Software Summit2012

El placer de cautivar y crear nuevos mercados

IAM: ¿Cómo Les Puede Ayudar A Mejorar Sus Controles De Acceso Y Cumplir Con Regulaciones?

Giancarlo V. Marchesi

Manager, Worldwide Security A-Team (SWAT)

IBM Security Systems Division

IBM

Identity Management 101

Managing
WHO has ACCESS to WHAT

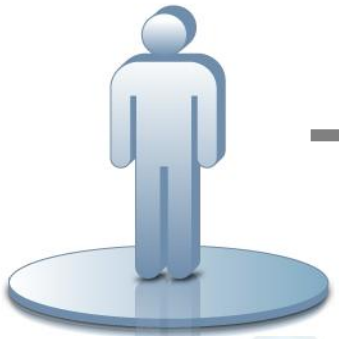
People	Policy	Resources

The *Who* in Identity Management

Who → Users → people who need access to resources.

Users can be internal or external to the organization.

- Employees
- Customers
- Business Partner
- Citizens



Jane Doe's HR information

HR System

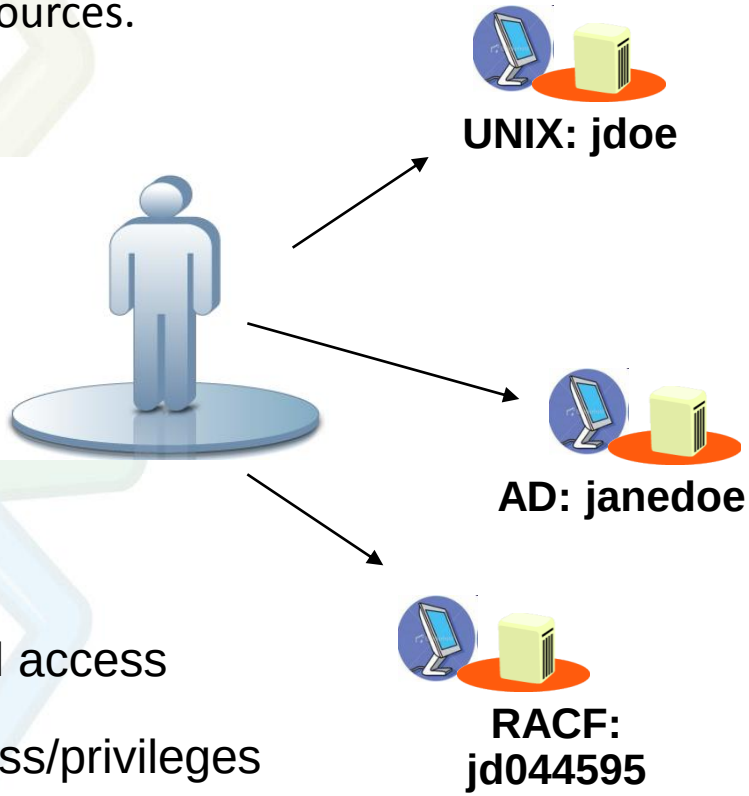
Name:	Jane Doe
Dept:	Accounting
Manager:	John Smith
Address:	10 Main St.
Tel. No:	555-1212
Bus Role:	Benefits Administrator

The *What* in Identity Management

What → Accounts → give people access to resources.

Examples of Resources:

Operating Systems	UNIX, Windows
Databases	DB2, Oracle
Applications	SAP, Lotus Notes
Directories	Active Directory



The user account generally consists of:

- A userid
- Password

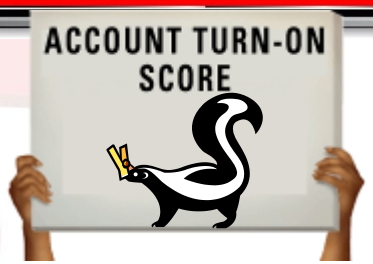
→ grant initial access

- Group or role assignments → grant access/privileges

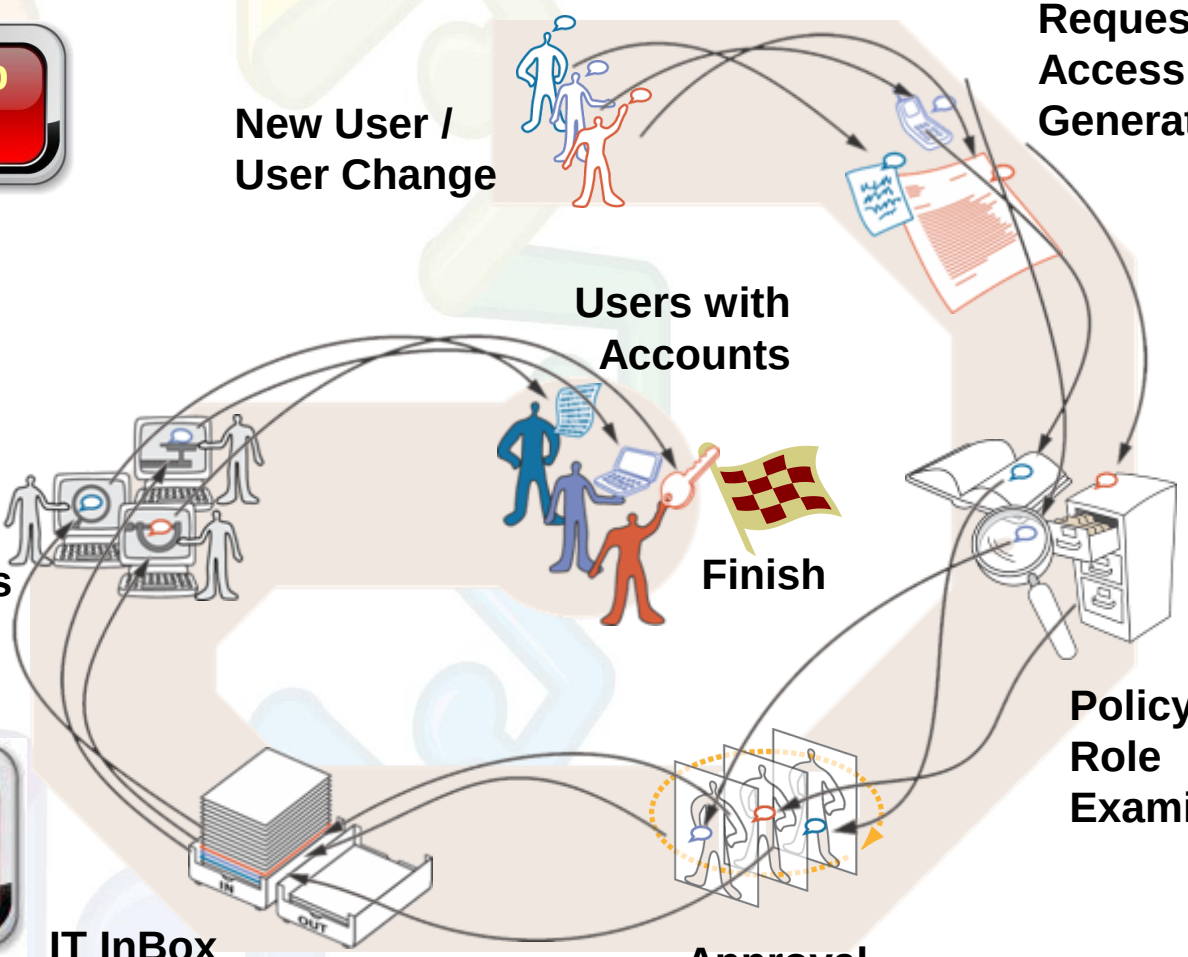
Customers Implement User Lifecycle Mgmt Manually or with Inadequate Tools

Software Summit2012

Elapsed turn-on time: up to 12 days per user



Account turn-off performance: 30-60% of accounts are invalid



Identity Management ++

Managing
WHO has ACCESS to WHAT

People	Policy	Resources

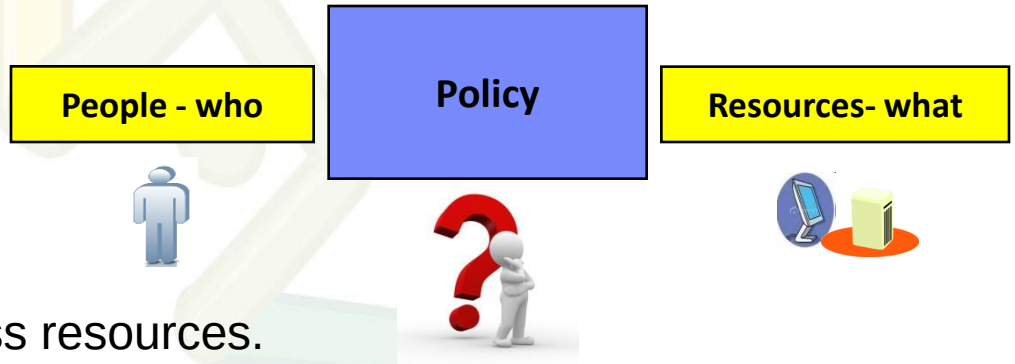
Delivering a
bridge between business and IT

IAM Governance

- Role Management
- Entitlement Management
- Privileged Identity Management
- Separation of Duties
- Access Certification

Roles	Apps, DB ..	Access Rights

How is *Access* Granted …



- Policy defines who can access resources.
- Policy is made up of membership and entitlements
- Workflow and Approvals define the business process and ensure that the right people are given the right access.
- Policy Membership can be defined through Roles

  Business Roles – collections of users by job function

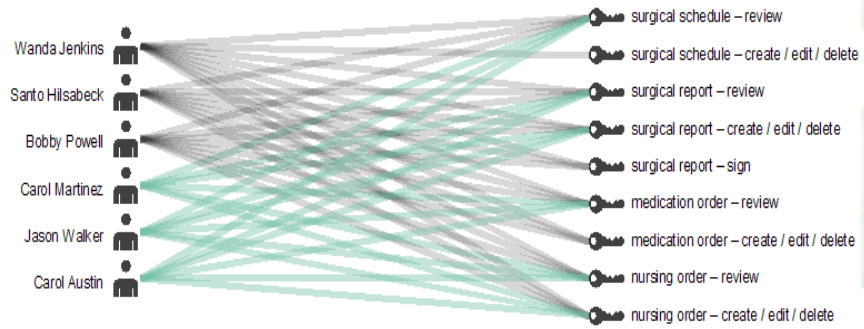
  Application Roles – collection of resources or entitlements.

- Membership - Individual vs Group

Examples of group Membership: Active Directory group policies, SAP authorizations

Customers demand the need to drive IAM Governance while reducing the risk & cost of managing people and their identities

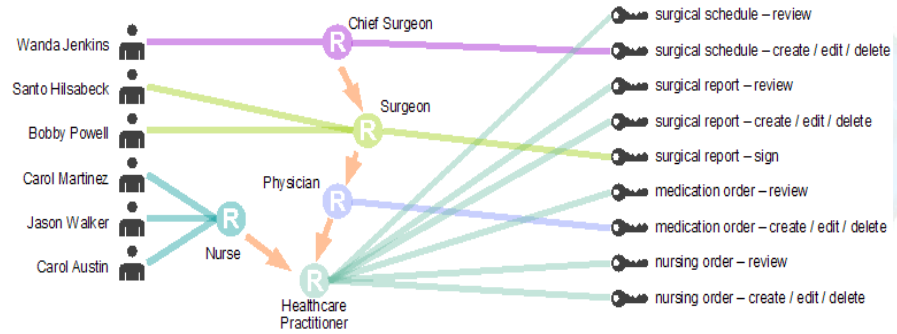
Before



Direct access assignments today are complex, difficult to track and change when needed

- **Simplify roles and access assignments**
- **Ability to handle growth and scale**
- **Facilitate accountability and compliance**

After

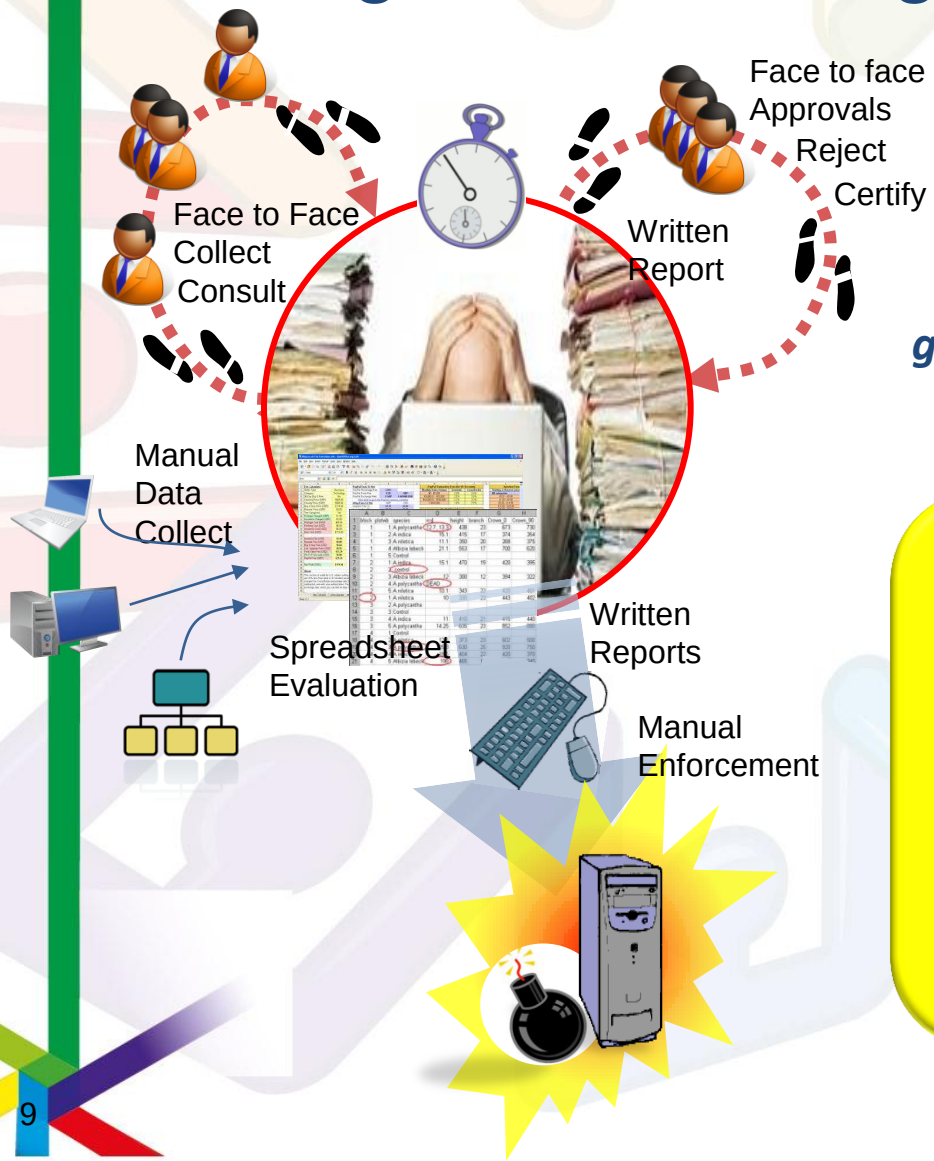


Role Based Access Control (RBAC) offers an effective operational model to drive IAM Governance

How to get the most effective role structure and policies?

Role and Policy Modeling and Lifecycle Management Project

But today's Role & Policy Modeling and Lifecycle Management projects are still challenged in achieving their target goals



The traditional Role Modeling solution generates results that are obsolete by the time they are ready

X Too time consuming
- Requires correlating massive data
- Lack integration with apps
- Lack business process integration

X High IT skill requirement
- Difficulty with correlation
- Not business user friendly

X Inaccurate results
- Delayed delivery

Web SSO & Web Access Management Now A Business Need

Software Summit2012

Employees

Customers, Partners, …

Web Single Sign-On
Governance
Web Access Control

WebSphere.
PeopleSoft.
Microsoft
Lotus
SAP
CITRIX
documentum a division of EMC
ORACLE

And other application targets

"How do I protect my Web applications?"

"Will security I add hurt performance/ scalability?"

"Can we lower our help desk costs in this area?"

"How can I provide Web single sign-on for my users?"

"What else do we need besides our FW/IPS to make this secure?"

"Can I control & report on who is accessing what?"

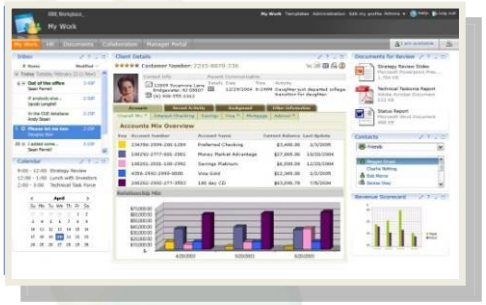
"Can I manage this on an enterprise level?"

IBM

Enforcing B2C & B2E Across the Enterprise With Centralized Access Mgmt

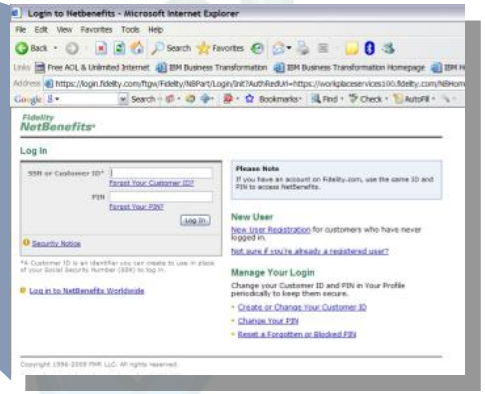
Software Summit2012

Web Applications & Employee Portal



WW Customers

Customer Portal



Access Manager for e-business

*Contributing factors

Primary customer requirements:

1. *Web SSO*
2. *Ability to set, enforce and audit access to Web applications*

*Strong Authentication**

*Scalability**

*Session Management**

*Availability**

IBM

Identity & Access Management (IAM) Connects Who to What through How

IdM:

- Manages exiting users identities
- Automates the creation of new identities
- Maintains enterprise wide Identity records for reports and audits.

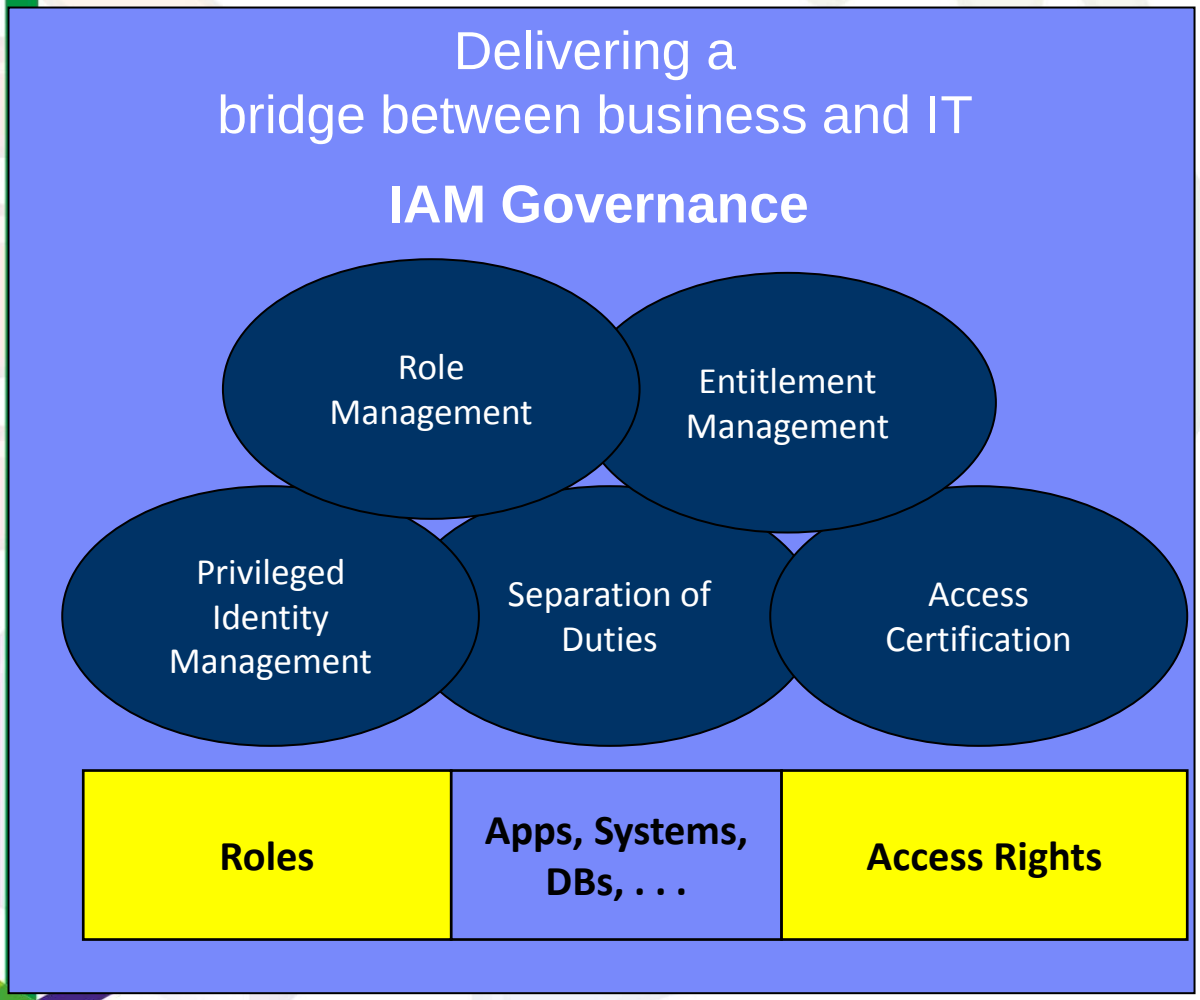
IAM:

- Maintains a unique identity-entitlement map for the enterprise
- Externalizes Security from applications
- Centralizes security policy management & access control

IdM:

- Manages existing entitlements, membership and accounts.
- Automates the creation of new entitlements.
- Maintains enterprise-wide entitlement records for reports and audits.

… and it gets even better!



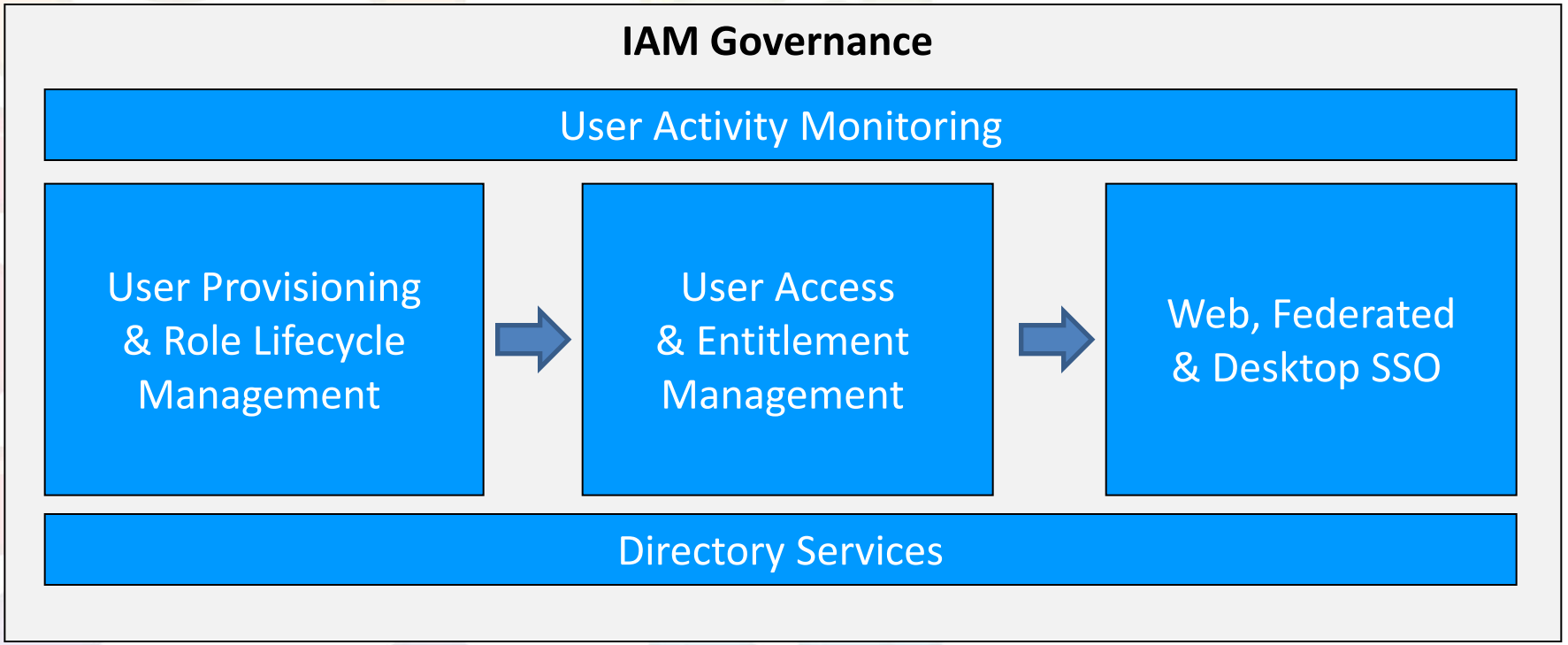
IAM

- Identity Lifecycle
- Workflow
- Role Engineering
- Password Self-Service
- Strong Authentication

Compliance

- Reconciliation
- Re-Certification
- Reporting

IBM Identity & Access Management
Visibility. Control. Automation.



- Provides closed-loop user life-cycle management, addressing audit/compliance
- Governs and enforces user access to applications across heterogeneous IT environments, including mobile clients and also covering cloud, SOA and SaaS-based user cases.
- Leverages identity and access data for business insight, including risks from distributed and mainframe environment
- Based on scalable/performant LDAP technology

Numerous IBM Customer Examples

Software Summit2012

THE LIST GOES ON ...

BRITISH PETROLEUM
5 DAYS -> 10 MINUTES

KOHL'S DEPT. STORES
15 DAYS -> 20 MINUTES

LARGE BANK
10 DAYS -> 1 HOUR