



# Periodic Access Re-certifications

ISACA Atlanta Geek Week

September 2008

 **ERNST & YOUNG**  
*Quality In Everything We Do*

# Agenda

---

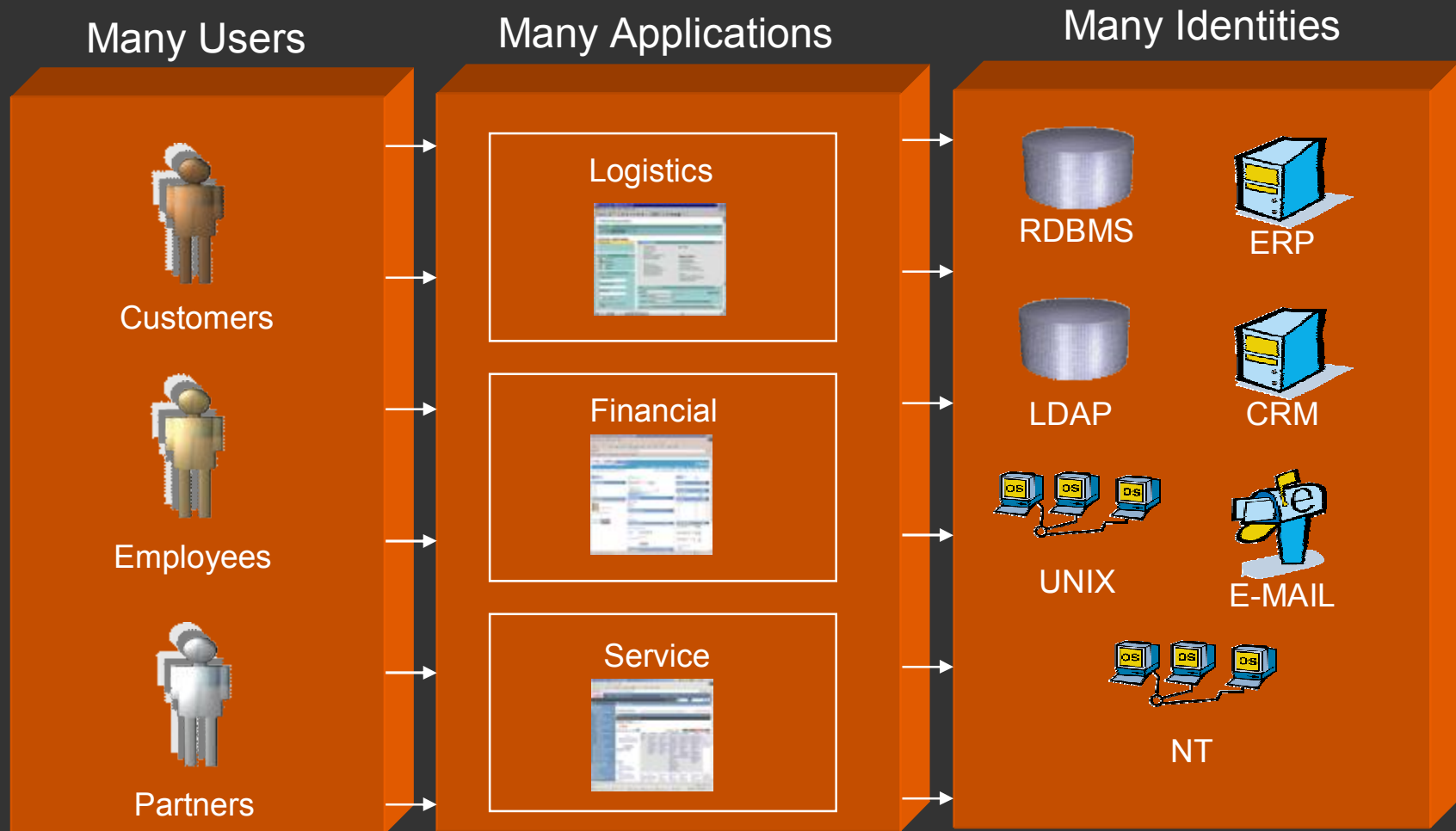
- ▶ IAM Challenges
- ▶ Key drivers for Access Recertification
- ▶ Definition of a Comprehensive Access Recertification
- ▶ Technology response to IAM

# IAM Challenges

---

- ▶ As organizations grow, acquire new businesses, expand their customer base, reorganize, or enter new lines of business, they face increasingly difficult challenges associated with the management of user identities and their entitlements to information assets.
- ▶ Information security concerns and regulatory compliance issues mandate appropriate controls on the access to organizational assets and information, increasing the importance of managing user identities and entitlements.
- ▶ Finally, the increasingly collaborative nature of modern business requires granting access to organizational assets and information to external entities like business partners, suppliers, joint ventures, and customers.
- ▶ These challenges must be addressed by any organization that desires to remain flexible and adaptable, to contain costs, to increase productivity, or comply with laws and regulations, and thus maintain or enhance its competitive advantage.

# Current State of User Access



# Access Recertification Addresses

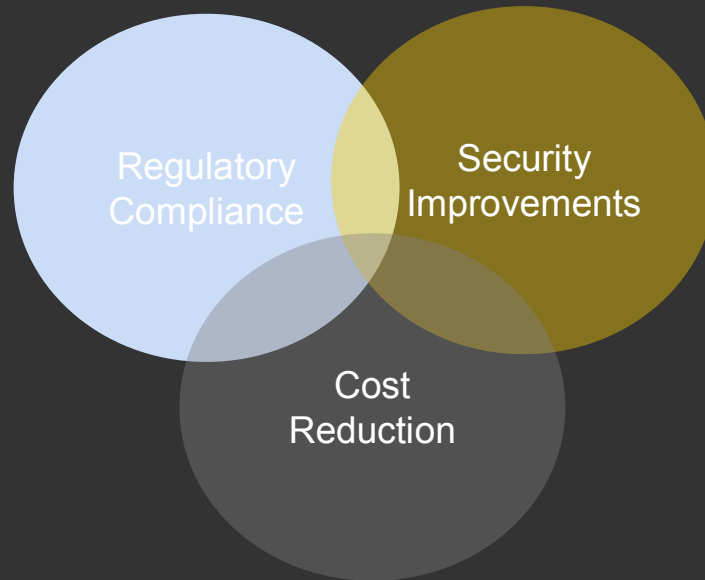
---

- ▶ Who has access to what
- ▶ Who has had access to what
- ▶ The correct people with right level of access to right applications at the right time
- ▶ A combination of people, process and technology to provide users access to information assets
- ▶ An integrated system that enables the control of user access to resources, while protecting confidential information

# Key Access Recertification Drivers

---

- Sarbanes Oxley
- HIPAA
- Regulators (ie. SEC)



- Improved segregation of duties
- Timely removal of dormant accounts
- Stronger audit trail
- Elimination of security weaknesses
- Proactive response to audit findings
- Speed of provisioning

- Helpdesk / Security Operations staff reduction
- Reduction in helpdesk calls
- Unified / more efficient processes
- Enabler for changes to sourcing models (eg, offshore outsourcing)
- Reduction in ongoing access management and compliance costs

# Technology Responses

---

## Manual

- ✓ Shorter implementation
- ✓ Simplified solution

- 
- × Doesn't build sustainability
  - × Time consuming / costly
  - × Non-comprehensive
  - × Non-integrated
  - × Reoccurrence of problems / compliance gaps
  - × Prone to errors

## Automated

- ✓ Extensive functionality
- ✓ Consulting support
- ✓ Improved quality of service
- ✓ Long term cost effective compliance with regulation
- ✓ Efficiency Gains

- 
- × Complexity
  - × Customization costs
  - × Risk of scope creep
  - × Fit against requirements

# Just some of the existing products

---

## Established Identity Mgmts Products: *(Provisioning Tools)*

- ▶ Oracle Identity Manager
- ▶ Sun Identity Manager
- ▶ IBM - Tivoli Identity Manager
- ▶ Novell Nsure Identity Manager
- ▶ CA - eTrust Admin

## *(Reporting Tool)*

- ▶ Aveksa – Reporting and Access Recertification Tool

## Observation

- Non-comprehensive
- Significant customisation required
- No silver bullet
- Cost / timescales / complexities
- Continuous product development
- Does not answer who has access to what within the company.

# Key Elements of Periodic Access Review

---

- ▶ Policies and Procedures, Training and Instructions
- ▶ Validation of completeness (i.e. “Good” data)
- ▶ Evaluating judgment of reviewers
  - ▶ Appropriate knowledge of system roles and permissions
  - ▶ Appropriate knowledge of job responsibilities
  - ▶ Segregation of duties
- ▶ Communications of system access changes
- ▶ Timeliness of system access changes made as requested

# Case Study Discussion

---

- ▶ Example of a manual review process
- ▶ Example of an automated review process

# Additional Questions?

---

- ▶ Eric Brothers
  - ▶ (404) 817-4419
  - ▶ [eric.brothers@ey.com](mailto:eric.brothers@ey.com)
  
- ▶ David Schroth
  - ▶ (336) 605-7656
  - ▶ [david.schroth@ey.com](mailto:david.schroth@ey.com)