Justifying Identity and Access Assurance to your management

Chi Sen GAY

Tivoli Security Sales Leader, ASEAN

Today's Identity Management Challenges

Trusting Identities

Customers or criminals?

Partners or competitors?

Employees or hackers?

Managing Access

Securing Services

Payroll

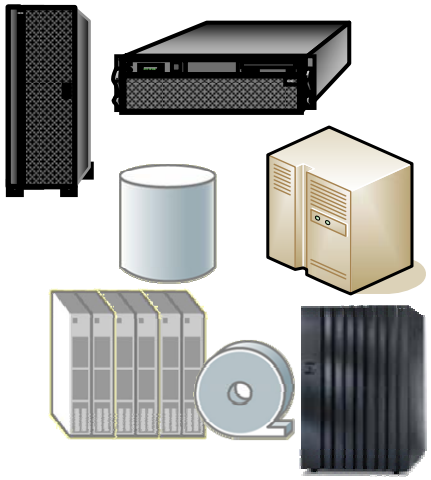
Online banking

Loan applications

Retail sales

Inventory

Protecting Data



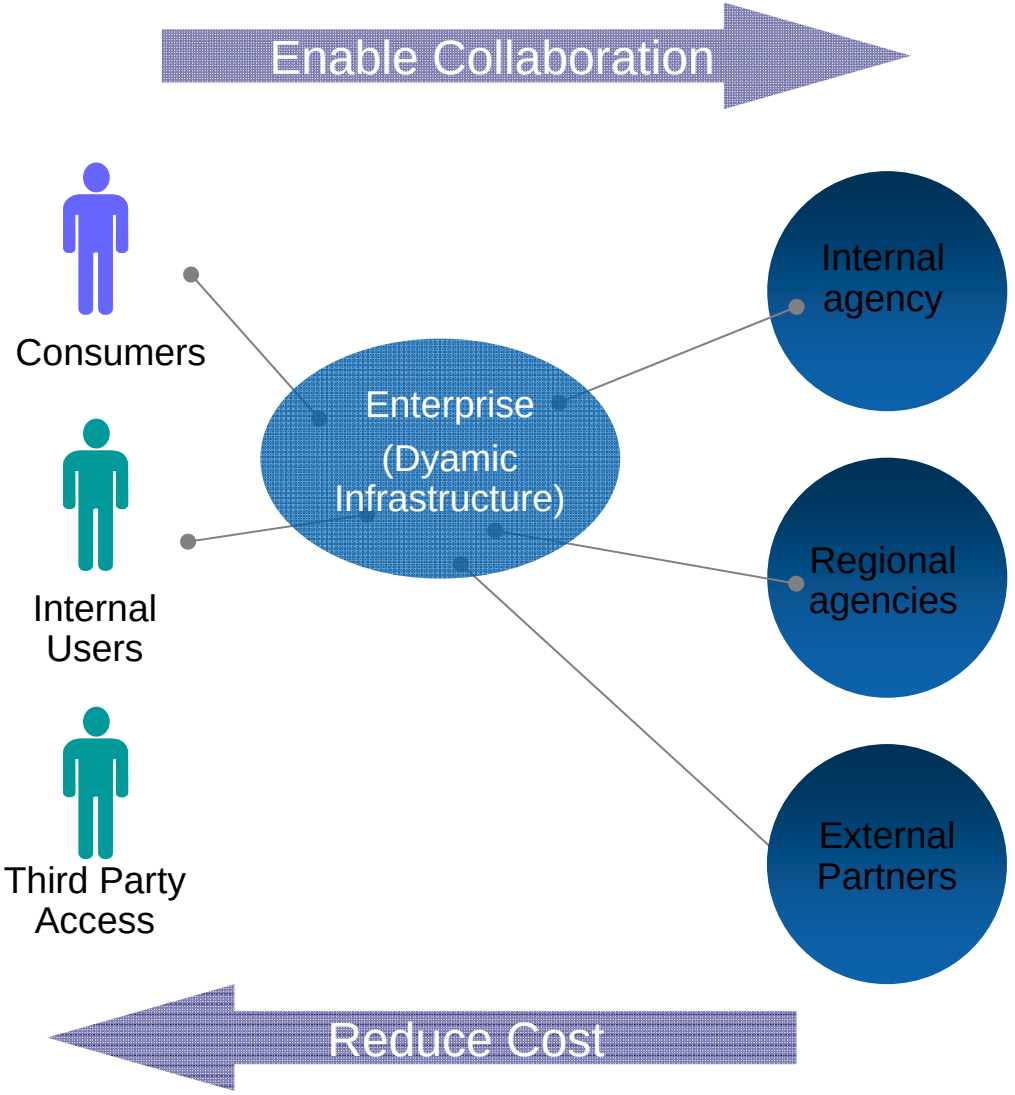
Growing security challenges driving the need for Identity & Access Assurance

- **Data and Information Security**
  - Growing risk of Intellectual Property Theft
  - Need to control access to critical data
- **Business and Application Compliance**
  - Increasing regulations requires deeper access control
  - Need to demonstrate that right people have access to right resources
- **Application Consolidation & IT Cost**
  - Reducing cost of business applications and services rollout
  - Need to manage and change access control without modifying applications

Identity, and Access Assurance provides secure collaboration and identity governance

Develop Identity and Access Management Strategy to help reduce IT cost and enable secure collaboration

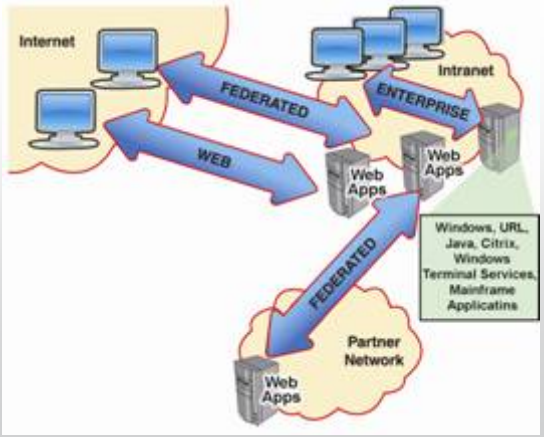
- Manage identity centrally to reduce cost of administration throughout lifecycle
  - User provisioning, role management
- Collaborate with partners and contractors on specific projects using business sensitive data
  - Federation and SSO
- Secure expansion of web services deployment in SOA
  - Message Protection & Enforcement
- Audit and reporting data usage
  - Compliance Reporting & Dashboard



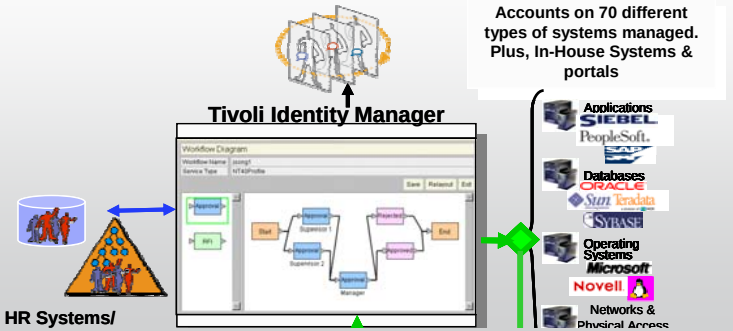
Getting started with Identity and Access Assurance

Single Sign On

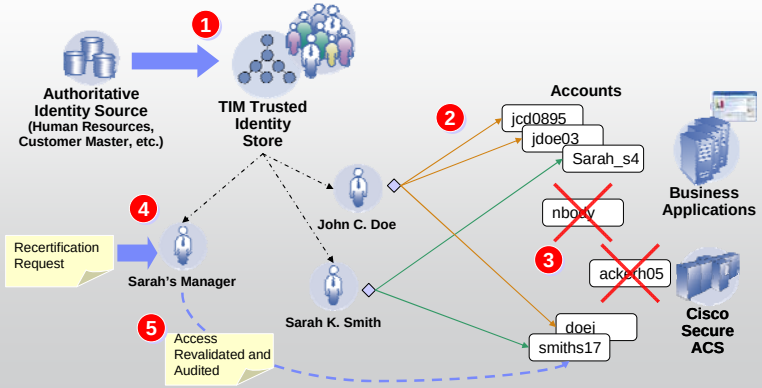
& Password Management



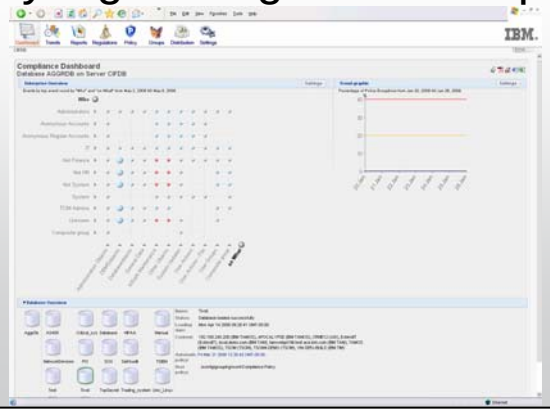
User Provisioning / Role Management



Access Attestation



Security log management & reporting



Identity and Access Assurance

Improve Service

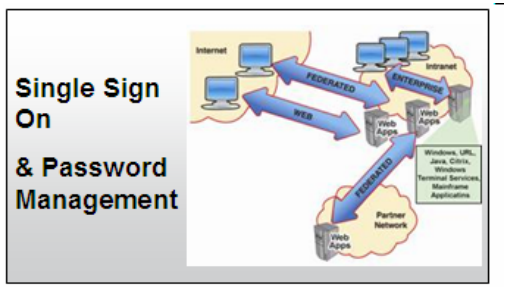
- Enable collaboration via role based portals with access to enterprise services and applications
- Increase market reach with federated business models leveraging trusted identity information

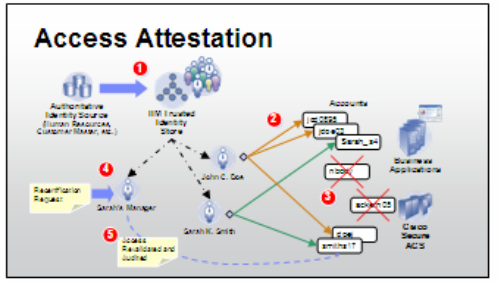
Reduce Cost

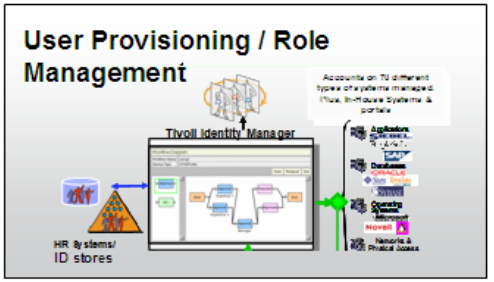
- Reduce help desk costs, password reset requests
- More efficiently manage restructuring
- ERP deployments / upgrades

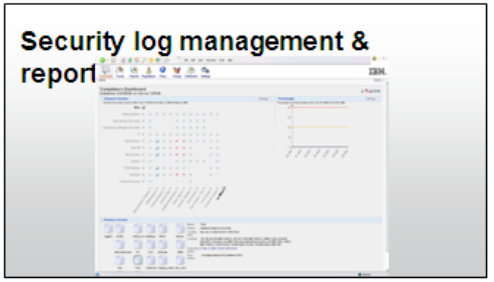
Manage Risk

- Privileged users
- Failed audits,
- Insider breach
- Recertification, entitlements management
- National ID / Trusted ID – provisioning of strong / trusted credentials.
- Unauthorized IT change detection







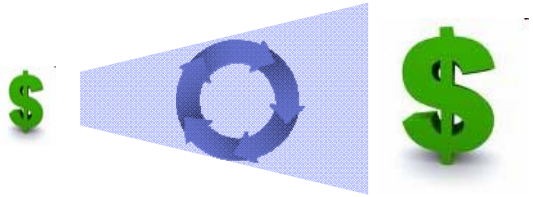


Drivers for Identity and Access Assurance have remained consistent

- 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

APRA
PCI-DSS
GLBA
FISMA
SOX
Basel II
ITAR
ISO 27001

- 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



- 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

What are the drivers and key projects for buying this solution?

- **Compliance**
  - Drivers
    - Audit failures and fines
    - New or existing regulatory pressures
  - Projects
    - Regulatory mandate projects (PCI DSS, HIPAA, SOX, Basel II, etc…), access certification, role management and user provisioning

- **Operational efficiency – cost reduction**
  - Drivers
    - End user productivity, Single Sign-On projects
    - IT operational efficiency (process automation)
  - Projects
    - Portal deployments
    - Single sign-on deployments
    - User provisioning deployments
    - ERP deployments and upgrades
    - Organizational restructuring

What are the drivers and key projects for buying this solution?

- **Security**
  - Drivers
    - Prevalence of data breaches – intellectual property, disclosure of customer/employee data
    - Insider information theft
    - Brand protection
    - Homeland security
  - Projects
    - Response to security incident
    - Entitlement management projects
    - Privileged user monitoring
    - Password management
    - National ID and ePassport projects
    - Employee ID projects
- **Improve user productivity and satisfaction**
  - Drivers
    - User frustration
  - Projects
    - Single sign-on
    - Self-service access request
    - Mobile banking / payments

Top 5 Security Deficiencies

Improper Change Management

- Lack of formal program change procedure
- Lack of understanding of system configurations
- Oversight of changes and review of change logs

Insufficient Segregation of Duties

- NOT JUST Separation of requestor, approver, implementer --Separation of developers and operators

Excessive Access to Systems / Databases

- Developer / programmer / DBA /Admin access to production environment
- Developer / programmer DBA /Admin access to production data

Lack of Access Controls

- User provisioning and administration
  - Changes in responsibilities
  - Changes in organization
  - Terminations
- No documented access policies and standards

Lack of general monitoring of the security infrastructure

Top 5 material deficiencies derived from last two years Auditors Reports

Threats and challenges

- **Threats continue to rise: mergers, acquisitions, layoffs. 59 percent of workers who left their positions took confidential information with them.**
  - 24% of these former employees responding to the survey said they still had access to their former employer's computer systems after they left,
  - 50% between one day to a week,
  - 20% more than a week.

study by Ponemon Institute

- **Weak passwords are easily compromised by insiders.**
  - Internal attacks cost 6% of gross annual revenue -- costing USD 400 billion in the U.S. alone.
- **30% of all help desk calls are password related.**
  - Password resets can cost as much as $20-$25 per call.

Who is buying/influencing the solution?

- Chief Security Officer (CSO, CISO),
  - Must meet operational security objectives under budget, as well as support ability to demonstrate compliance regulations
- Chief Risk Officer
  - Preserve company's Intellectual property, external reputation, and risks to the business

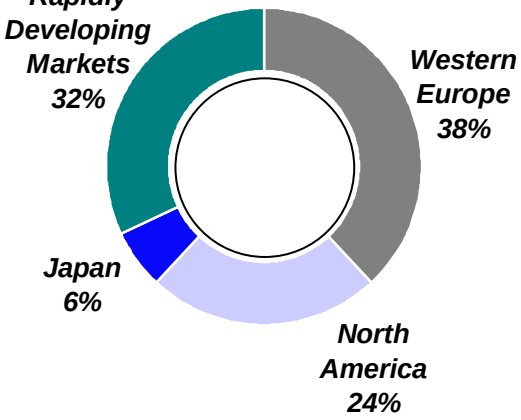
- Line of Business (LOB)
  - Needs business agility to respond to new opportunities by enabling new complex applications, securely leveraging partner collaboration, outsourcing, etc.
- Security Administrator
  - Needs to understand any breaches or attempts
  - Need to understand current controls meet business needs

- IT Operations
  - Keep operational costs under control, while meeting growing demands of a complex IT environment

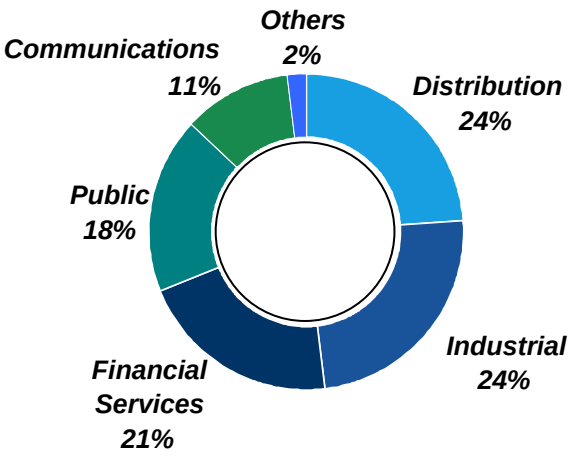
IBM 2009 CIO Study: In largest known such study, we spoke face-to-face with 2,500+ CIOs to understand their goals and challenges

The study represents different-sized organizations in 78 countries and 19 industries

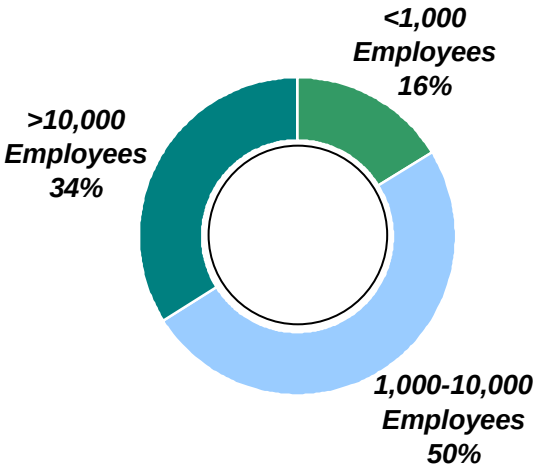
Geography



Sector



Organization Size



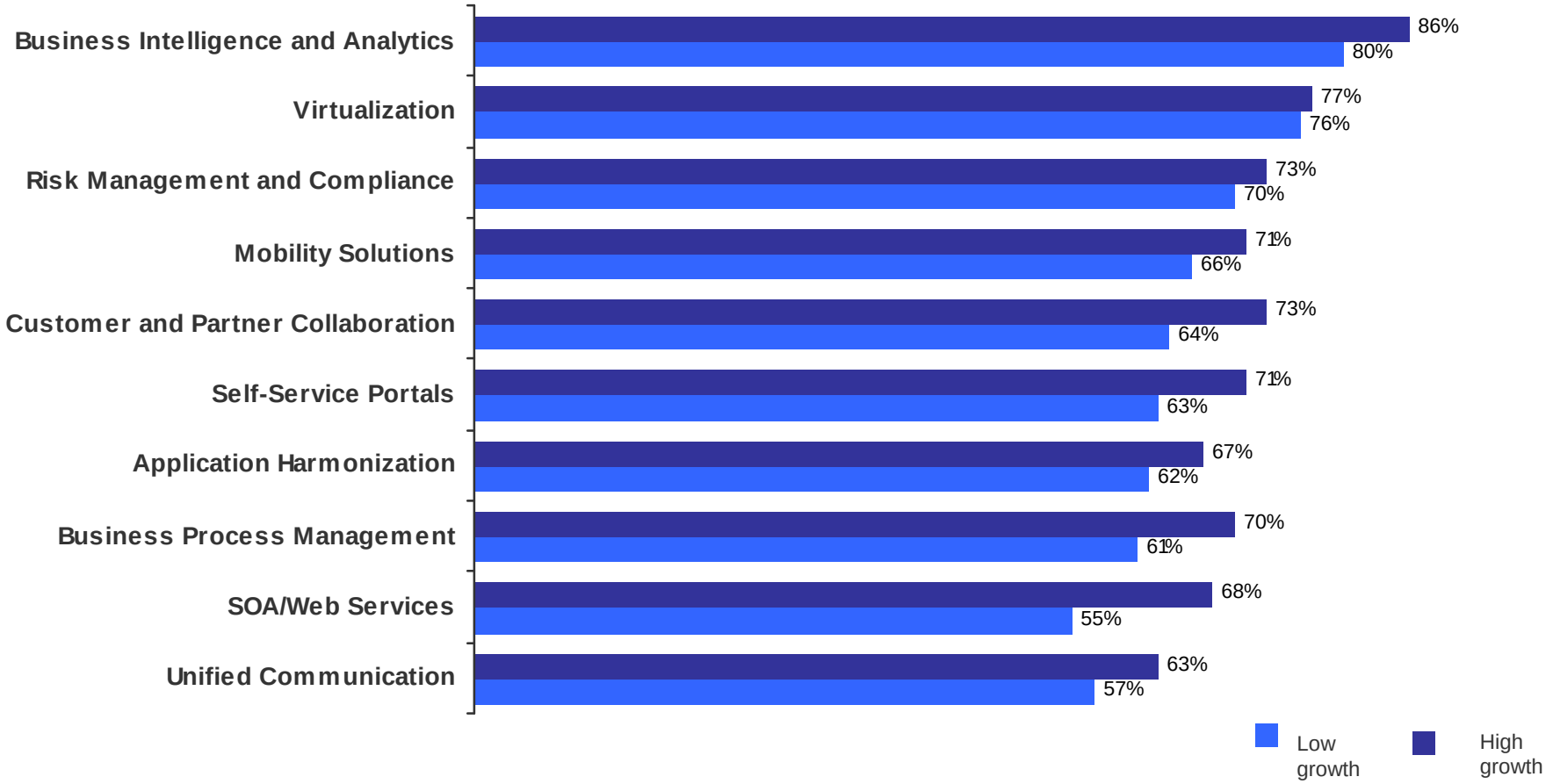
Our analysis used 2004-2007 Profit before Tax (PBT) growth, relative to peers in their industries, to associate organizations with one of three growth levels: High, Medium or Low. For organizations where this information was not available, we used statistical correlation to assign levels, based on closest overall similarity of answers.

In this presentation, we primarily refer to CIOs who work in organizations with high PBT growth as “High-growth CIOs” and to those working in organizations with low PBT growth as “Low-growth CIOs.”

Almost 3 out of 4 CIOs make risk management and compliance one of their top priorities

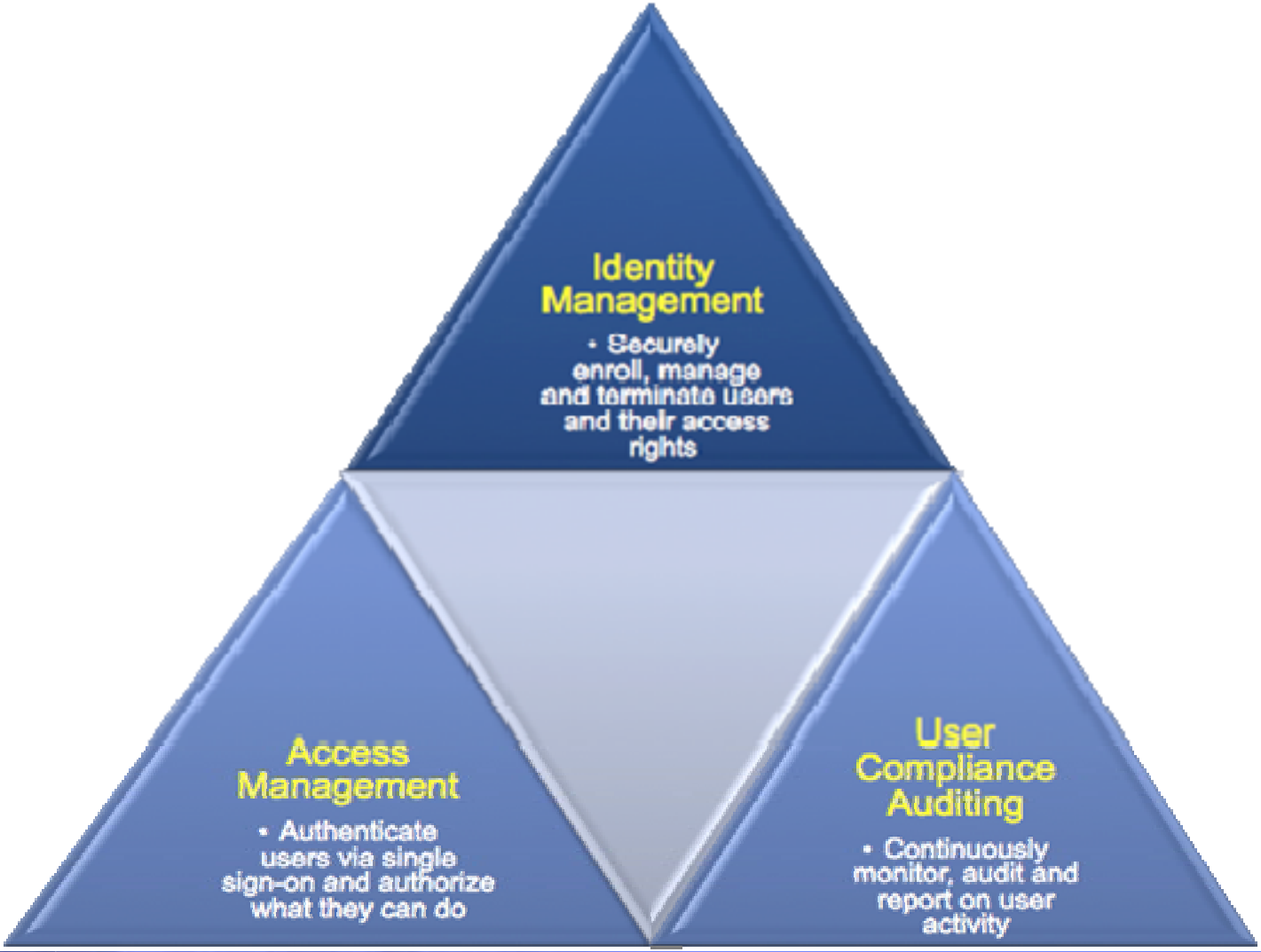
Ten Most Important Visionary Plan Elements

Interviewed CIOs could select as many as they wanted

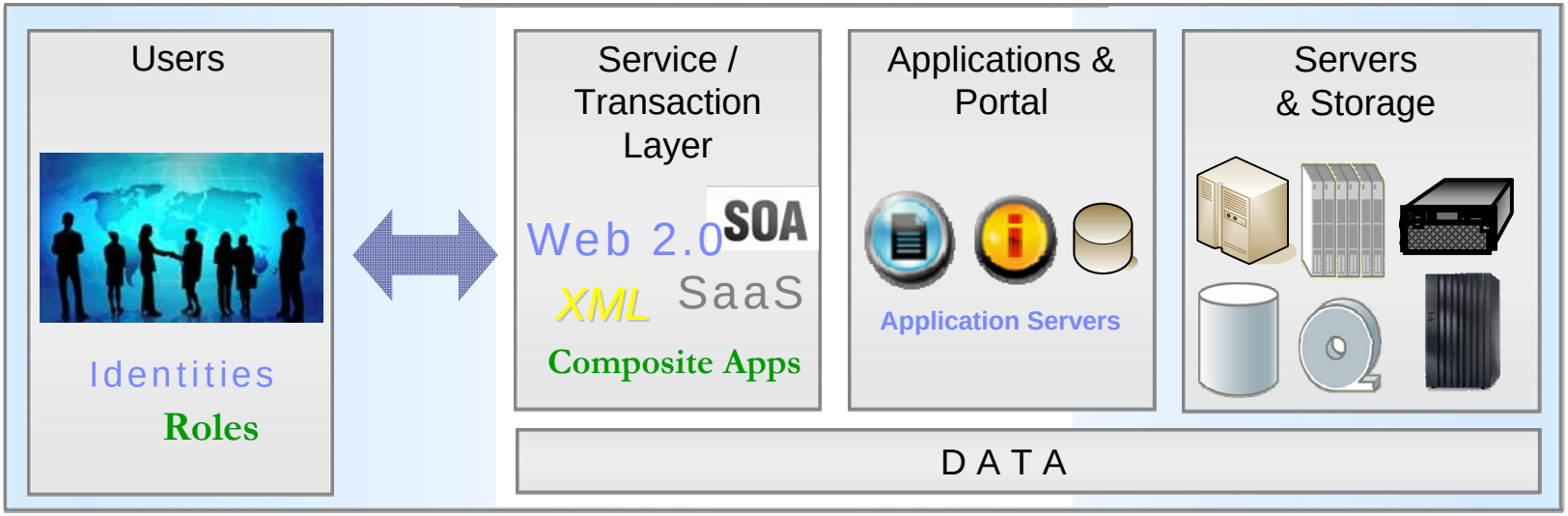


What is the management buying?

Identity and Access Assurance allows your management to:



IBM Solution Approach to Identity & Access Assurance



- **Tivoli Identity Manager** : New operational role management capabilities in role hierarchy, separation of duties, access recertification, group management and compliance reporting
- **Tivoli Access Manager e-business and Tivoli Federated Identity Manager:** Manage and enforce user access control and Web SSO across Portal and Web applications
- Mitigate against common threats with **centralized session management** (e.g. cross-site request forgery, insecure communication, restrict URL access, etc.)
- **Tivoli Security Information and Event Manager:** Demonstrate audit & compliance reporting with data from multiple enforcement points, other platforms and security applications
- **Tivoli Security Policy Manager :** Protect data-level access across Portal, applications and services with entitlement management
- Provide **security run-time services** for application development & reduce cost of siloed control
- **Tivoli Key Lifecycle Manager :** Centrally Manage encryption keys for tapes and disks

What are the key value propositions & capabilities?

- **Manage security and compliance risk posture**
  - Adhere to internal corporate security policies and external regulatory mandates (SOX, HIPAA, DSS PCI, etc…) through:
    - user activity monitoring
    - strong authentication
    - automated compliance reporting
    - validating user identity before enrollment
    - revalidating user access rights
    - eliminating poor user password behavior
    - a process that governs the enrollment, proofing, issuance and usage of ID credentials

- **Streamline operational efficiency**
  - Reduce manual user administration and associated costs through automated on-boarding and off-boarding of users
  - Reduce IT help desk calls via self service password reset
  - Reduce time spent collecting logs through centralized log management

- **Enhance user productivity**
  - Automate initial granting of user access to applications
  - Enable access automation to applications via single sign-on
  - Enable efficient kiosk sharing while maintaining security and compliance

- **Monitor privileged users**
  - Establish special controls and monitoring for users that carry privileged access (DB administrator or CEO)

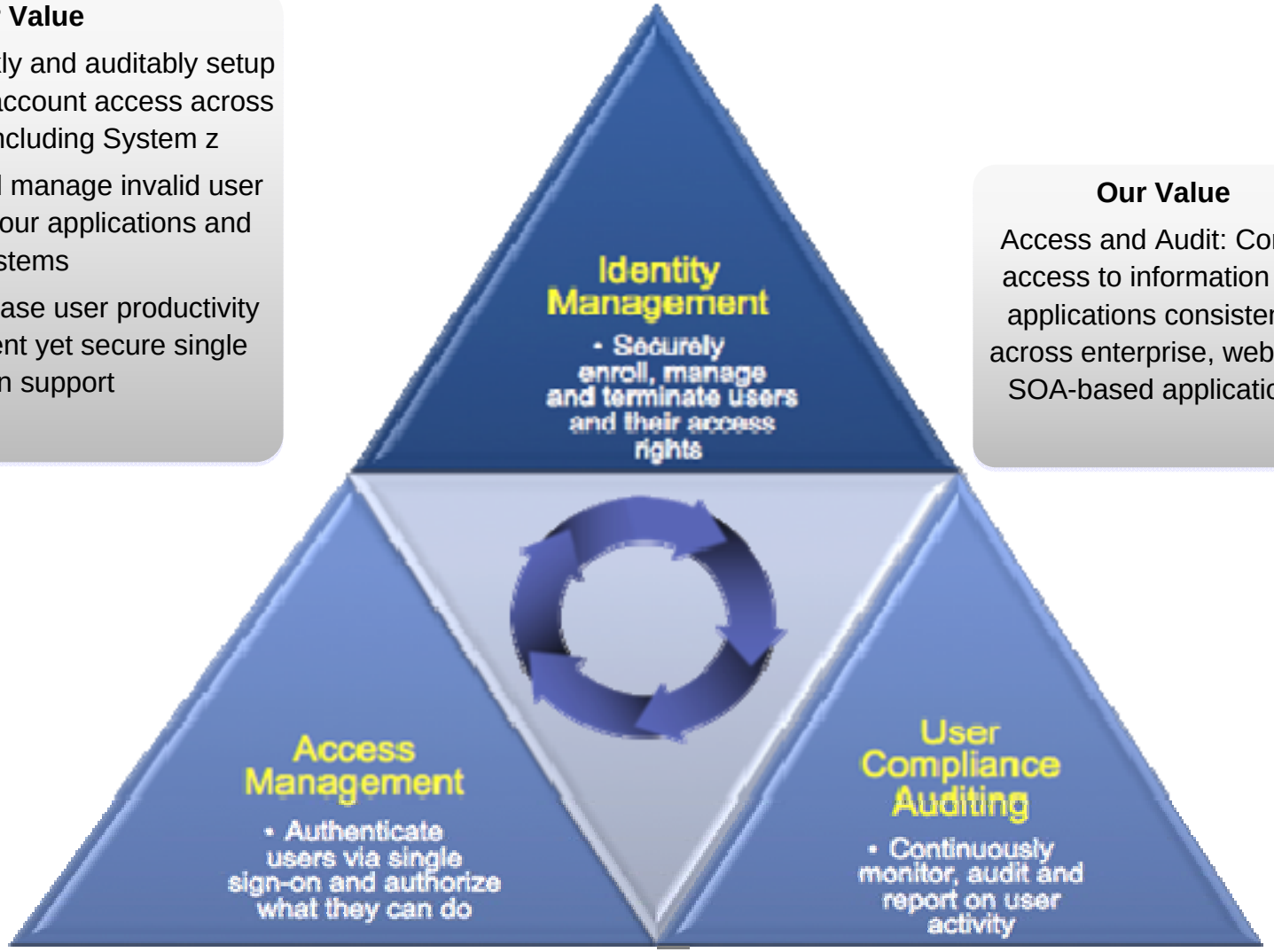
Identity and Access Assurance – closing the loop

Our Value

Provisioning: Quickly and auditably setup and recertify user account access across all platforms, including System z

Quickly locate and manage invalid user accounts within your applications and systems

Productivity: Increase user productivity through convenient yet secure single sign-on support



Our Value

Access and Audit: Control access to information and applications consistently, across enterprise, web, and SOA-based applications.

Case Study – Tax and Revenue Agency

- Background
  - Consolidate existing financial and banking applications to reduce application development costs
- Challenges
  - Address internal audit requirements to improve transparency without modifying the applications and services
  - Protecting access to client sensitive information requires complex, authorization policies
  - Application owners need an external security services and capture data and application entitlements without IT details
- IBM Solution
  - Tivoli IAM, Federation and Compliance Management