Identity Assurance

Managing Identities, Roles and the Associated Governance Requirements

IBM Software

PCTY2010

Pulse Comes to You

Optimising the World's Infrastructure

27 May 2010 London

Today's Security Challenges

Trusting Identities

Customers or criminals?

Partners or competitors?

Employees or hackers?

Managing Access

Securing Services

Payroll

Online banking

Loan applications

Retail sales

Inventory

Protecting Data

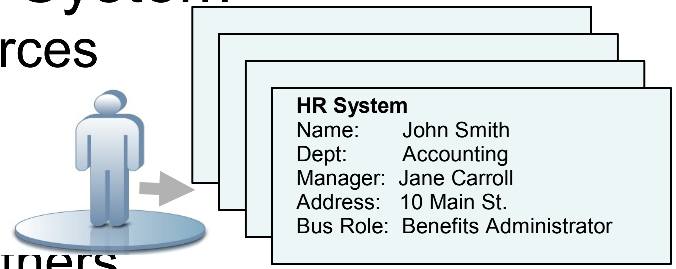
– Security has to be applied within a Business Context

Managing
WHO has ACCESS to WHAT

People	Policy	Resources

The Who in Identity Management

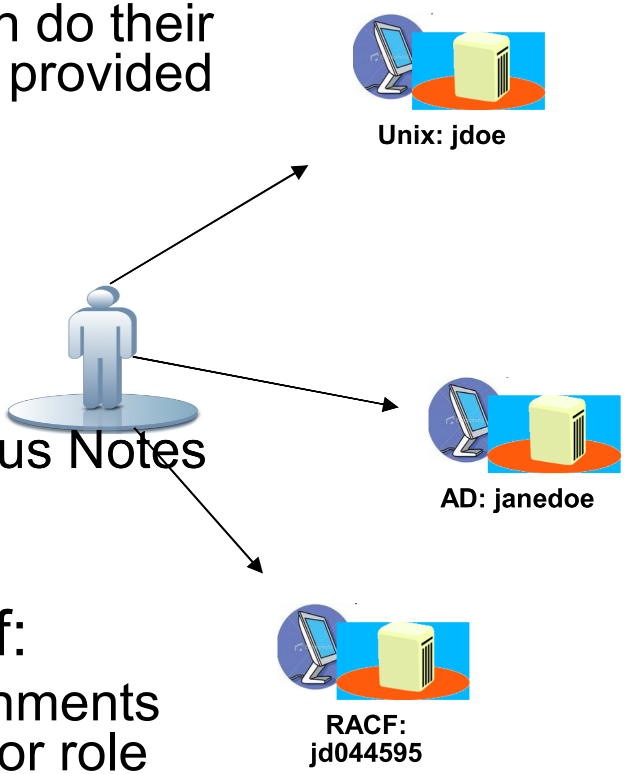
- Users defined in Identity Management System
  - The people that need access to resources
  - –
- External or internal to the organization
  - Employees, Customers, Business Partners
  - –
- Each user has an identity and related attribute information
  - Used to make decisions about resources access
  - –
- Over the lifecycle of the user, the process of identity administration manages what the user gets access to, changes to that access and the removal of access



HR System
Name: John Smith
Dept: Accounting
Manager: Jane Carroll
Address: 10 Main St.
Bus Role: Benefits Administrator

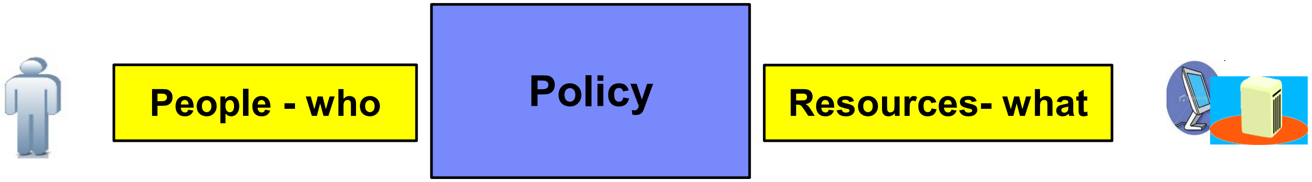
The What in Identity Management

- The What is a user account on an IT resource
  - The account is needed so the user can do their job or perform a function. Access is provided through the account.
  -
- Examples of Resources:
  - Operating Systems Unix, Windows
  - Databases DB2, Oracle
  - Applications SAP, Lotus Notes
  - Directories Active Directory
-
- The user account generally consists of:
  - Userid, password, group or role assignments related to that resource. The group or role membership grants some type of privilege.



How is *Access* granted ...

- Policy defines who can have access to the resource
  - Policy is made up of membership and entitlements
-
- Workflow and Approvals define the business process
  - 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: collections of resources or entitlements. In identity management systems, application roles typically map to group or roles on the target resource and are considered coarse grained.



Consistent Drivers for Managing Identities

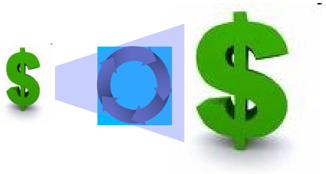
- Governance, Risk and Compliance
  - Deliver accountability and an audit trail for external regulatory mandates and internal policies
-
- Cost Reduction (via Automation)
  - Streamline Business and IT processes for user access to resources
  -
- Security
  - Mitigate the Risk of Fraud, Theft of IP, loss of customer data, etc.

PCI-DSS

SOX

Basel II

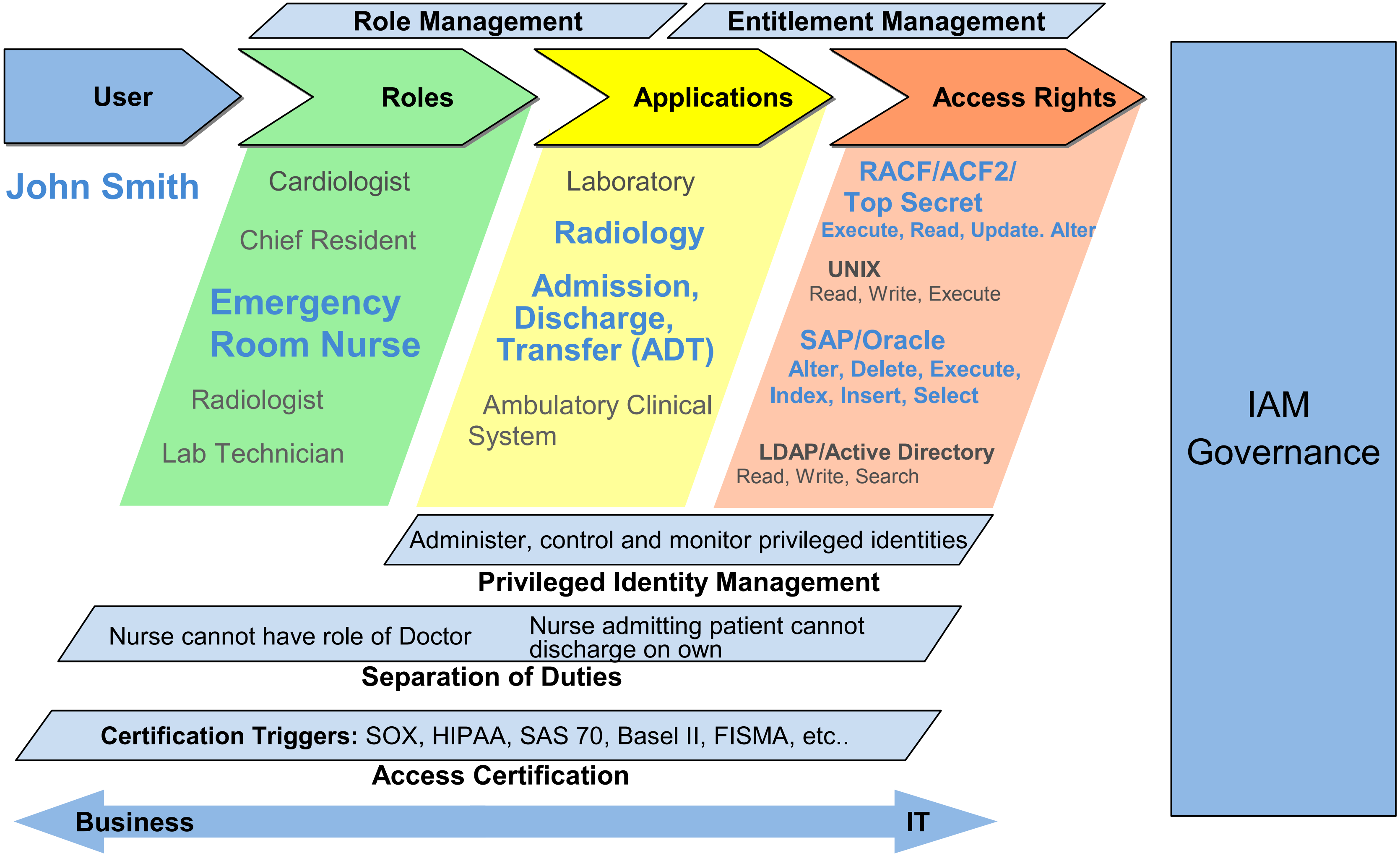
ISO 27001



Challenges with current deployments

- User Provisioning deployments stall without scalable administration
-
- Inability to manage business conflict that arises due to granting of user access
-
- Lack of flexible and continuous validation of user access
-
- Poor integration with Security Information and Event Management for user activity monitoring
-
-
-
-

IAM Governance: A bridge between Business & IT



Role Management

Entitlement Management

User

John Smith

Roles

Cardiologist

Chief Resident

Emergency Room Nurse

Radiologist

Lab Technician

Applications

Laboratory

Radiology

Admission, Discharge, Transfer (ADT)

Ambulatory Clinical System

Access Rights

RACF/ACF2/ Top Secret

Execute, Read, Update. Alter

UNIX

Read, Write, Execute

SAP/Oracle

Alter, Delete, Execute, Index, Insert, Select

LDAP/Active Directory

Read, Write, Search

Administer, control and monitor privileged identities

Privileged Identity Management

Nurse cannot have role of Doctor

Nurse admitting patient cannot discharge on own

Separation of Duties

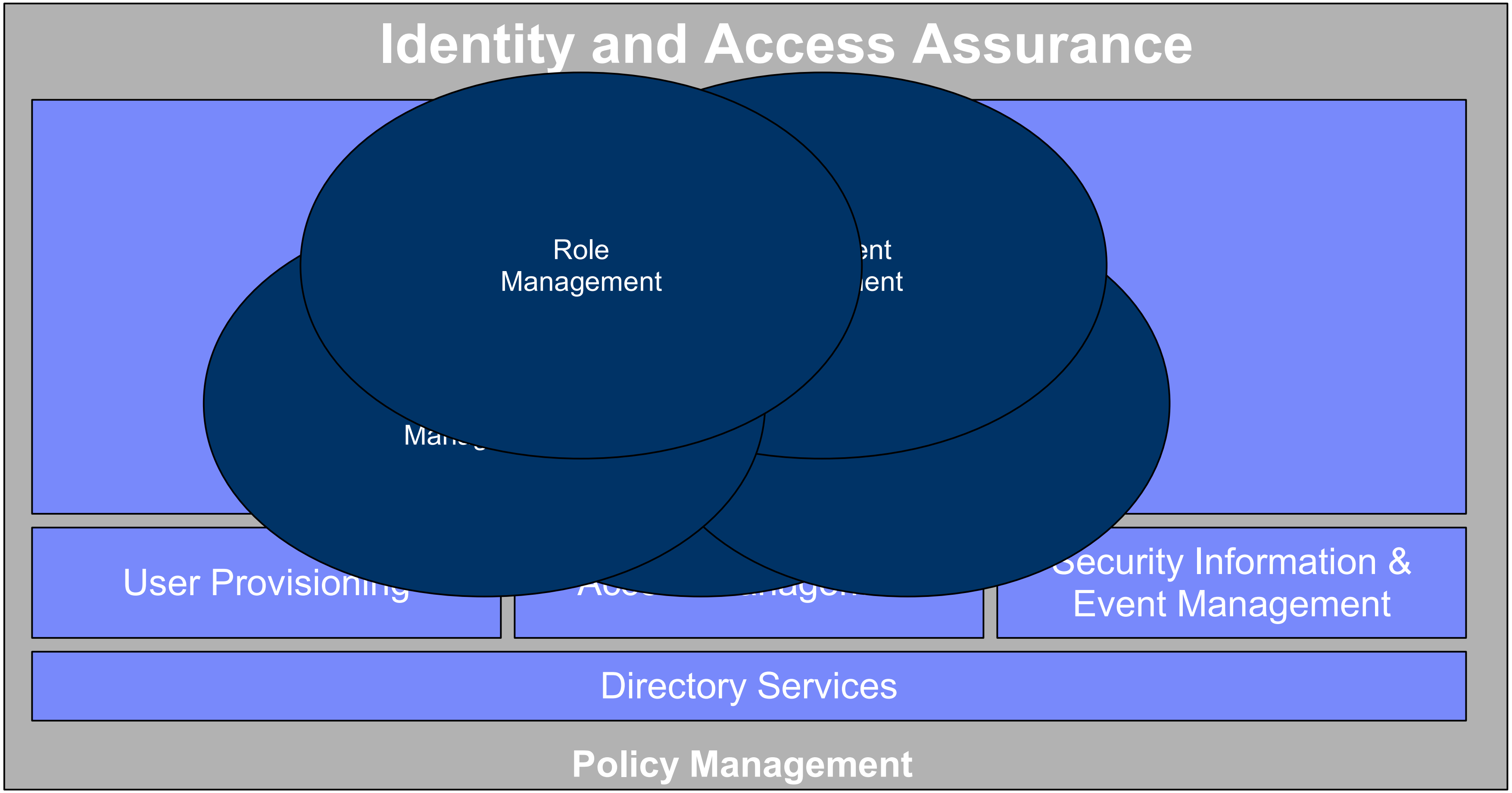
Certification Triggers: SOX, HIPAA, SAS 70, Basel II, FISMA, etc..

Access Certification

Business

IT

IAM Governance



Identity and Access Assurance

Role
Management

ent
ent

Man

User Provisioning

Acc
nage

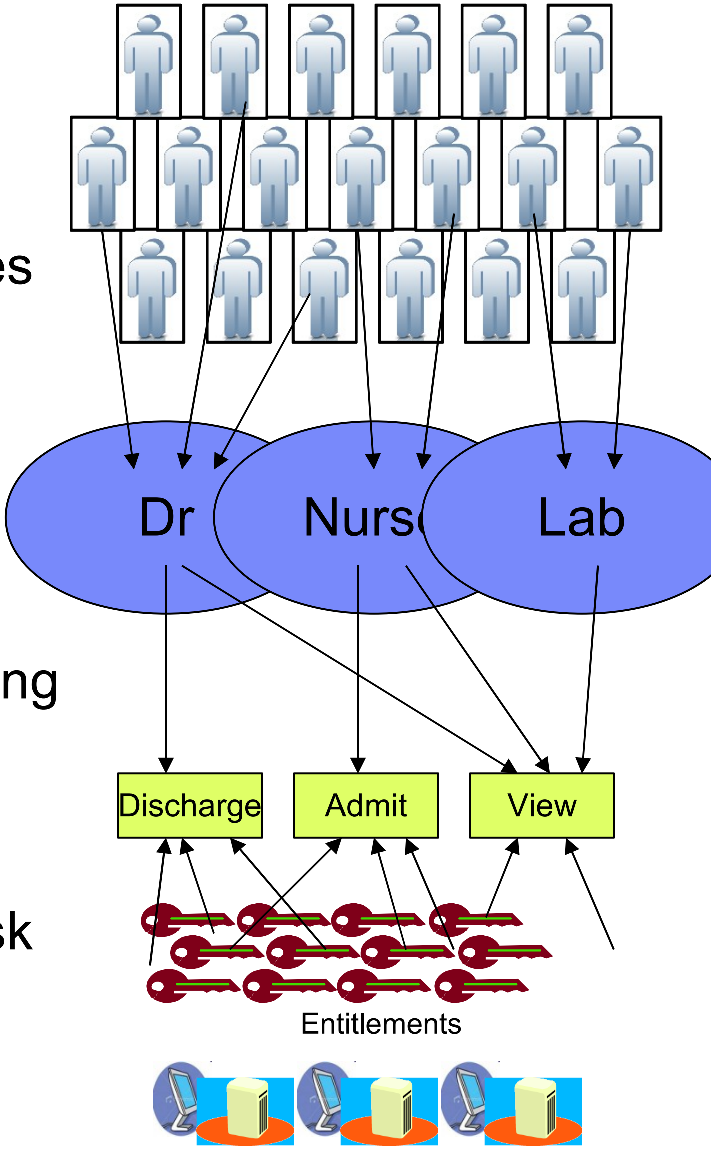
Security Information &
Event Management

Directory Services

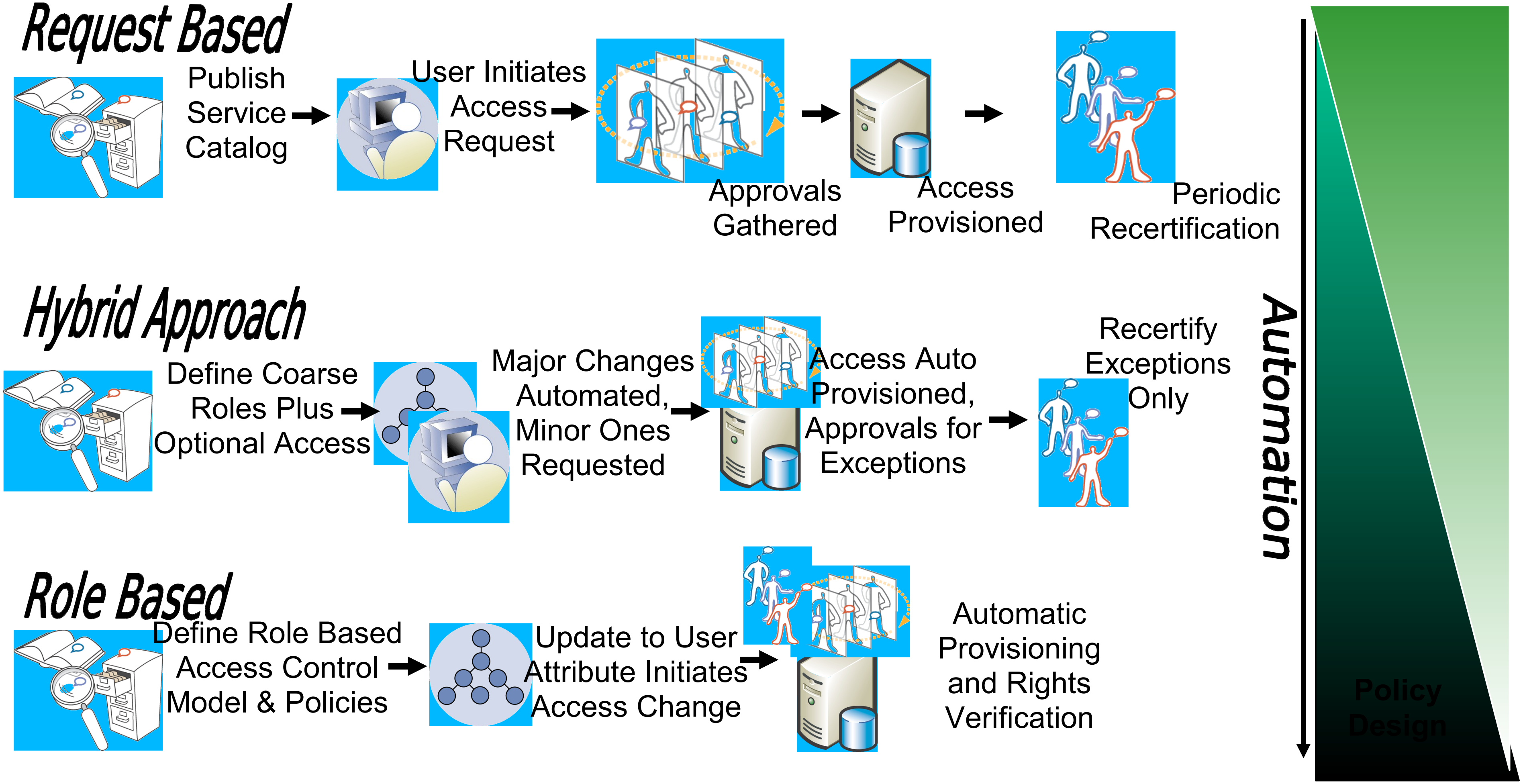
Policy Management

Role Management

- User
  - Entity requesting access to resources
- Resources
  - System, DB, Applications, etc.
- Entitlement
  - A permission to access a resource
- Business Role
  - A logical collection of users performing a similar business function
- Application Role
  - A logical collection of entitlements needed to perform a particular task



Phased Approach: Increasing Efficiency/Control



Request Based

Publish Service Catalog → User Initiates Access Request → Approvals Gathered → Access Provisioned → Periodic Recertification

Hybrid Approach

Define Coarse Roles Plus Optional Access → Major Changes Automated, Minor Ones Requested → Access Auto Provisioned, Approvals for Exceptions → Recertify Exceptions Only

Role Based

Define Role Based Access Control Model & Policies → Update to User Attribute Initiates Access Change → Automatic Provisioning and Rights Verification

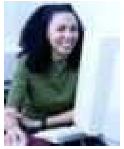
How to apply Entitlements consistently?

The business *requirement* is to protect access and disclosure of client and customer PII
Client Transaction, Patient Records, Financial Results

Security Officer
Corporate Intranet

Security Architect
Internal Tool

Translates it as need to encrypt that information in all services using message security *policy*



App Owner
Eclipse

Translates it as application specific data entitlement *policy*

IT Operations
IAM Console

Translates it as configurations and tool-specific access *policy*

How to demonstrate compliance back to the business?

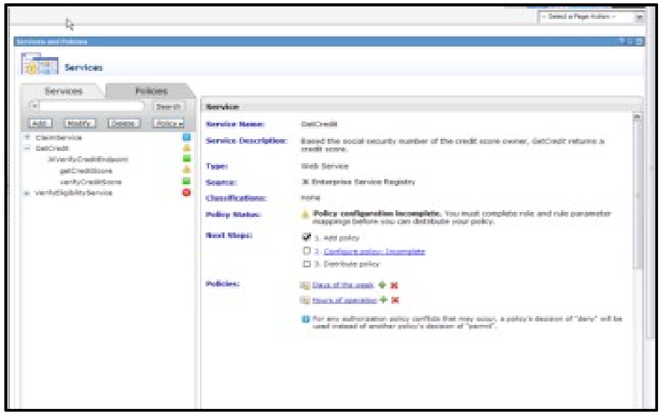
Policy driven Approach to Entitlements

Policy Modelling & Store → Policy Administration & Decision → Policy Enforcement

Policy Management

Service Repository, DB Schema, etc

App Roles, Identity Stores



- ClaimService
- GetCredit
  - IVerifyCreditEndpoint
    - getCreditScore
    - verifyCreditScore
- VerifyEligibilityService

Service

Service Name: GetCredit

Service Description: Based the social security number of the credit score owner, GetCredit returns a credit score.

Type: Web Service

Source: Enterprise Service Registry

Classifications: none

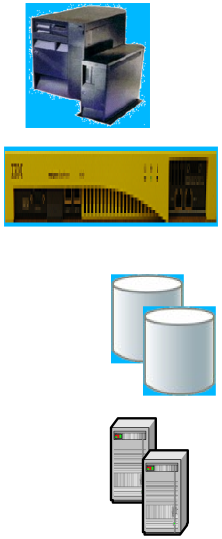
Policy Status: **Policy configuration incomplete.** You must complete role and rule parameter mappings before you can distribute your policy.

Next Steps:

☑ 1. Add policy
□ 2. Configure policy: Incomplete
□ 3. Distribute policy

Policies: Days of the week; Hours of operation

For any authorization policy conflicts that may occur, a policy's decision of "deny" will be used instead of another policy's decision of "permit".



Portal & Applications

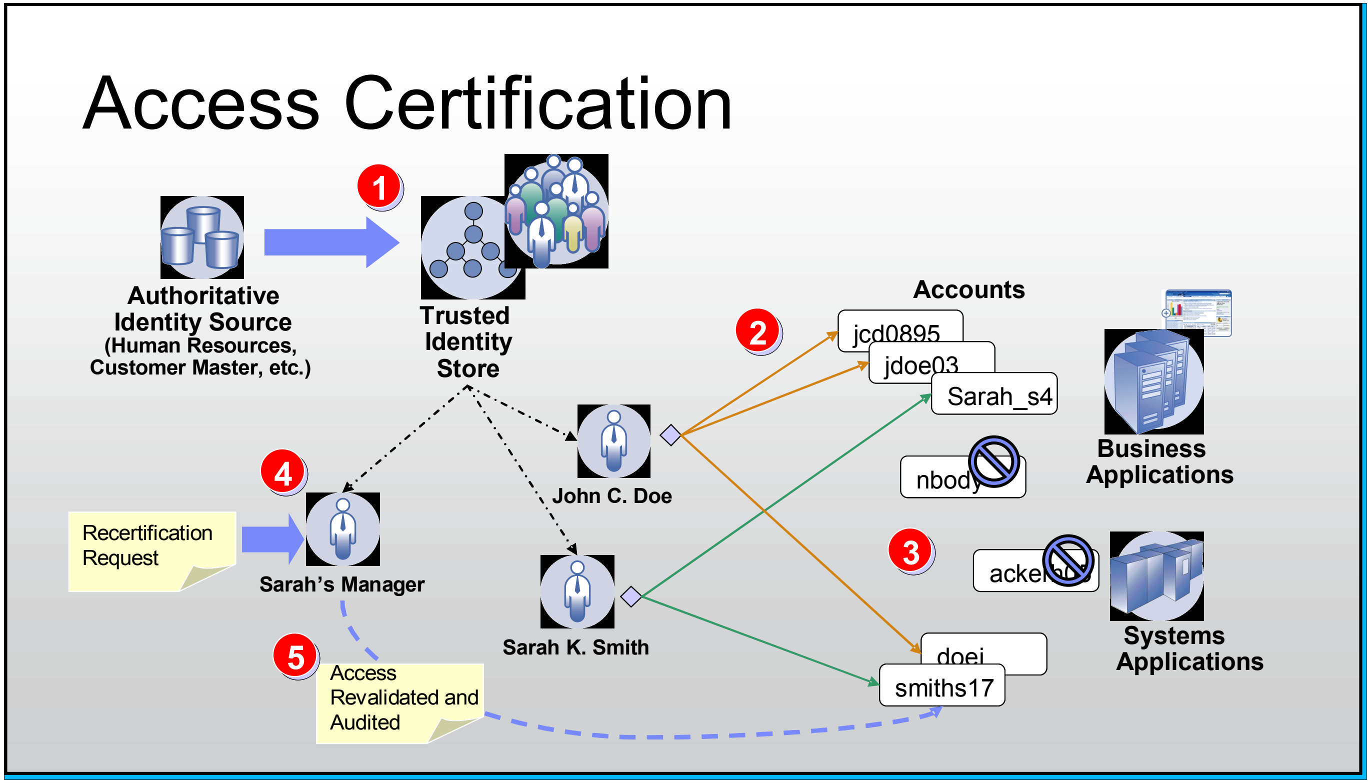
Web Services

Database s

Operating Systems

- Provide access to data entitlements on a need to know basis
- Centrally administer SOA security policies
- Automate access control across application lifecycle

Validate that Access remains appropriate



Separation of Duties

- Used to reduce risk/fraud by separating duties
  - Prevent/highlight inappropriate combination of privileges
  - Introduces good governance and accountability
  -
- Separation of Duties helps prevent combination of roles that are invalid or inconsistent with business policy
-
- To most effectively avoid conflicts, combine:
  - Preventative separation of duties, where policy prevents the granting of overlapping responsibilities that could present a potential conflict to the organization and its policies
  - Detective separation of duties, analysis to see if conflicts already exist

Privileged Identity Management

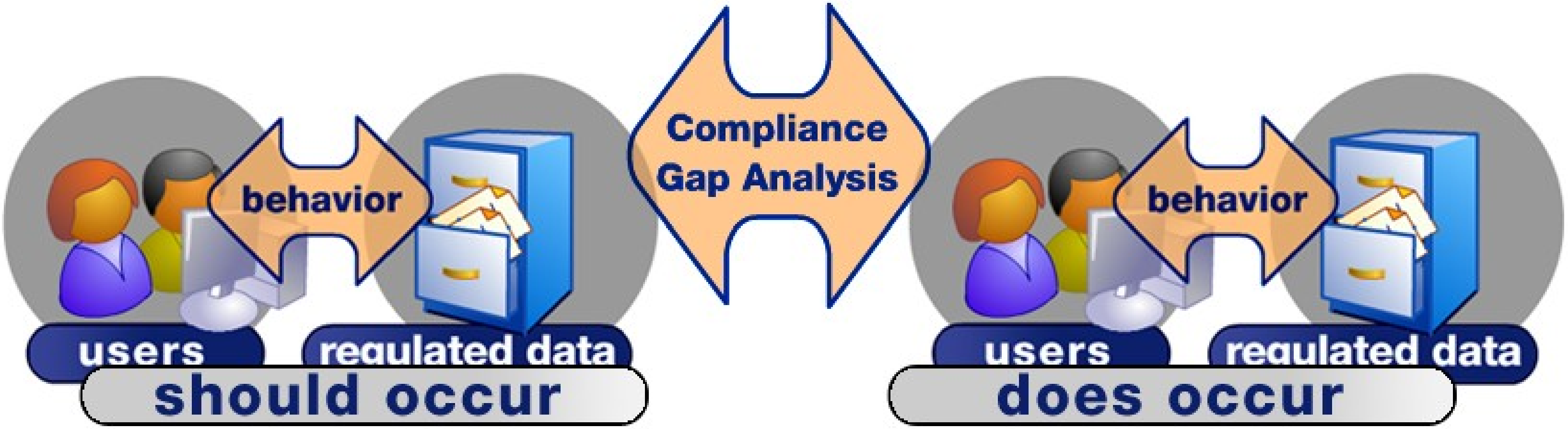
- Traditional Identity Management approach requires EITHER:
  - Each administrator to have a userid on every system they administer
    - Exponential increase in privileged userids
    - Increased risk of mismanagement of privileged userids
    - Increased userid administration costs
  - OR
  - Administrators share privileged userids
    - Risk of losing ‘accountability’
    - Issues with password management and security
    - Out of step with regulatory thinking
    -
- Privilege Identity Management combines the best features of both approaches, without the disadvantages

Privileged Identity Management - Components

- Credential Vault - Store privilege & shared accounts securely
- Identity Management Services
  - Workflow – including the ability to allow users to get access to privilege accounts, recertification, auditing/reporting
  - Privilege Account Management – Flexibility to allow users to have entitlements to shared accounts, securely ensuring maximum one person (or less) at a point in time knows the password
- Enterprise Single Sign-On
  - reducing complexity and allowing automation for usability
- Security Information and Event Management
  - for audit and compliance, reducing risk
- Vault as an extension of Identity Management infrastructure
  - Opportunity to reduce deployment and other costs

Security Information and Event Management

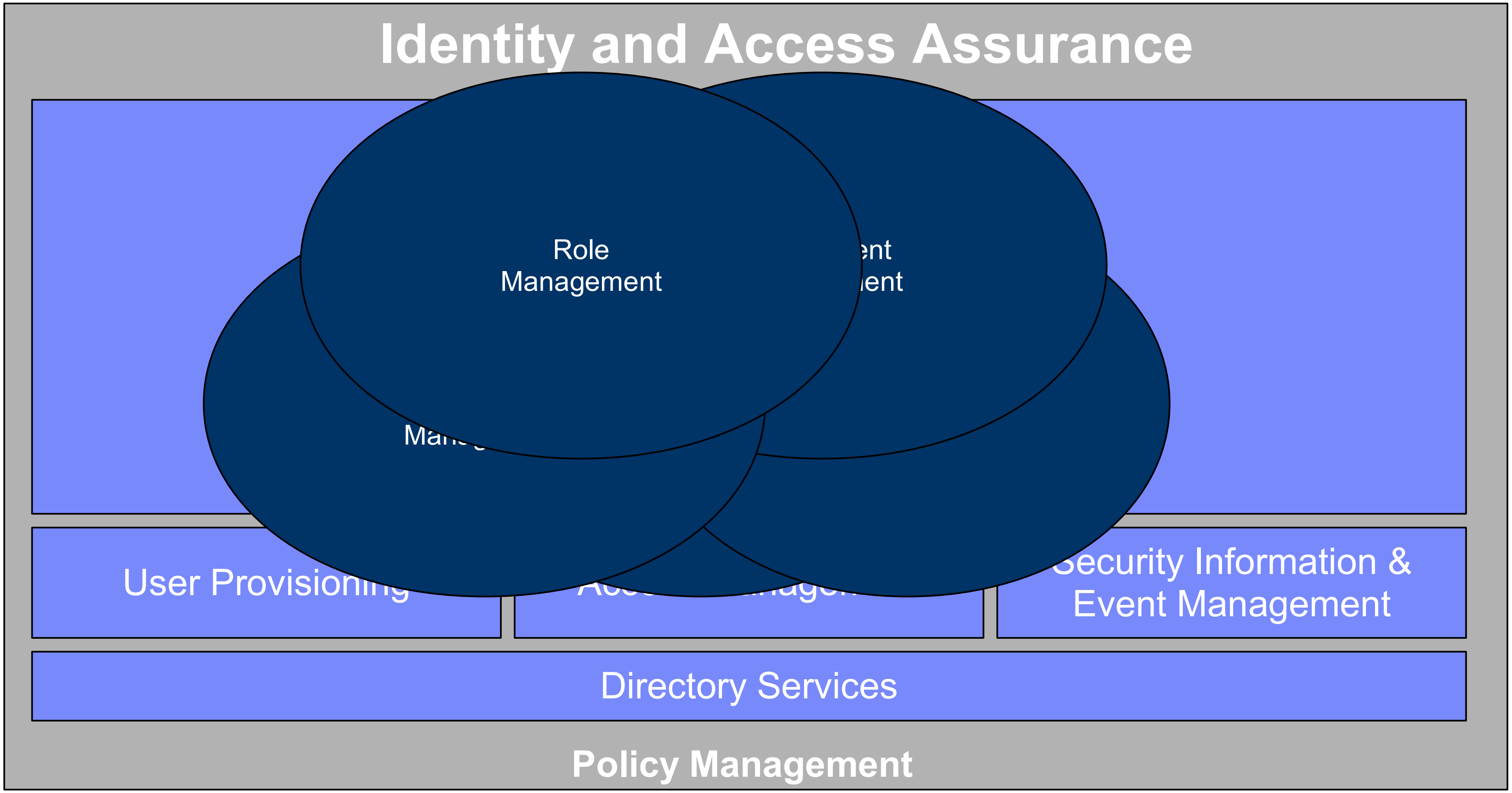
-
  - Compare desired versus actual behaviour ...



... like an auditor does.

What have users done with their rights?

- Closed Loop SIEM and IAM integration offers end-to-end identity management across the lifecycle
-
- Continual monitoring of users, their rights and what users have done with those rights
  - –
- Closed-loop user management and compliance, especially for privileged users
  - –
-
-



Identity and Access Assurance

Role
Management

ent
ent

Man

User Provisioning

Acc Manage

Security Information &
Event Management

Directory Services

Policy Management

Identity Assurance

Managing Identities, Roles and the Associated Governance Requirements

IBM Software

PCTY2010

Pulse Comes to You

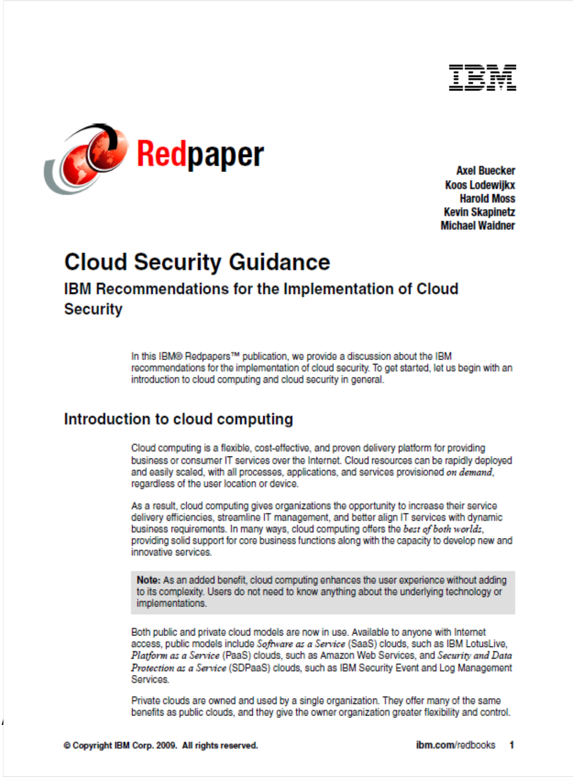
Optimising the World's Infrastructure

27 May 2010 London

IBM Cloud Security Guidance

- Based on customer interaction and cross-IBM research
- Highlights series of best practice controls
- 7 critical infrastructure components:
  - – Building a Security Program
  - – Confidential Data Protection
  - – Implementing Strong Access and Identity
  - – Application Provisioning and De-provisioning
  - – Governance Audit Management
  - – Vulnerability Management
  - – Testing and Validation

- http:/



IBM

Redpaper

Axel Buecker
Koos Lodewijkx
Harold Moss
Kevin Skapinetz
Michael Waidner

Cloud Security Guidance

IBM Recommendations for the Implementation of Cloud Security

In this IBM® Redpapers™ publication, we provide a discussion about the IBM recommendations for the implementation of cloud security. To get started, let us begin with an introduction to cloud computing and cloud security in general.

Introduction to cloud computing

Cloud computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications, and services provisioned *on demand*, regardless of the user location or device.

As a result, cloud computing gives organizations the opportunity to increase their service delivery efficiencies, streamline IT management, and better align IT services with dynamic business requirements. In many ways, cloud computing offers the *best of both worlds*, providing solid support for core business functions along with the capacity to develop new and innovative services.

Note: As an added benefit, cloud computing enhances the user experience without adding to its complexity. Users do not need to know anything about the underlying technology or implementations.

Both public and private cloud models are now in use. Available to anyone with Internet access, public models include *Software as a Service* (SaaS) clouds, such as IBM LotusLive, *Platform as a Service* (PaaS) clouds, such as Amazon Web Services, and *Security and Data Protection as a Service* (SDPaaS) clouds, such as IBM Security Event and Log Management Services.

Private clouds are owned and used by a single organization. They offer many of the same benefits as public clouds, and they give the owner organization greater flexibility and control.

© Copyright IBM Corp. 2009. All rights reserved. **ibm.com**/redbooks 1

Trademarks and Disclaimers

- Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries./ Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.
- The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.
- Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.
- All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
- Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.
- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.
- Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.
- Photographs shown may be engineering prototypes. Changes may be incorporated in production models.
- © IBM Corporation 1994-2010. All rights reserved.
- References in this document to IBM products or services do not imply that IBM intends to make them available in every country.
- Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at http://www.ibm.com/legal/copytrade.shtml.