Deloitte.

Identity and Access Management Point of View

Audit.Tax.Consulting.Financial Advisory.

Agenda

What is Identity and Access Management (IAM)?

Business Drivers and Challenges

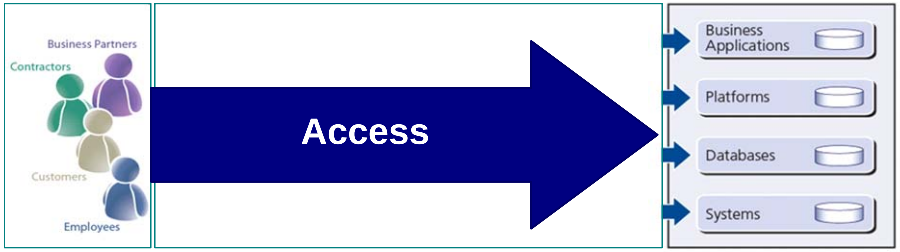
Compliance and Business Benefits

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

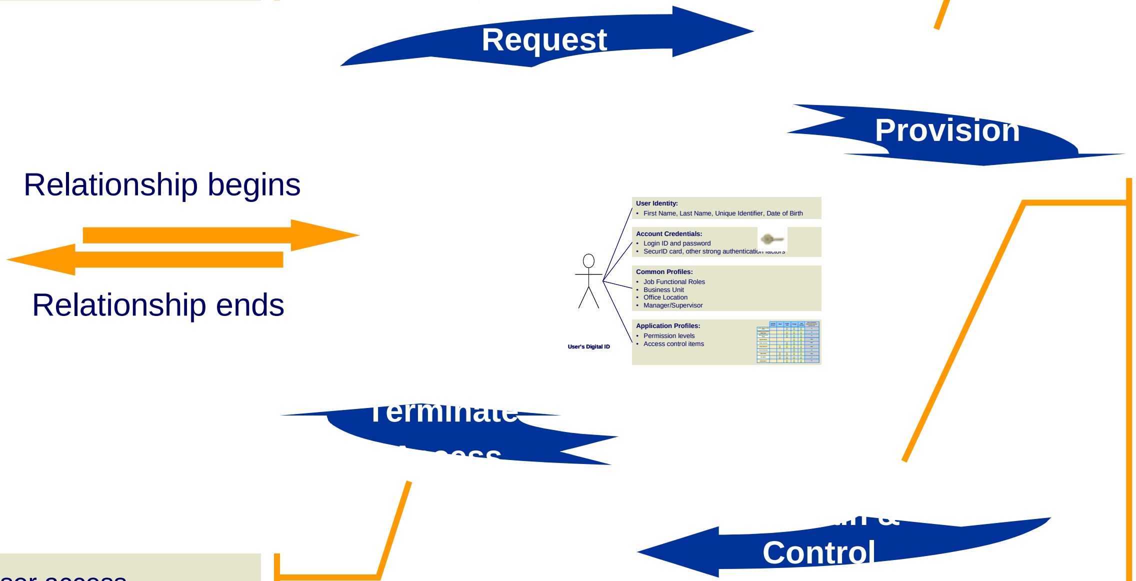
- Administration and Audit tools

- 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

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

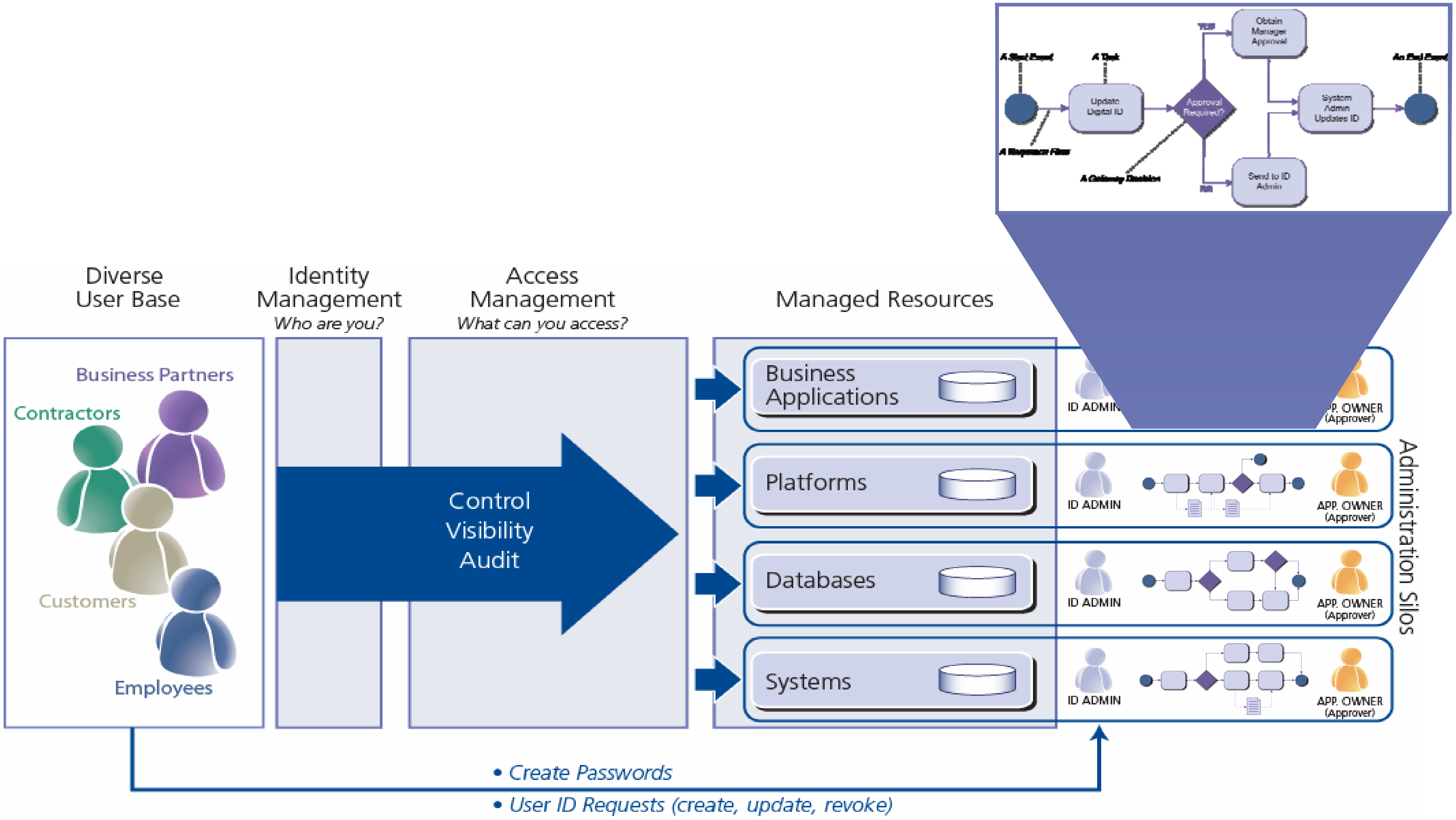


- User Life Cycle Management:
  - Access Request
  - Promotion/Transfer
  - Status change
  - Password reset
  - Approvals
- Role Life Cycle Management
  - Role Approval
  - Role Assignment
- Access Management
  - User Authentication
  - User Authorization
- Audit
  - User Access Review
  - User Access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

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

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**.*



A Start Event

A Task

Update Digital ID

Approval Required?

YES

Obtain Manager Approval

NO

Send to ID Admin

System Admin Updates ID

An End Event

A Sequence Flow

A Gateway Decision

Diverse User Base

Business Partners

Contractors

Customers

Employees

Identity Management

Who are you?

Access Management

What can you access?

Control

Visibility

Audit

Managed Resources

Business Applications

Platforms

Databases

Systems

ID ADMIN

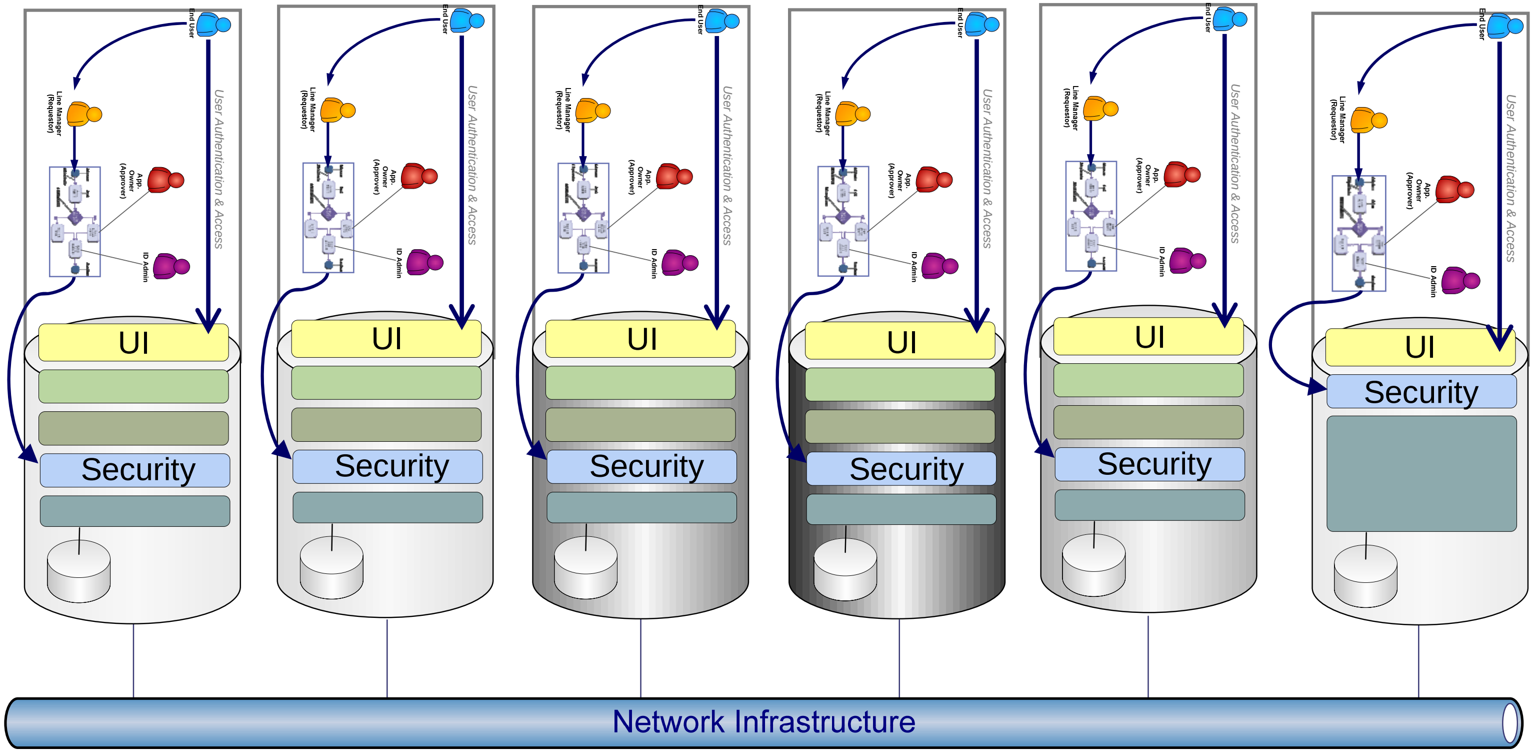
APP. OWNER (Approver)

Administration Silos

- *Create Passwords*
- *User ID Requests (create, update, revoke)*

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 on-going 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

4 Business Facilitation

- Improve User Experience
- Enable Collaboration with Business Partners
- Time-to-Market
- Post-M&A Integration

1 Compliance

- Regulatory
- Audit Management
- Protection of Personally Identifiable Information (PII)

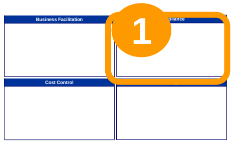
3 Cost Control

- Reduce Time-to-Productivity
- Reduce On-Going User Administration Costs
  - –Security administration
  - –Help desk
- Standardize IAM Infrastructure
- Contain Development Costs

2 Risk Management

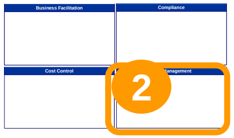
- Enforce Enterprise Risk Management policies
- Manage User Access Privileges
- Timely revocation of inactive accounts
- Strong authentication to protect sensitive digital assets

1. Compliance



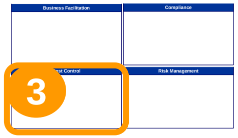
Business Drivers	Description
• Regulatory Compliance – Sarbanes-Oxley Act – Payment Card Industry Data Security Standard (PCI DSS) – U.S. Gramm-Leach-Bliley Act (GLBA) – Breach notification laws (CA SB1386) – EU Data Protection Directive – Industry-specific mandates (HIPPA, FFIEC, NERC, and others.)	• Management must report on internal controls within the enterprise • 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 – Address audit issues – Perform periodic user access reviews – Test control effectiveness	• Review user identities, job functions, and access privileges • 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

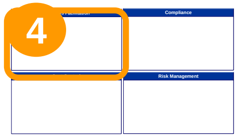


Risk Management Drivers	Description
• Enforce Enterprise Risk Management policies	• Implement controls to manage risk of unauthorized access access to business applications and systems • Reduce risk of revenue and reputation loss through failed or inadequate user ID management processes • Enforce enterprise 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



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



4. Business Facilitation

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

Agenda

What is Identity and Access Management (IAM)?

Business Drivers and Challenges

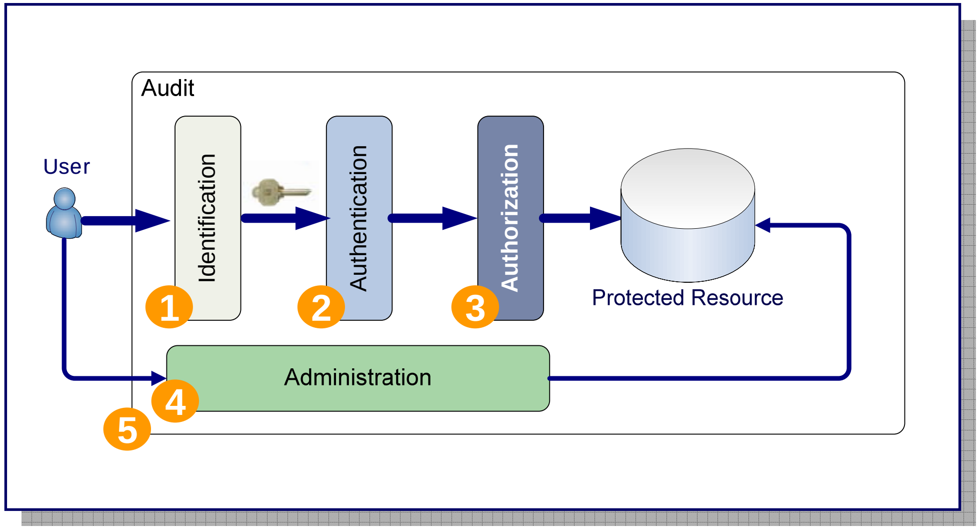
Compliance and Business Benefits

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

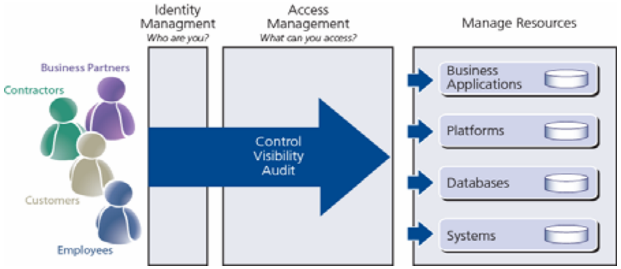


5. **Audit**: Reduce the cost and effort required to demonstrate control effectiveness and maintain compliance
   - Facilitate business and IT collaboration through a common risk and compliance framework

Compliance Issues addressed by IAM

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

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

A Strategic, Enterprise Approach will Result in Significant Improvements

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

﹢ * 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

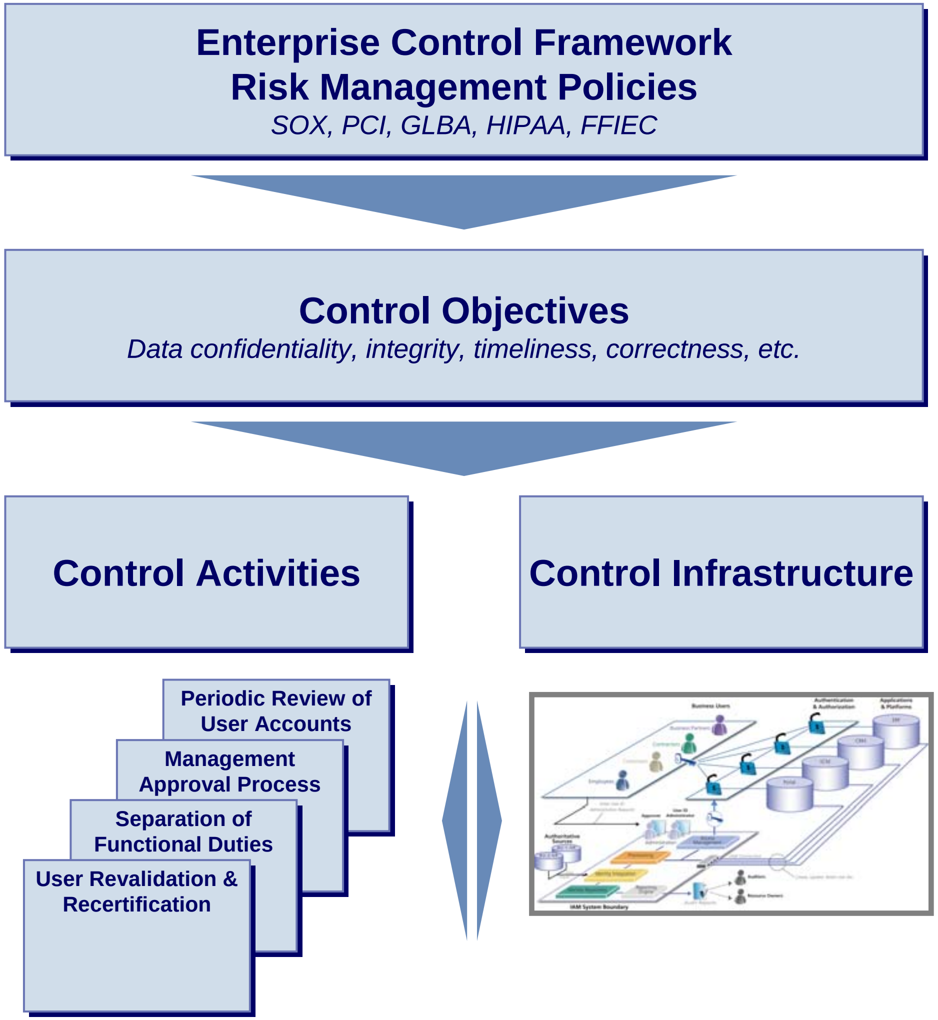
IAM Implementation

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



Enterprise Control Framework
Risk Management Policies
SOX, PCI, GLBA, HIPAA, FFIEC

Control Objectives
Data confidentiality, integrity, timeliness, correctness, etc.

Control Activities

Control Infrastructure

Periodic Review of User Accounts

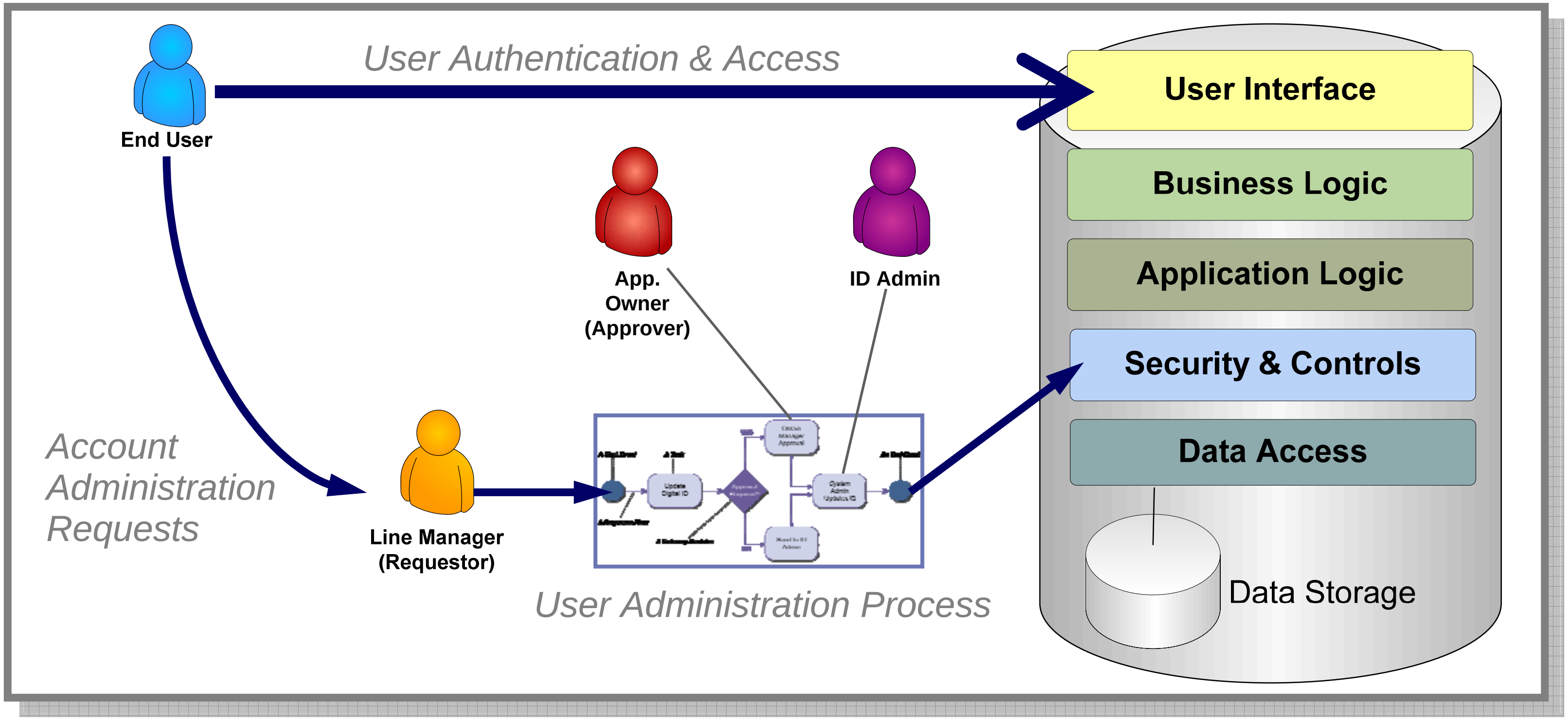
Management Approval Process

Separation of Functional Duties

User Revalidation & Recertification

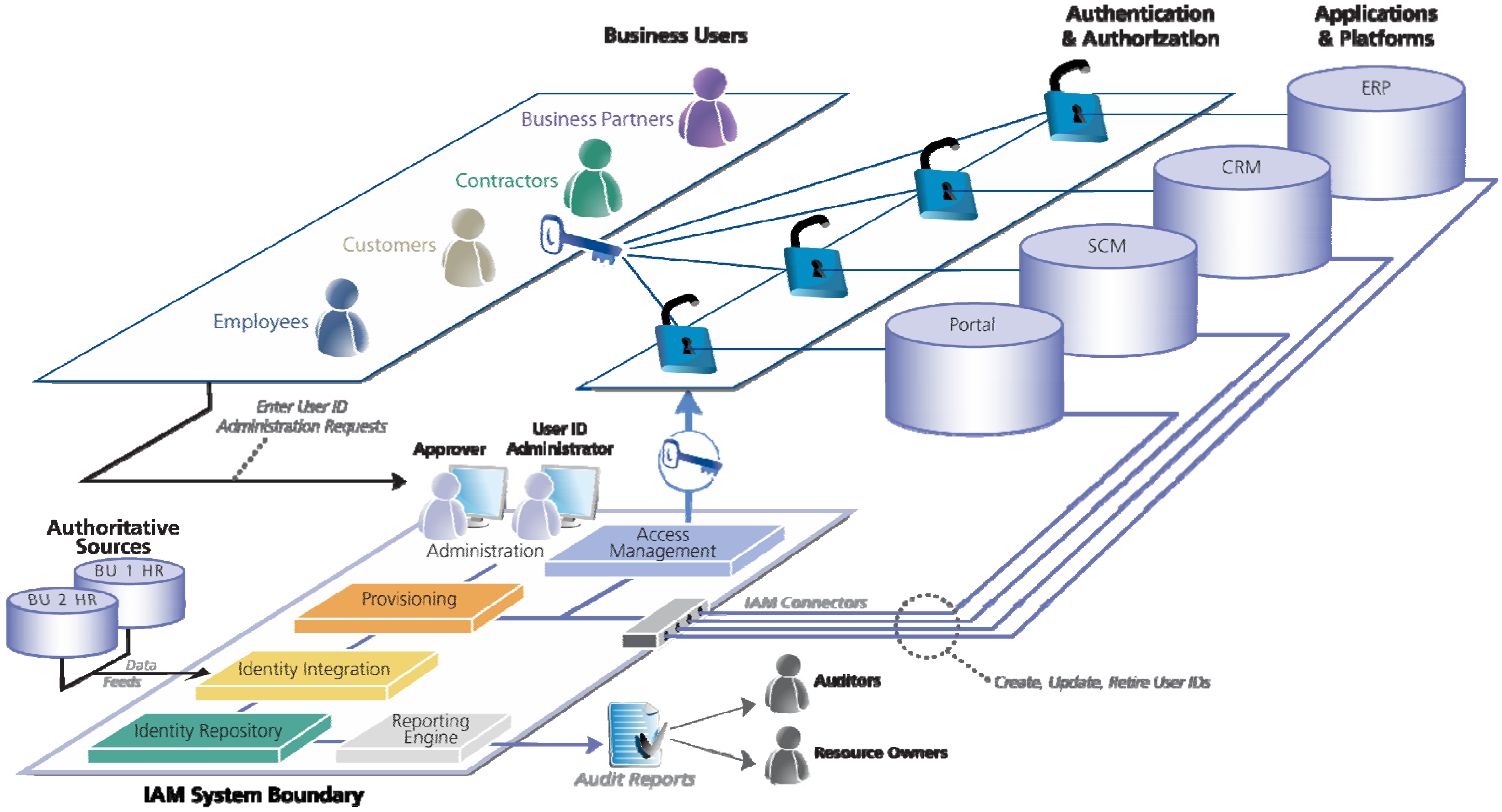
IAM Context

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



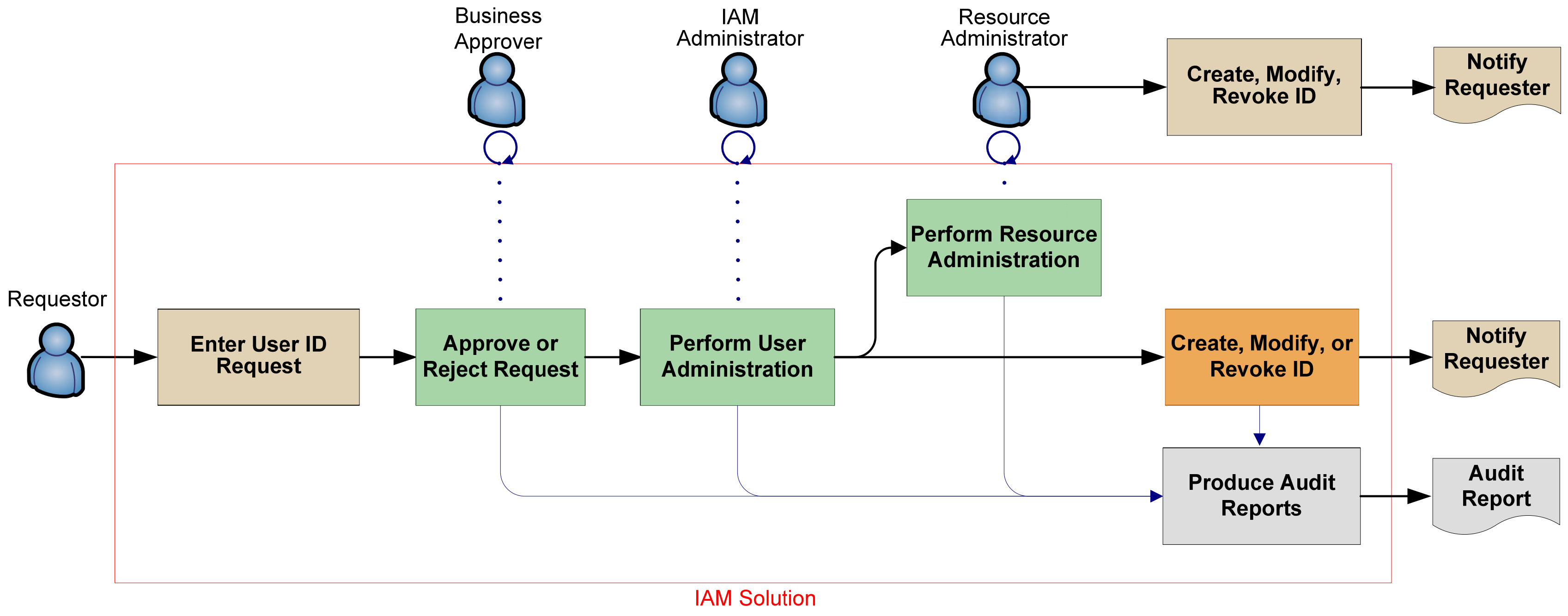
IAM Conceptual Model

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)?

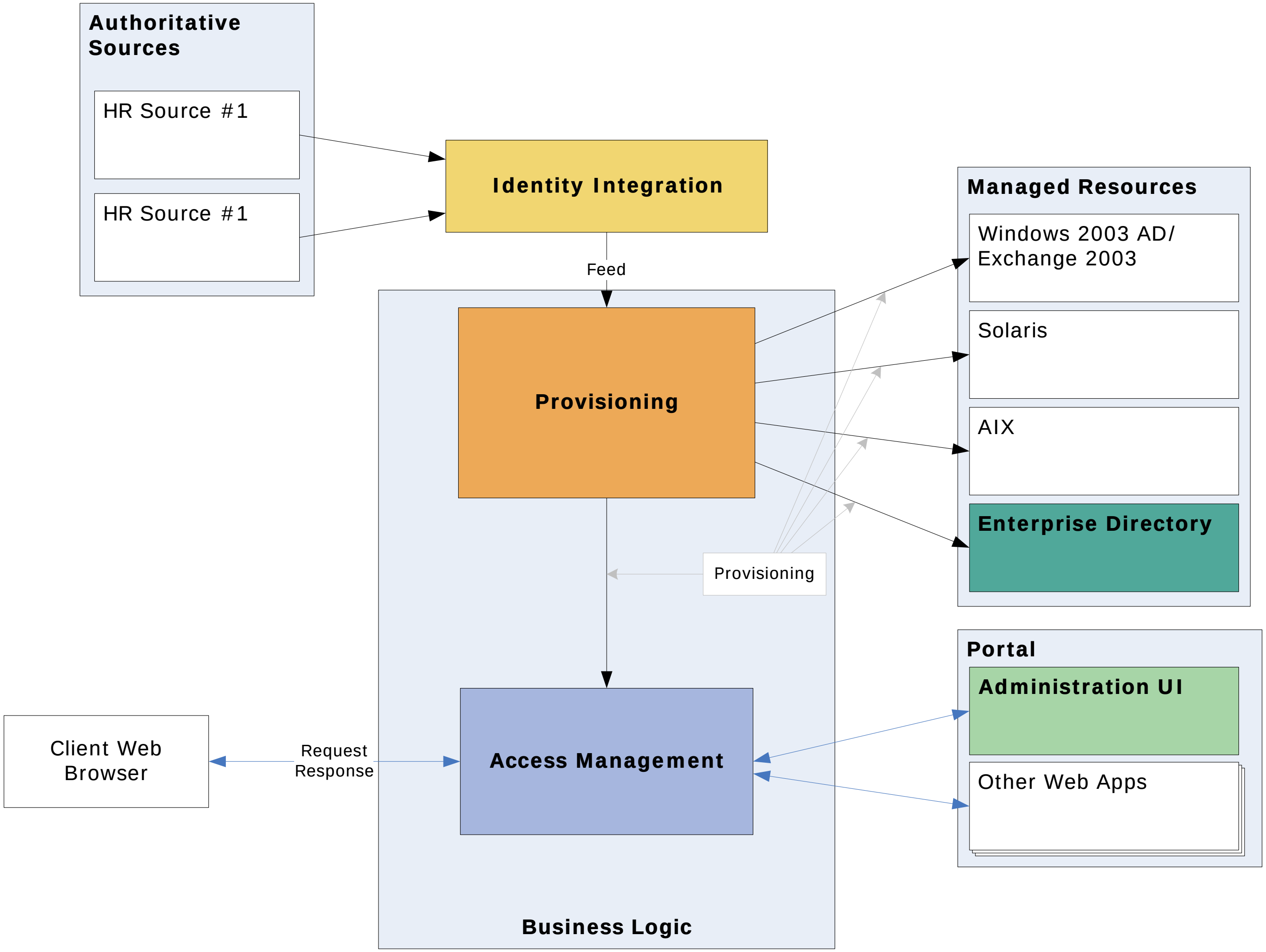
Business Drivers and Challenges

Compliance and Business Benefits

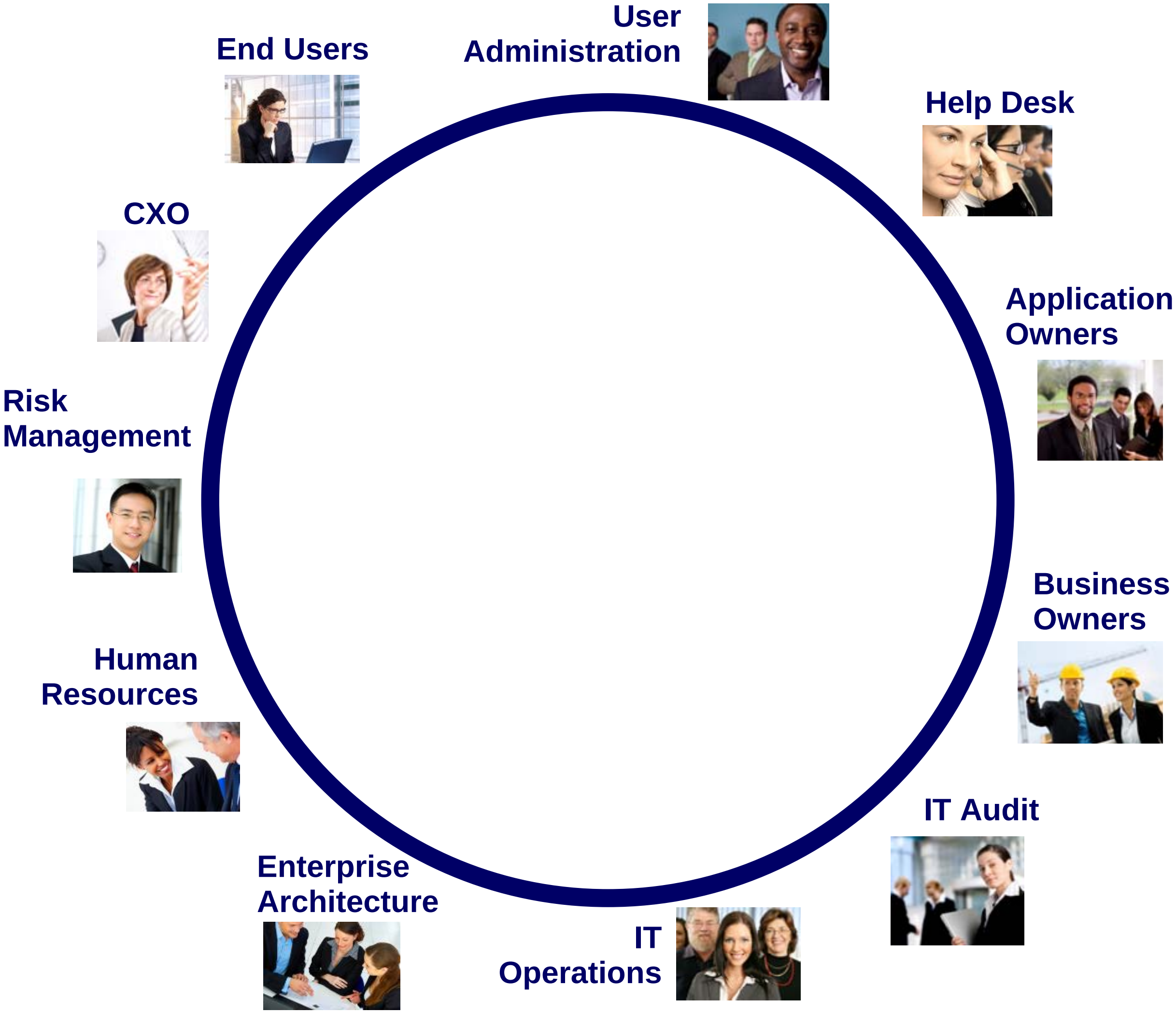
IAM Solution Framework

IAM Implementation

Conceptual Architecture



IAM Stakeholders



User Administration

Help Desk

Application Owners

Business Owners

IT Audit

IT Operations

Enterprise Architecture

Human Resources

Risk Management

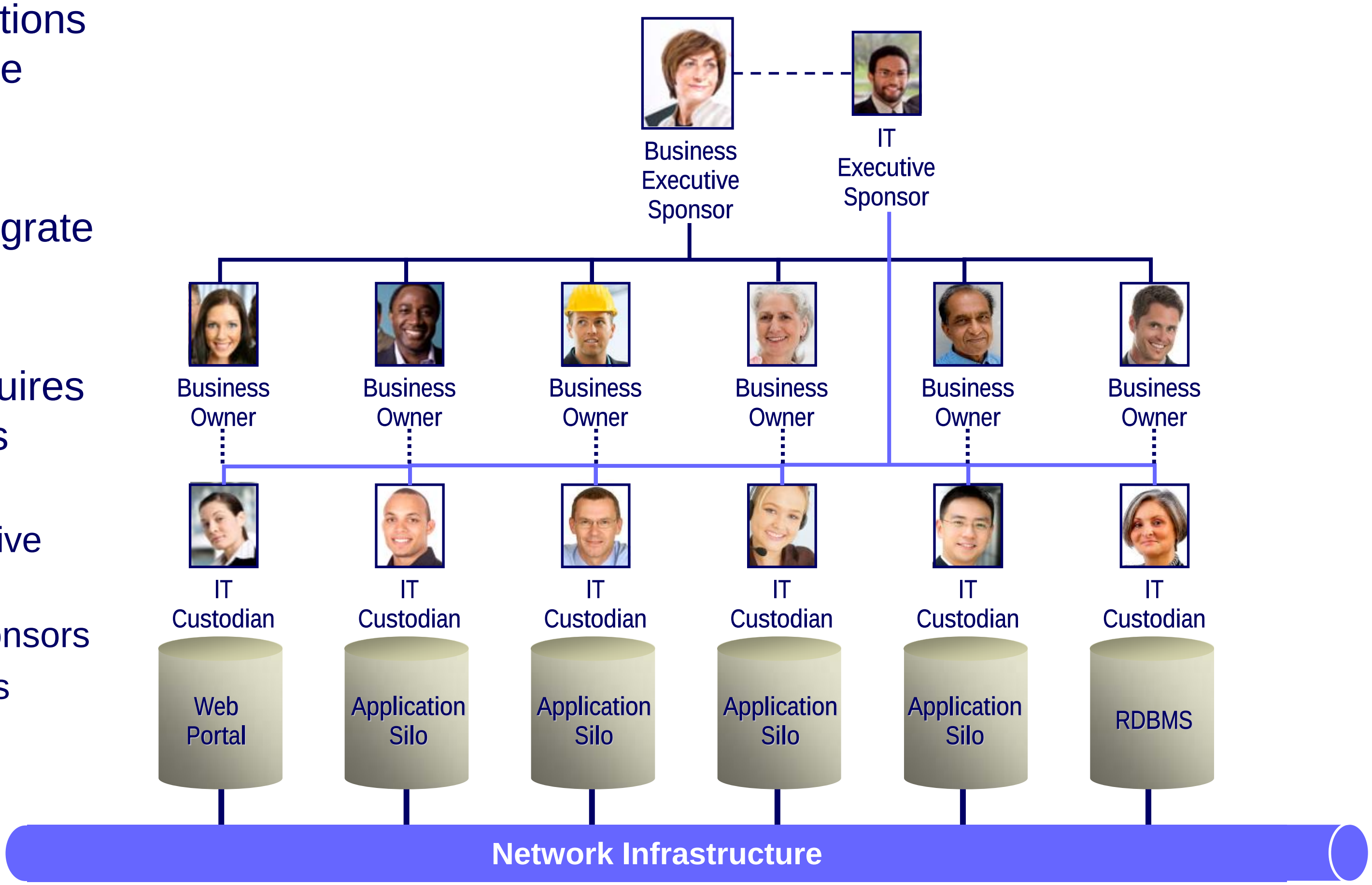
CXO

End Users

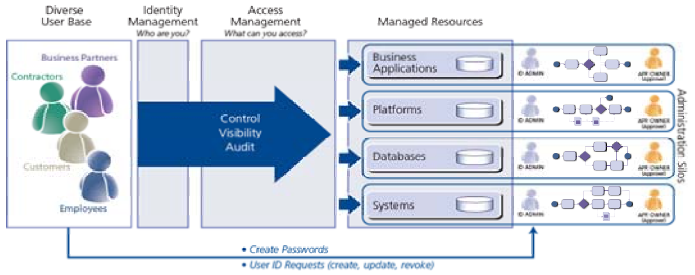
Business Value

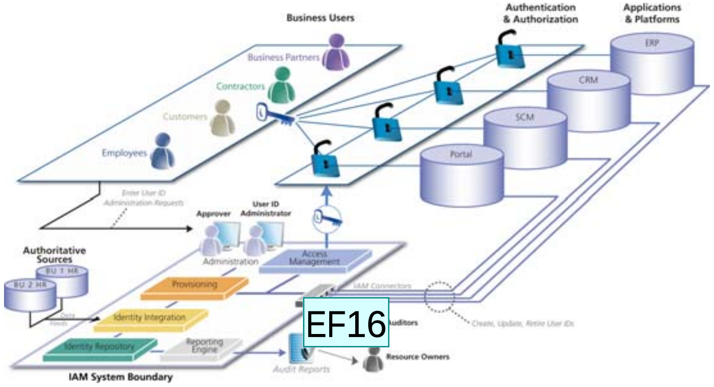
*The **business value** of an IAM Solution is directly proportional to the **number** of integrated applications and systems*

- 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 use base (employees, non-employees)
- Audit issues with current User Administration Process

2 Goal State

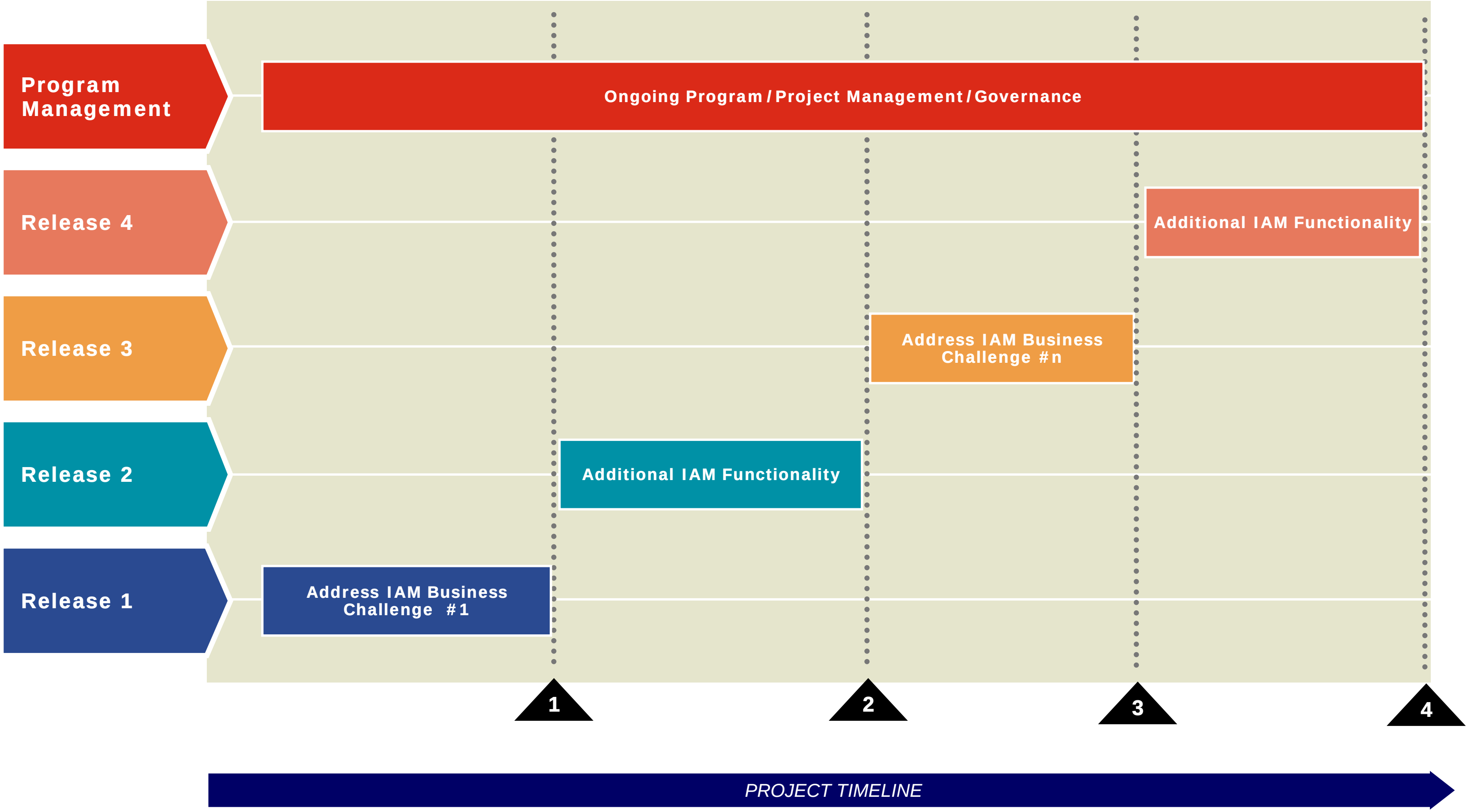
- Manage risk of unauthorized access to information resources
- Standard user administration and IT Audit processes, procedures, and technology platform
  - Approval and Recertification workflows
  - Consistent revocation of access when a user leaves
- Reduced risk of regulatory non-compliance, revenue, and reputation loss through inadequate IAM processes

EF16 Need more visual tie-in wth previous slides. For example, use process flow, represent the users

Fisk, Elisha, 12/4/2007

IAM Implementation Strategy

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


Program Management
Ongoing Program / Project Management / Governance
Release 4
Additional IAM Functionality
Release 3
Address IAM Business Challenge #n
Release 2
Additional IAM Functionality
Release 1
Address IAM Business Challenge #1
1
2
3
4
PROJECT TIMELINE

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

Deloitte.

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

Member of
Deloitte Touche Tohmatsu