Agenda

What is Identity and Access Management (IAM)?

Business Drivers and Challenges

Compliance and Business Benefits

IAM Solution Framework

IAM Implementation
What is Identity and Access Management (IAM)?

IAM: the set of business processes, information, and technology for managing and using digital identities

### Business Processes
- User and Role Life Cycle Management
- IAM Organization, Roles and Responsibilities

### Information
- Risk Management Policies, Controls
- Digital IDs, Data Flow, and Reporting

### Technology
- Administration and Audit tools
- Provisioning, Access Management, Identity Integration, and Identity Repository
User and Role Life Cycle Management

- Identity is created as the first step of on-boarding employees, contractors, or business partners
- Identity is created in Authoritative Sources such as SAP HR

Request

- User accounts are set up for each of the resources that user will access
- Initial access permissions and rules are configured on each resource

Provision

- User Life Cycle Management:
  - Access Request
  - Promotion/Transfer
  - Status change
  - Password reset
  - Approvals
- Role Life Cycle Management
  - Role Approval
  - Role Assignment
- Access Management
  - User Authentication
  - User Authorization
- Audit
  - User Access Review
  - User Access Recertification
  - Approver Actions
  - Administrator Actions

Control

- User's Digital ID

Update Personal Web Parts

- Limited Access
- Add/Remove Personal Web Parts
- Read
- Manage Personal Views
- Contribute
- Delete Versions
- Full Control
- Approve Items
- Design
- Cancel Checkout
- View Versions
- View Items
- Open Items
- Delete Items
- New in Window
- SharePoint Services (version 3)?

No, No, No, New, New, New, No, New, No, No, No

Relationship begins

Relationship ends

- Removing user access permissions from all managed resources
- Scheduled User Termination
- Unscheduled User Termination
- Archive user identity

Copyright © 2007 Deloitte Development LLC. All rights reserved.
Administration Process Perspective

Across an enterprise, user and role life cycle management processes can vary by business unit, by user type, and by managed resource, resulting in **complexity** and **cost**.
Application-Specific IAM

Security and Controls are re-invented on a per-application basis, resulting in administration silos, one-off user life cycle management processes and high ongoing administration costs.
Agenda

What is Identity and Access Management (IAM)?

Business Drivers and Challenges

Compliance and Business Benefits

IAM Solution Framework

IAM Implementation
# IAM Business Drivers

<table>
<thead>
<tr>
<th>Business Facilitation</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Improve User Experience</td>
<td>• Regulatory</td>
</tr>
<tr>
<td>• Enable Collaboration with Business Partners</td>
<td>• Audit Management</td>
</tr>
<tr>
<td>• Time-to-Market</td>
<td>• Protection of Personally Identifiable Information (PII)</td>
</tr>
<tr>
<td>• Post-M&amp;A Integration</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cost Control</th>
<th>Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reduce Time-to-Productivity</td>
<td>• Enforce Enterprise Risk Management policies</td>
</tr>
<tr>
<td>• Reduce On-Going User Administration Costs</td>
<td></td>
</tr>
<tr>
<td>• Security administration</td>
<td>• Manage User Access Privileges</td>
</tr>
<tr>
<td>• Help desk</td>
<td>• Timely revocation of inactive accounts</td>
</tr>
<tr>
<td>• Standardize IAM Infrastructure</td>
<td>• Strong authentication to protect sensitive digital assets</td>
</tr>
<tr>
<td>• Contain Development Costs</td>
<td></td>
</tr>
</tbody>
</table>
## 1. Compliance

### Business Drivers

<table>
<thead>
<tr>
<th>Business Drivers</th>
<th>Description</th>
</tr>
</thead>
</table>
| • Regulatory Compliance | • Management must report on internal controls within the enterprise  
  – Sarbanes-Oxley Act  
  – Payment Card Industry Data Security Standard (PCI DSS)  
  – U.S. Gramm-Leach-Bliley Act (GLBA)  
  – Breach notification laws (CA SB1386)  
  – EU Data Protection Directive  
  – Industry-specific mandates (HIPPA, FFIEC, NERC, and others.) | • Provide evidence that controls over user accounts and access privileges function as intended  
  – Preventive, detective, and monitoring controls  
  – Issue remediation  
• Protect Personally Identifiable Information (PII) such as customer data from unauthorized disclosure or modification |
| • Audit Management | • Review user identities, job functions, and access privileges  
  – Address audit issues  
  – Perform periodic user access reviews  
  – Test control effectiveness | • Audit access requests, approvals, and administrative actions  
• Assign resource owners to review and recertify user access to enterprise information resources  
• Identify and remove user access not justified by job role/function |
## 2. Risk Management

<table>
<thead>
<tr>
<th>Risk Management Drivers</th>
<th>Description</th>
</tr>
</thead>
</table>
| • Enforce Enterprise Risk Management policies                | • Implement controls to manage risk of unauthorized access to business applications and systems  
|                                                              | • Reduce risk of revenue and reputation loss through failed or inadequate user ID management processes  
|                                                              | • Enforce enterprise control framework and risk management policies  
|                                                              |   – Implement access control policies in user administration and audit processes and IT resource security settings  |
| • Manage User Access Privileges                              | • Support controls for segregation of duties, limited powerful access, developer access to production, and related controls  
|                                                              | • Assign Business Owners for authorizing resource access  
|                                                              | • Manage access to information resources based on a user’s business relationship to the enterprise  
|                                                              | • Assign unique ID to each user, enforce password policies, remove inactive and duplicate accounts  |
| • Protect Sensitive Information Resources                    | • Support stronger authentication factors such as Kerberos, SecurID, smart cards, and digital certificates  |
## 3. Cost Control

<table>
<thead>
<tr>
<th>Cost Control Drivers</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reduce Administrative Costs</td>
<td>• Reduce user administration costs via process standardization and automation</td>
</tr>
<tr>
<td>– User administration</td>
<td>• Establish standard access request and approval processes across the enterprise</td>
</tr>
<tr>
<td>– Help Desk</td>
<td>• Provide delegated and self-service administration capabilities to reduce workloads on centralized resources</td>
</tr>
<tr>
<td>• Reduce Audit Costs</td>
<td>• Implement automated process and technical controls</td>
</tr>
<tr>
<td></td>
<td>• Automate labor-intensive manual audit processes</td>
</tr>
<tr>
<td></td>
<td>• Support collaboration between Business, IT, and Auditors</td>
</tr>
<tr>
<td>• Standardize IAM Infrastructure</td>
<td>• Leverage standard IAM platform for user lifecycle management activities</td>
</tr>
<tr>
<td></td>
<td>• Standardize IAM technologies via deployment of Commercial-Off-The-Shelf (COTS) IAM vendor products</td>
</tr>
<tr>
<td>• Contain Development Costs</td>
<td>• Leverage reusable IAM services in application development projects</td>
</tr>
<tr>
<td></td>
<td>– Reduce building redundant security and control logic into applications</td>
</tr>
</tbody>
</table>
# 4. Business Facilitation

<table>
<thead>
<tr>
<th>Business Facilitation Drivers</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Improve User Experience</td>
<td>• Improve employee, contractor, and business partner productivity by creating accounts by first day of work</td>
</tr>
<tr>
<td></td>
<td>• Reduce the time required for user provisioning to specific applications/systems (access controls for applications, database, OS)</td>
</tr>
<tr>
<td></td>
<td>• Improve collaboration between Business and IT for user access requests, approvals, provisioning and access reviews:</td>
</tr>
<tr>
<td></td>
<td>–Self-service request capabilities</td>
</tr>
<tr>
<td></td>
<td>–Understandable resource descriptions for business users not familiar with IT terminology</td>
</tr>
<tr>
<td>• Enable Collaboration with Business Partners</td>
<td>• Support business growth in a competitive market</td>
</tr>
<tr>
<td></td>
<td>• Integrate business processes and applications</td>
</tr>
<tr>
<td></td>
<td>• Scale services in line with business growth</td>
</tr>
<tr>
<td>• Reduce Time-to-Market</td>
<td>• Accelerate delivery of new business applications, functionality, and services</td>
</tr>
<tr>
<td></td>
<td>• Reduce deployment costs for internal and external applications</td>
</tr>
</tbody>
</table>
Agenda

What is Identity and Access Management (IAM)?

Business Drivers and Challenges

Compliance and Business Benefits

IAM Solution Framework

IAM Implementation
Benefits of IAM Services

1. **Identification**: Improve registration process controls, management of user identity and associated account data
   - Employees, Contractors Business Partners, and Customers

2. **Authentication**: Efficient, policy-based management of user logon to enterprise application and system resources

3. **Authorization**: Rationalized process and technical controls over user access to information resources; Balancing compliance, risk management, cost, and business factors

4. **Administration**: Streamlined, standardized user administration processes, improving efficiency and reducing operations costs

5. **Audit**: Reduce the cost and effort required to demonstrate control effectiveness and maintain compliance
   - Facilitate business and IT collaboration through a common risk and compliance framework
Identity and Access Management solutions can address common audit points and issues such as:

1. Inadequate controls over requesting, authorizing and granting access to financial applications

2. No periodic review of users and user access rights

3. No formal process to ensure leavers accounts are disabled/deleted in a timely manner

4. For transfers or job changes, access permissions and authorizations in applications are not changed accordingly or access revoked

5. Audit reports are required for applications in order to provide appropriate controls for protecting customer data

6. Developers can promote code changes to production; highly privileged accounts not suspended
### “Pain Points” addressed by IAM Solutions

<table>
<thead>
<tr>
<th>Key “Pain Points”</th>
<th>IAM Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Administration Process</strong></td>
<td>• Standardized Request-Approval process reduces errors and rework</td>
</tr>
<tr>
<td>• Access Approvals</td>
<td>• Online reauthorization reports and automated “correction” of issues</td>
</tr>
<tr>
<td>• User Reauthorization</td>
<td>• Automated revocation of “leaver” IDs, based on HR data feeds and administration requests</td>
</tr>
<tr>
<td>• Controls for user transfer process</td>
<td>• Audit reporting of administrator actions</td>
</tr>
<tr>
<td>• Revocation of IDs for leavers</td>
<td></td>
</tr>
<tr>
<td><strong>Segregation of Duties and Limited Powerful Access</strong></td>
<td></td>
</tr>
<tr>
<td>• Users accumulate access over time, more than required for job function</td>
<td>• User access is “right-sized” as applications and platforms are integrated with IAM System</td>
</tr>
<tr>
<td>• IAM user management processes and audit reporting support sustained compliance</td>
<td></td>
</tr>
<tr>
<td><strong>Developer Access to Production</strong></td>
<td>• Bringing employee, contractor, business partner, and customers under management provides a view of “who has access to what”</td>
</tr>
<tr>
<td>• Developers have inappropriate access to production</td>
<td></td>
</tr>
</tbody>
</table>
## A Strategic, Enterprise Approach will Result in Significant Improvements

<table>
<thead>
<tr>
<th>Core IAM Components</th>
<th>Efficiency</th>
<th>Effectiveness</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Administration:</strong></td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Streamlined and standardized processes and technology; automated account updates (provisioning)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Periodic Access Review:</strong></td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Ability to discern data risk rating and perform only necessary reviews: refined access reports stated in business terms</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resource Owner and User Tracking:</strong></td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Defined owners and supervisors; processes implemented to keep data maintained</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Access Control:</strong></td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Defined user access requirements; Segregation of Duties (SOD) checks between applications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Authentication:</strong></td>
<td>++</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Password self service and automated password synchronization</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Marginal Gain  
* Moderate Gain  
* Significant Gain
Agenda

What is Identity and Access Management (IAM)?

Business Drivers and Challenges

Compliance and Business Benefits

IAM Solution Framework

IAM Implementation
Enterprise Control Framework & Policy

An IAM Solution enables process and technical controls to be applied across multiple business applications and systems.

IAM provides a Control Infrastructure that supports:

- Enterprise Control Framework
- Risk Management Policies and Standards
- Control Objectives
- Control Activities

**Control Infrastructure**

- Periodic Review of User Accounts
- Management Approval Process
- Separation of Functional Duties
- User Revalidation & Recertification
IAM Context

Core IAM activities include user access to business applications, as well as access requests and processing according to defined User and Role Life Cycle.
IAM Conceptual Model

Business users enter requests for creating, modifying, and revoking digital IDs, which are passed to IAM for processing and fulfillment. Managed resources may be integrated at process or technical levels.
User & Role Life Cycle Management

Processes for on-boarding, transfers, and off-boarding of employees, contractors third-party business partner users, and customers. Revalidation of user identities and recertification of their access to information resources is also addressed.
Agenda

What is Identity and Access Management (IAM)?

Business Drivers and Challenges

Compliance and Business Benefits

IAM Solution Framework

IAM Implementation
Conceptual Architecture

Authoritative Sources
- HR Source #1
- HR Source #1

Identity Integration

Managed Resources
- Windows 2003 AD/Exchange 2003
- Solaris
- AIX
- Enterprise Directory

Provisioning

Portal
- Administration UI
- Other Web Apps

Access Management

Business Logic

Client Web Browser

Request Response Feed

Provisioning

Feed
IAM Stakeholders

- End Users
- CXO
- Risk Management
- Human Resources
- Enterprise Architecture
- User Administration
- IT Audit
- Business Owners
- Application Owners
- Help Desk
- IT Operations
- Business Owners
The **business value** of an IAM Solution is directly proportional to the **number** of integrated applications and systems

- Business applications and systems have owners
- Owners must be convinced to integrate with IAM
- Convincing stakeholders requires tangible business benefits:
  - Business Executive Sponsors
  - IT Executive Sponsors
  - Business Owners
  - IT Custodians
IAM Solution Implementation

1. **Current State**
   - Complex and overlapping legacy user administration processes and tools
     - Per-application request and approval processes
   - Diverse user base (employees, non-employees)
   - Audit issues with current User Administration Process

2. **Goal State**
   - Manage risk of unauthorized access to information resources
   - Standard user administration and IT Audit processes, procedures, and technology platform
     - Approval and Recertification workflows
     - Consistent revocation of access when a user leaves
   - Reduced risk of regulatory non-compliance, revenue, and reputation loss through inadequate IAM processes
Need more visual tie-in with previous slides. For example, use process flow, represent the users
IAM Implementation Strategy

Establish a rhythm of delivery, focusing on highest-priority business challenges first, pushing additional functionality to the next Release

![Diagram showing IAM implementation strategy with program management, release 1 to 4, and corresponding IAM business challenges and functionalities over a project timeline.](image-url)
IAM Implementation Success Factors I

**Executive Sponsorship**
- IAM implementation projects cross organizational boundaries and require strong sponsorship to set direction and priorities
- Governance function with engaged stakeholders from management, business, Information Technology is challenging to establish, but vital for the long-term

**Business Focus**
- Achieve clarity on the business challenges being addressed by the IAM solution
- Identify business drivers - Compliance, Risk Management, Cost Control, Business Facilitation – based upon enterprise needs and determine priority with stakeholders

**Change Leadership**
- Obtaining organizational buy-in for moving from application-specific to enterprise identity and access management is an exercise in diplomacy
- IAM Implementations are about people and organizations, about re-engineering processes for managing user access to business information resources

**Value Delivery**
- Initial IAM projects should deliver "quick wins" to build business support for continuing the IAM program
- The “big-bang” implementation approach is unlikely to build stakeholder trust and involvement required for continuing along the IAM maturity curve
IAM Implementation Success Factors II

| IAM Experience | • IAM projects have unique characteristics, so domain experience is vital  
|               | • IAM projects are complex, demand effective managers who can not only track schedule and budget, but effectively communicate with a diverse set of stakeholders and make sure everyone is pulling in the same direction. |
| Process Alignment | • Assess existing per-application user lifecycle processes and move toward standardization wherever possible  
|               | • Determine how identity information will be used to support periodic user access assessments, internal, and external audits. |
| Identity Definition | • Define identity populations (such as employees, contractors, business associates, and customers)  
|               | • Establish required identity characteristics and required data attributes  
|               | • Establish authoritative sources for identity information  
|               | • Define requirements associated with role-based access controls |
| Technology Integration | • Determine point of diminishing returns for automated and manual processes  
|               | • Pilot the implementation to prove the solution  
|               | • Implement the solution by delivering in phases (top value first)  
|               | • Test performance and functionality |
About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 140 countries. With access to the deep intellectual capital of approximately 135,000 people worldwide, Deloitte delivers services in four professional areas, audit, tax, consulting and financial advisory services, and serves more than 80 percent of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies. Services are not provided by the Deloitte Touche Tohmatsu Verein and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names “Deloitte”, “Deloitte & Touche”, “Deloitte Touche Tohmatsu” or other related names.

In the United States, Deloitte & Touche USA LLP is the U.S. member firm of Deloitte Touche Tohmatsu and services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Financial Advisory Services LLP, Deloitte Tax LLP, and their subsidiaries), and not by Deloitte & Touche USA LLP. The subsidiaries of the U.S. member firm are among the nation's leading professional services firms, providing audit, tax, consulting, and financial advisory services through nearly 40,000 people in more than 90 cities. Known as employers of choice for innovative human resources programs, they are dedicated to helping their clients and their people excel. For more information, please visit the U.S. member firm's Web site at www.deloitte.com

Copyright © 2007 Deloitte Development LLC. All rights reserved.