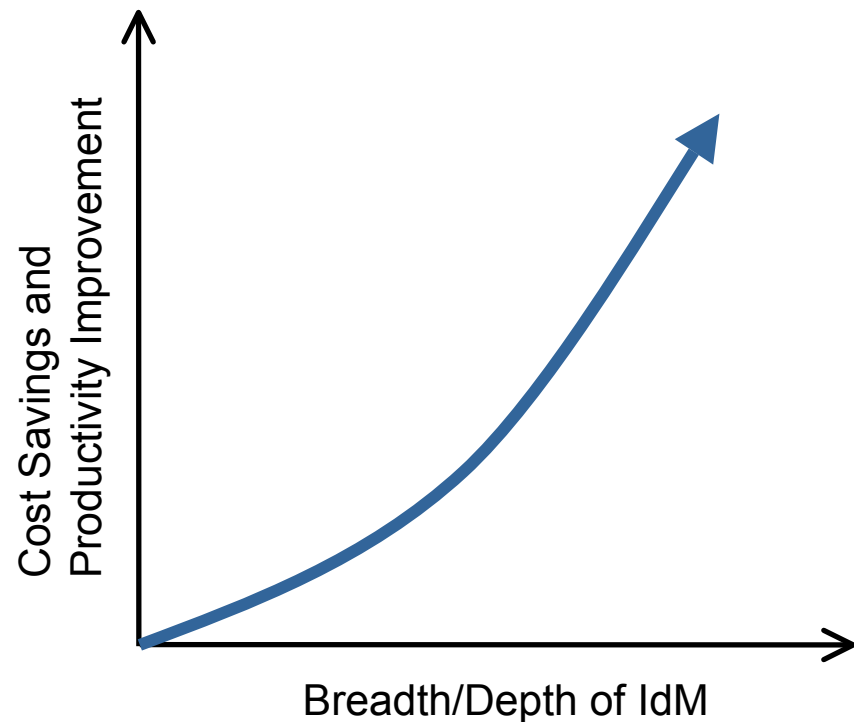


What is the IdM value?

According to the Gartner/PwC market study, organizations are targeting identity management for **compliance**, **cost savings**, **productivity improvement**, increased security and increased user satisfaction.

Lower user administration costs through centralized administrative functions for multiple platforms: “saved 40 percent in less than one year”

Gartner/PwC Market Study



Sarbanes-Oxley Act of 2002: Overview

Basic requirements of the Act

- Management of “publicly traded companies” are required to make an assertion regarding the effectiveness of their internal controls over financial reporting.
- The internal controls must be documented and management must be in a position to demonstrate to its auditors and regulators its support for its assertion.
- An external auditor will have to attest to management’s assertion and include a report in public filings the results of the attestation.
- Management must utilize a framework such as COSO for assessing its controls and making its assertion.

Potential Ramifications of Non-Compliance

- Violation of Federal law and regulations.
- Civil and criminal liability exposure.
- Damage to reputation, brand, and/or regulatory relationships.
- Diminution in value of the company.



Section 302 of Sarbanes Oxley

Who

- A company's management, with the participation of the principal executive and financial officer (the certifying officers)

What

- Certifying officers are responsible for establishing and maintaining internal control over financial reporting.
- Certifying officers have designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under their supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles.



Section 302 of Sarbanes Oxley

- Any changes in the company's internal control over financial reporting that have occurred during the most recent fiscal quarter and have materially affected, or are reasonably likely to materially affect, the company's internal control over financial reporting are disclosed.
- When the reason for a change in internal control over financial reporting is the correction of a material weakness, management has a responsibility to determine whether the reason for the change and the circumstances surrounding that change are material information necessary to make the disclosure about the change not misleading.

When

- Already in effect as of July 2002



Section 404 of Sarbanes Oxley

Who

- Corporate management, executives and participation of the principal executive and financial officer (“management” has not been defined by the PCAOB—Public Company Accounting Oversight Board.)

What

- A statement of management’s responsibility for establishing and maintaining adequate internal control over financial reporting for the company
- A statement identifying the framework used by management to conduct the required assessment of the effectiveness of the company’s internal control over financial reporting
- An assessment of the effectiveness of the company’s internal control over financial reporting as of the end of the company’s most recent fiscal year, including an explicit statement as to whether internal control over financial reporting is effective



Section 404 of Sarbanes Oxley – Cont'd

- A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the company's internal control over financial reporting
- A written conclusion by management about the effectiveness of the company's internal control over financial reporting.
- Management is precluded from concluding that the company's internal control over financial reporting is effective if there are one or more material weaknesses. In addition, management is required to disclose all material weaknesses that exist as of the end of the most recent fiscal year.

When

- Year-ends beginning on or after 15 November 2004**

**Non-accelerated filers (<US \$75 million market capitalization) can defer to 15 July 2005



Control Objectives of Sarbanes Oxley that Identity Management can address

▪ Procedures exist and are followed to authenticate all users to the system to support the validity of transactions.

- Authentication/Authorization

▪ Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., regular password changes).

- Authentication/Authorization

▪ Procedures exist and are followed to ensure timely action relating to requesting, establishing, issuing, suspending and user accounts.

- User Provisioning/De-provisioning

▪ A control process exists and is followed to periodically review and confirm access rights.

- Monitoring of User Access

▪ Where appropriate, controls exist to ensure that neither party can deny transactions and controls are implemented to provide transaction initiation and approval.

- Workflow and monitoring of workflows



Control Objectives of Sarbanes Oxley that Identity Management can address

▪ Controls relating to appropriate segregation of duties over requesting and granting access to systems and data exist and are followed.

▪ Access to user-developed systems is restricted to a limited number of users.

- User Provisioning/Work Flow

- Authentication/Authorization



How is Sarbanes affecting a company's technology infrastructure and capabilities

- Many companies are putting manual processes & “solutions” in place for first year compliance, which is acceptable. However, automating those processes & solutions for long term effectiveness is “critical”.
- Key technology areas impacted within a company include:
 - ✓ ERP systems
 - ✓ Network infrastructure
 - ✓ Directories, Identity provisioning, and access management systems
 - ✓ Documentation control & monitoring
 - ✓ Data quality & governance
- Understanding the relationship between the Sarbanes-Oxley requirements and the tactical and strategic technology enablers is “critical” for the C suite of these companies.



The Issue

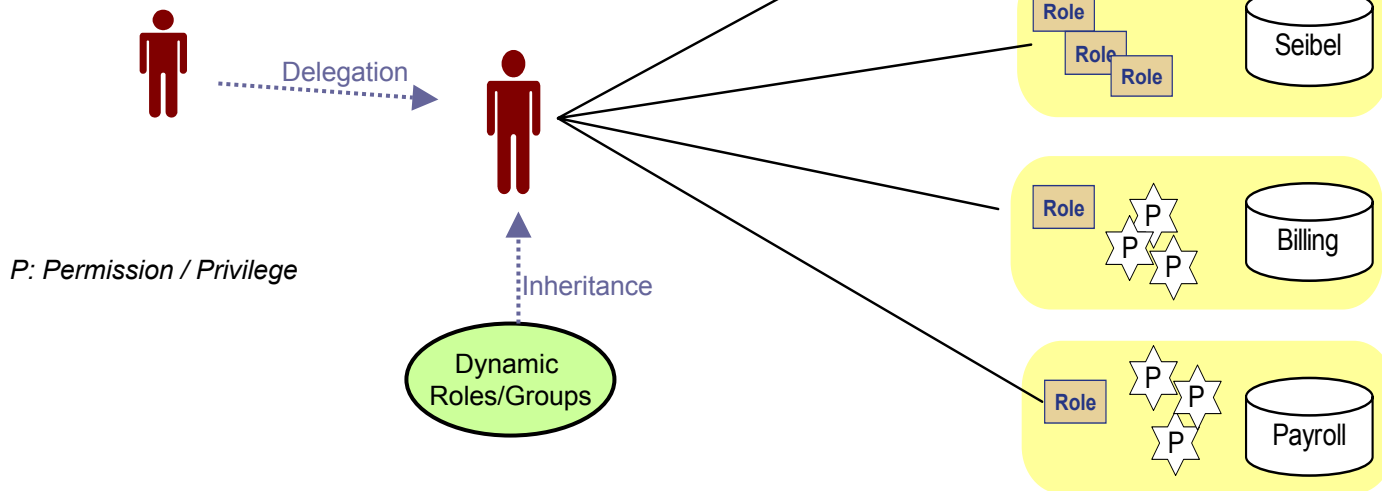
A potential for a control deficiency to be identified concerning conflicts in segregation of duties within the key applications, and potentially across other financial applications.

The lack of user access controls over one or more of these applications can have a pervasive impact over financial processes that lead to a significant deficiency and/or material weakness if not remediated.



Root Cause

- User retains old Roles and privileges from previous positions
- User may inherit Roles from others through delegation of authority
- Users may gain additional access privileges due to dynamic Roles/groups
- No global view of user access rights
- Unauthorized sharing of passwords



- Roles are designed specific to applications
- Each application maintains its own list of Roles and Access Control List
- Segregation of duties are implemented on each application individually
- Lack of centralized Access Control systems to enforce security policies

Results

- ✓ Lack of check for segregation of duties across the enterprise
- ✓ Lack of enterprise user access control model!

Recommended Solution

Design a user access control model and framework that supports key security principles:

- **Least Privilege:** users to operate with minimum set of privileges necessary to do their jobs
- **Segregation of duties:** for particular set of transactions, no single individual be allowed to execute all transaction within the set.
- **Data Abstraction:**
 - Security policies be independent from data and system specific resources and
 - Adaptable across various systems

Develop a reference architecture for the user access control systems to enforce the defined model

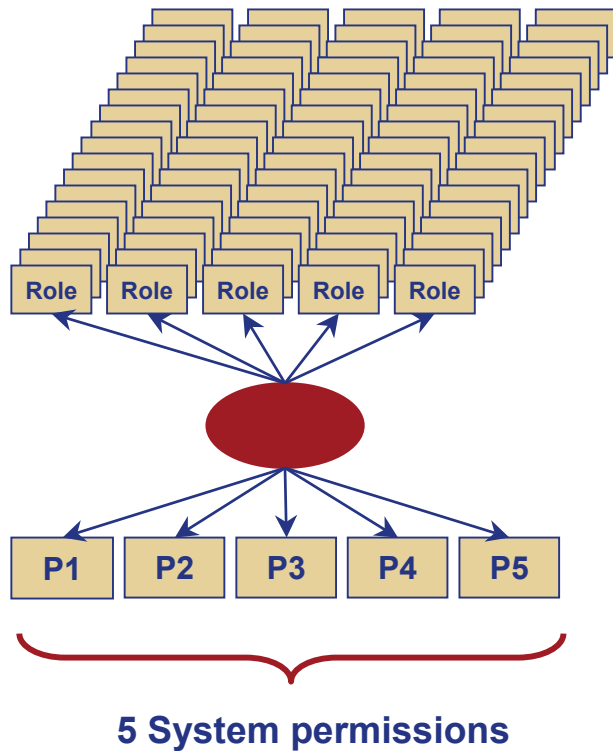
Solution = Role Engineering + IdM Infrastructure



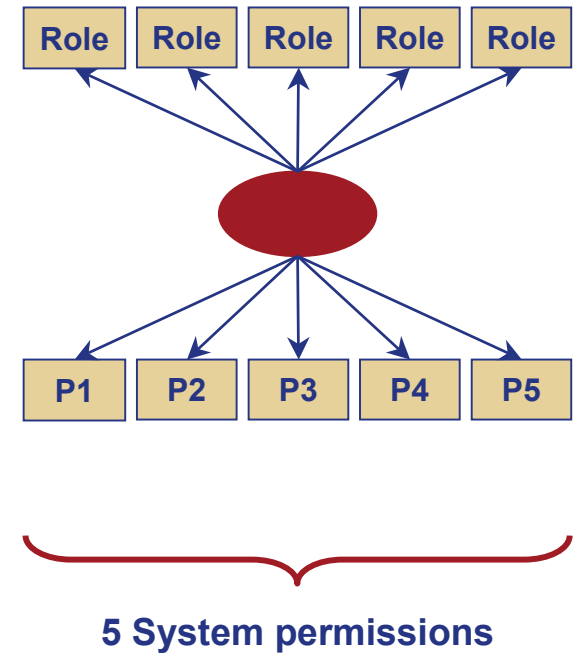
Role Proliferation

Many-to-one vs. many-to-many

- Many-to-many relationship:
- Role Permutation of five permissions: $(5!)$
 $5 \times 4 \times 3 \times 2 \times 1 = \text{up to 120 unique roles to manage}$



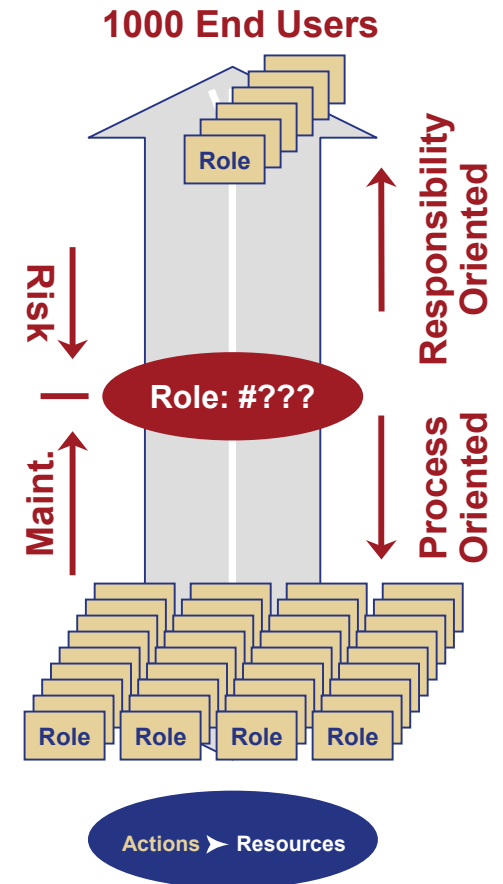
- Many-to-one relationship:
- Role Permutation: Max of 5 Roles



Role Engineering Concepts

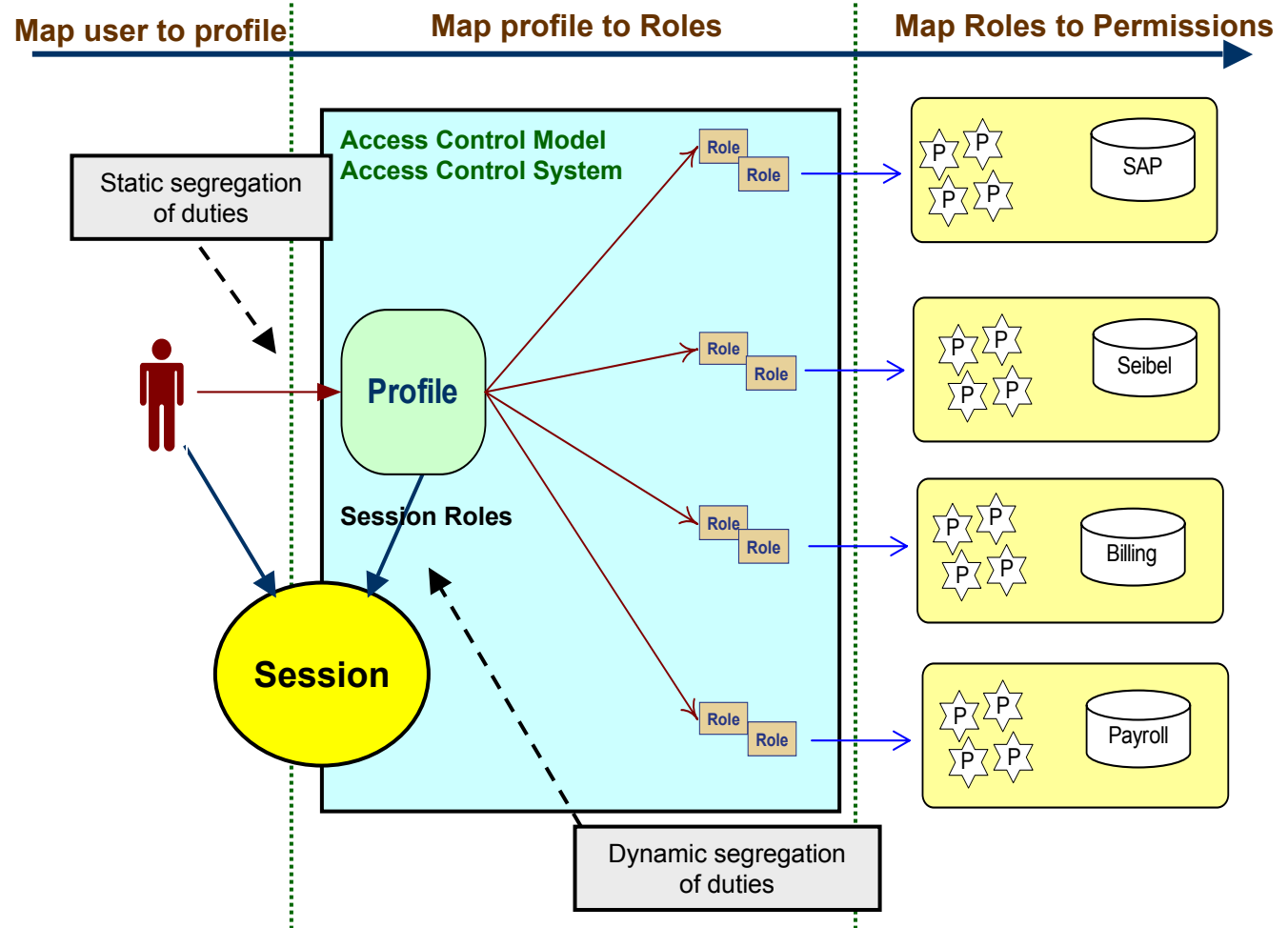
- **Background information:** 1000 end users, 500 permissions
- **Issue:** How many roles are needed?

Design Factors	Responsibility Oriented Roles	Process Oriented Roles
Function of Role	<ul style="list-style-type: none"> ■ Desire for less administration ■ Responsibility oriented roles ■ Results in few roles 	<ul style="list-style-type: none"> ■ Need for more granular access ■ Process oriented roles ■ Results in more roles
Maintenance Implication	<ul style="list-style-type: none"> ■ Lower number of roles ■ Reduced administrative maintenance 	<ul style="list-style-type: none"> ■ Higher number of roles ■ Increased administrative maintenance
Risk Implication	<ul style="list-style-type: none"> ■ Increased risk, through less granular permission groupings 	<ul style="list-style-type: none"> ■ Decreased risk, through more granular permission groupings
Content of Role	<ul style="list-style-type: none"> ■ 10 roles ■ Each role has average of 50 permissions 	<ul style="list-style-type: none"> ■ 50 roles ■ Each role has average of 10 permissions

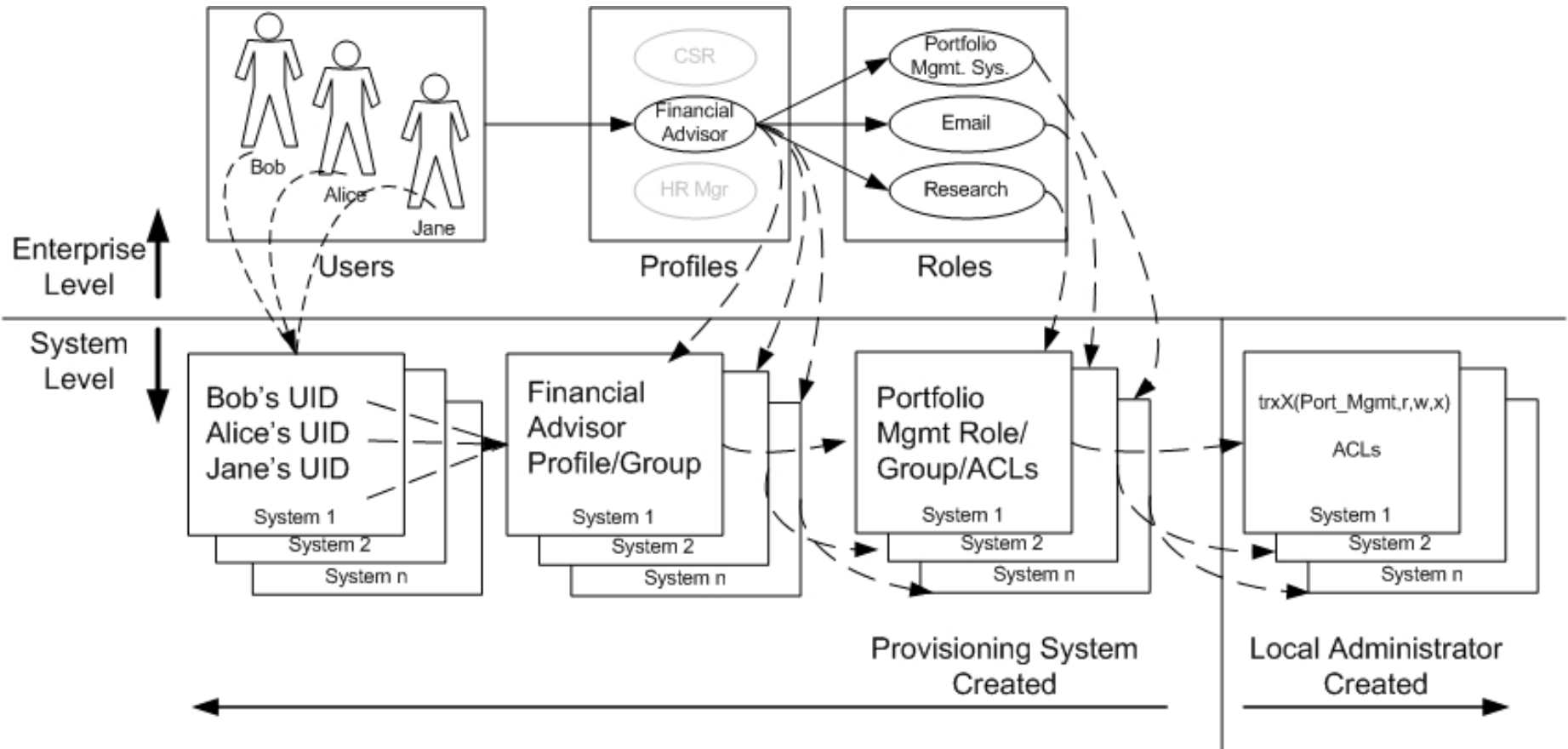


Solution Concepts

- Profile represents a global view of user access rights
- Each user can assume one profile at any given session
- Each profile can map to multiple Roles
- There is a centralized access control system to enforce security policies
- Access control systems that monitor segregation of duties to include:
 - ✓ Static Roles
 - ✓ Dynamic Roles
 - ✓ Delegation of authority

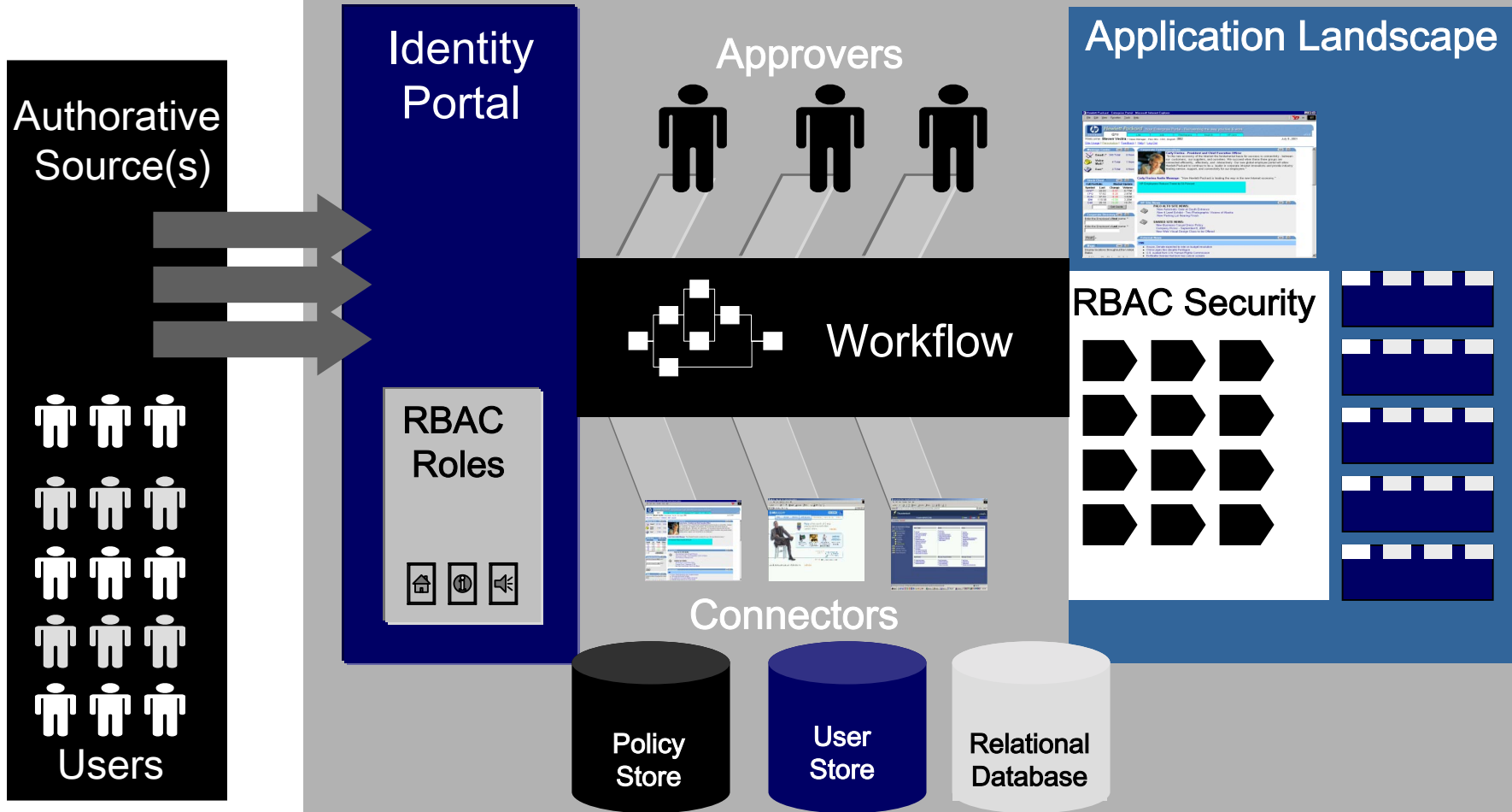


Enterprise Level and System Level View



Reference Architecture

User Provisioning and Workflow Process Flow



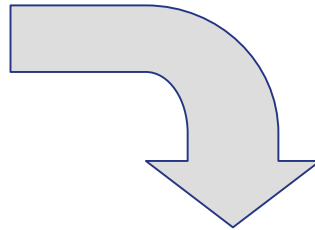
Key Deliverable - Organizational Access Matrix

The screenshot shows a software application interface with two tables. The 'User' table has columns for 'User' and 'Region Code'. The 'User Region Code' table is a grid with 'User Region Code' in the header and a grid of data below.

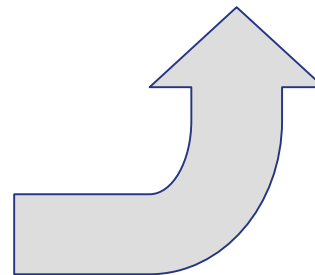
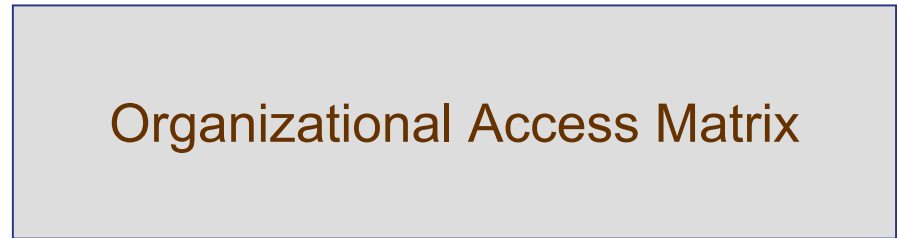
- User to Process Responsibility
- Process to System
- User to Profile

The screenshot shows a software application interface with two tables. The 'Task' table has columns for 'Task' and 'User Region Code'. The 'User Region Code' table is a grid with 'User Region Code' in the header and a grid of data below.

- Process to Task
- Task to Permission
- Permission to Role



•The Organizational Access Matrix is composed of multiple relationships and provides a central repository for the RBAC design specifications.



• Profile to Role

Key Task – Role to Profile Mapping



- This sample matrix represents the alignment of the previously created Profiles and Roles.
- This relationship defines the underlying roles that a user will inherit when assigned a Profile.

	EP 1	EP 2	EP 3	EP 4	EP 5	EP 6	EP 7	EP 8	EP 9	EP 10	EP 11	EP 12	EP 13	EP 14	EP 15	EP 16	EP 17	EP 18	EP 19	EP 20	EP 21	EP 22	EP 23	EP 24	EP 25	EP 26	EP 27	EP 28	EP 29
Role1																													
Role2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Role3																													
Role4	X	X	X								X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Role5																													
Role6	X								X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Role7	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Role8	X				X																X	X	X	X	X	X	X	X	X
Role9	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Role10																													
Role11	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Role12																													
Role13	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Role14																													
Role15	X	X	X																		X	X	X	X	X	X	X	X	X
Role16	X	X	X																		X	X	X	X	X	X	X	X	X
Role17	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Role18	X																	X	X	X	X	X	X	X	X	X	X	X	X
Role19	X																	X	X	X	X	X	X	X	X	X	X	X	X
Role20																													
Role21	X																	X	X	X	X	X	X	X	X	X	X	X	X
Role22																													
Role23	X																	X	X	X	X	X	X	X	X	X	X	X	X



Conclusion

- IdM is an enabling tool to implement a sustained-automated process for:
 - User Access Control
 - Segregation of Duties
 - Delegation of Authority
- Most companies have 60-70% of their enterprise role already defined
- Limit the number of key application list to 6-8 apps.
- Validate and prototype the model for a subset of users. This group of users should include those who are involved with financial transactions.



Ehab Dawoud

edawoud@us.pwc.com

415-498-7333

Gretchen Lott

Gretchen.L.lott@us.pwc.com

415-281-4749

PRICewaterhouseCOOPERS 

Your Worlds



Our People

© 2002, PricewaterhouseCoopers LLP. All rights reserved.

PricewaterhouseCoopers refers to the US firm of PricewaterhouseCoopers LLP and other member firms of the worldwide PricewaterhouseCoopers organization.