



# Identity and Access Management Governance



Glen Gooding  
AP Security Sales Leader



## Agenda

- The IBM Security Framework and Managing Identities
- Technical Overview of Tivoli Identity Manager
  - Core User Provisioning Functionality
  - Identity Governance Functionality
- Tivoli Security Information and Event Manager
  - Log Management
  - Enterprise wide compliance engine
- Identity & Access Assurance
  - Architectural Overview
- Privileged Identity Management
  - Watching the admins
- Why Choose IBM and TIM?





# Background...

## The IBM Security Framework and Managing Identities



# Welcome to the **smart planet**... *and a smarter infrastructure*

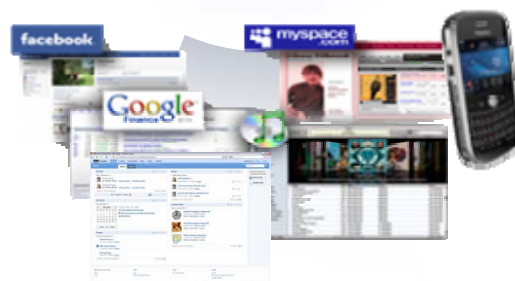


Globalization and Globally Available Resources

Billions of mobile devices accessing the Web



Access to streams of information in Real Time



New Forms of Collaboration

**New possibilities.**  
**New complexities.**  
**New risks.**



## IBM's comprehensive approach to managing risk end-to-end

Security is a growing focus area as organizations try to:

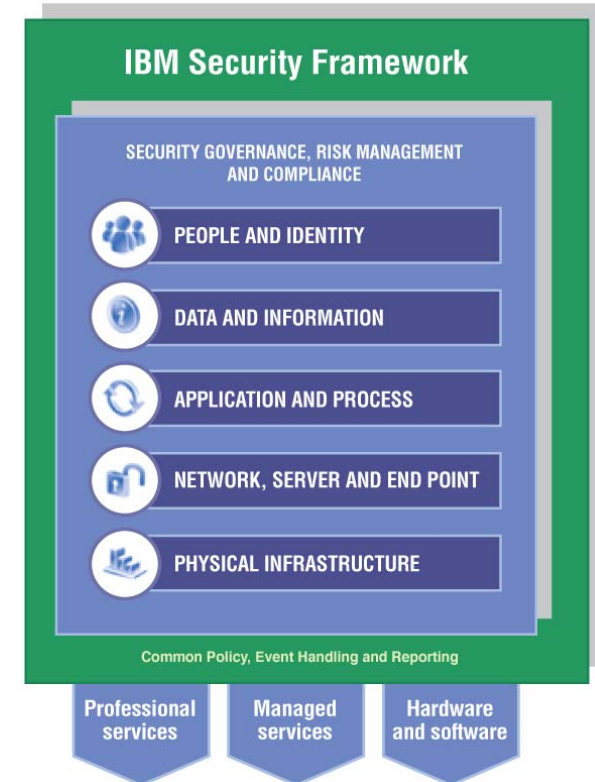
- Stay ahead of evolving threats
- Take advantage of new business opportunities
- Pursue more efficient IT business models (e.g. cloud computing)

IBM Security Framework, introduced in 2007, is embraced by customers to:

- Orchestrate their strategy across a broad set of issues in each domain
- Identify gaps and prioritize investment to meet their security goals
- Implement security where their specific environment most requires it

The Framework also guides IBM solutions:

- Accelerated, customer-driven integrations across IBM brands
- Improved customer-facing aspects of IBM Security

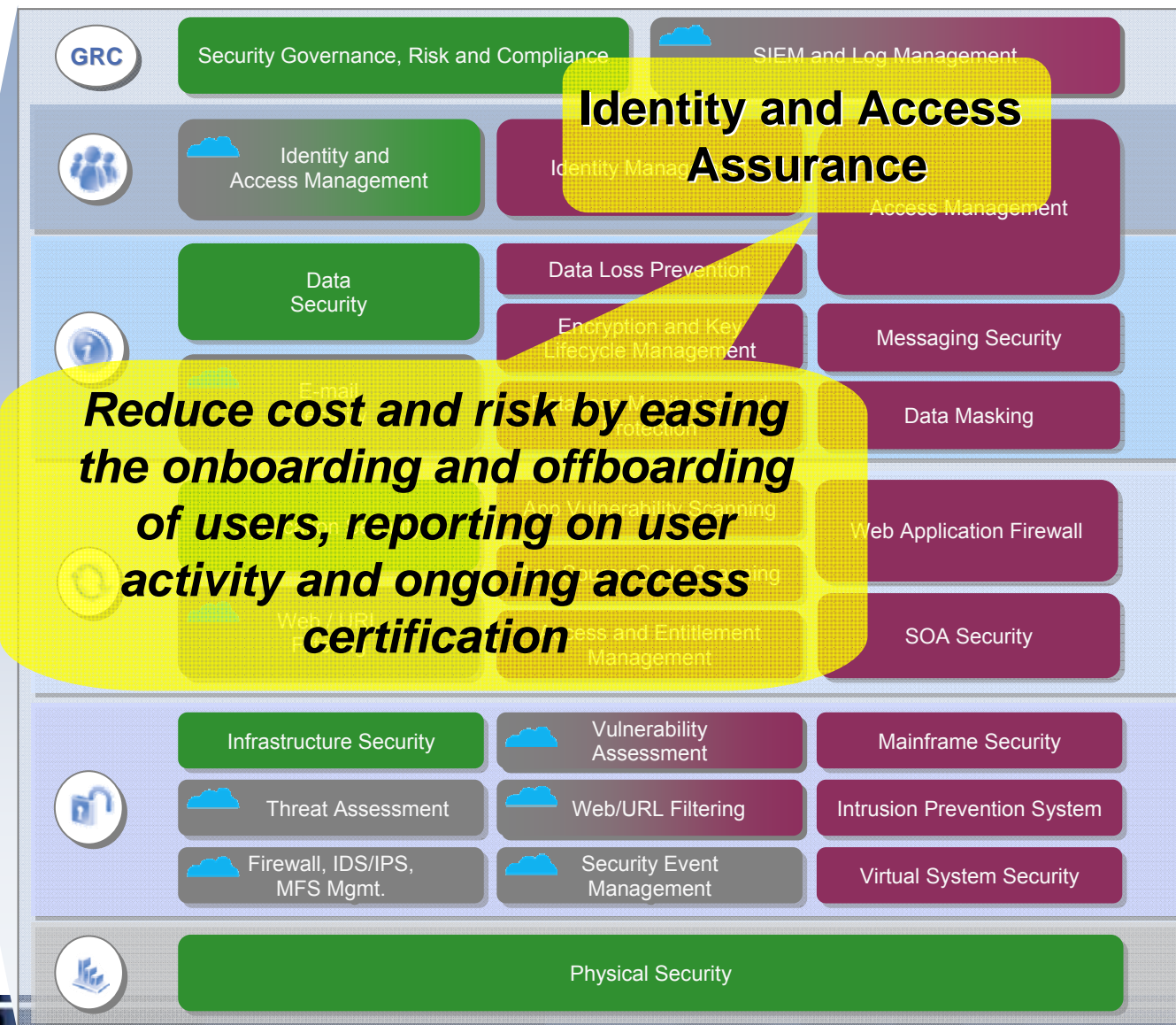


# IBM Security Framework – Products and Services

= Professional Services

= Cloud-based & Managed Services

= Products



# Identity and Access Assurance drivers remain consistent

## Governance, risk and compliance

- Driver
  - Deliver accountability and audit trail for external regulatory mandates and internal policies
- Trigger
  - Time/cost of compliance preparation
  - Failed compliance audit
  - Access certification requirements

**PCI-DSS**      **HIPAA**  
**GLBA**          **FISMA**  
**Basel II**        **SOX J-SOX**  
**ITAR**          **ISO 27001**



## Security

- Driver
  - Mitigate risk of fraud, theft of IP, loss of customer data, etc...
- Trigger
  - Prior incident/compromise
  - Poor visibility of risk based on user access
  - Stalled or expanding user provisioning project

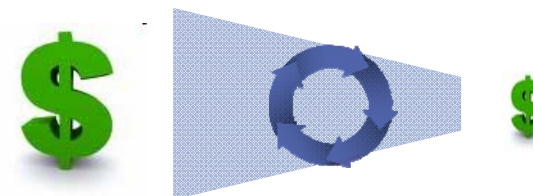
**PCWorld**

**Nearly Two-Thirds of Ex-Employees Steal Data on the Way Out**

59 percent of workers who left their positions took confidential information with them

## Cost reduction (via automation)

- Driver
  - Streamline business and IT processes for user access to resources
- Trigger
  - Cost and time associated with manual administration of user access
  - Stalled or expanding user provisioning project



... but some customers experience pains with current solutions

User provisioning products deliver value, but deployments **can stall without scalable administration**

- Role and entitlement management can deliver an abstraction to manage administration and access

Web access management solutions **fail when not integrated** to offer business context

- Entitlement management can provide business context (e.g. location, data classification, time of day, etc...) for access control policies

Inability to manage **business conflicts** that arise due to **granting of user access**

- Separation of duty policies can manage access conflict

Lack of **flexible and continuous validation** of user access and remediation

- Access certification tightly integrated with user provisioning can deliver validation and remediation of user access

**Poor integration** with security information and event management for **user activity monitoring**

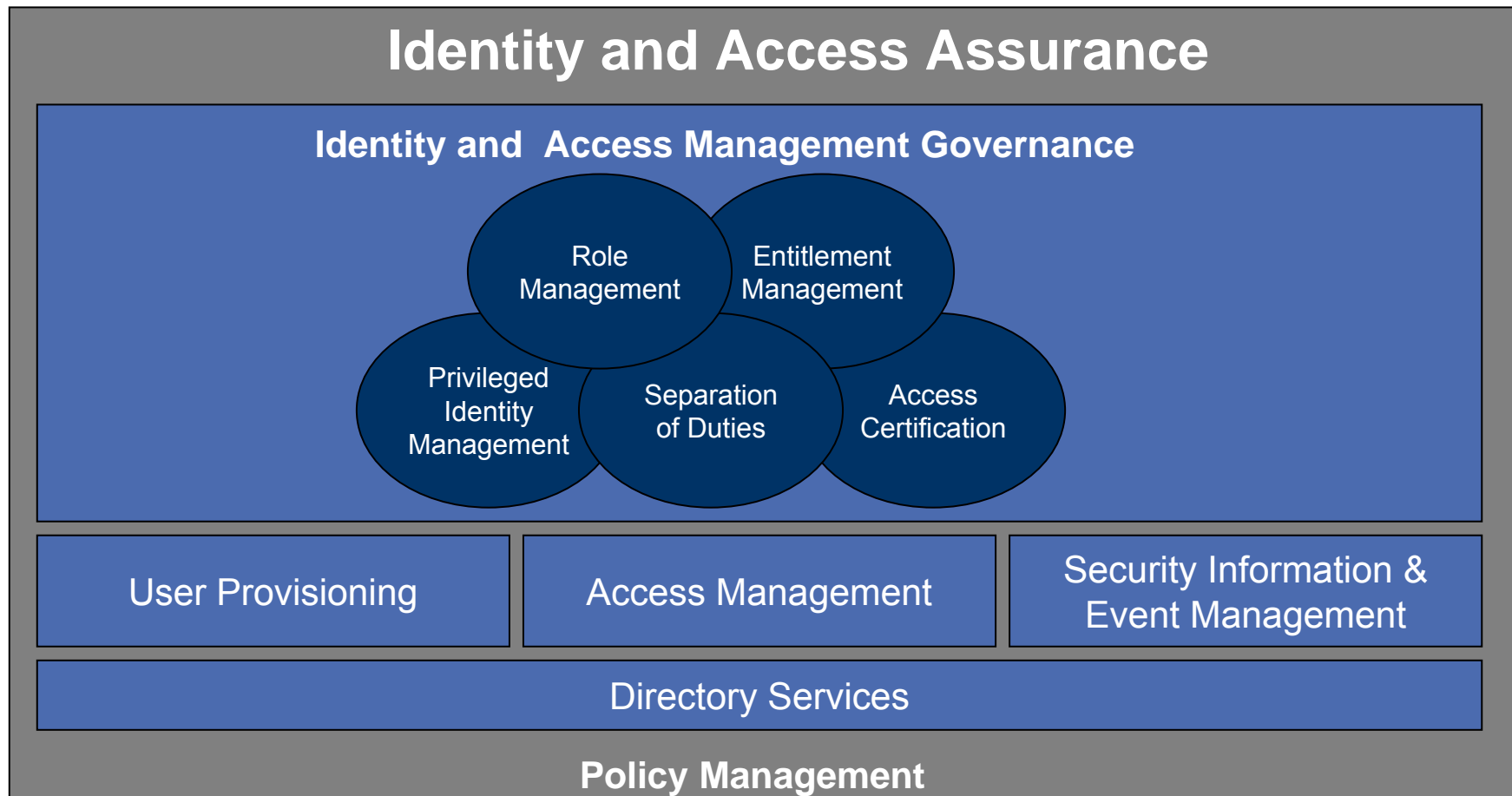
- Log collection is good, integrated suspension of access based on abnormal activity is better

Desire for more integrated/holistic **policy-based governance** around IAM





# Identity and Access Assurance for Business Solutions

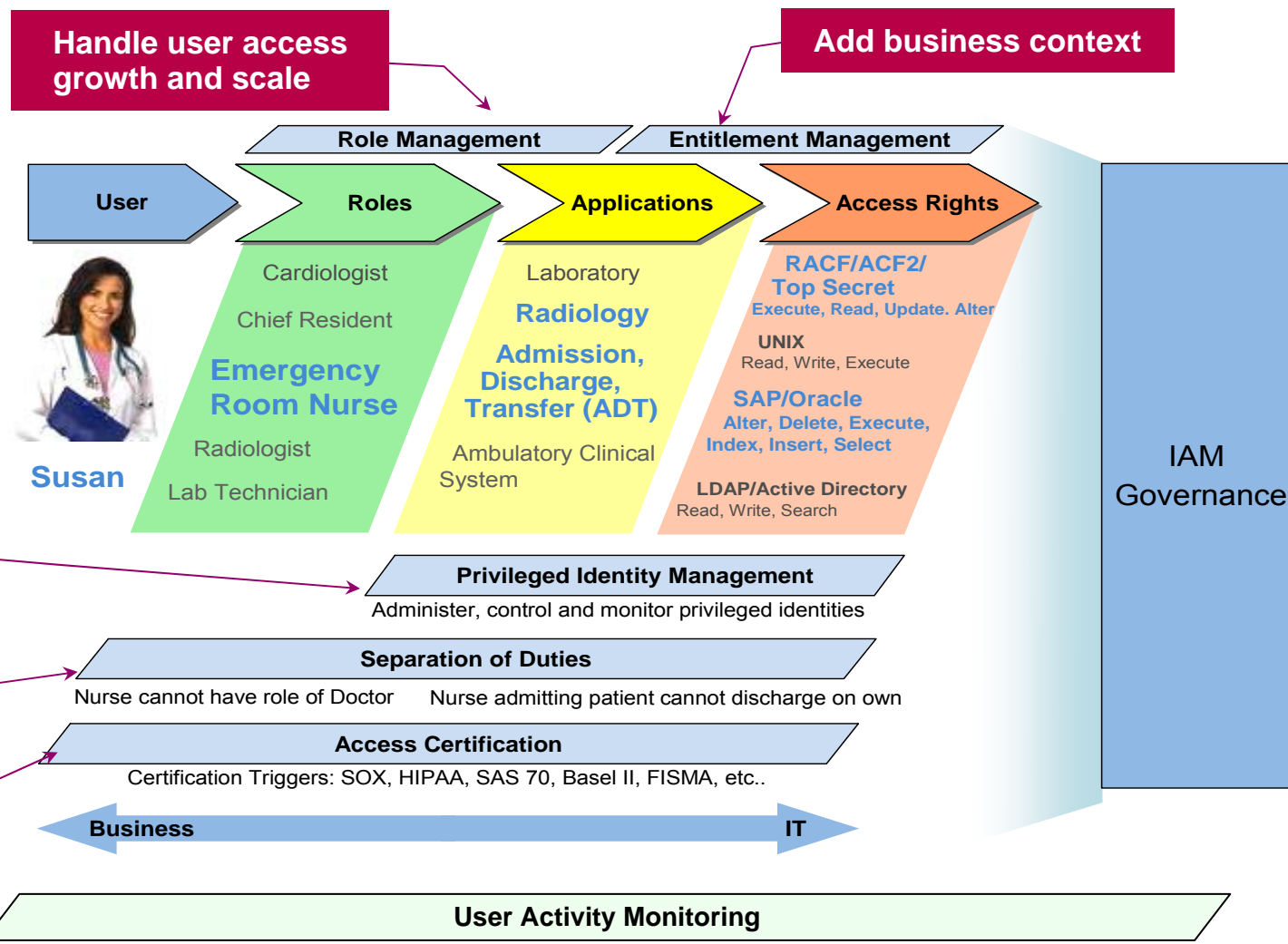


Identity and Access Assurance governs and enforces access while providing the closed loop to audit/compliance



# IBM IAM Governance delivers a bridge between business and IT, to meet the evolving access mgmt customer requirements

**Example: Hospital Access Policy**  
 Nurse has read-only access to confidential patient data in the ADT application only within the hospital network



**Resolve weak admin access controls**

**Handle business access conflict**

**Avoid access loopholes**

**Compliance and policy effectiveness**

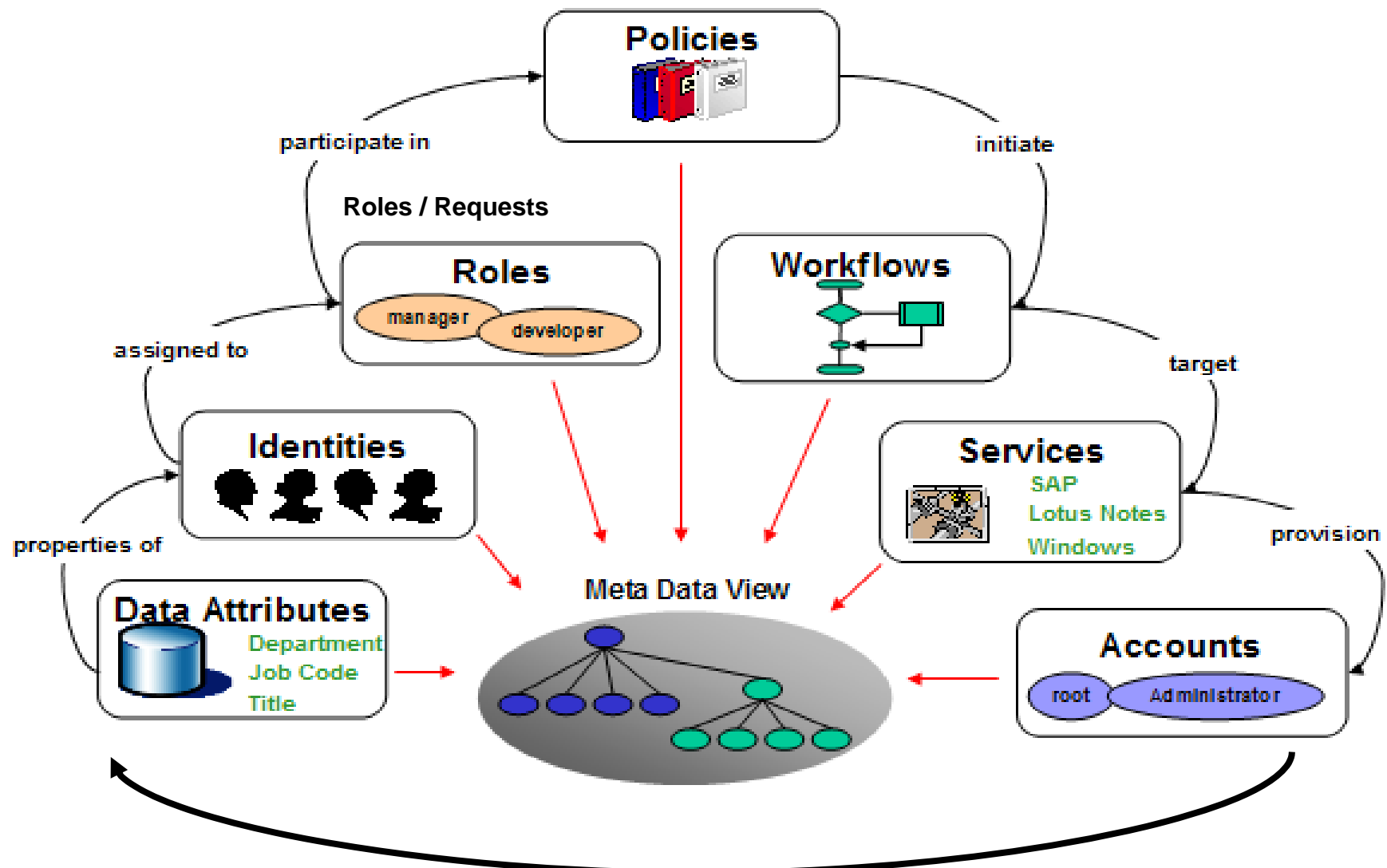


# An Overview of Tivoli Identity Manager

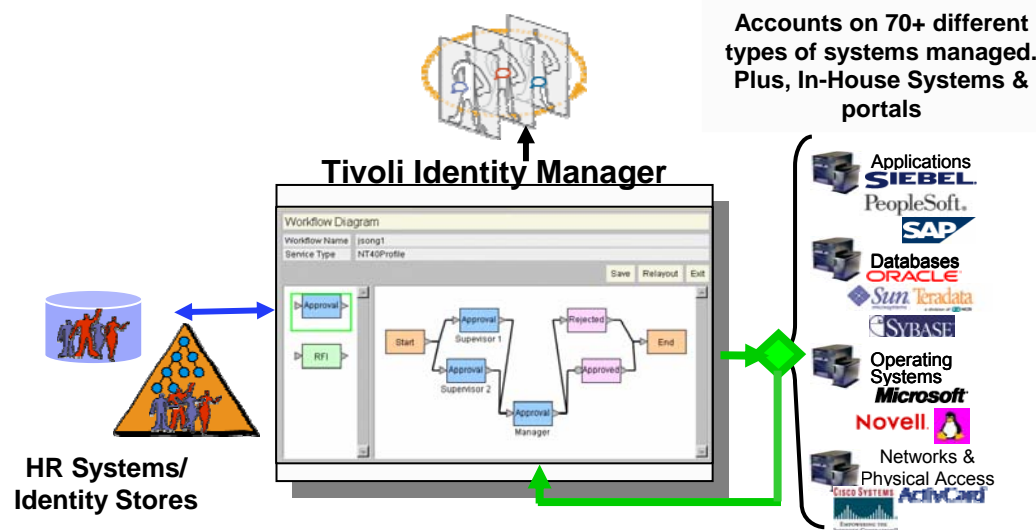
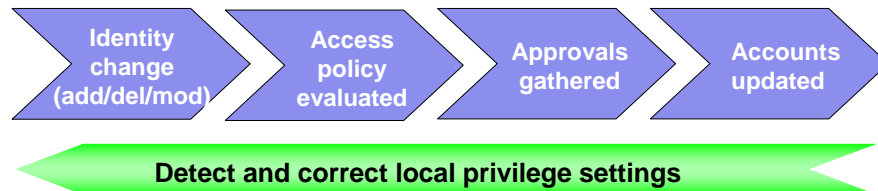
Core User Provisioning Functionality



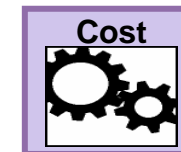
# Tivoli Identity Manager – How it works



# Tivoli Identity Manager automates, audits, and remediates user access rights across your IT infrastructure

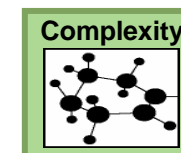


- Know the **people** behind the accounts and **why** they have the access they do
- Automate user privileges lifecycle across entire IT infrastructure
- Fix non-compliant accounts
- Match your workflow processes



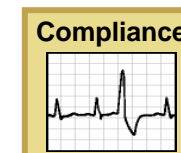
## Reduce Costs

- Self-service password reset
- Automated user provisioning



## Manage Complexity

- Consistent security policy
- Quickly integrate new users & apps



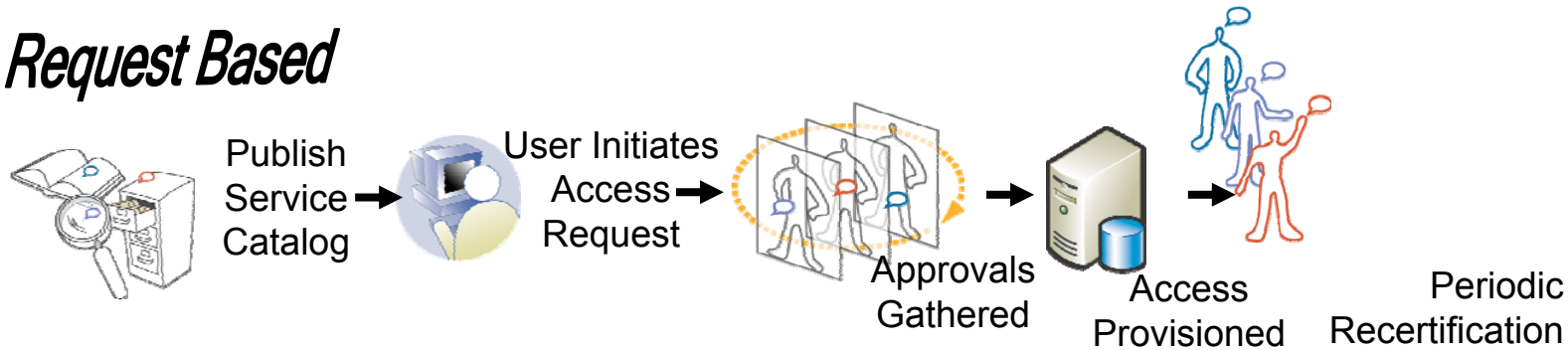
## Address Compliance

- Closed-loop provisioning
- Access rights audit & reports

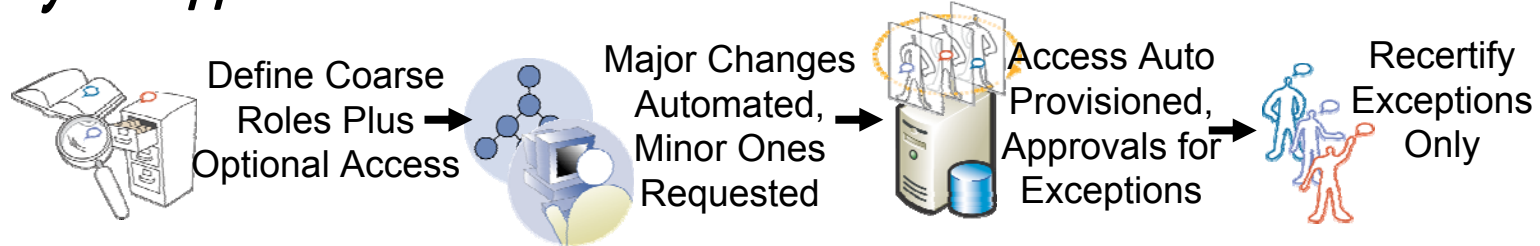


# TIM offers multiple ways to administer user access rights

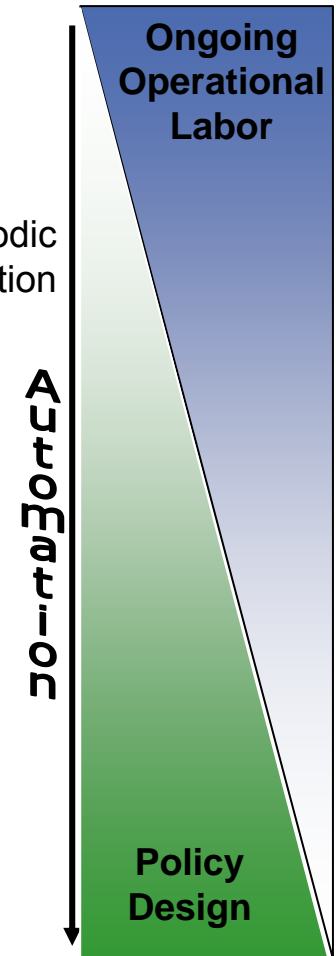
## Request Based



## Hybrid Approach



## Role Based



## Tailored user interface views for IT and business users

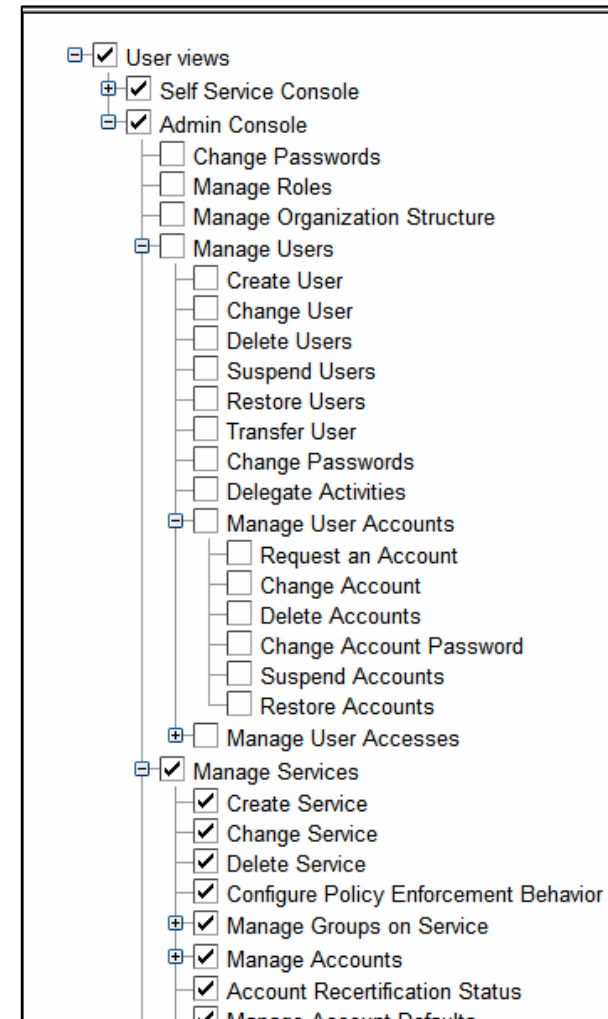
### Separate Self-service and Admin Consoles

Designed with more than just system administrators in mind

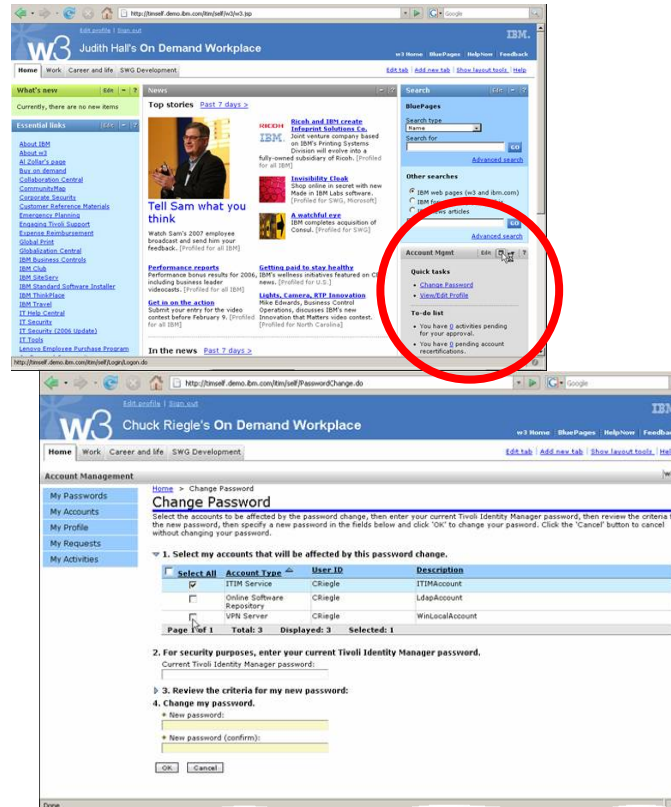
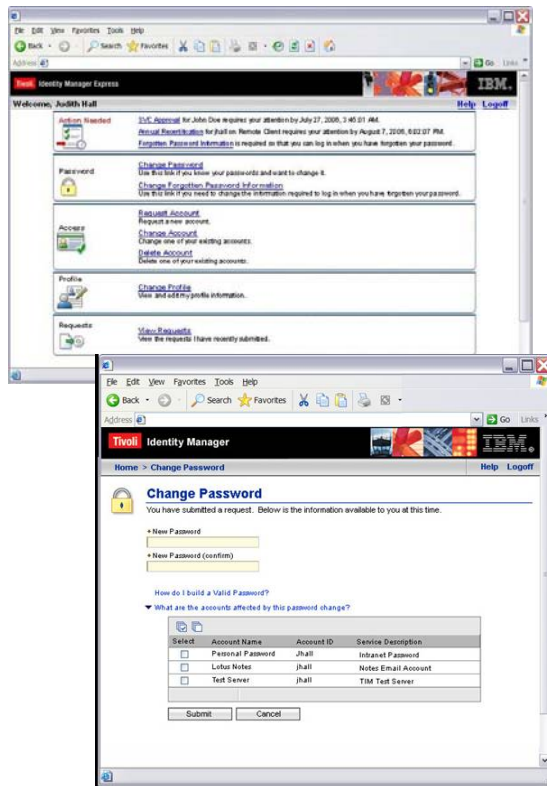
- TIM administrators
- Help desk assistants
- Service/Application owners
- Managers
- Auditors
- End users

Customize default user views and security settings or create additional views unique for users in your organization

Intuitive user interface shows users only what they need to do their jobs



# Tailored UI's, Customizable Self-Service User Interface, Accelerate ROI



## Self-Service for end-users

- Request Access
- Reset Password
- Approvals

## Customizable

- Update via style sheets
- Portal-friendly

## Upgrade-friendly

- Customizations maintained
- New features added

**Help Desk costs \$20-per-call for password resets**  
Gartner Group

**Employees request an average of 3-4 resets per year**  
Meta Group



# Make the “simple things simple” ...while still allowing for advanced customization

The screenshot displays the IBM Tivoli Identity Manager console in Microsoft Internet Explorer. The main content area is titled "Manage Policies > Manage Recertification Policies > Policy". It provides instructions: "To configure a policy, select simple and complete the configuration fields, or select advanced mode to use the workflow editor. When you are done, click the appropriate button." Below this, the "Configuration mode" section has two radio buttons: "Simple" (unselected) and "Advanced" (selected). A red circle highlights the "Advanced" option. Below the configuration mode are sections for "Operation Diagram" and "Policy" details.



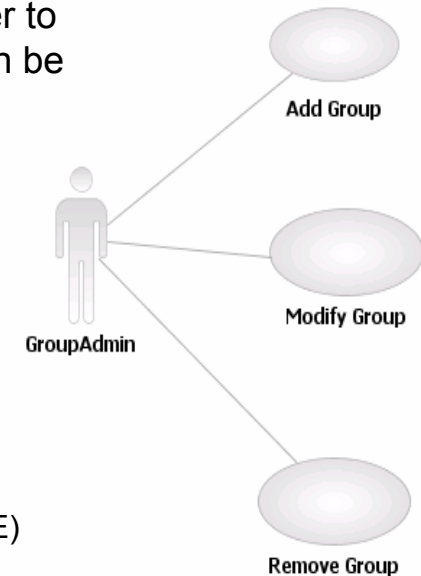
## Group management simplifies and reduces cost of user administration

### Customer challenge – business delay

- Business delay while TIM administrator waits for native application owner to create group, then TIM reconciliation with target system before users can be assigned to groups

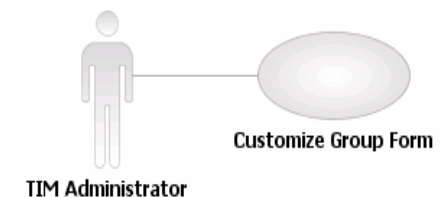
### Answer: TIM group management

- Administration of groups on the provisioning target
  - Create New Groups
  - Delete existing Groups
  - Modify – add, remove members
- Nesting of groups supported for those targets that support nesting
- Eligible provisioning targets
  - LDAP, Active Directory, Unix (AIX, HP-UX, Solaris) and Linux (RHEL and SuSE)
  - Additional targets via TIM adapter updates



The screenshot shows a web-based form for creating a group. The title is 'Manage Groups > Create Group > General Information'. Below the title is a brief instruction: 'To create a group of type Windows Active Directory Groups on OFN Active Directory service, type the name of the group and any other information on the form. Then click Next.' The form contains several fields:
 

- \*Group unique name: ProjectA
- Common Name: Project A
- Container: ou=ofn, with Search... and Clear buttons.
- Group Type: Security (dropdown menu)
- Group Scope: Local (dropdown menu)
- Member of: (empty field)



## Centralised password mgmt enhances security and reduces help desk costs

### Self-service password management across all systems

- Apply targeted or global password rules
- Verify compliance with target systems

### Password synchronization

- Propagate and intercept
- Integrate with Windows password mgmt

### Challenge/response questions for forgotten user ids and/or passwords

- User or site defined questions
- Email notification

### Integration with TAM E-SSO

- Desktop password reset/unlock at Windows logon prompt
- Provisioning user access to TAM E-SSO

**Tivoli Identity Manager**

Home > Change Password Help Logoff

### Change Password

You have submitted a request. Below is the information available to you at this time.

+ New Password

+ New Password (confirm)

How do I build a Valid Password?

▼ What are the accounts affected by this password change?

Select	Account Name	Account ID	Service Description
<input type="checkbox"/>	Personal Password	Jhall	Intranet Password
<input type="checkbox"/>	Lotus Notes	jhall	Notes Email Account
<input type="checkbox"/>	Test Server	jhall	TIM Test Server

Submit Cancel



# TIM reporting system facilitates audit requirements and integrates reporting across Tivoli

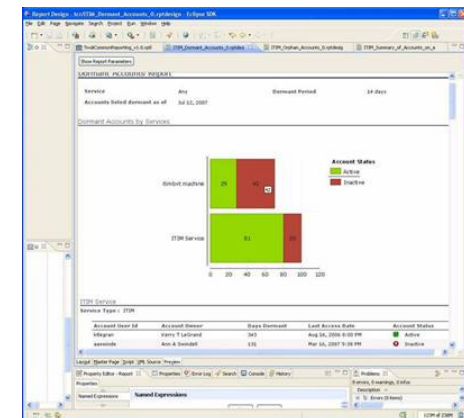
## TIM Reporting

- Aimed at the IT Administrator
- Uses TIM reporting database and schema
- Supports large PDF reports
- BIRT designs for TIM reports



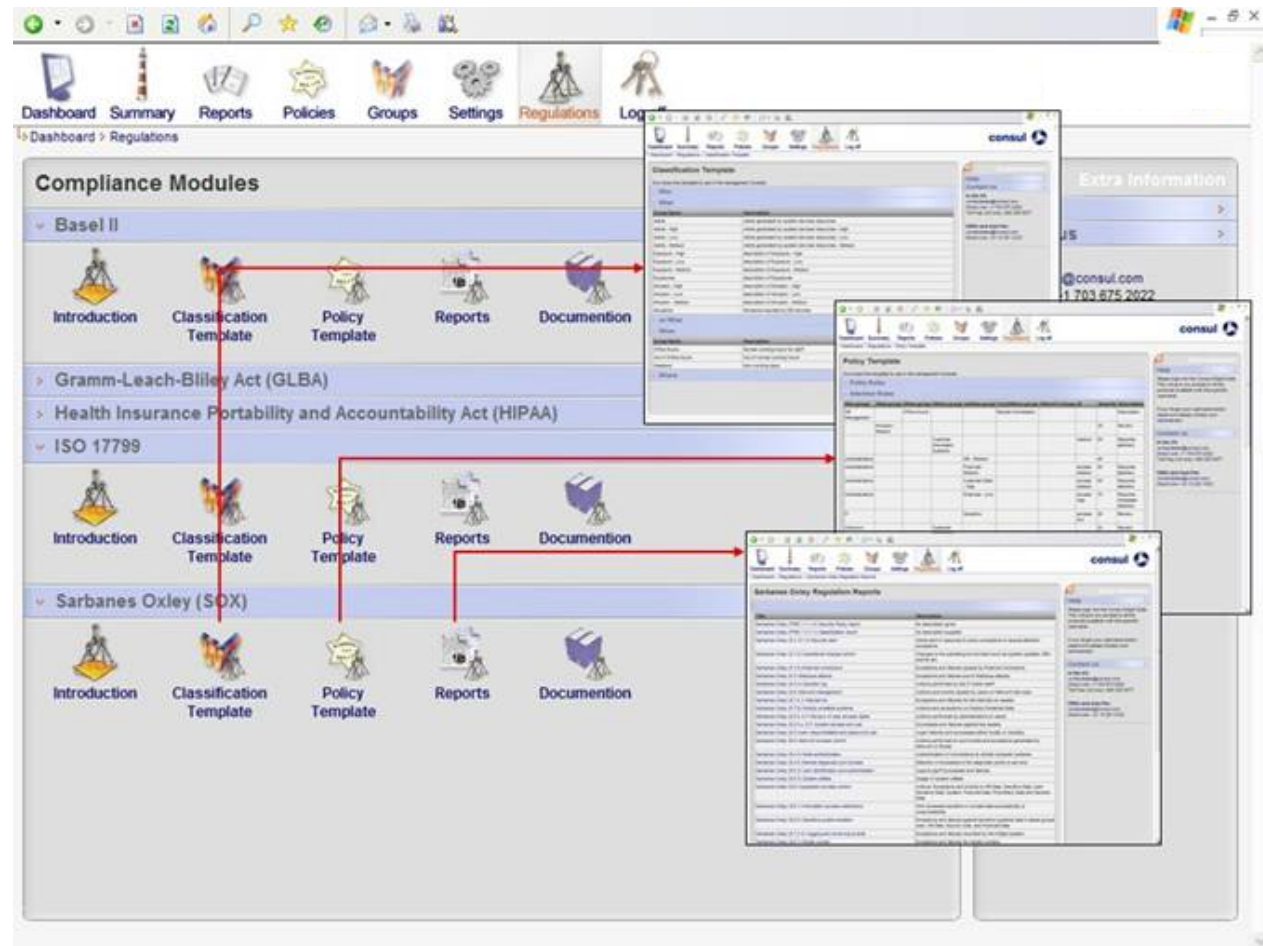
## Tivoli Common Reporting Module

- Report Administration
  - Import of TIM report pack, report scheduling, accessible via email and URL
- Report customization using the Eclipse BIRT designer
- Common Console for Report Viewing



# Closed loop management via integration with Tivoli Security Information Event Manager

TIM integration with TSIEM provides pre-built reports for regulation and best practices





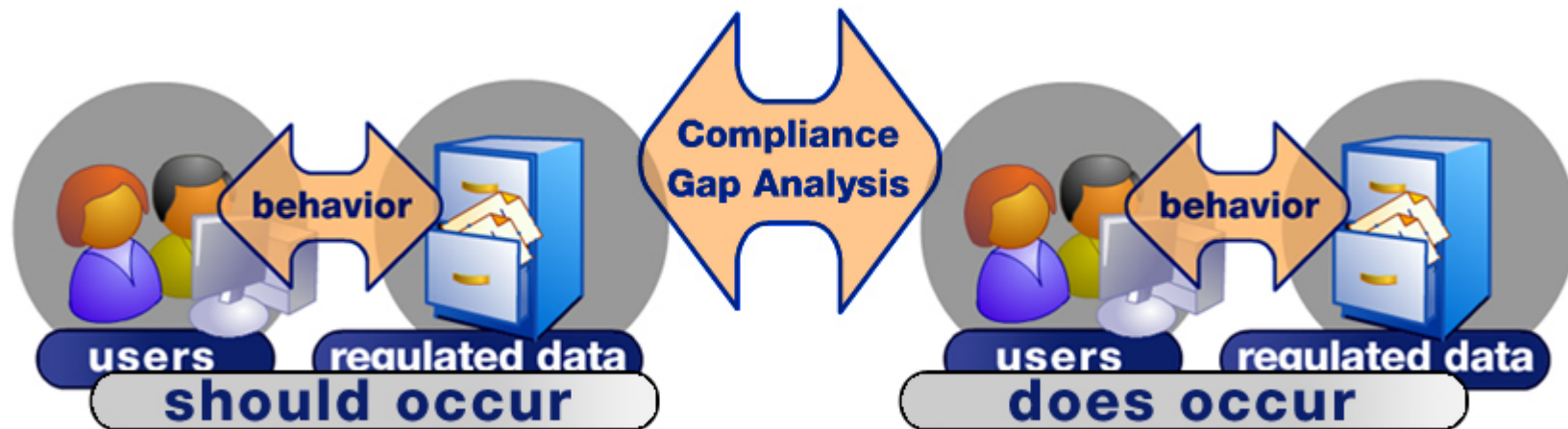
# Tivoli Security Information and Event Manager

Enterprise wide security compliance reports  
Log management



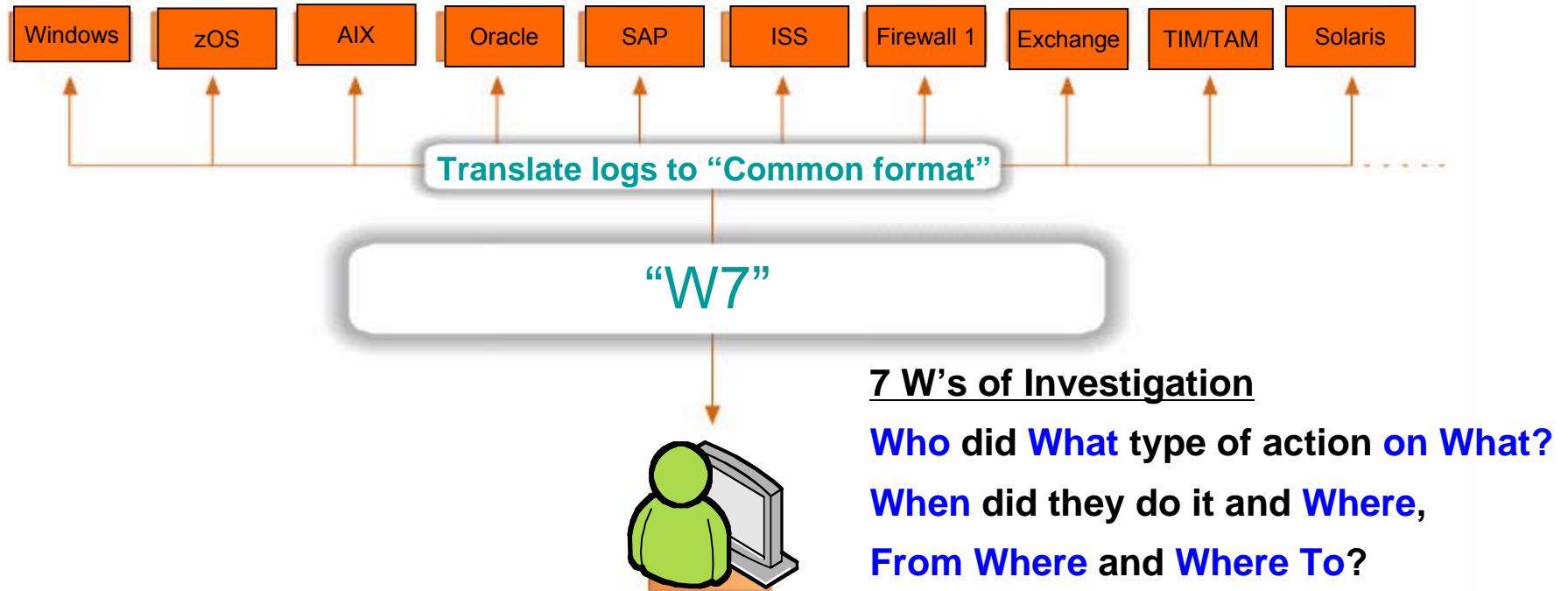
## TSIEM enables governance

Compares desired versus actual behavior...



... like an auditor does.

# All Logs in Your Enterprise in a Single Language



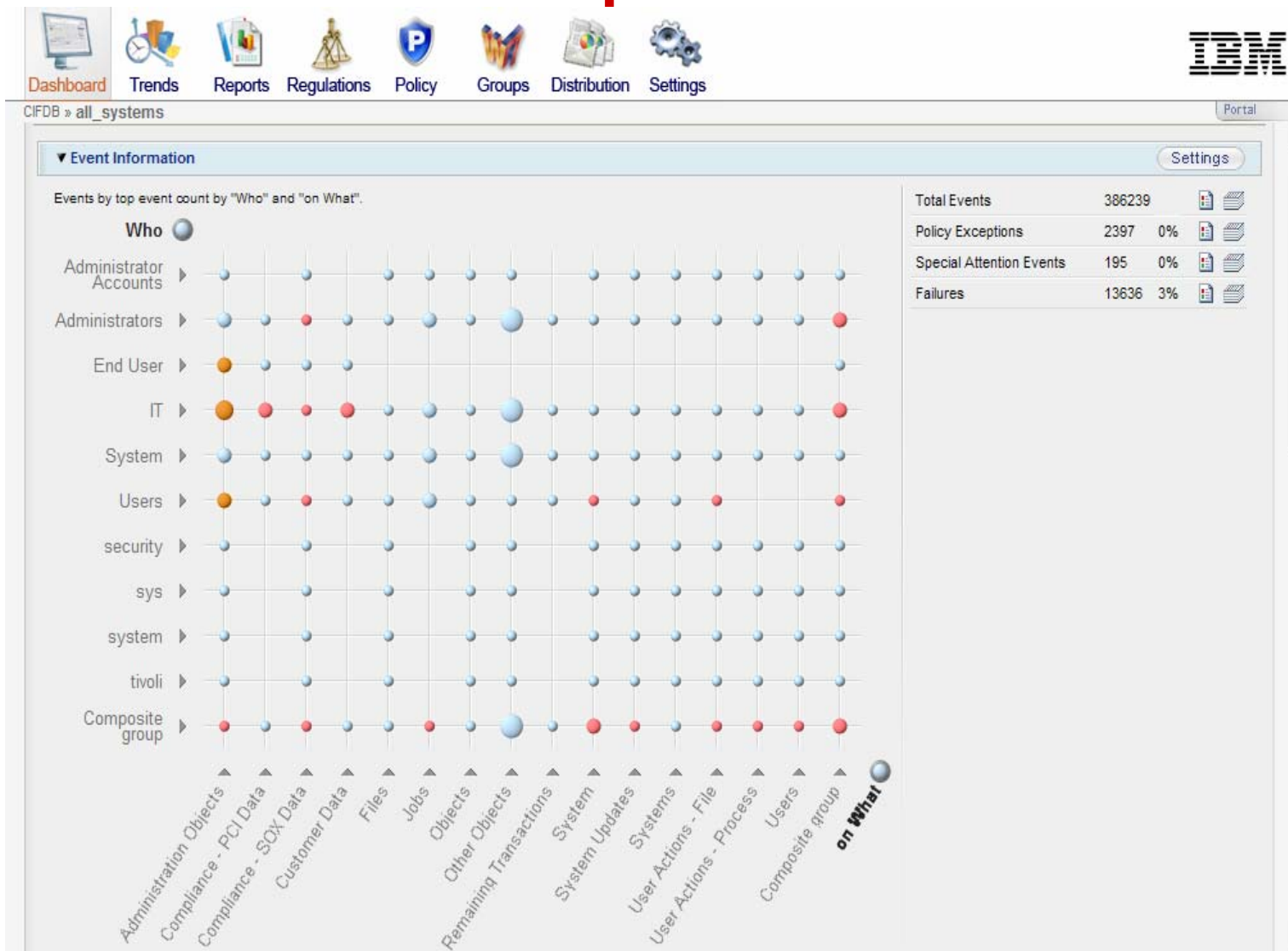
**TSIEM's W7 saves your information security and compliance staff time and money.**

- reduces the need for skilled staff
- produces reports auditors can understand
- automates monitoring across the enterprise.





# Demonstrate Compliance



- Quick Drill-down
- Policy Exceptions
- Special Attentions
- Failures
- Trends
- Reporting DBs
- Aggregation DBs
- Enterprise Overview
- Reports Distribution
- Self-audit

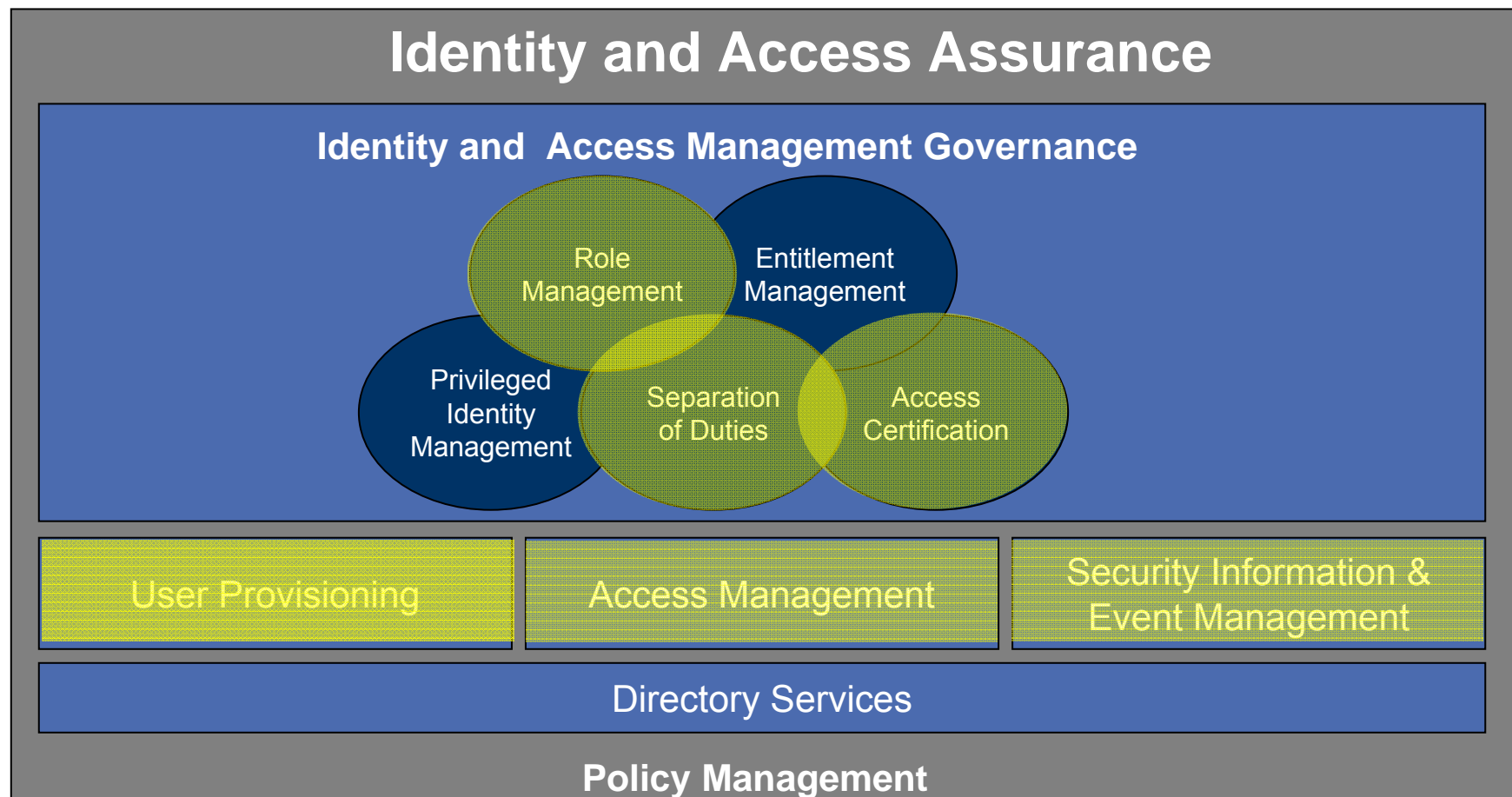


# Tivoli Identity Manager

Identity Governance Functionality



# Identity and Access Assurance for Business Solutions



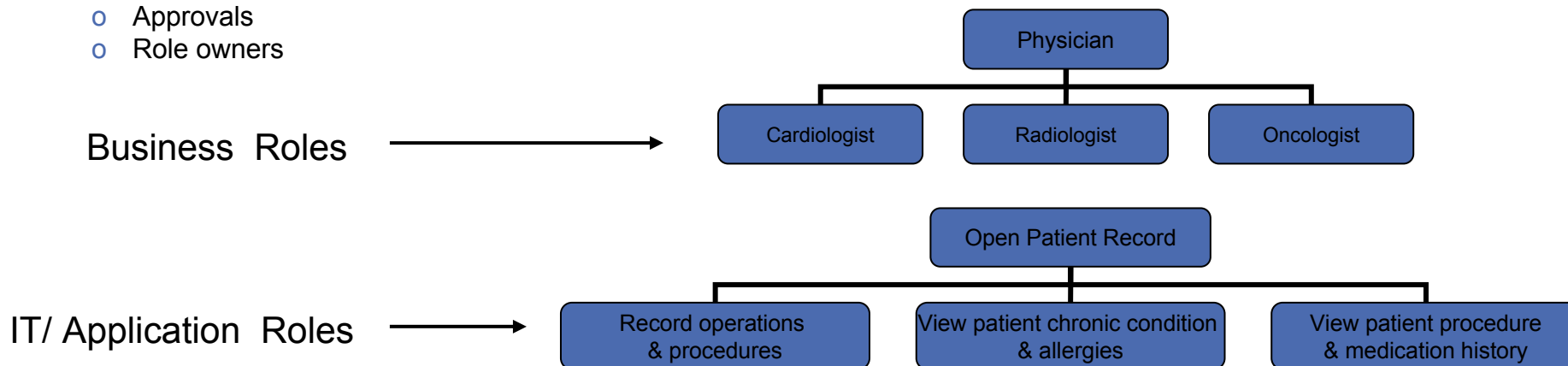
## Role management: Hierarchy simplifies & expands automation of user access

### Business challenge

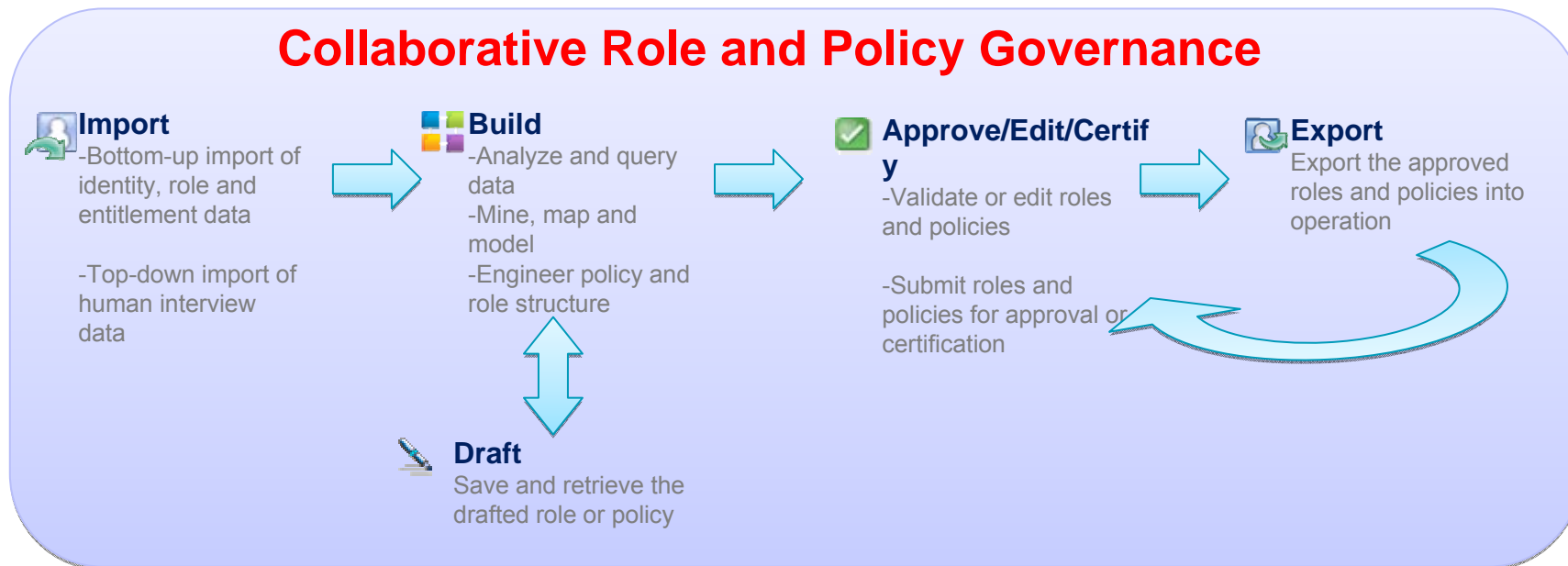
- Administration of user access can be increasingly complex and time consuming through the direct user-permission mapping

### TIM capabilities

- Establish parent/child role relationship and apply inheritance through role membership
  - Add or remove roles as members to other roles
- Parent roles can have multiple children
  - Physician = parent role
  - Cardiologist, Radiologist = child roles
- Child roles can have multiple parents
  - Cardiologist = child role
  - Physician, Health care practitioner, Employee = parent roles
- Inheritance flows to all objects that use roles
  - Provisioning policy
  - Approvals
  - Role owners



# Role Management: modeling and lifecycle management of roles and policies



## Role Modeling Assistant and Role Management Assistant

Import data from interviews and data sources

Analyze and engineer roles

Approve, edit or certify roles

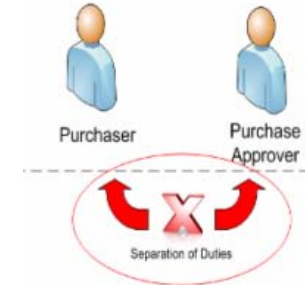
Export roles into Tivoli Identity Manager for operational usage



# Separation of duties enhances security and compliance

## Business challenge

- Avoiding business conflicts that could heighten their risk exposure
  - e.g. same person making purchases is also allowed to approve them
- Exclude users from having access rights that create a business conflict



## TIM capabilities

- Provides preventative and detective control over role conflicts by creating/modifying/deleting SoD policies that exclude users from having membership to conflicting roles
  - User cannot be a member of Role A and Role B
  - User may not have membership to more than N roles within accounts receivable process
- Upon assigning or requesting access, TIM detects if a conflicting rule exists and prevents a violation from occurring
- Can support exemptions via approval workflow process when a violation is detected
- Violation and exemptions auditing via reports, which helps prevent or highlight inappropriate use of privileges

### Separation of Duty Policy Violations

The request when adding members to the role Log Receipt of Medications on February 16, 2009 has caused separation of duty policy violations.

#### Separation of Duty Policy Violation Details

The separation of duty policy violation details are specified in the following table. Click Submit to add members to this role with separation of duty policy violations.

Person Name	Rule	Roles in Conflict
Judith Hill	Controlled Substances Inventory Mgmt	Log Receipt of Medications, Dispense Medication App Authority



# TIM access recertification facilitates compliance

## Customer challenge

- Compliance – enabling an access validation process to those who can responsibly and accurately make that decision

## TIM capabilities

- 3 types of recertification policies to validate continued need for resources
  1. Account recertification policies
    - Account recertification policies target accounts on specific services
  2. Access recertification policies
    - Access recertification policies target specific accesses (in decipherable terms, i.e. AD group UK3g8saleww\_R = sales pipeline portlet)
  3. User recertification policies
    - A type of certification process that combines recertification of a user's role, account and group membership into a single activity

**Reviewer Action**

Indicate whether or not Barbara Cash still requires each of the following roles:

\* Please note that all items require a decision

Roles	Description	Still Required	<a href="#">All</a>   <a href="#">None</a>
Project A	access to resources needed for project A	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Project C	access to resources needed for Project C	<input type="radio"/> Yes <input type="radio"/> No	

Indicate whether or not Barbara Cash still requires each of the following accounts and groups:

\* Please note that all items require a decision

Accounts and Groups	Description	Still Required	<a href="#">All</a>   <a href="#">None</a>
bcash on Access Manager for .NET Banking App	Access Manager on ADAM directory	<input type="radio"/> Yes <input type="radio"/> No	<a href="#">All</a>   <a href="#">None</a>
◆ Branch Teller	Branch Teller	<input checked="" type="radio"/> Yes <input type="radio"/> No	
bcash on LedgerAccount	Reinsurance Satellite Ledger System	<input checked="" type="radio"/> Yes <input type="radio"/> No	



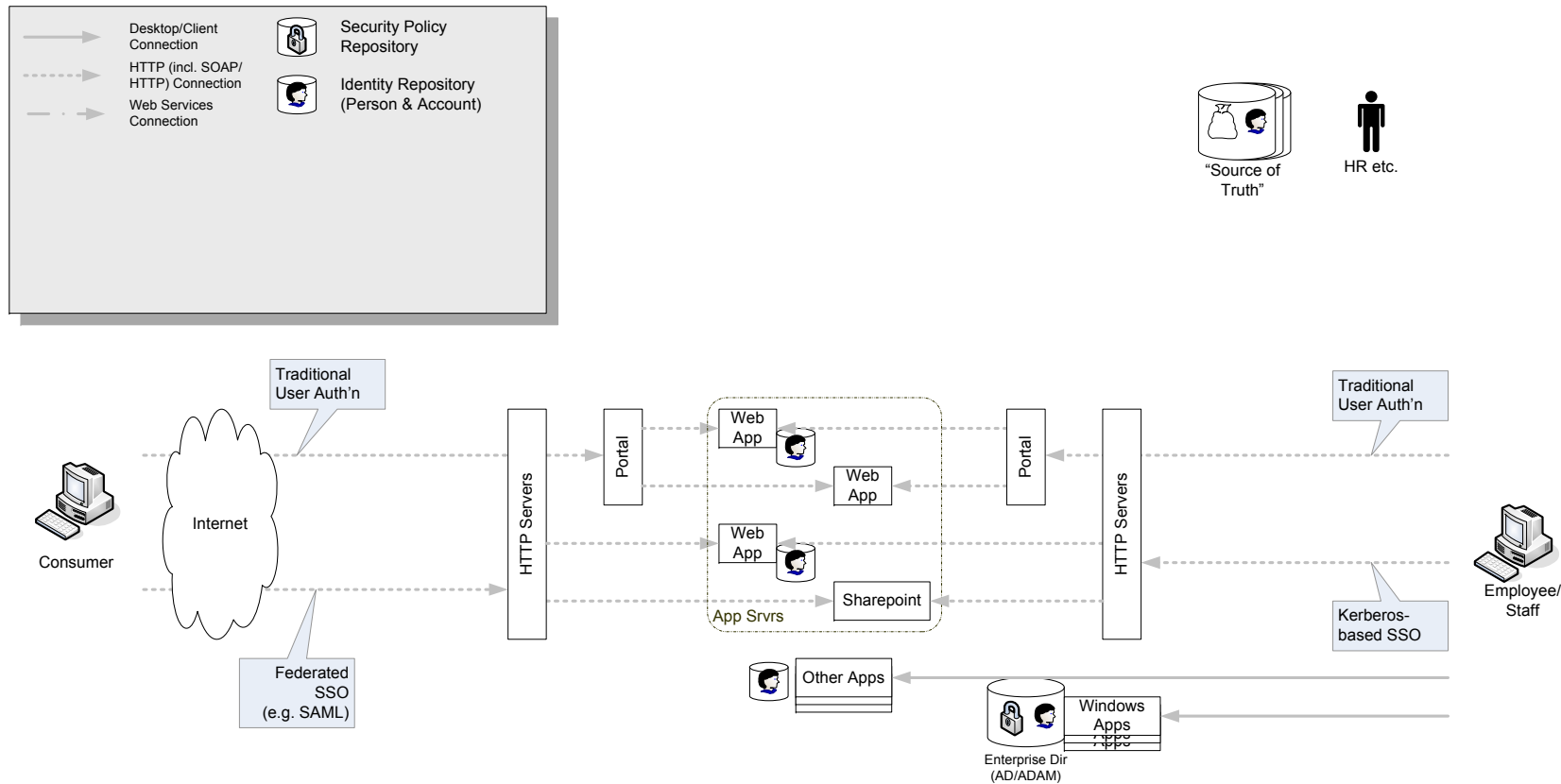


# Identity and Access Assurance – Architectural Overview

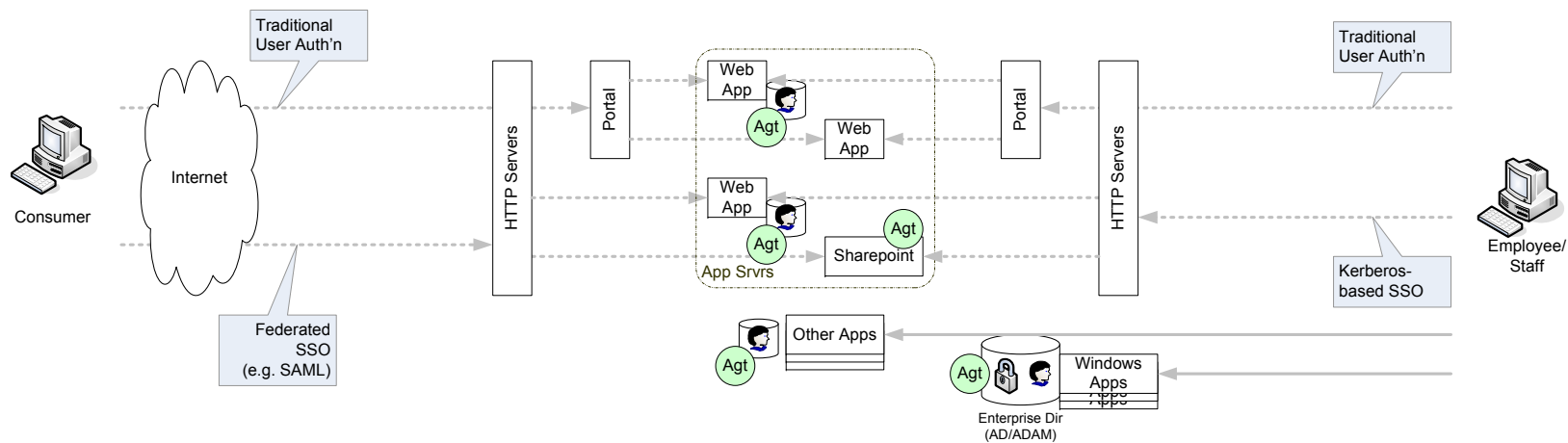
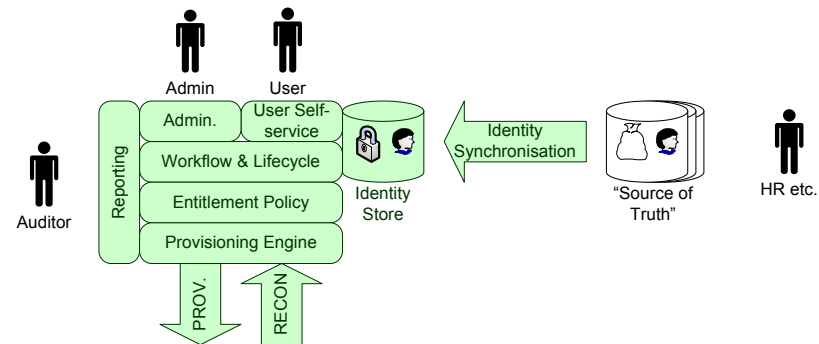




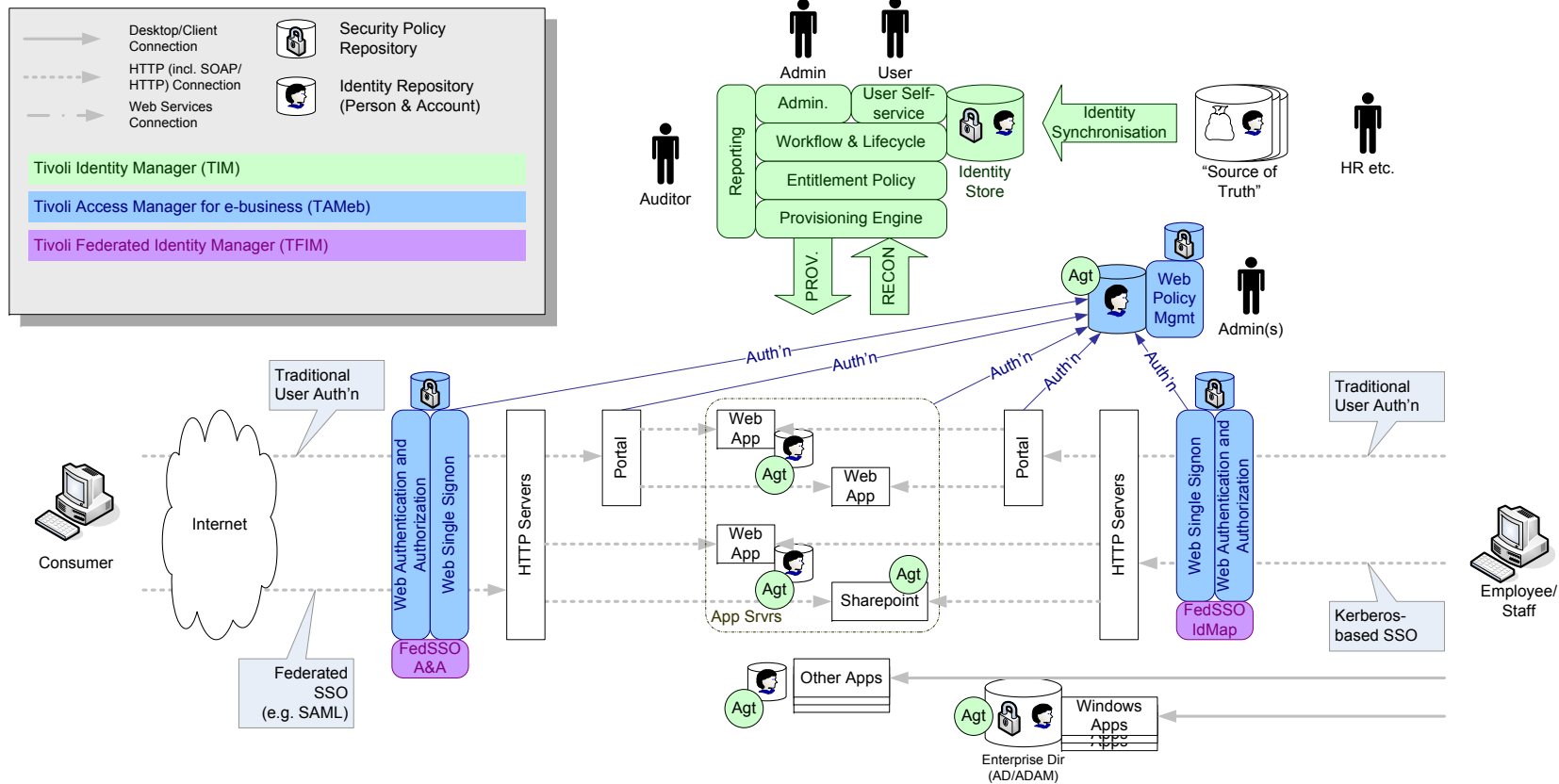
# Identity and Access Assurance – Typical Customer Environments



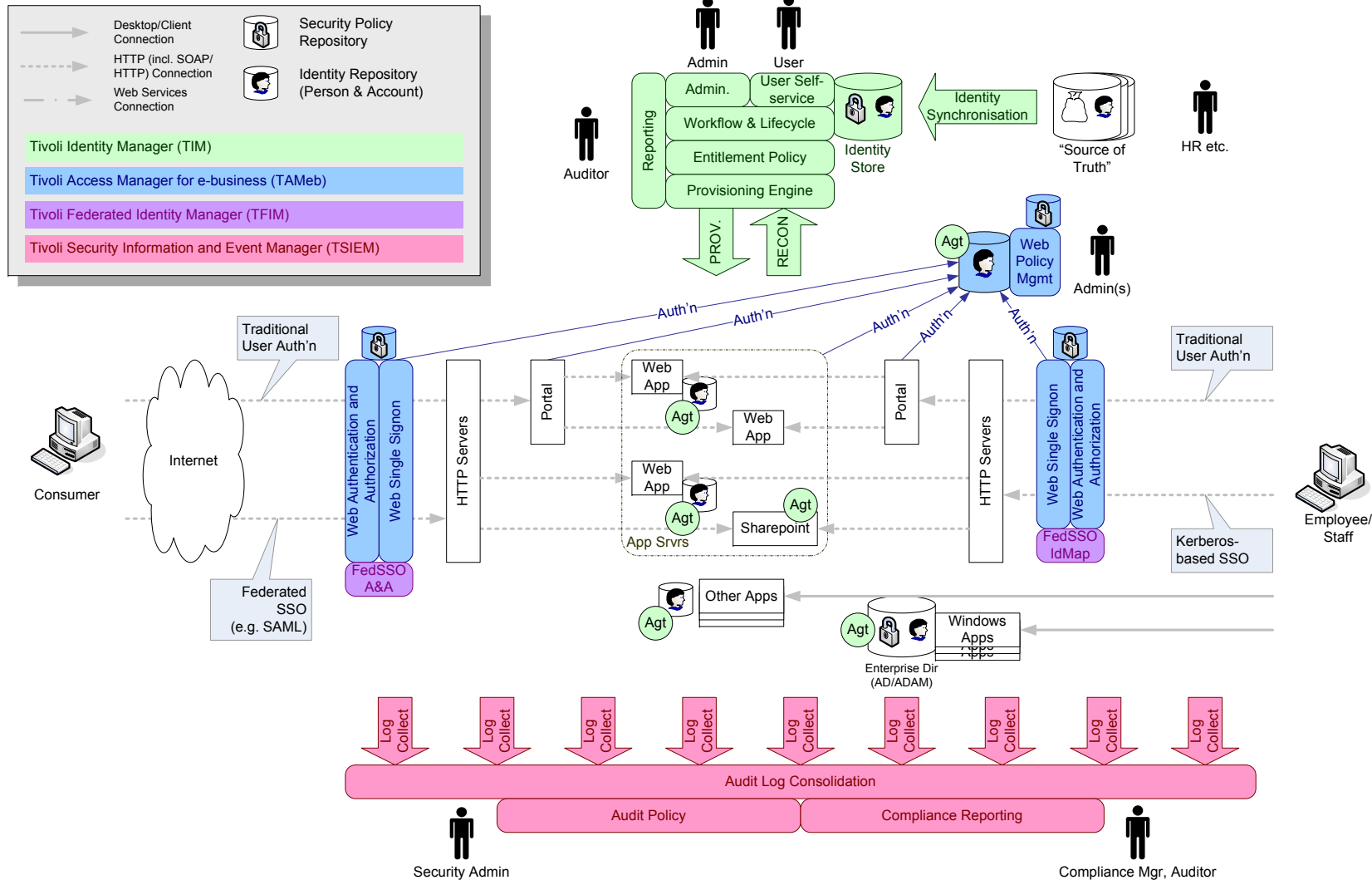
# Identity and Access Assurance – Tivoli Identity Manager



# Identity and Access Assurance – Tivoli Access Manager & TFIM



# Identity and Access Assurance – Tivoli Security Info & Event Mgr





# Privileged Identity Management

New way of keeping track on super users  
Watching our admins...



# Privileged Identity Management

## Business Challenge:

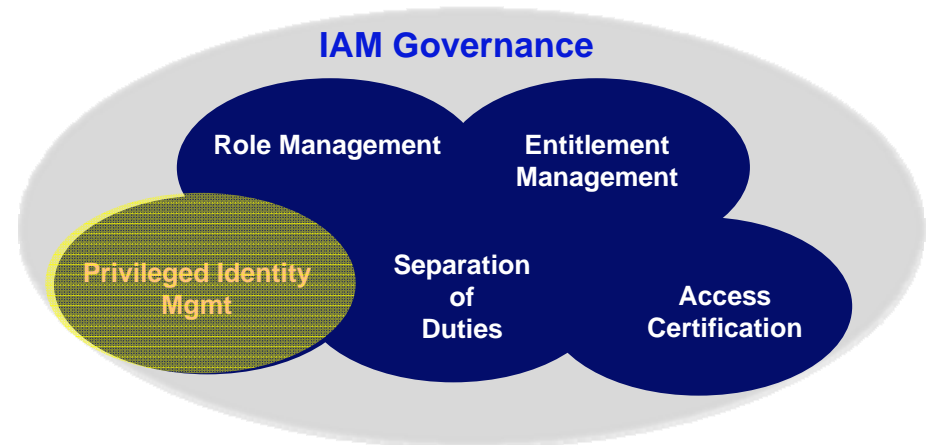
### Rapid increase in privileged ID's

- Administrators
- Root
- other broad access id's

### Exacerbated by:

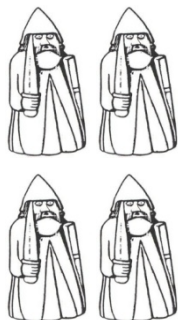
- Virtualization and increased number of virtual systems
- Cloud Computing
- Data center consolidation

**Need to share, control, track access**



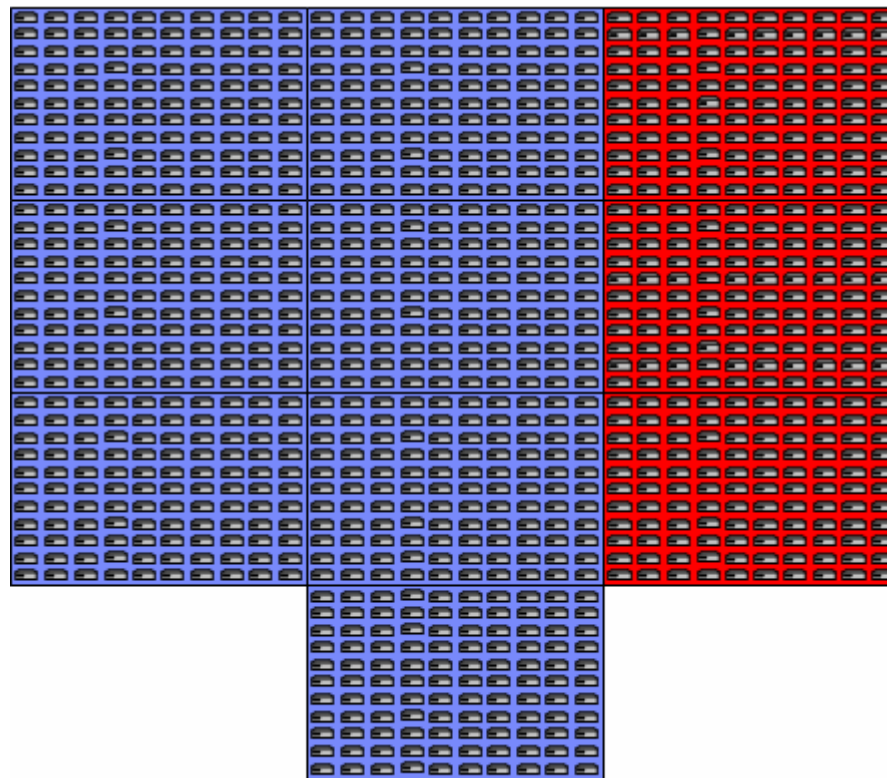
## System Support Model Evolution – Local Administration

Support Model	Administrators		Servers		Administrative IDs
Local Administration	4	X	100	=	400



## Support Model Evolution – Centralized Support

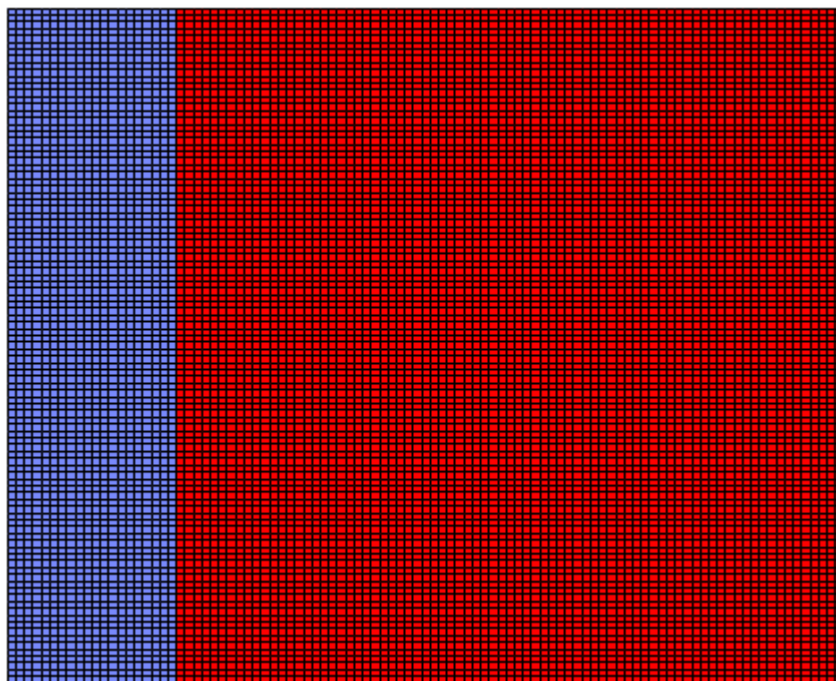
Support Model	Administrators		Servers		Administrative IDs
Local Administration	4	X	100	=	400
Data Centers	40	X	1,000	=	40,000



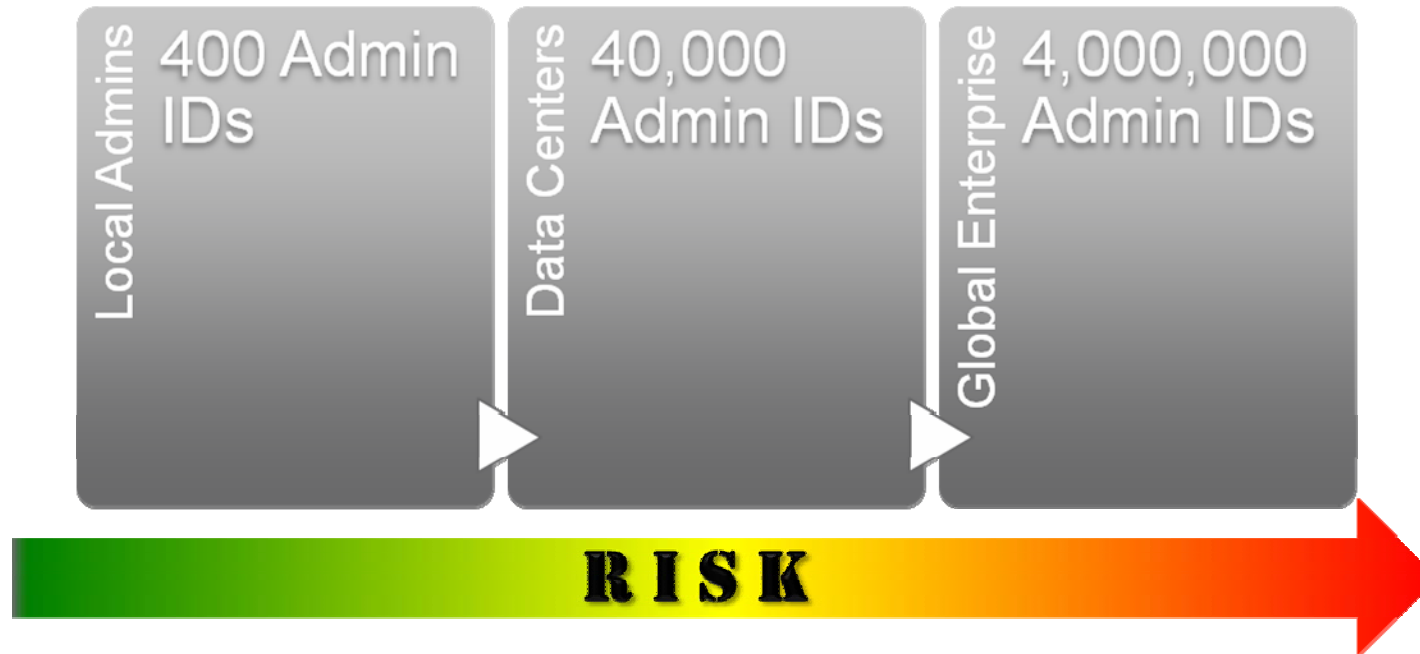


## Support Model Evolution – Mergers, Acquisitions, and Global Enterprises

Support Model	Administrators		Servers		Administrative IDs
Local Administration	4	X	100	=	400
Data Centers	40	X	1,000	=	40,000
Mergers and Global Enterprises	400	X	10,000	=	4,000,000



## Problem Statement



**10,000 times as much risk**

## Additional Considerations

- Increased Attrition Rate
- Employees Changing Jobs
- Continued Business Need (effective?)



## Privileged User Management- Problem Statement

‘Classic’ Delivery Model leads to an exponential increase in the number of privileged userids



## Traditional Thinking – 2 Solutions

Each administrator / user 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

Administrators / user share privileged userids

- Risk of losing Individual Accountability
- Issues with password management and security
- Out of step with regulatory thinking

The strategic Privileged Identity Management solution combines the best features of both approaches, without the disadvantages

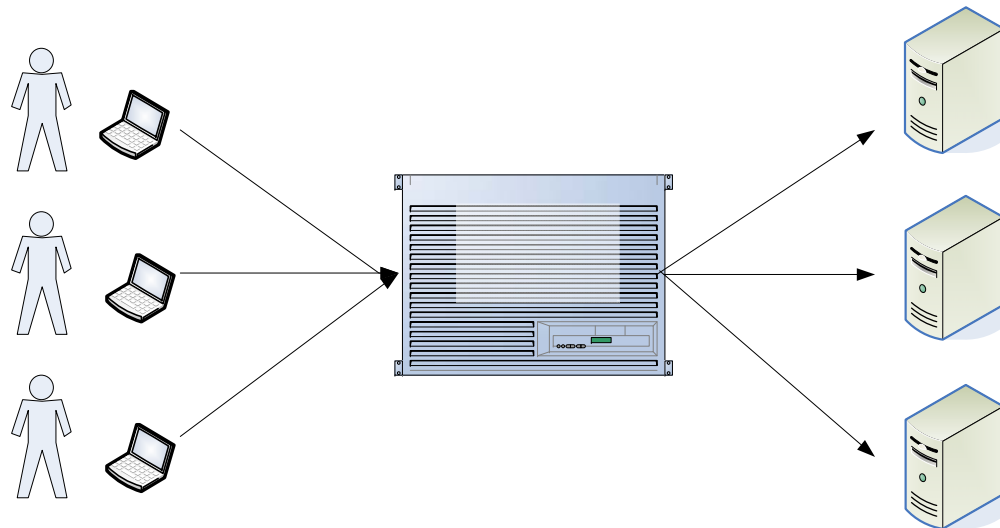


## The Components of PIM

### 1. Tivoli Identity Manager Vault: A vault solution for reusable userids

#### Controls:

- Who can access the userid
- What privileges the userid has
- Which systems the userid can access



## The Components of PIM

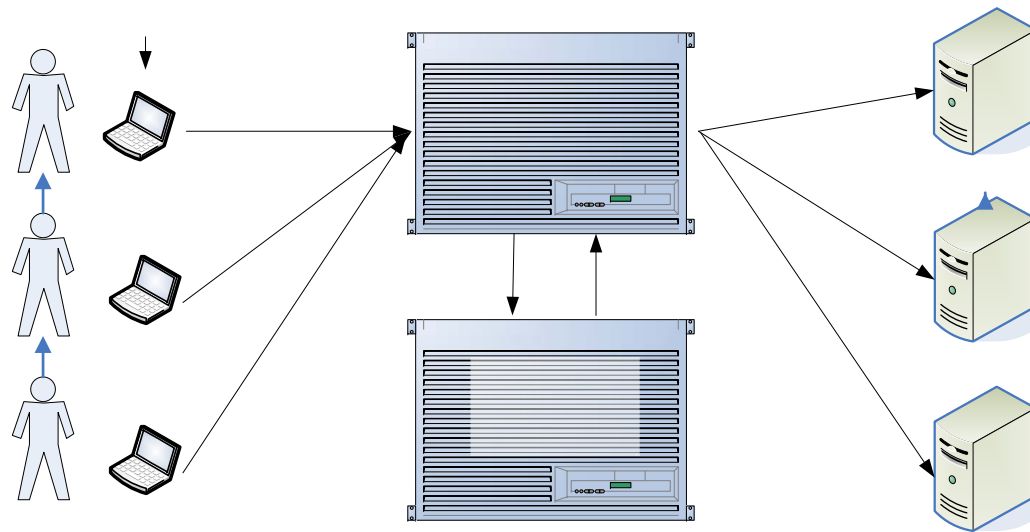
### 1. A vault solution for reusable userids

Controls:

- Who can access the userid
- What privileges the userid has
- Which systems the userid can access

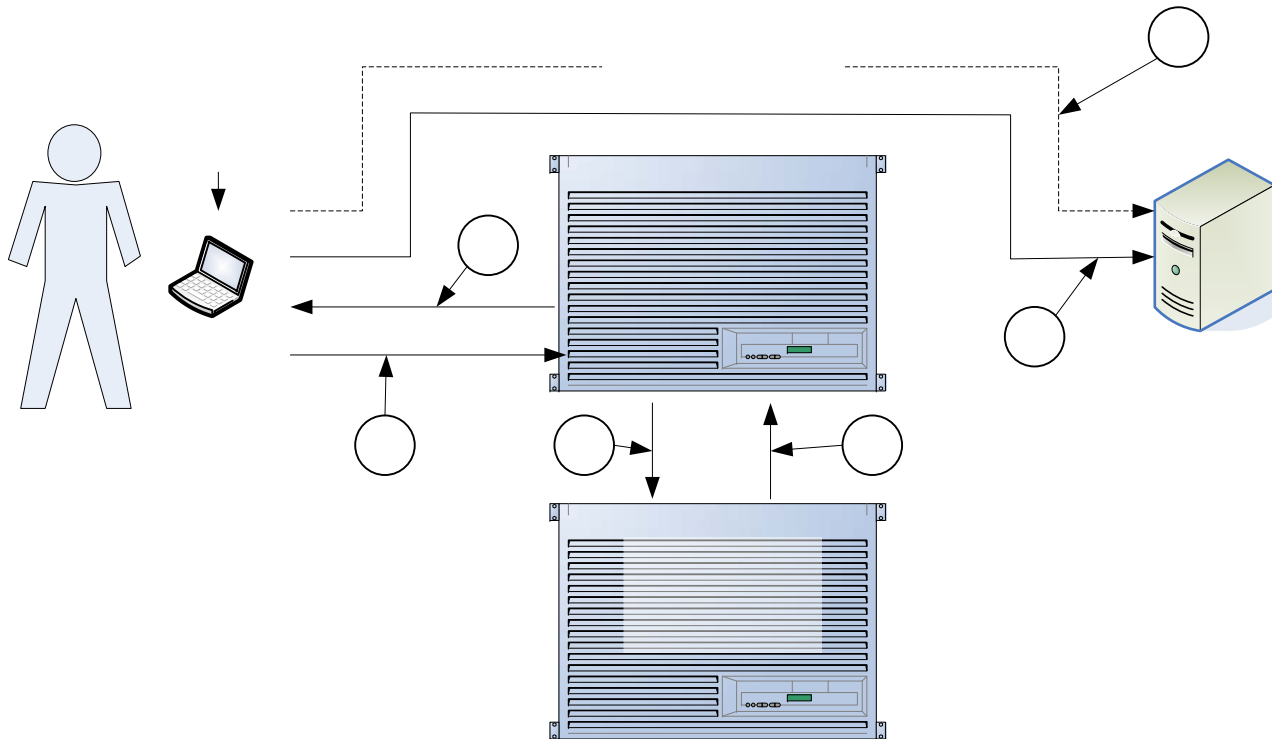
### 2. TAMeSSO: A Role, UserID and Password Broker relying on ITIM to provide the necessary "Access Control" information

- Client Component
- Server Component



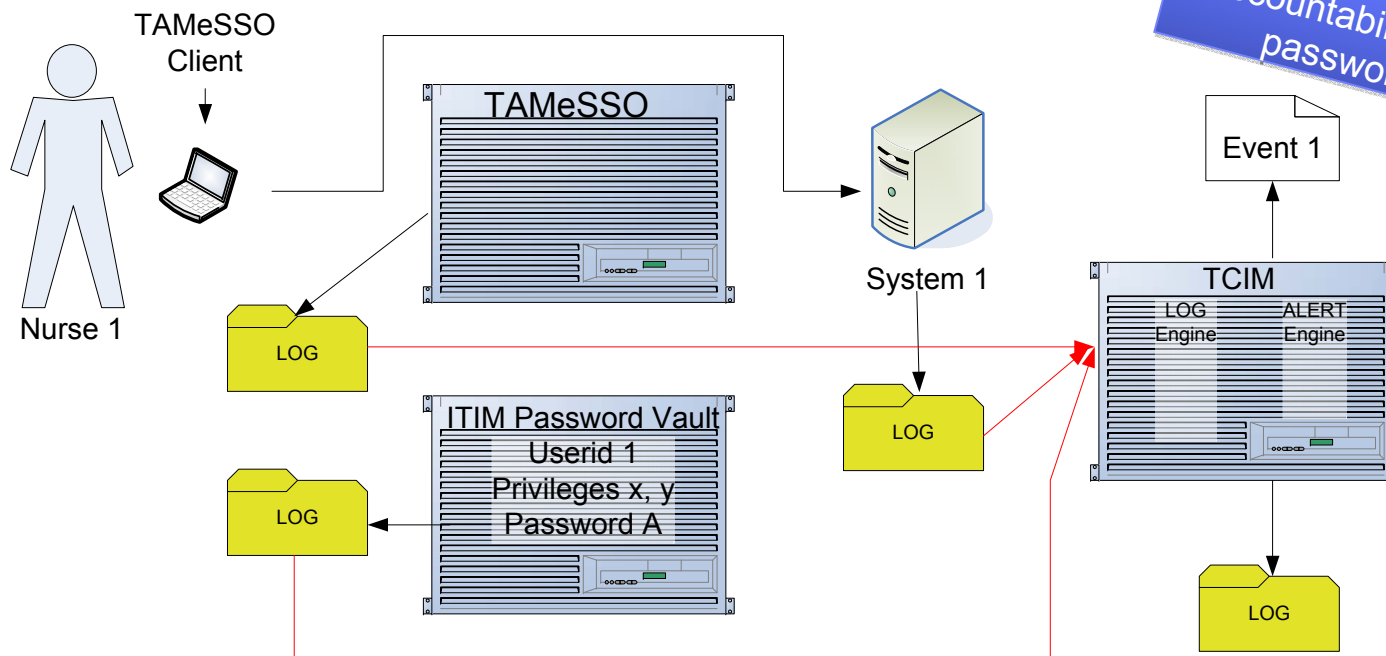
## PIM – Use Case Scenario

1. User requests TAmESSO for access to system 1, using his/her TAmESSO UserID 1
2. TAmESSO queries ITIM
3. ITIM returns to TAmESSO the Privileged UserID 1 and password
4. User connects to system 1, using the Privileged UserID 1
5. At logon, TAmESSO enters the Privileged UserID1 and Password  
*(End-User does not see the password)*



## PIM Usage – Logging

1. User requests TAMESSO for access to system 1, using his/her TAMESSO UserID 1
2. TAMESSO queries ITIM
3. ITIM returns to TAMESSO the Privileged UserID 1 and password
4. User connects to system 1, using the Privileged UserID 1
5. At logon, TAMESSO enters the Privileged UserID1 and Password  
*(End-User does not see the password)*
6. All stages of the process are logged independently
7. TCIM available for Privilege Monitoring if required





## Benefits of the New Model – Privileged Identity Management Solution

We are moving away from two obsolete concepts:

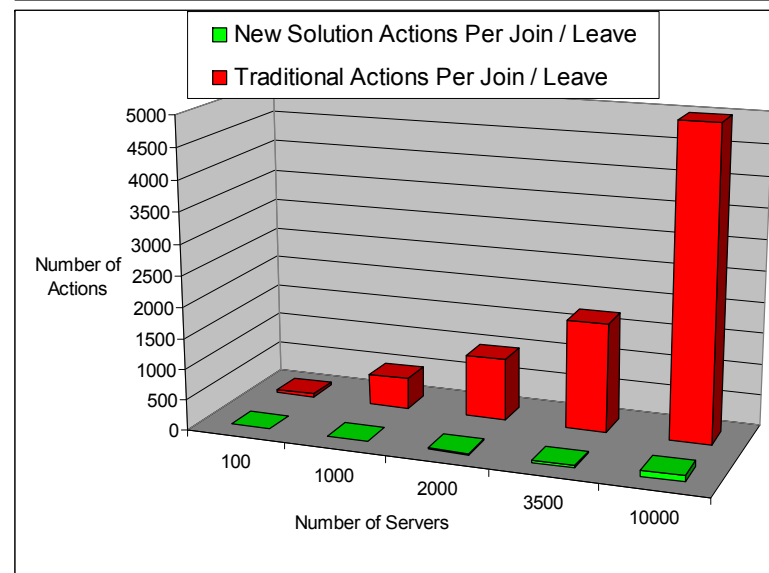
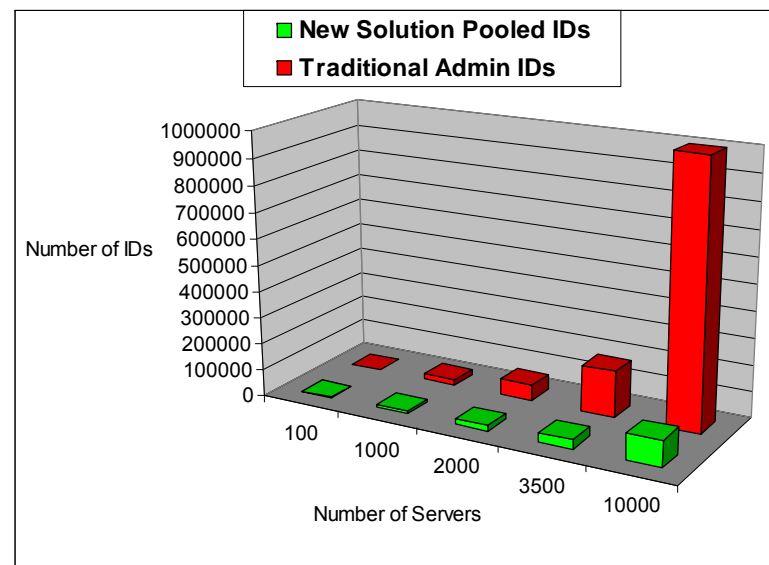
- “Everyone has a userid on every system, all the time, just in case” (Admin x Servers)
- “Everyone shares access to a single userid for ease of administration”

We are moving to a new concept

- “A user gets an individual userid on a system – but only...
  - If they need it
  - When they need it
  - For only as long as they need it

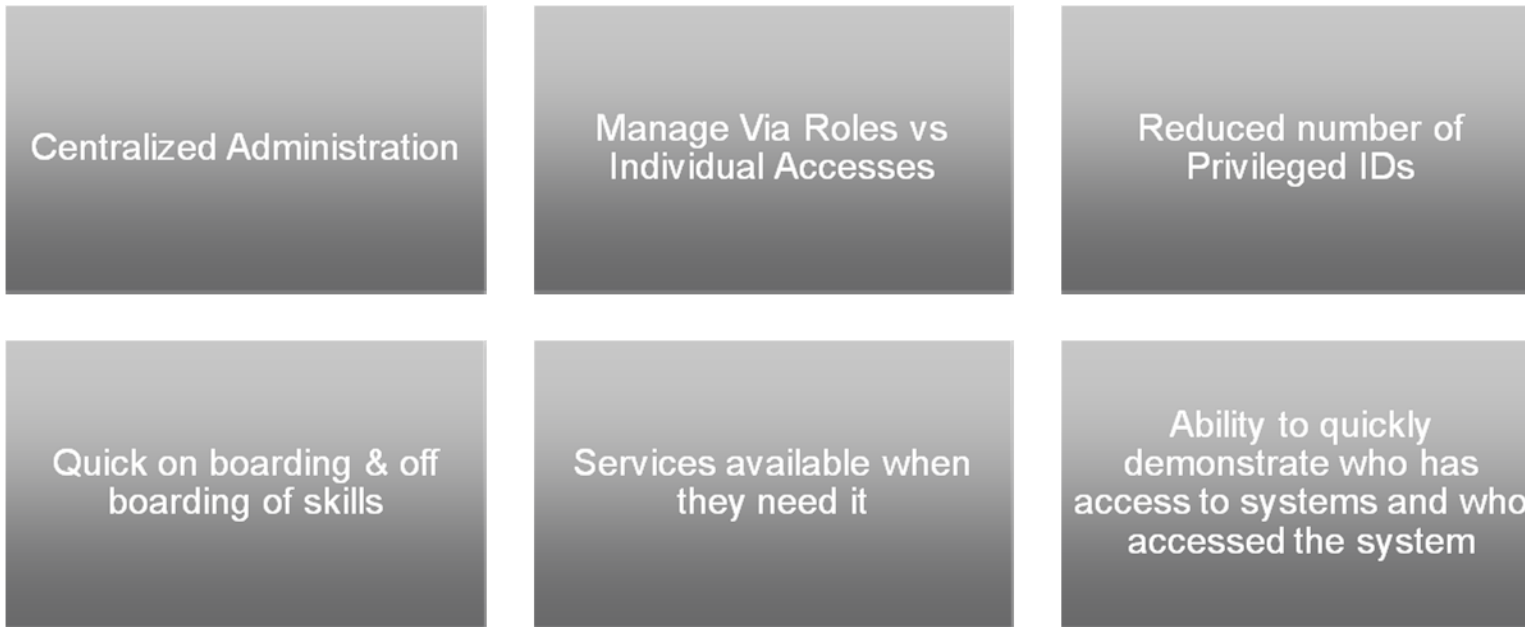
The new model reduces

- Number of individual Admin IDs (Roles x Servers only)
- Number of Provisioning Activities per joiner / leaver (access to role only)



## Privileged Identity Management- Benefits

Total paradigm shift in the method of administering and controlling access to systems.



# Tivoli addresses the growing Privileged ID problem with a complete Life Cycle Solution

IBM offers 2 solutions:

- **TAMOS** provides OS level enforcement of non-shared IDs
- **Integration Services for Privileged Identity Management** provides centralized management of **shared** and privileged accounts to improve compliance, lower cost and reduce risk\*

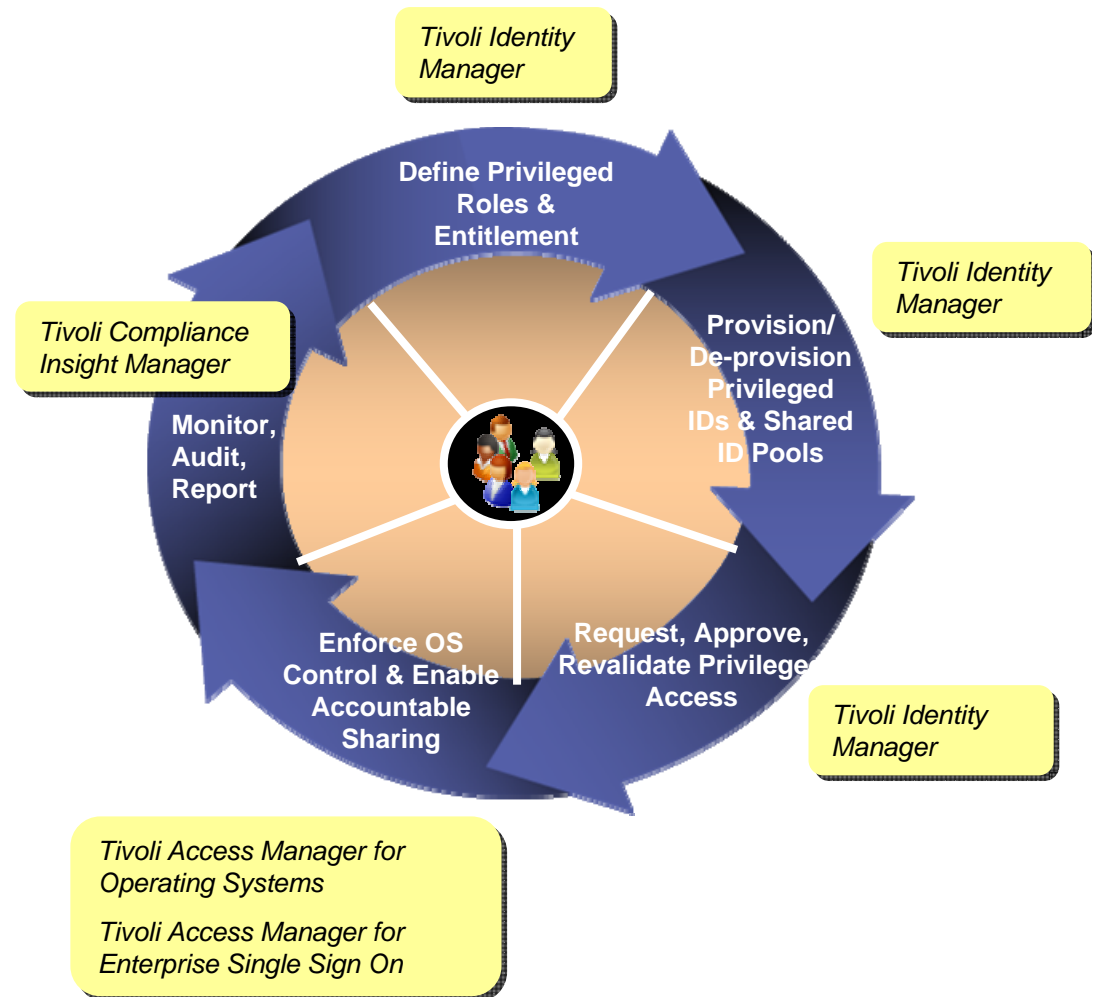
Key PIM functions include:

- Centralized management of privileged and shared identities. Privileged identities can be centrally provisioned, de-provisioned, and shared.
- Secure access and storage of shared identities
- Request, approve and re-validate privileged access
- Single sign-on with automated check in and check out of shared and privileged IDs
- End to end monitoring and reporting

Benefits

- Centralized Privileged ID management improves IT control and **reduces risk**
- Automated sign on and check-in/out simplifies usage and **reduces cost**
- Comprehensive tracking and reporting **enhances accountability and compliance**

\* Lab services required



## Harley-Davidson Gets Value from **TIM**, **TAM** and **TSIEM**

### Requirements/Challenges

- Minimize the damage from high profile attacks and defacements
- Address PCI and SOX 404 mandates for monitoring of privileged users

### Solution


- Implemented IBM Tivoli Security Information and Event Manager (**TSIEM**), IBM Tivoli Identity Manager (**TIM**), IBM Tivoli Access manager (**TAM**)

### Benefits

- Monitor user activity at the enterprise level
- Create Security Event Management platform
- Reduce the time to address security events from days to hours
- Streamline compliance reporting for multiple regulations
- Integrate SIEM in their Enterprise Services Management strategy for a foundational security solution



# Why IBM? – IBM is your trusted partner...




**Know how to ensure your success**

Successfully implemented 1000s of client projects



**Deliver value by understanding the big picture**

Security across mainframes, desktops, networks, handheld devices



**Help you to choose**

Create the right solution for you




**Expertise to meet your industry needs**

Tailor solutions to meet your industry challenges



**Ensure success by execution**

Manage security for 400,000 IBM employees, 7B events/day for clients



**Client success stories to demonstrate results**

Provided IT Security for 30+ yrs, 200 client references



**Leverage our skills to meet your goals**

1000s of researchers and SMEs



**Partnership with a huge ecosystem**

Large business partner community



Delivering solutions that enable enterprises to be Secure by Design



# Thank You.



**ONE** voice for  
security.

**IBM SECURITY  
SOLUTIONS**

**INNOVATIVE**  
products and services.

**IBM SECURITY  
FRAMEWORK**

**COMMITTED** to the vision  
of a Secure Smarter Planet.

**SECURE BY  
DESIGN**

