



Identity Management Overview

Bill Nelson

bill.nelson@gca.net

Vice President of Professional Services



Technology Services
Software. Training. Consulting.

Agenda

- Common Identity-related Requests
- Business Drivers for Identity Management
- Account (Identity) Management
- Identity Management Solution Areas
- Oracle Identity Management Suite



Pop Quiz!

User Provisioning

Q: What determines your **employee's access**?

- a - Give Wally access to whatever Alice has
- b - Provide access based on his business roles
- c - Do whatever his manager says



DILBERT: © Scott Adams, Inc. / Dist. by UFS, Inc.



DILBERT: © Scott Adams, Inc. / Dist. by UFS, Inc.

User Entitlements

Q: Who is the **most privileged user** in your enterprise?

- a - Security administrator
- b - Chief Financial Officer
- c - The summer intern who is now working for your competitor



Q: How do you **control access** to your sensitive applications?

- a - Usernames and passwords
- b - Contextual authentication
- c - Hardware token



Cost of Compliance

Q: How much are manual **compliance** controls **costing** your organization?

- a - Nothing, no new headcount
- b - Don't ask
- c - Don't know



Auditing and Reporting

Q: Can you **prove** that it was Professor Plum who did it in the library with a candlestick?

a - Yeah right

b - I haven't a CLUE!



Common Identity-Related Requests

We Must Have:

- **More control** over our account management processes
- A **reduction in calls** to the help desk for:
 - Resetting account passwords
 - Updating account information
- **Accurate reporting** in order to pass audits

We Would Like to:

- Implement a **roles-based account management** solution
- Implement **single sign on**
- Provide our **users with self-service**
- **Synchronize account data** between repositories

So what is driving these requests?

Business Drivers for Identity Management

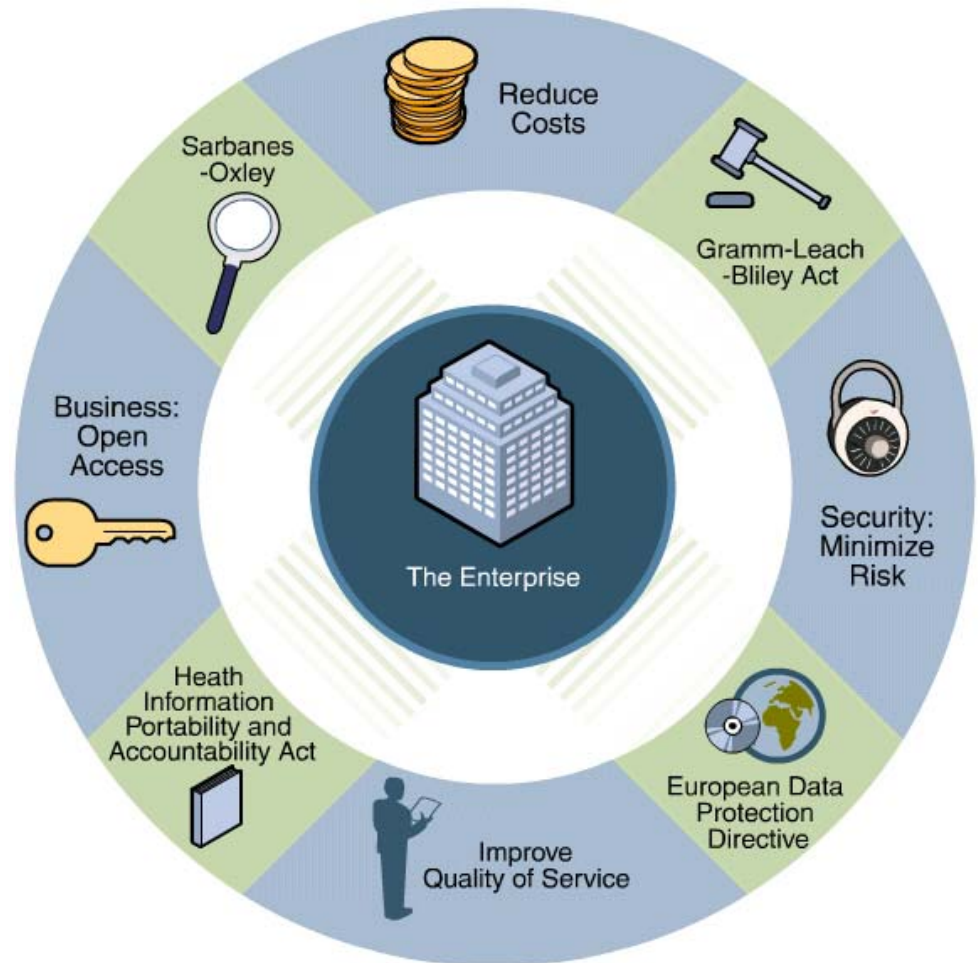
Companies are being asked to:

- Reduce Cost while Improving QoS
- Open Access and provide more services but expected to Minimize Risk
- Adhere to regulatory compliance

In general:

- => Do more with less
- => Do it safely and securely

The enterprise is getting “squeezed”



Solution: Identity Management

Features:

Identity Management focus areas:

1. Data Synchronization
2. Account Management (Provisioning/Deprovisioning)
3. Password Management (self-service)
4. Single Sign-On
5. Attestation and Non-repudiation

It all boils down to how do we **create** an identity, **use** the identity during the course of normal business activity, **review** the identity to ensure it is still necessary, and then **remove** (or disable) it when it is not needed.

What is Identity?

Before we go any further, let's review the concept of an *identity*.

1. Virtual representation of a user
2. Rights and relationships to enterprise resources
3. Profile that tells a company's network:
 - **Who** you are
 - **What** you are entitled to do
 - **When** you are allowed to perform specific functions
 - **Where** you are allows to perform functions from
 - **Why** you have been granted permissions
 - **How** you are using your identity over time



Contextual Identities

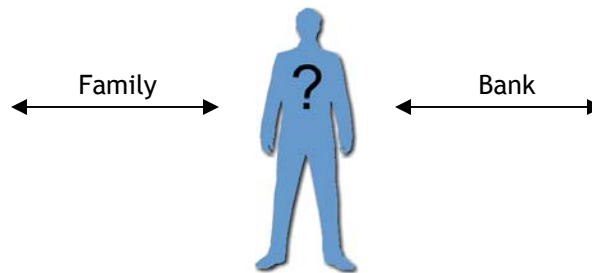
You have a different identity based on your relationships

Name: Dad
Nickname: Snuggles
Address: 1234 Somewhere Street
Home Phone: 813-555-1212
Roles: Lawn Guy, Dish Washer,
Heavy Hand



Broker

First name: William
Last name: Nelson
Investor Type: Moderate
Account numbers: 123456789
User name: bnelson
Password: *****
PIN: ****



First name: William (Bill)
Last name: Nelson
Department: Prof Svcs
Office location: 1A2F
Manager: Attila
User Name: bnelson
Password: *****



Office

First name: William
Last name: Nelson
Address: 1234 Somewhere Street
Account number: 987654321
User name: bnelson_1234
Password: *****
PIN: ****

What is Identity Management?

So then, what is *identity management*?

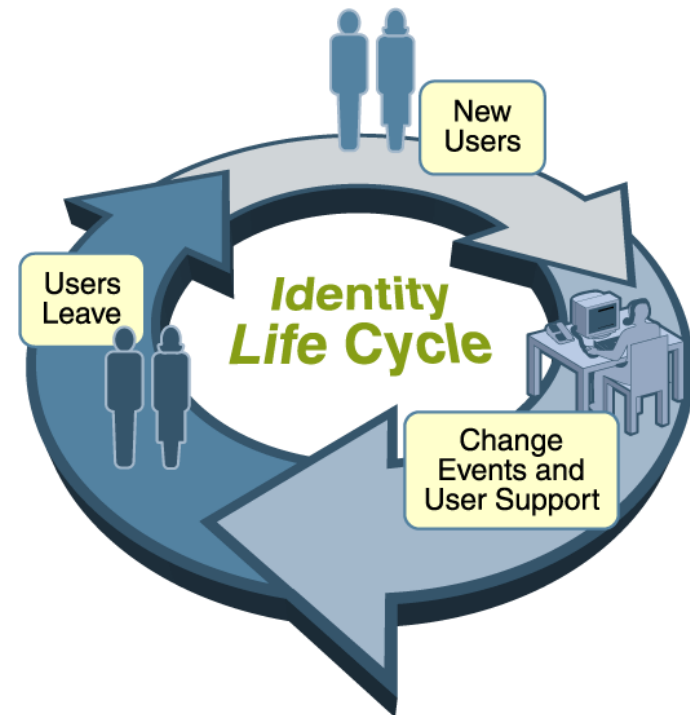
Involves User Account **Creation**, **Modification**, **Disablement** and **Deletion**...

Across **heterogeneous** platforms using a scalable, secure, rapid deployment architecture...

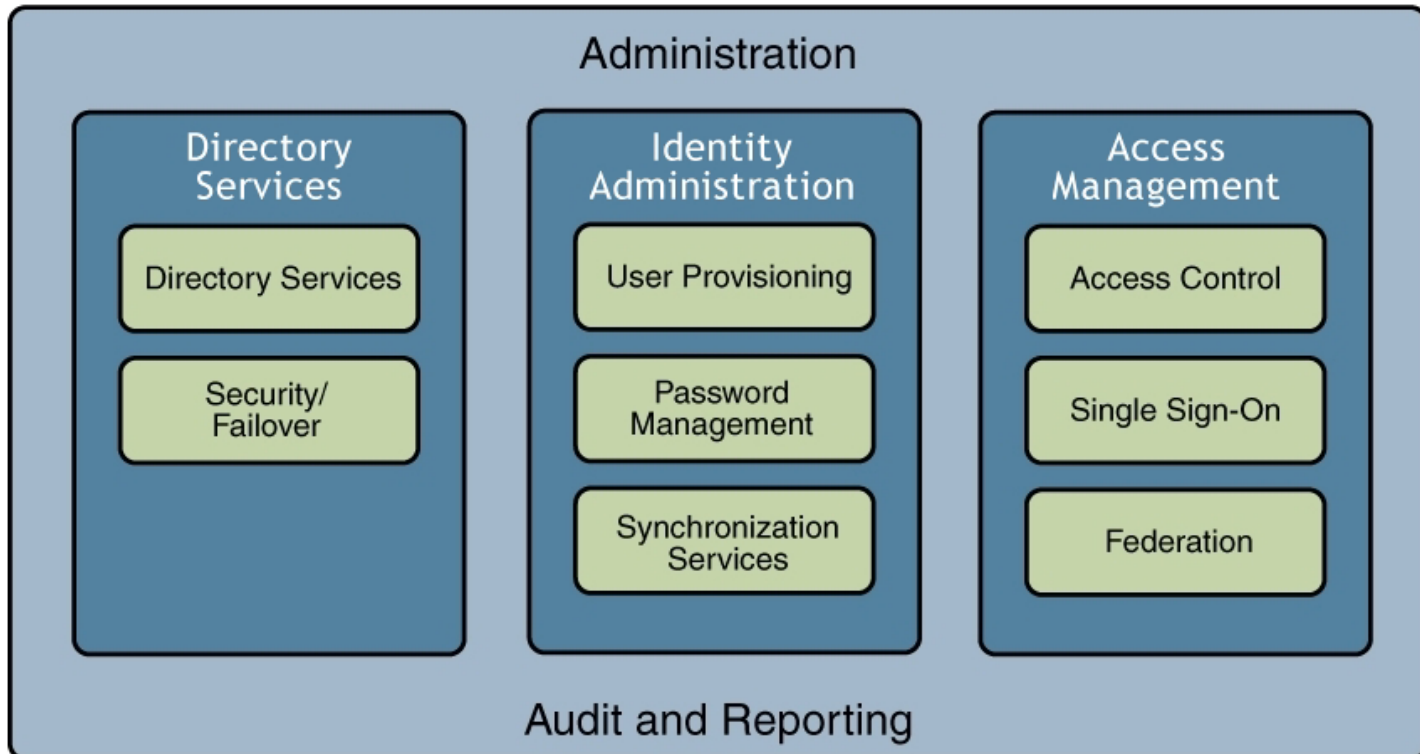
Utilizes **delegated administration**, workflow, rules and policies...

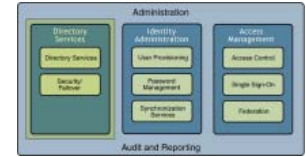
Supports **end-user self service** password reset and provisioning...

With **centralized auditing** and **reporting**



Categories for Identity Management

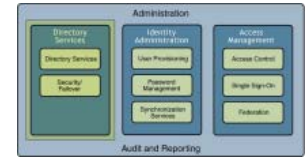




Identity Management focus areas:

1. Data Synchronization
2. Account Management
3. Password Management (self-service)
4. Single Sign-On
5. Attestation and Non-repudiation

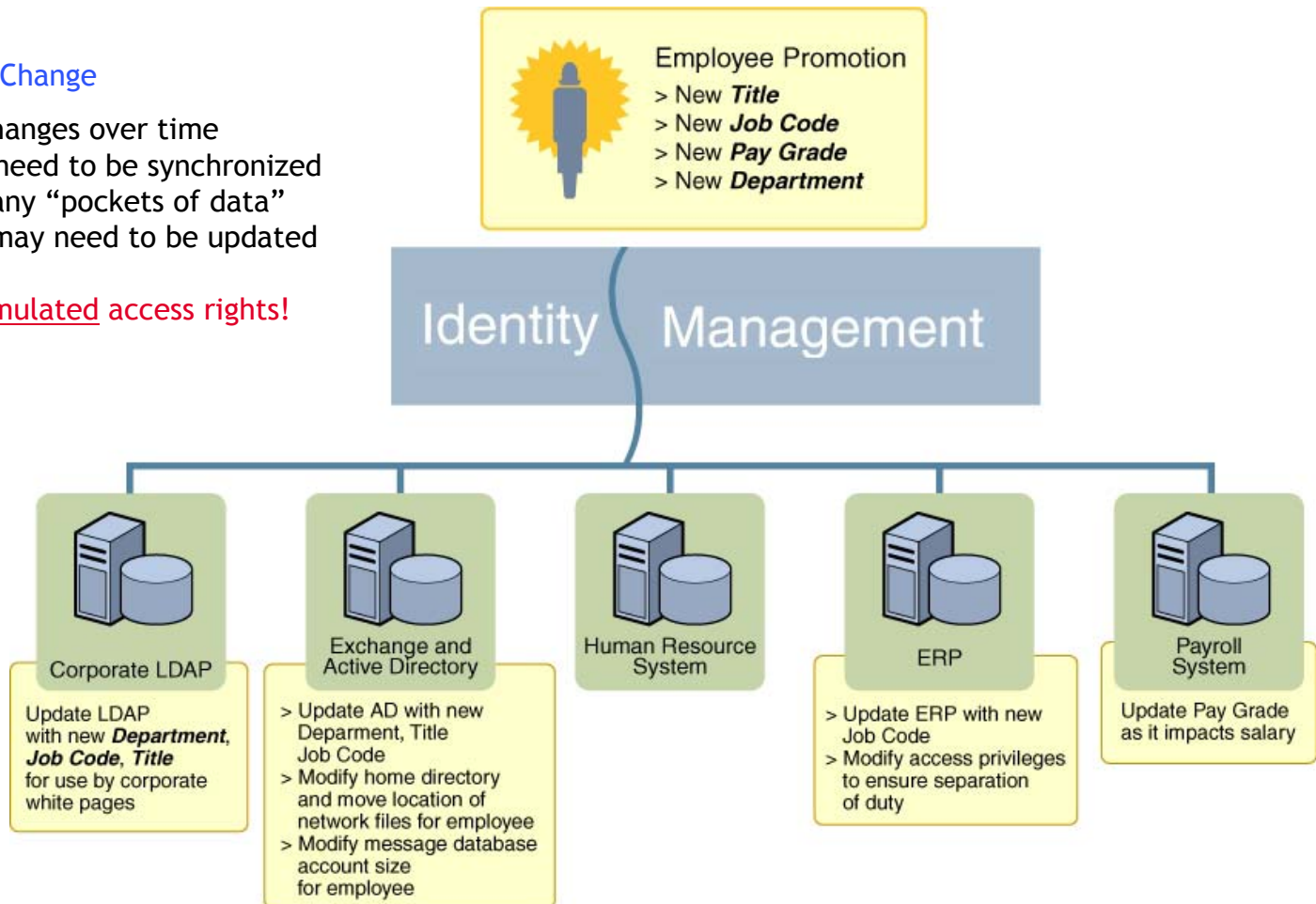
Data Synchronization



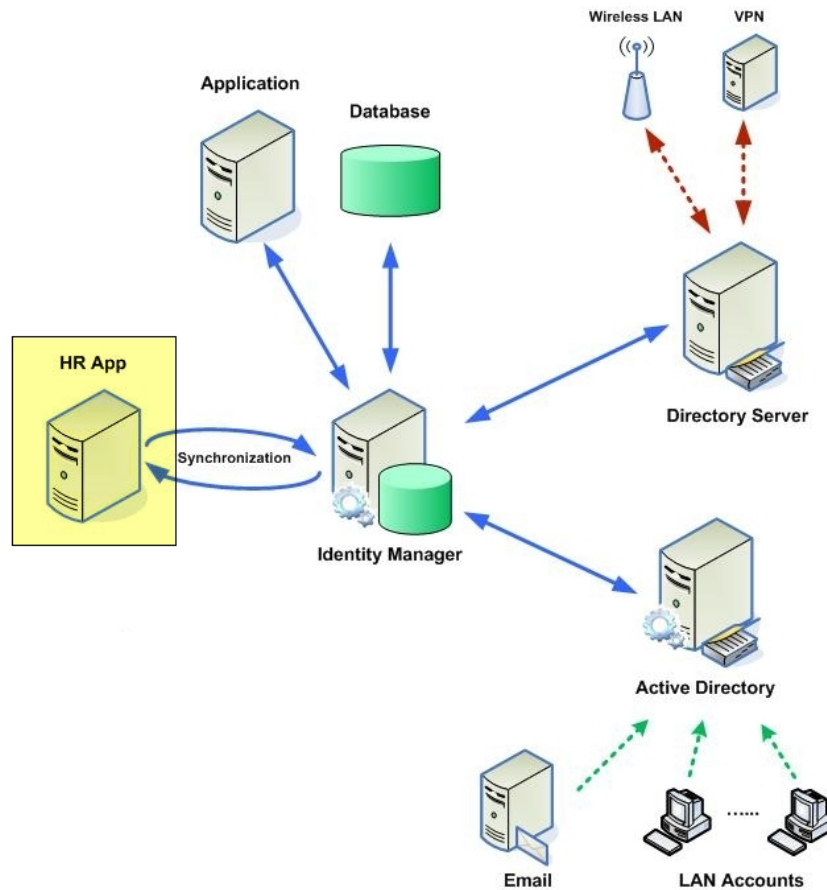
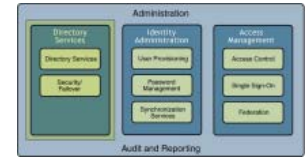
Reality: **Things Change**

- Information changes over time
- Data changes need to be synchronized across the many “pockets of data”
- Access rights may need to be updated

Beware of accumulated access rights!

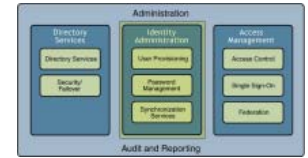


Identity “Hub”



1. Change event occurs in HR
2. Data is synchronized between:
 - Human Resources Application
 - Downstream Resources
3. Manual modifications at Identity Hub
4. Process can involve:
 - Approvals
 - Notifications

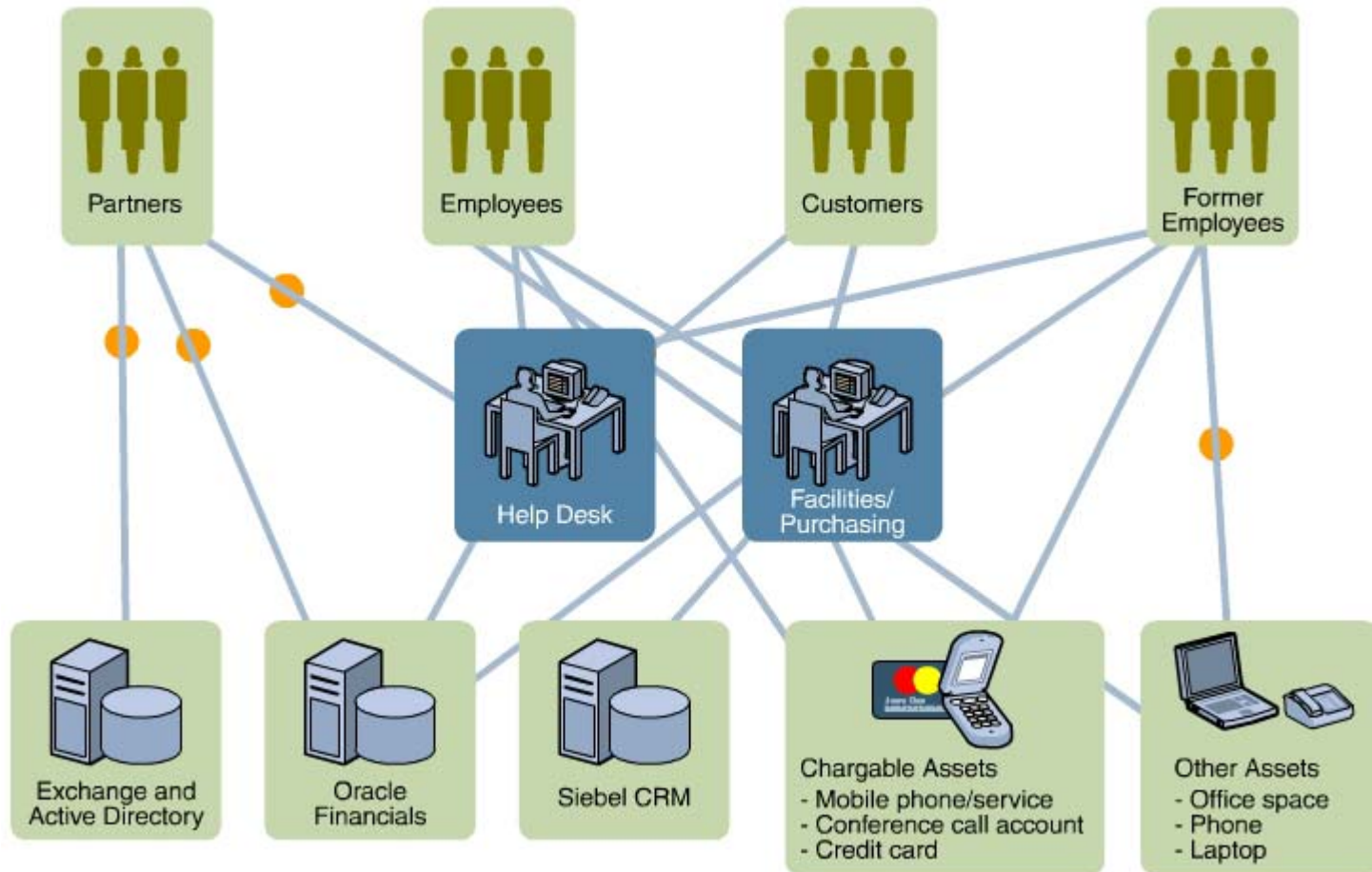
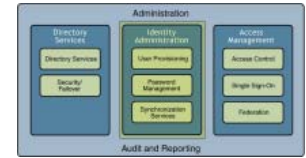
Identity Management Categories



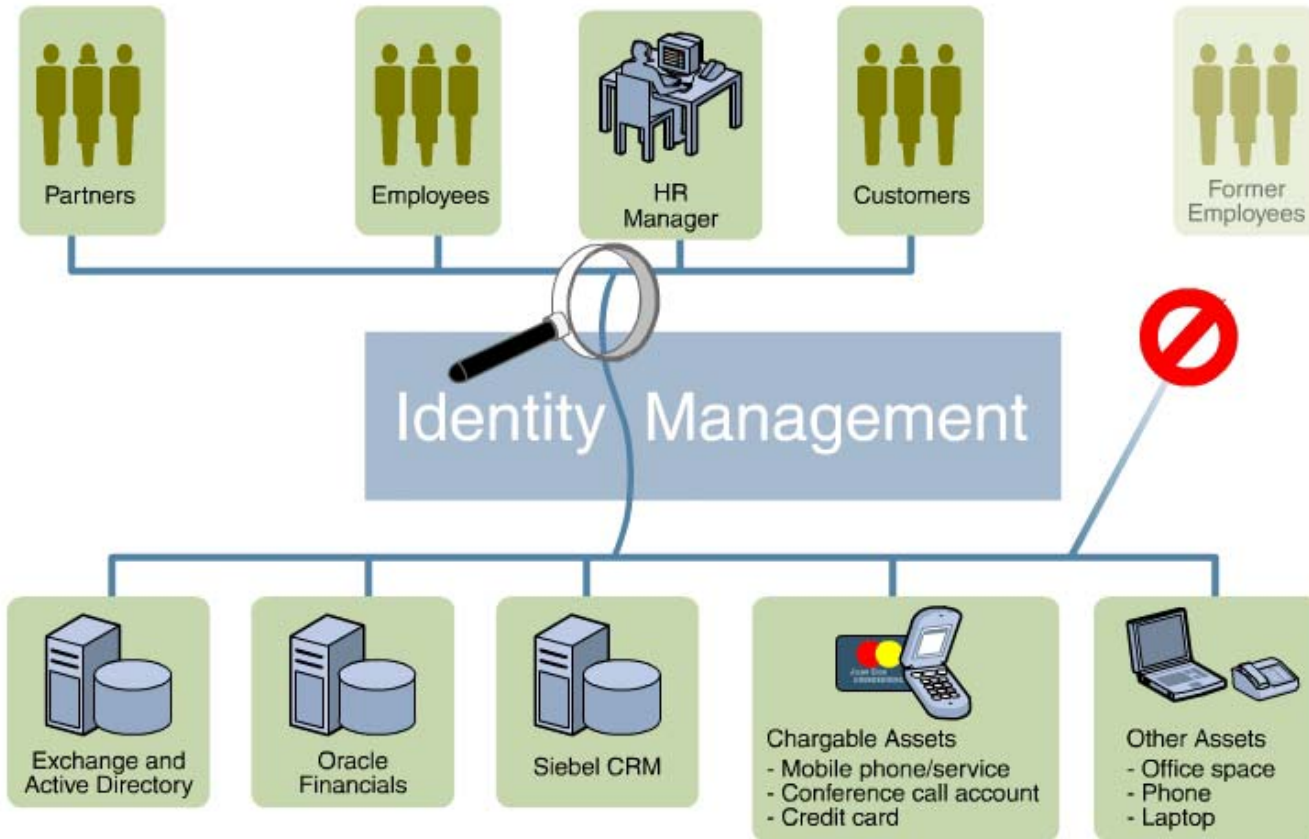
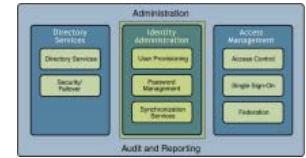
Identity Management focus areas:

1. Data Synchronization
2. Account Management
3. Password Management (self-service)
4. Single Sign-On
5. Attestation and Non-repudiation

Typical Identity Provisioning

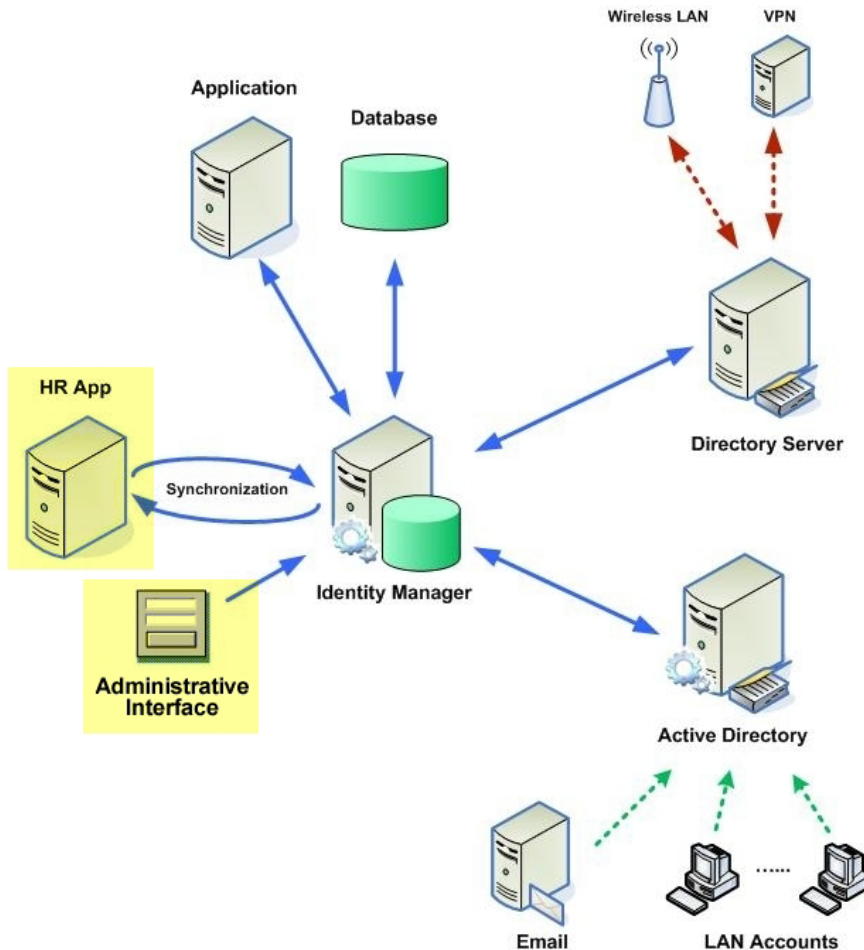
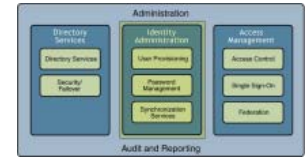


Streamlined Identity Provisioning



Complete view of identity information

Account Management

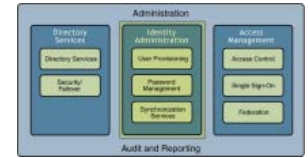


1. Automatic account updates
 - Synchronization with HR
 - Role-based provisioning
 - Support for Sunrise/Sunset

2. Manual account updates
 - Delegated administration
 - Immediate account lockout
 - Password Resets
 - User data modifications

3. Process can involve:
 - Approvals
 - Notifications

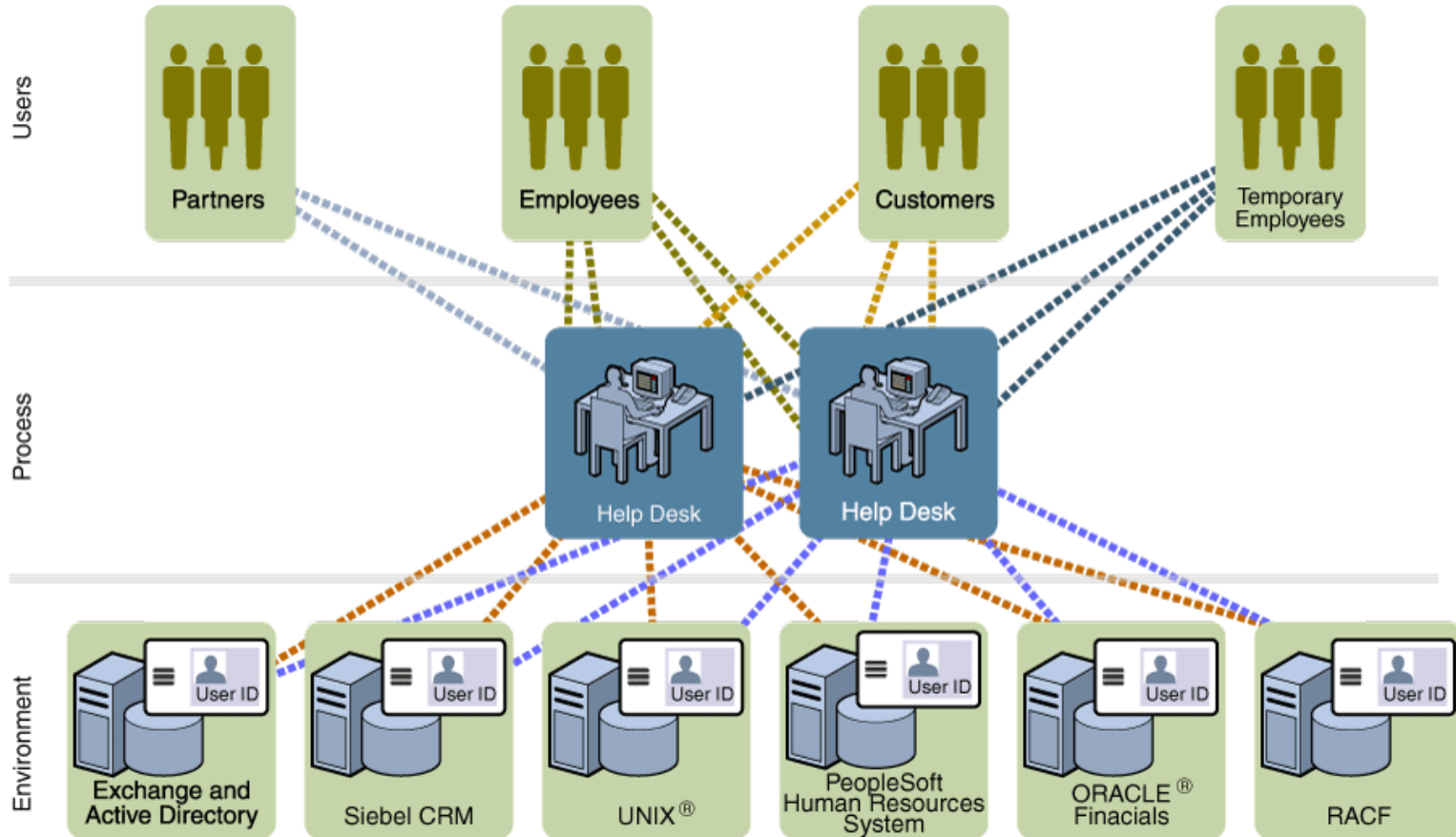
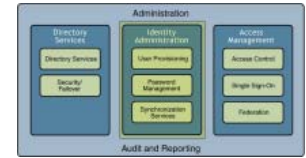
Identity Management Categories



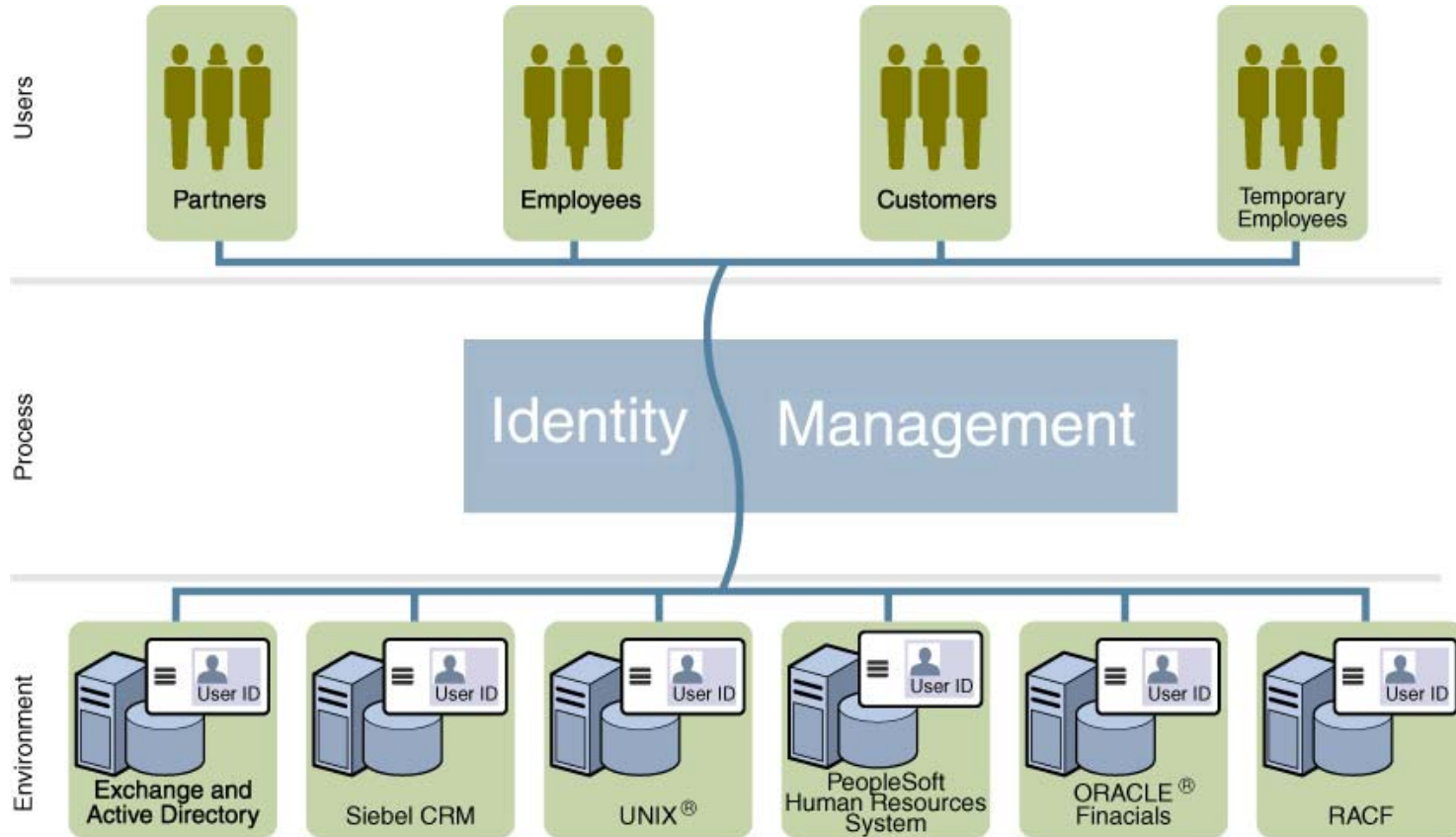
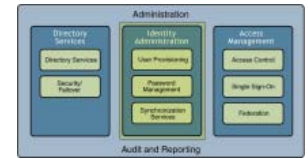
Identity Management focus areas:

1. Data Synchronization
2. Account Management
3. Password Management (self-service)
4. Single Sign-On
5. Attestation and Non-repudiation

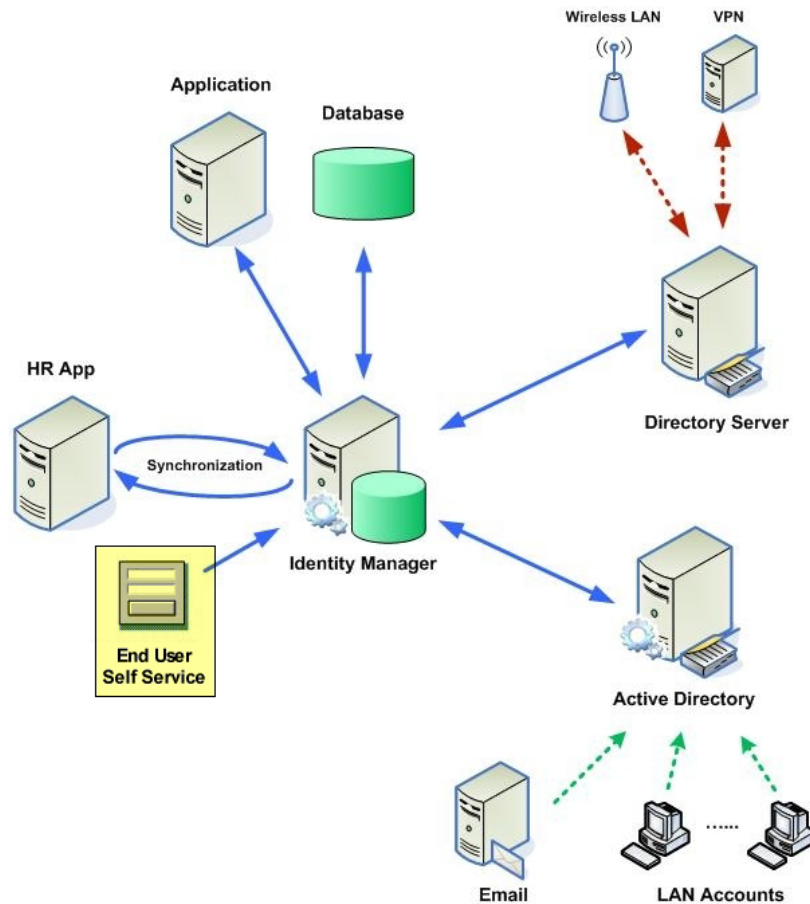
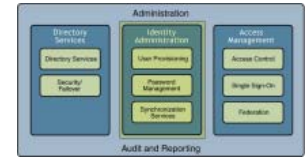
Typical Password Mgmt



Streamlined Password Mgmt

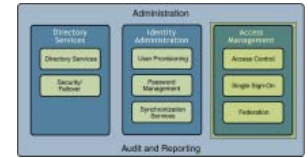


End-User Self-Service



1. Users access a web interface
 - Answers to Auth Questions
 - Password Changes
 - Personal Data Changes
 - Request Access to Resources
2. Data is synchronized:
 - Upstream (HR; maybe)
 - Downstream (Resources)
3. Process can involve:
 - Approvals
 - Notifications

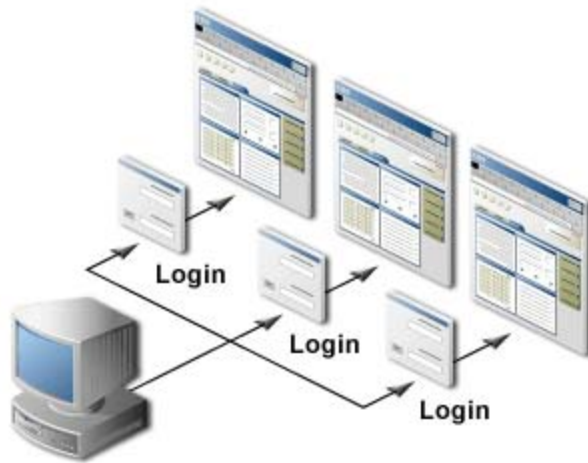
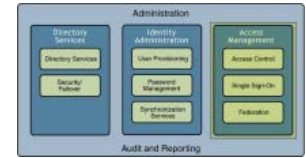
Identity Management Categories



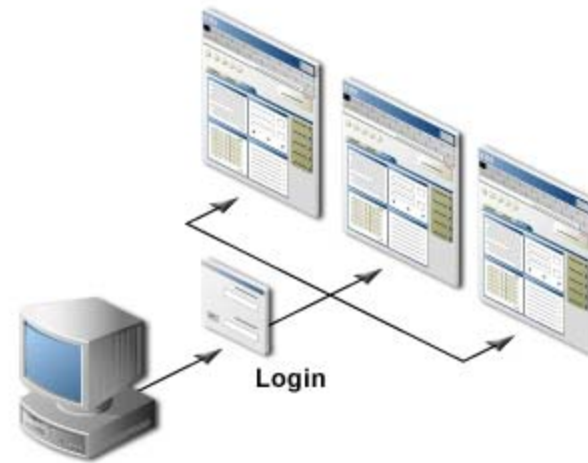
Identity Management focus areas:

1. Data Synchronization
2. Account Management
3. Password Management (self-service)
4. Single Sign-On
5. Attestation and Non-repudiation

Enterprise Single Sign On

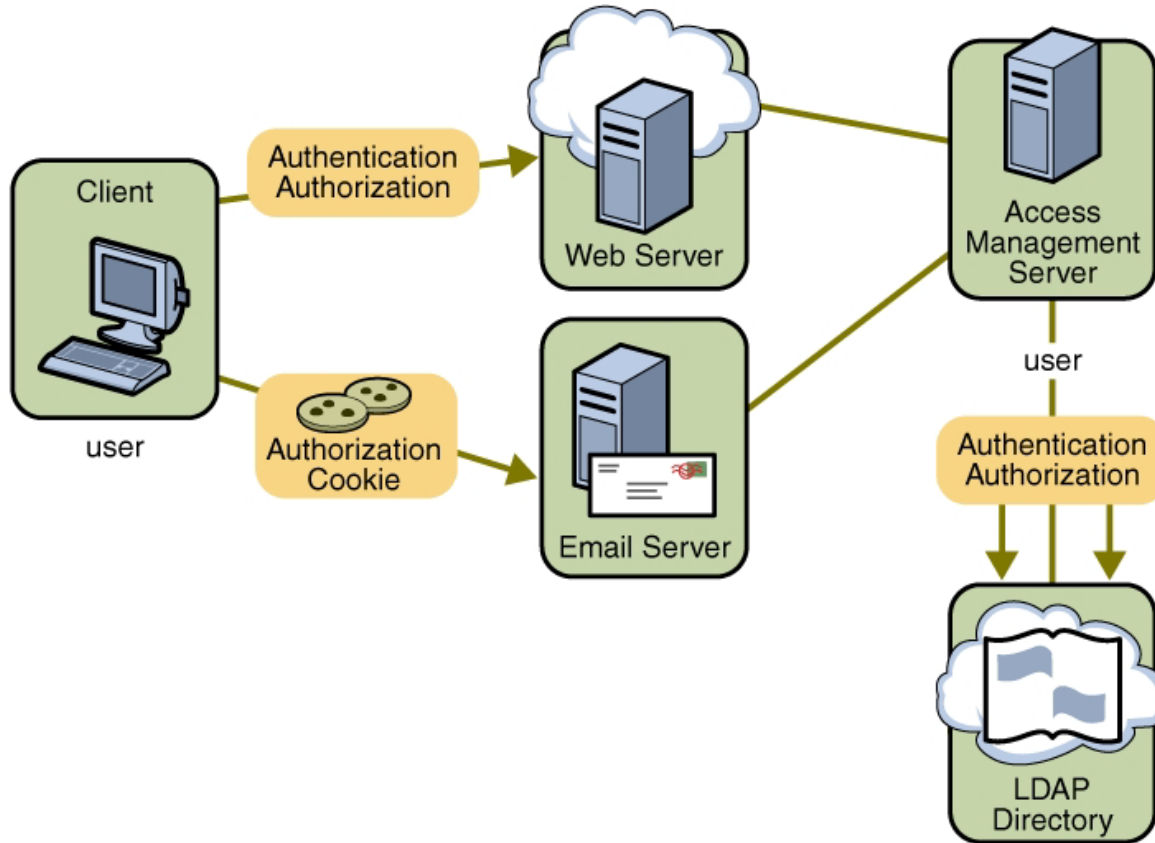
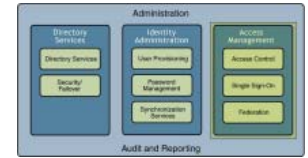


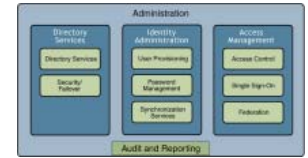
- User logs into Windows desktop
- User logs into each subsequent application
- User must keep track of multiple IDs and passwords



- User logs into Windows desktop
- Software on the desktop intercepts login requests
- Windows password acts as SSO to other applications
- Users do not need to know IDs and passwords
- Users can add their own applications (if allowed)
- Credentials are stored/cached encrypted
 - centralized database
 - desktop/laptop

Web Single Sign On

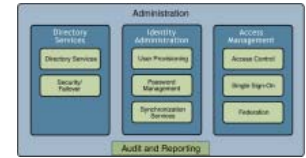




Identity Management focus areas:

1. Data Synchronization
2. Account Management
3. Password Management (self-service)
4. Single Sign-On
5. Attestation and Non-repudiation

Audit and Attestation



SECURITIES ACT OF 1933 SECURITIES AND EXCHANGE ACT OF 1934

TITLE III CORPORATE RESPONSIBILITIES

Sec. 301 Public Company Audit Committees

All organizations governed by SEC regulations are required to establish and maintain an audit committee that shall be responsible for the appointment, compensation and oversight of any registered public accounting firm employed by that issuer. The accounting firm shall report directly to the audit committee. All audit committee members shall be members of the organization's board of directors but shall be otherwise independent. They may therefore not be an affiliated person of the organization or an associated company, nor may they accept consulting, advisory or other compensatory fees other than in their capacity as audit committee members.

The audit committee shall establish procedures regarding the handling of complaints relating to accounting, controls, or auditing matters. They must also develop procedures for the confidential, anonymous submissions by the organization's employees concerning questionable accounting or auditing practices.

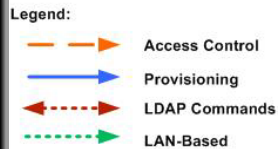
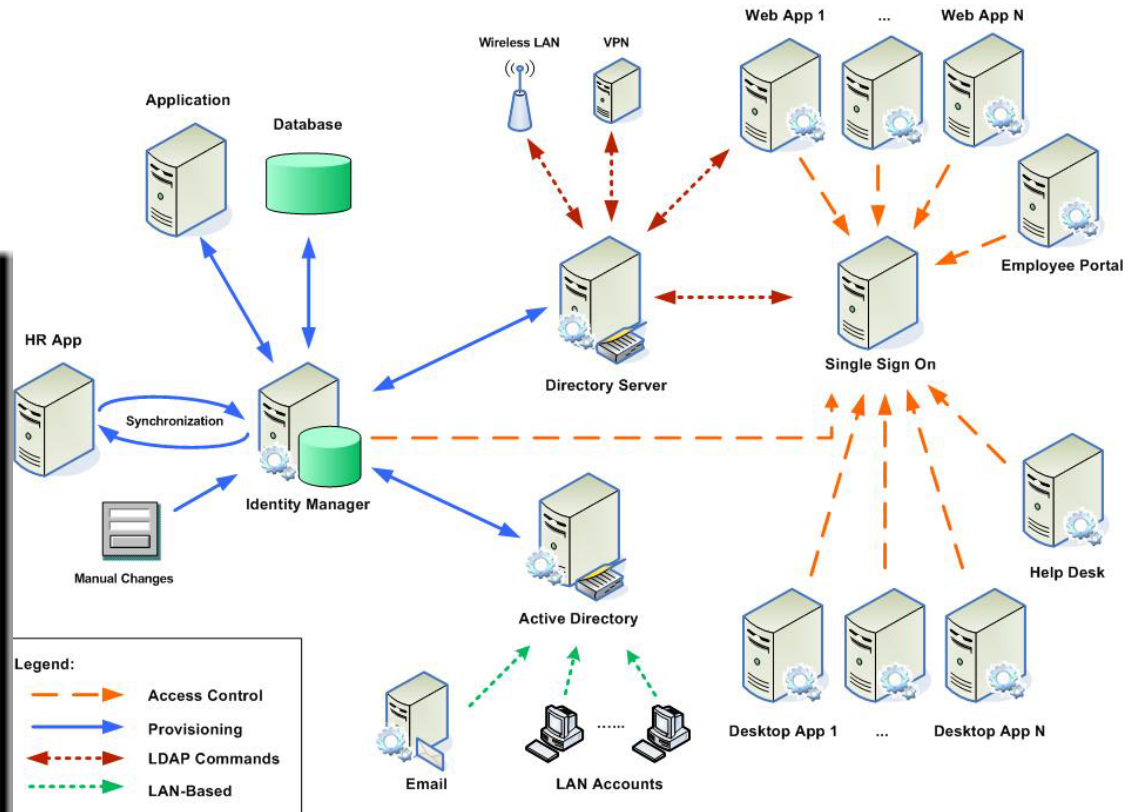
Audit committee shall be able to appoint advisors as considered necessary and to receive adequate funding for the organization for such purposes.

Sec. 302 Corporate Responsibility for Financial Reports

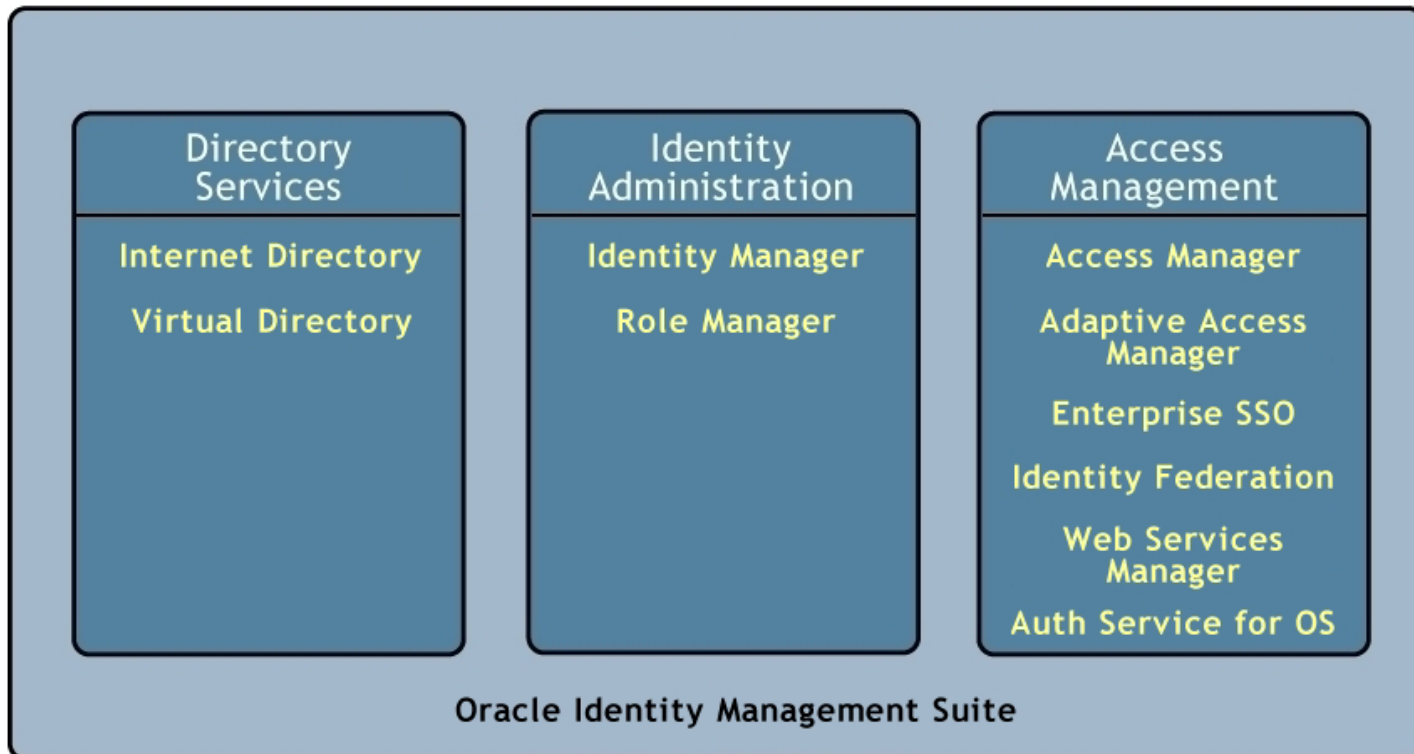
Periodic statutory financial reports are to include certifications that:

- The signing officers have reviewed the report
- The report does not contain any material untrue statements or material omission or be considered misleading
- The financial statements and related information fairly present the financial condition and the results in all material respects
- The signing officers are responsible for internal controls and have evaluated these internal controls within the previous ninety days and have reported on their findings
- A list of all deficiencies in the internal controls and information on any fraud that involves employees who are involved with internal activities
- Any significant changes in internal controls or related factors that could have a negative impact on the internal controls

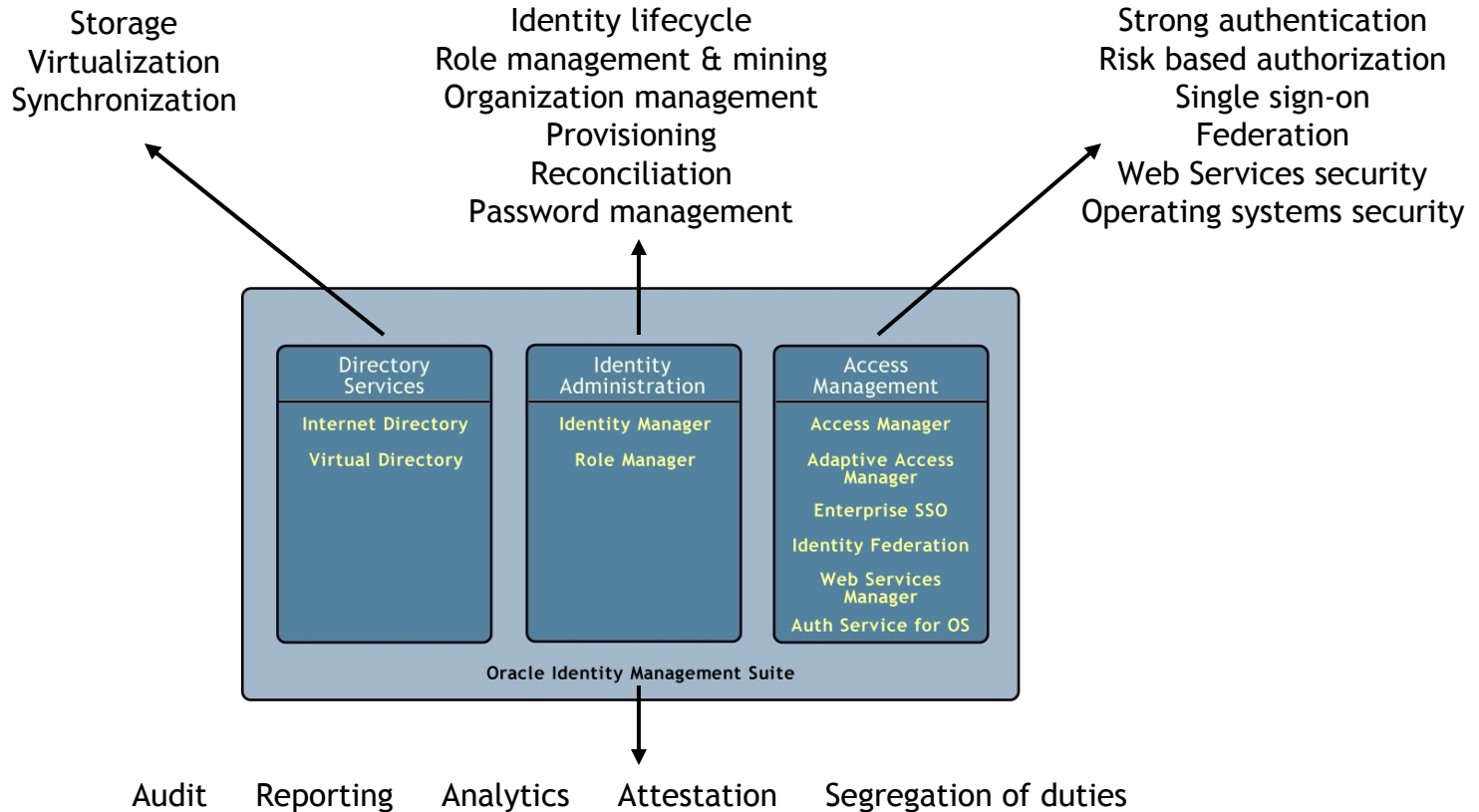
Organizations may not attempt to avoid these requirements by reincorporating their activities or transferring their activities outside of the United States



Oracle Identity Management Suite



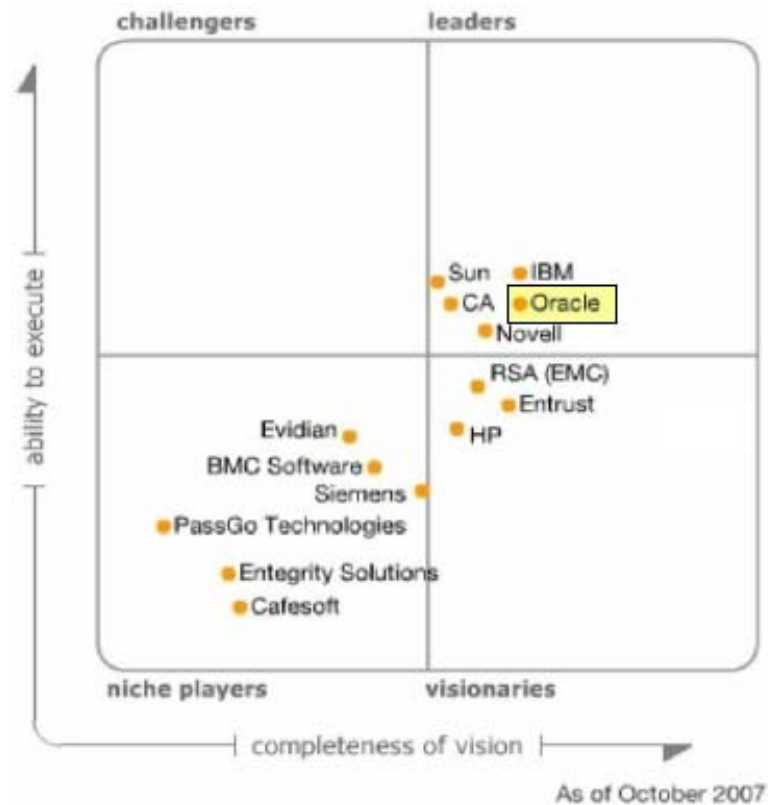
Oracle Identity Management Suite



Gartner Says: Leader in Magic Quadrants

User Provisioning H2, 2007

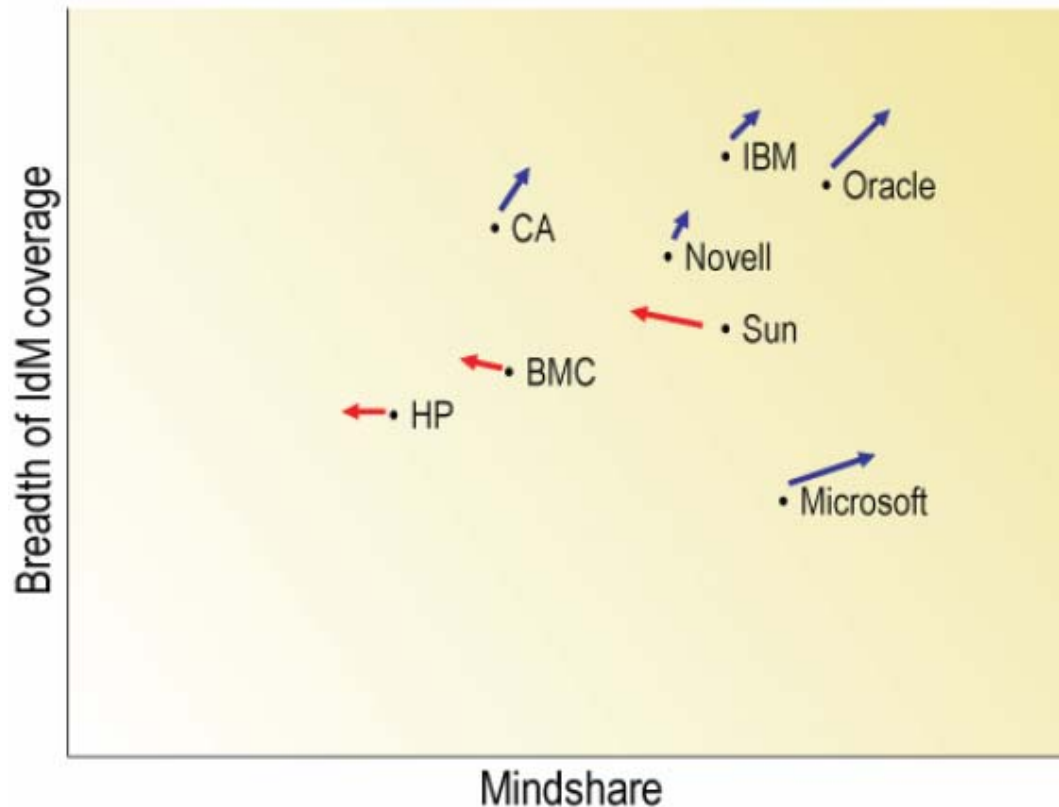
Web Access Mgmt H2, 2007



Burton Group Says: Strongest Vendor

“Oracle is currently the IdM vendor to beat”

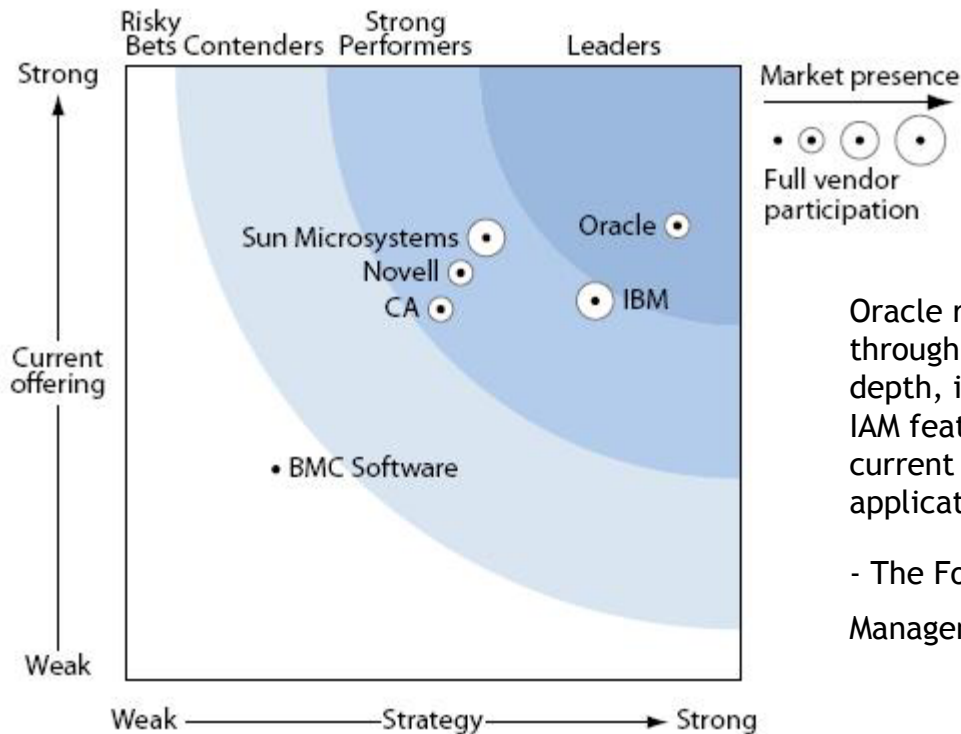
- VantagePoint 2007: Identity and Privacy Trends in Enterprise IT



Forrester Says: Market Leader

“Oracle has established itself as Leader.”

- The Forrester Wave: Identity And Access Management, Q1 2008



Oracle reached the top of our evaluation through a combination of the breadth, depth, interoperability, and packaging of its IAM features alongside the strategy and current state of market execution on its application-centric identity vision.

- The Forrester Wave: Identity And Access Management, Q1 2008

Oracle Identity Management Customers

Financial Services



Transportation & Services



Manufacturing & Technology



Telecommunication



Public Sector



Retail



Key Differentiators

- ✓ **Complete suite of best-of-breed products**
 - Complete & best integrated identity management suite
 - Includes compliance, virtualization and system mgmt
 - Market leadership validated by press and analysts
- ✓ **Proven for large scale deployments**
 - Large, complex, and award winning deployments
 - Broad customer base and use cases
 - Large referenceable customer base
- ✓ **Best long-term investment**
 - Strong support of open standards and hot-pluggable strategy
 - Pre-integrated with leading applications and infrastructure

Questions?



Identity Management Overview

Bill Nelson

bill.nelson@gca.net

Vice President of Professional Services



Technology Services
Software. Training. Consulting.