

ORACLE®

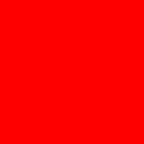


ORACLE®



Identity Management for Oracle Applications Including Oracle E-Business Suite, PeopleSoft, and Siebel

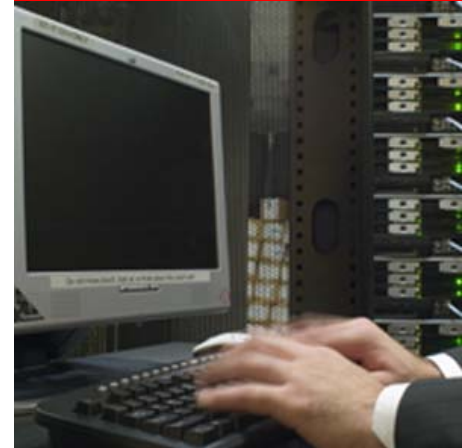
Manh-Kiet Yap – Senior Principal Product Manager
Oracle Fusion Middleware – Oracle Corporation



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

Program Agenda

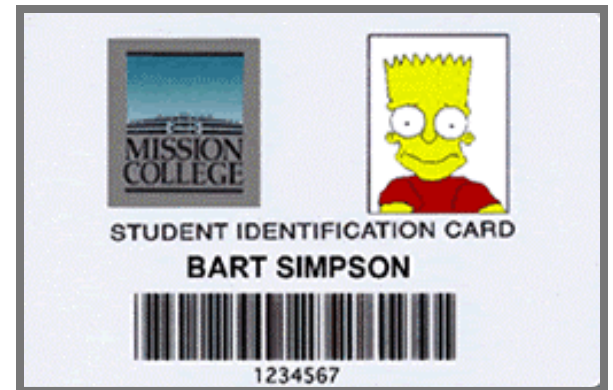
- Issues and Challenges
- Best Practices
- Identity Management Solutions
 - Features and Offerings
- Customer Case Study: Silicon Image
- The Future of Identity Management
- Q&A



Application Management Reality Quiz



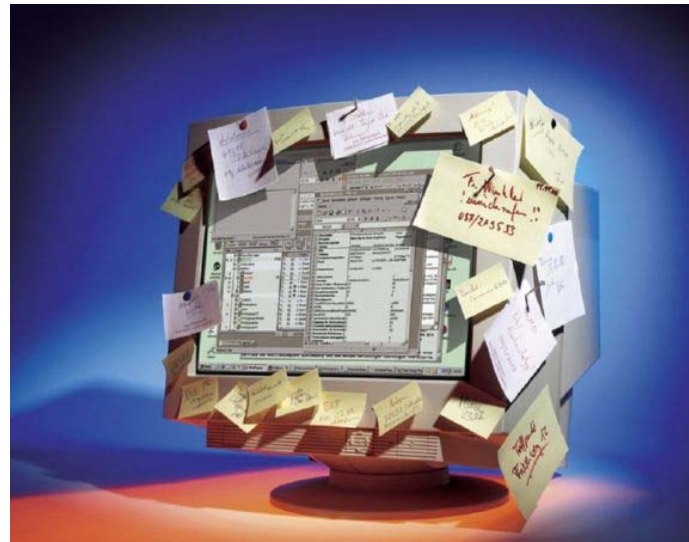
Q: Who is the most privileged application user in your enterprise?



- (A) CFO
- (B) app security administrator
- (C) the 3-peat summer intern who is now working for your competitor

Q: What's posted on this monitor?

- (A) passwords to financial applications
- (B) phone messages
- (C) to-do's



Q: When does a new employee have access to all necessary application functions?



- (A) 1 week after start
- (B) how proactive is the employee?
- (C) when he shows up for work

Q: What determines your employee's application ac



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

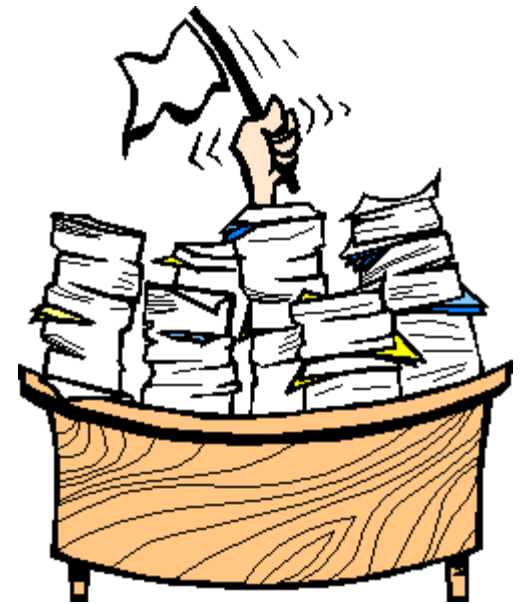
- (A) give Alice whatever Wally has
- (B) roles, attributes, and requests
- (C) whatever her manager says



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

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

- (A) nothing, no new headcount
- (B) don't ask
- (C) don't know



Reality Check: Issues and Challenges



Issues and Challenges

- Low quality identity data
 - Lack of single source of truth for identity
 - Lack of mapping amongst application accounts
 - Lack of mapping between application accounts and HR records
- Inefficient and scattered administrative processes
 - Manual user on-boarding processes across different applications
 - Lack of centralized self-service processes
 - Multiple workflows, policies and rules across applications
 - Inconsistent delegated administration across applications

Issues and Challenges (continued)

- Poor and inconsistent security
 - Too many and unsecured passwords
 - Excessive and outdated access privileges
 - Inconsistent authentication and authorization across applications
- Incomplete and crude audit and compliance framework
 - Lack of comprehensive historical data
 - Manual attestation process lacks data and process integrity
 - Lack of control for segregation of duties
- Non-scalable integration framework
 - Custom hard-wired point-to-point integrations
 - Not leveraging industry standards such as SPML and SAML
 - Expensive deployment and upgrade of integrations

Application Specific Challenges

- Oracle eBusiness Suite
 - Multiple user management modules
 - CRM user management and UMX
 - Role management support is UMX only
- PeopleSoft
 - No provisioning or role management support
 - Multiple integration interfaces
 - Component Interface, Integration Broker / Application Messaging
 - PDI is for synchronization from PSFT HRMS to LDAP only
- Siebel
 - No provisioning or role management support, relies on 3r party tools
 - No directory integration tools
- SAP
 - Mixture of CUA and non-CUA managed servers
 - Mixture of Basis, WAS, end HR repositories
 - CUA cannot synchronize password among parent-child servers
 - Mixed APAB and Java architectures

How Should Applications Be Managed?



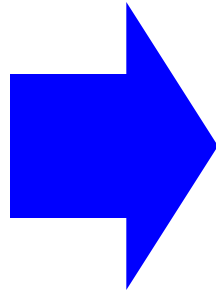
Best Practices

Rule #1: Establish enterprise identity

- Consolidation of complex identity environment with multiple repositories
- Automatic linkage of employee records with user accounts
- Eliminate rogue and orphaned accounts



Best Practices



Rule #2: Define framework and control of access levels

- Enforce strong password policies via synchronization or SSO
- Enforce minimal access rights based on roles, attributes, and requests

Best Practices

Rule #3: Automate security related processes

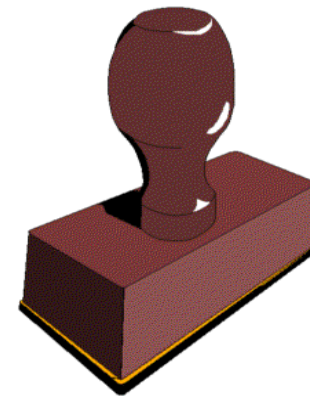
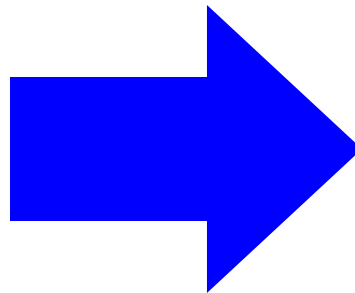
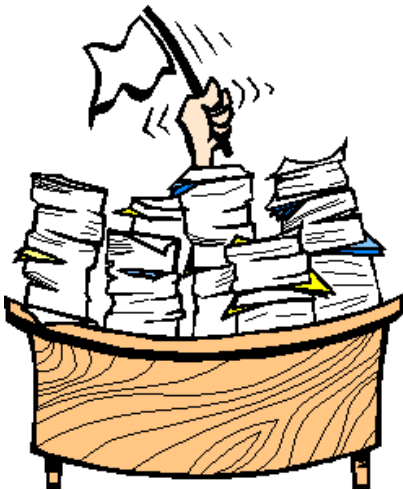
- Approval workflow for self service request
- Role and attribute driven provisioning workflow to automate orchestration of IT tasks



Best Practices

Rule #4: Define audit and control framework

- Change management process of workflows, policies and rules
- Attestation of entitlements, roles, policies, workflows....
- Exception based process automation
- Segregation of duties around roles and entitlements

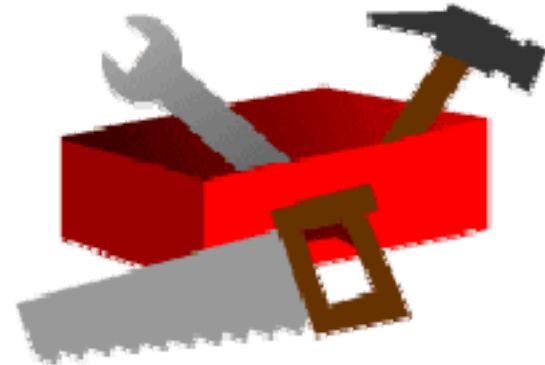


APPROVED

Best Practices

Rule #5: Deploy a scalable and flexible integration architecture

- Define an enterprise standard integration standard
- Leverage all integrations through a single interface / application
- Heavily leverage open standards

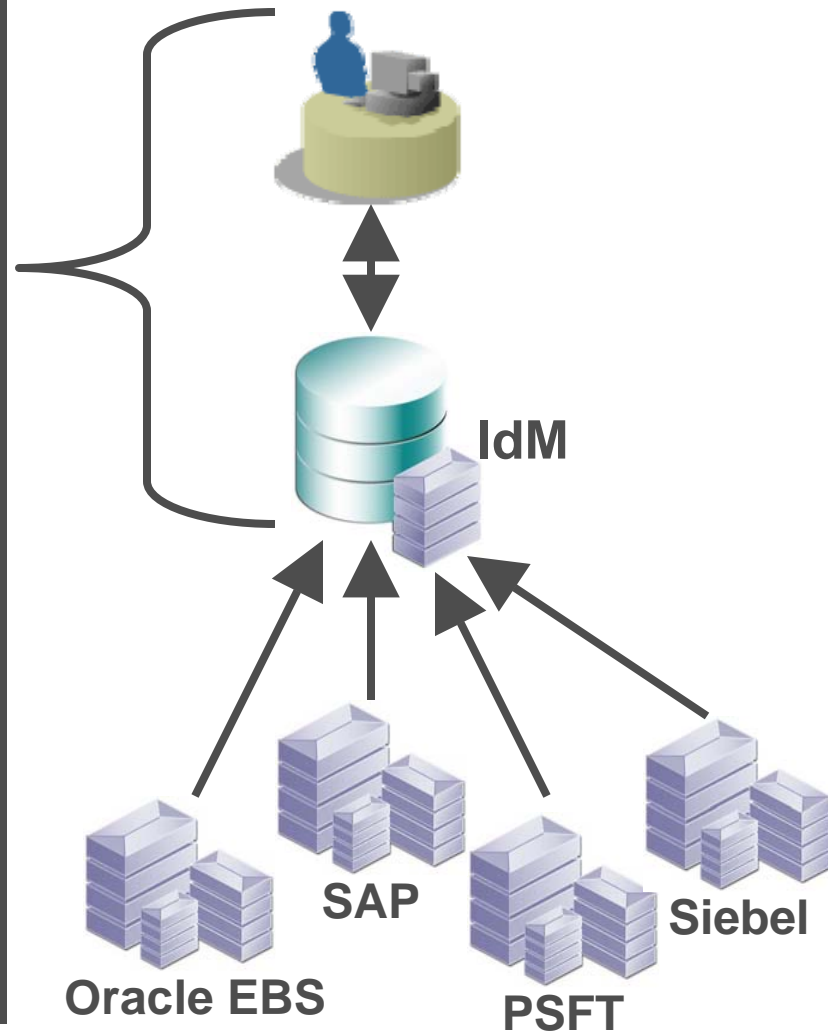


How Can Identity Management Help?



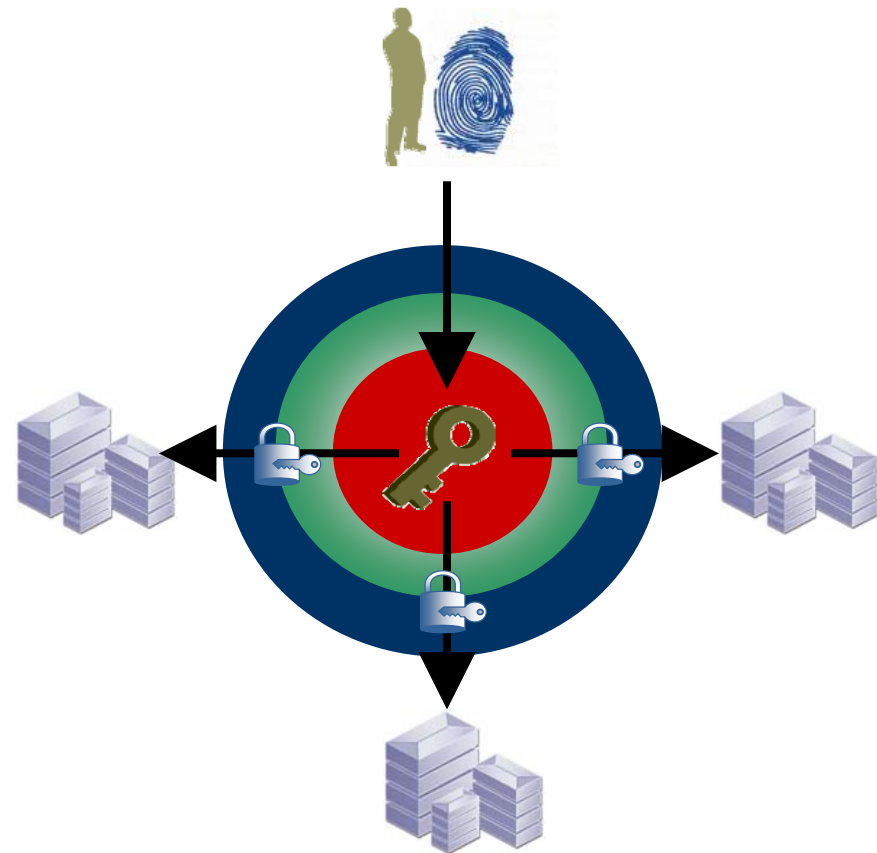
Centralized User and Role Mgmt

- Centralized user data management
 - Bi-directional user management: provisioning and reconciliation
 - Trusted source reconciliation by target and by user type
 - Dynamic linking of employee, customer and vendor records to user records
- Centralized and delegated administration
- Rule, policy and workflow management
- Role and profile management



Improved Usability and Security

- Customizable administration and applications user interface
- Centralized self-services
 - Registration
 - Resource request
 - Password reset
- Single-Sign On
- Federated sign-on
- Strong authentication and authorization



Audit & Compliance Management

Lockdown Systems/Processes

- Policy based access control
- Role & attribute driven policies
- Request and approval process
- Segregation of duties

Control Access Points

- Authentication and authorization authority
- Strong / multi-factor authentication
- Entry and session logging

Manage Exceptions

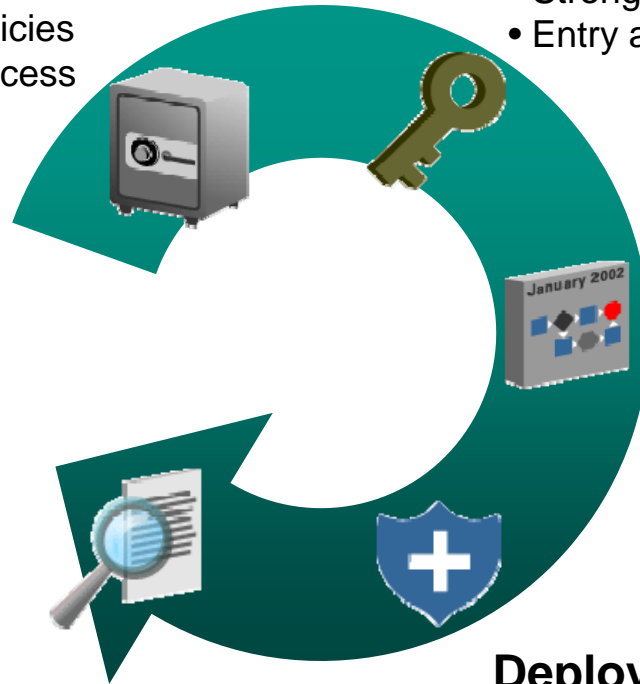
- Rogue account discovery
- Exception based automation
- Alert and event management

Validate Controls

- Attestation of controls
- Policy synchronization
- Gap and what-if analysis

Deploy Safety Mechanisms

- Attestation of entitlements & access log
- Redundant controls
- Trending and activity level monitoring



OIM Integration Offerings

Features

- Agent-less integration framework
- Application-centric and technology-centric OOTB connectors
- Abstraction of functional layers
- Componentized architecture
- N-tier J2EE architecture
- Deploys on wide range of J2EE application + DB servers
- Highly customizable and extensible

Oracle Applications

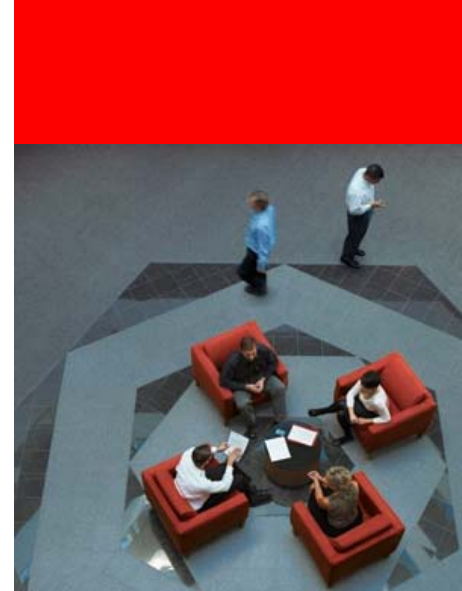
- Oracle e-Business Suite
- PeopleSoft
- Siebel
- JD Edwards (Dec 2006)
- Telecom/Portal (2007)
- Oracle Retail (2007)
- Oracle Clinical Solutions (2007)
- PeopleSoft Campus (2007)

SAP & Other Applications

- SAP R/3, Basis, CUA
- SAP HRMS
- SAP Certification (2007)
- Sungard Banner (2007)
- Lawson (2007)
- QAD (2007)
- other tier-2 applications

Customer Case Study: Silicon Image

Managing Oracle e-Business Applications using Oracle Identity Manager



About Silicon Image

- Fabless Semiconductor based in Sunnyvale, CA.
- 400+ employees + contingents
- Analyst estimate of \$285 million revenue for 2006
- Oracle Application Live May 2003
- Current release 11.5.10 modules include:
 - Finance, Manufacturing, Distribution, HR, iStore, iSupport, Service Contracts, Quality
 - Self-service (iProcurement, iExpense and HR Manager)
 - Tools (Alerts, Workflow, OAM, Discoverer, BEPL, Portal, ADI , UPK and OID)

Business Challenge

- Lack of consistent password policy across key applications
- Lack of automated processes & workflow management to support on-boarding and off-boarding employees
- Lack of a centralized data repository for single source of identity information
- Consistent, orderly and timely provisioning of key accounts for SOX auditing
- Too many user names and passwords to multiple systems led to endless helpdesk tickets for forgotten passwords or locked accounts
- Multiple processes for on-boarding and off-boarding employees, temps and contractors

Before Identity Management

Before Oracle Identity Manager



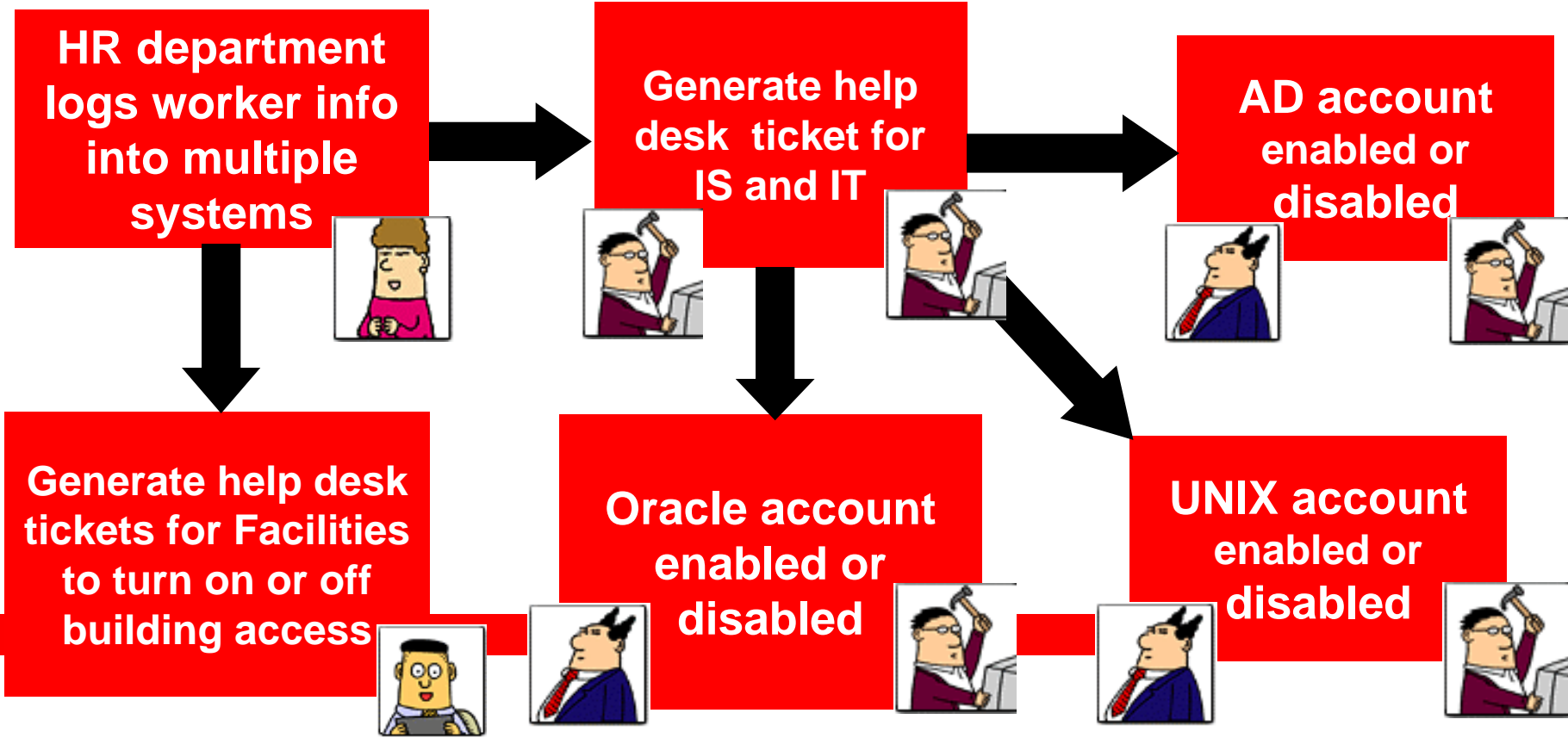
HR Rep.



IT Dude



Approving Manager



Why Oracle?

Why we selected Oracle Identity Manager over other vendors in the Market?

- Solution covered all of our current needs.
- Road map that includes customer opinions
- Support and maintenance is with one single vendor
- Out-of-the-box integration with Oracle applications
- Leverage existing investments
- Flexible architecture

Solution

- Oracle Identity Manager - User provisioning
 - Data Feed from Oracle HR
 - Master Identity Store IdM
 - Target systems
 - UNIX LDAP (SunOne)
 - AD
 - Oracle Applications
 - Single password policy
 - Auditors have one password policy to audit
 - Users have one password policy bringing elimination of the sticky note.

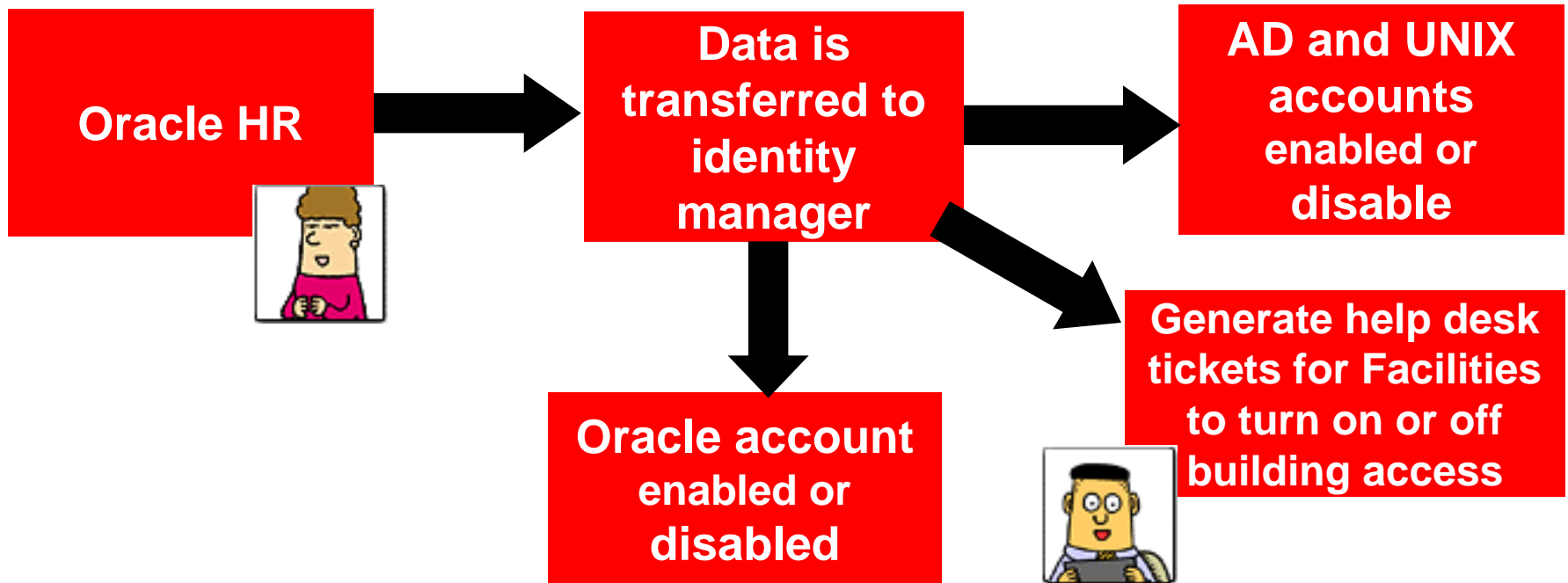
Solution (Continued)

- Provisioned resources include
 - Computer systems
 - Outlook distribution lists
 - Mobile phone
 - New placement and extensions of contingent workers
 - Oracle responsibilities
 - Non Standard Unix Groups
 - Management Portal
 - SonicWall
 - ActivCard
 - Network directory

After Identity Management

After Oracle Identity Manager

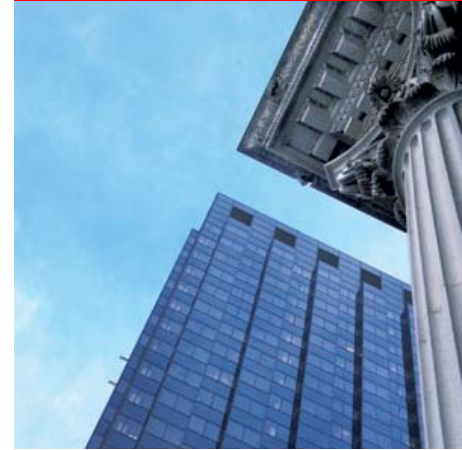
- HR has one system to work with and no longer has to create multiple helpdesk tickets
- IT get requests that have been pre-approved by the BPO recorded in the workflow
- SOX auditors are happy because controls are very tight and de-provisioning is fast.



Lessons Learned

- Don't take the same old process and try to make it work in the new tool without first evaluating best business practice.
- Way too many flavors of UNIX
- Make sure you set up error monitoring processes for all events
- Involve internal SOX audit in design meetings
- Understand the skill set required for administrator.

The Future of Application Management



Enterprise Apps IdM Evolution



Pre-UMX
Oracle
e-Business
Suite



Oracle
e-Business
Suite + UMX



Enterprise
Apps + OIM



Fusion:
Application-
Centric IdM

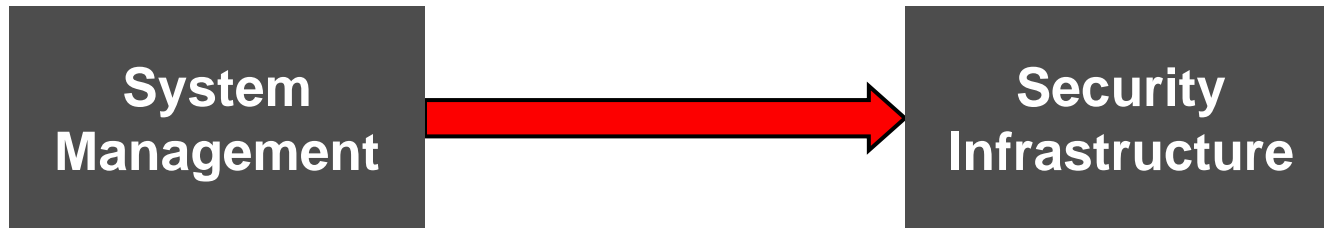
No
Identity
Mgmt

App-
Specific
IdM

Enterprise
IdM

IdM As
Infrastructure

Application-Centric Identity Management



Extraction of IdM services as “utilities”

- Separation of IdM infrastructure and administration
- Separation of security-related policy administration
- Standardize & commercialize IdM functions
- Abstraction and virtualization of IdM repository management

For More IdM Information

- Oracle Technology Network:
http://www.oracle.com/technology/products/id_mgmt/index.html
- Oracle.com:
<http://www.oracle.com/products/middleware/identity-management/identity-management.html>

For More Information

<http://search.oracle.com>



or

<http://www.oracle.com/>



ORA



ORACLE IS THE INFORMATION COMPANY