

# Protecting Accenture

Lock. Block. Protect.

accenture



## Automating Compliance Evidence

Jeff McIlrath, CISSP

May 10, 2005



**A control without evidence, is not a control**



For any Caddyshack fans in the audience -

***“The Zen philosopher Basho once wrote -***

**A flute without holes, is not a flute;**

**And a donut without a hole, ....**

**(Gift to the first person completing the quote)**



.... is a danish.



## Agenda



- Business Problem
- Identity & Access Management Components @ Accenture
- Identity Management Activities Completed
- Implementation of Self-Service Functionality
- Upcoming Identity Management Activities
- Launching Your I&AM Program
- Lessons Learned
- Questions



# BUSINESS PROBLEM

# Accenture's IT Infrastructure / User Demographics



- **Globally distributed infrastructure**
  - 4 globally dispersed Data Centers – US, Spain, Philippines, India
  - US Data Center outsourced
  - 180 Accenture offices
  - 99% Microsoft shop
- **Applications**
  - Over 1,900 applications
  - Move to make most internet-accessible
  - Strong push to consolidate onto SAP and Microsoft Sharepoint
- **User Base**
  - Approx. 140k users in 48 different countries
  - Comprised of Accenture employees, Affiliated Companies, independent contractors, clients, vendors
  - Complex access requirements based on user type
  - 80% of workforce on any given day working outside of Accenture offices

# “Before” I&AM



## Before a formal Identity & Access Management program was launched at Accenture –

- No governance over access control administered at the application level
- Individual security administration processes for each application
- No central view of “who has access to what” across applications
- Repetitive authentications
- Redundant provisioning processes
- Reliance on the Help Desk to adhere to control processes

# Accenture's Response



**In response, Accenture has launched an Identity & Access Management program with the following objectives -**

- Strengthen internal controls thru standardized provisioning processes
- Decrease cost of controls thru automation, self-service and re-use
- Aggressively leverage an offshore delivery model
- Provide easily auditable evidence of efficient, effective control operations

The program was launched due to it's **business case** for cost savings and control improvements. Sarbanes-Oxley has emphasized the program, and helped shape its evolution.

# Business Problem



**What can be done to ease the burden on operations, while ensuring that controls are operating effectively and adequately evidenced?**

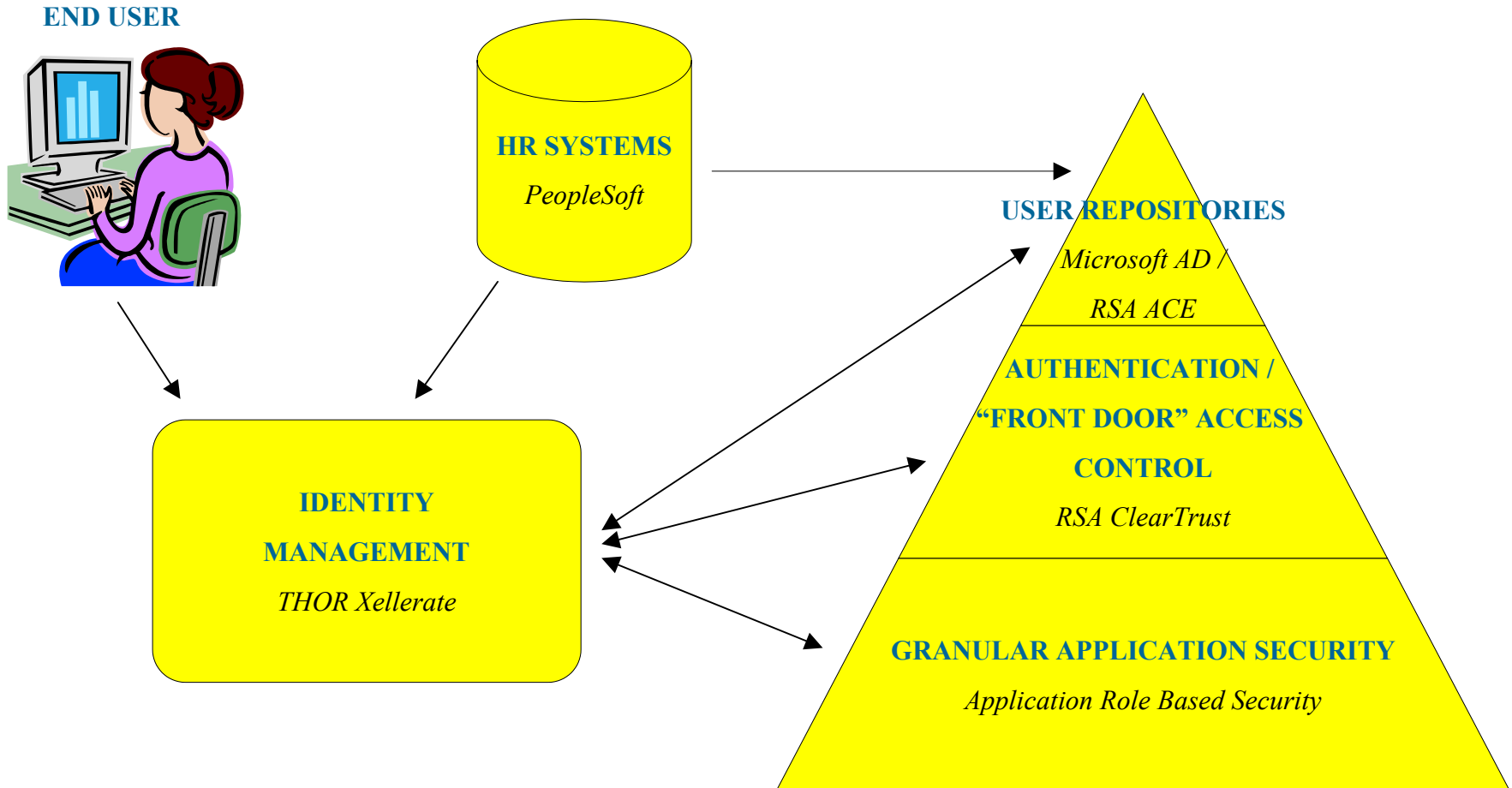
- Sarbanes-Oxley is requiring companies, like Accenture, to operationalize appropriate internal controls to ensure the integrity of their financial statements.
- This requires documentation of the control and periodic testing to ensure the control is operating effectively.
- This periodic internal testing, and periodic testing by Auditors, requires extensive evidence to be available to substantiate the controls existence and effectiveness.
- Accumulating and retaining control evidence is time consuming, monotonous, tedious, and **one of the most important activities of operations**.



# IDENTITY & ACCESS MANAGEMENT COMPONENTS AT ACCENTURE



# I&AM @ Accenture



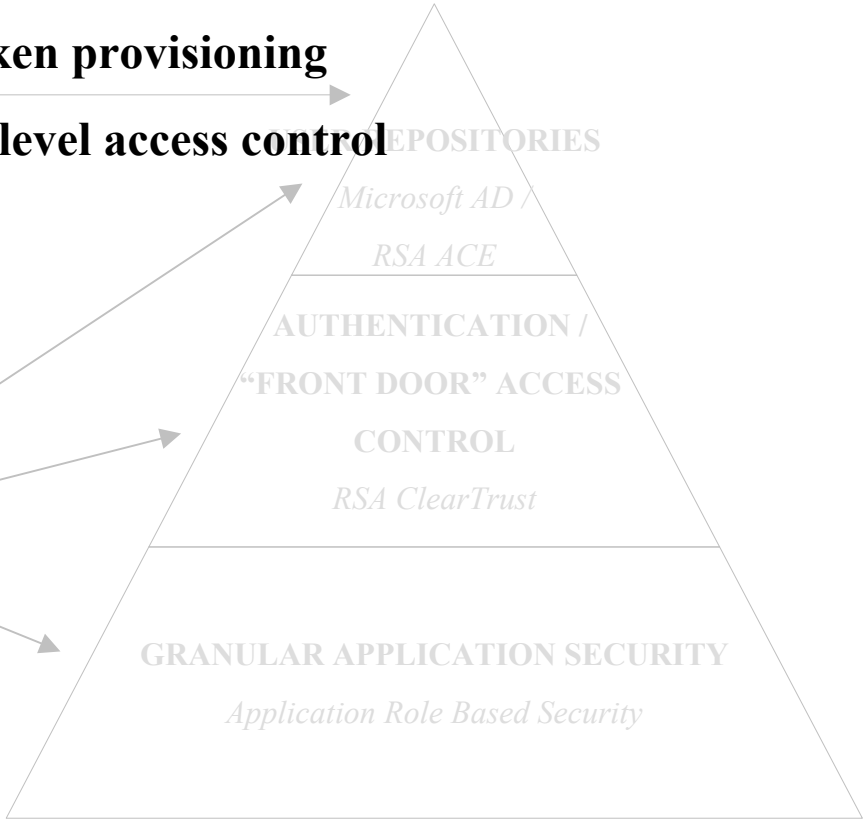
# I&AM @ Accenture – End User



## END USER



- Self-service PW Reset
- Self-service SecurID Token provisioning
- Self-service Application level access control



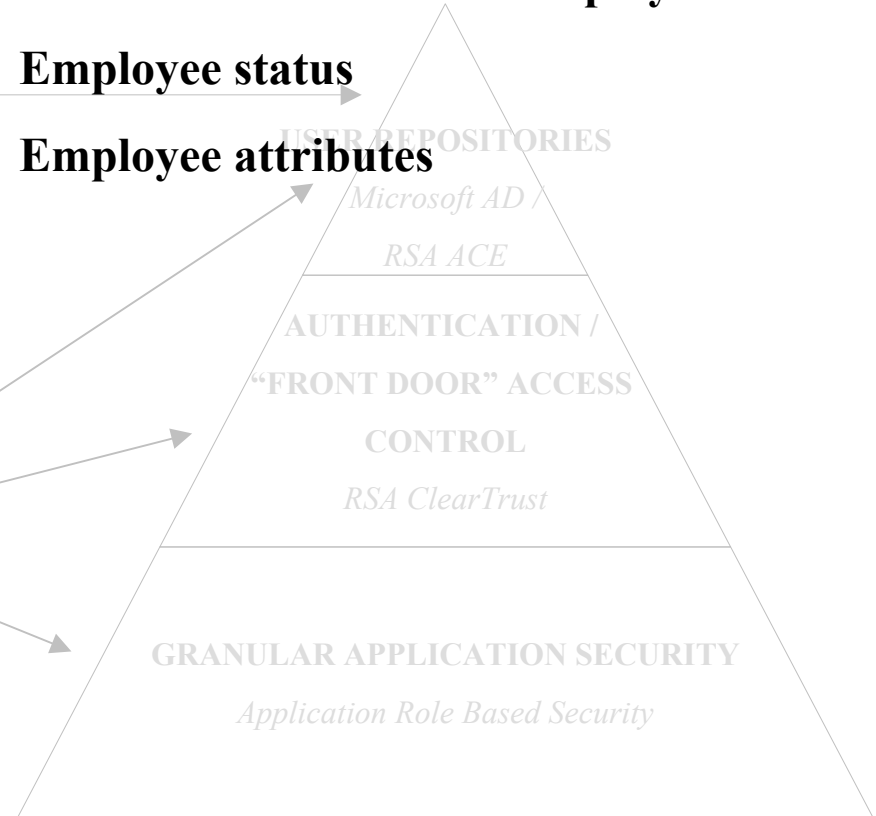
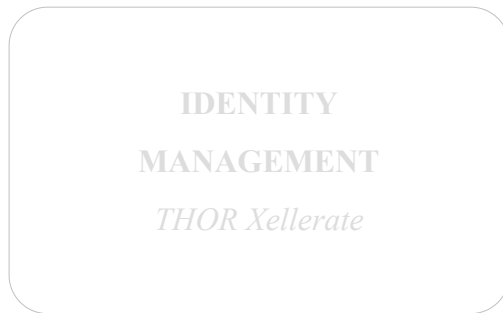


# I&AM @ Accenture - HR

END USER

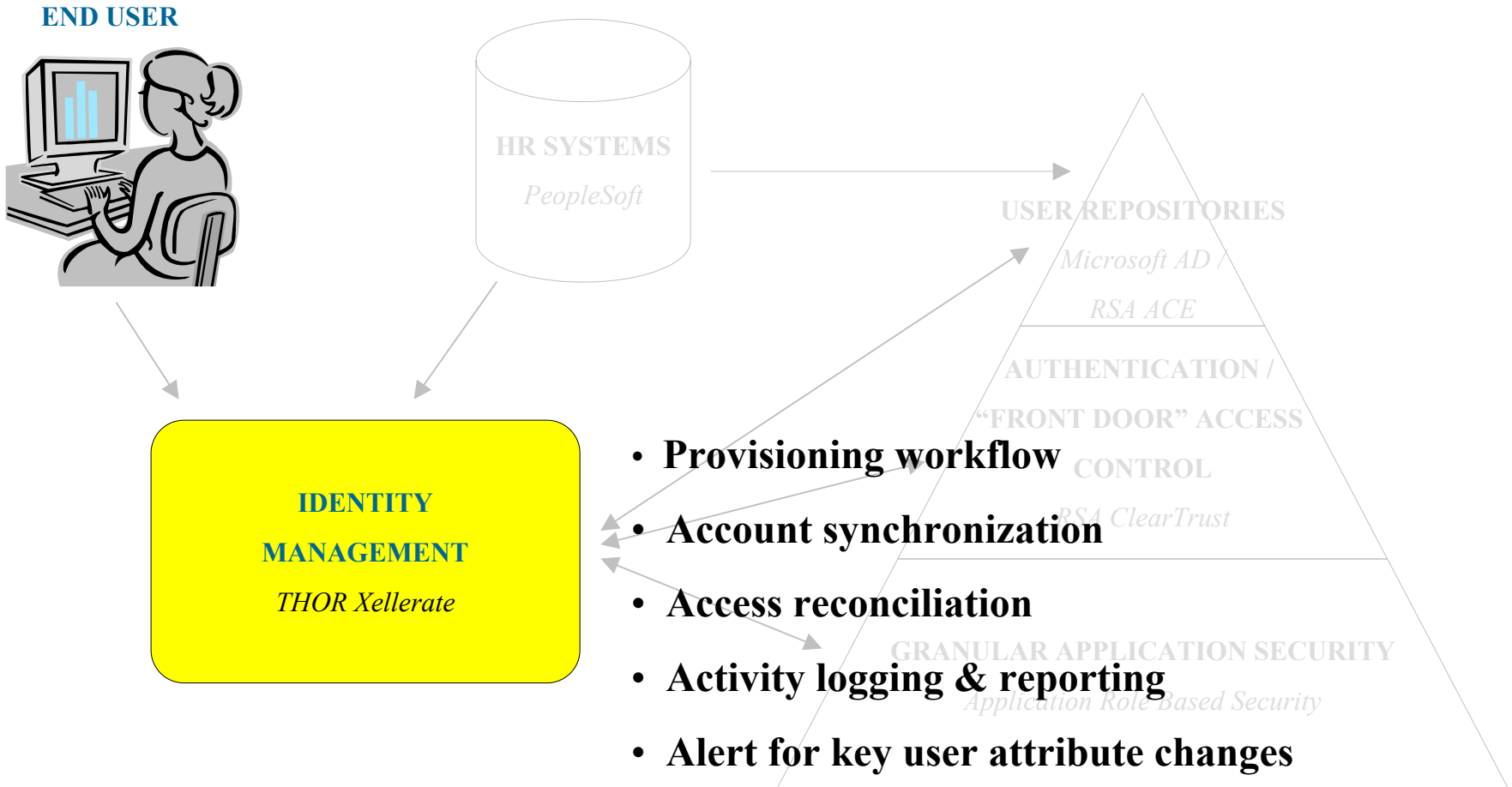


- **Authoritative source for employees**
- **Employee status**
- **Employee attributes**





# I&AM @ Accenture - Xellerate



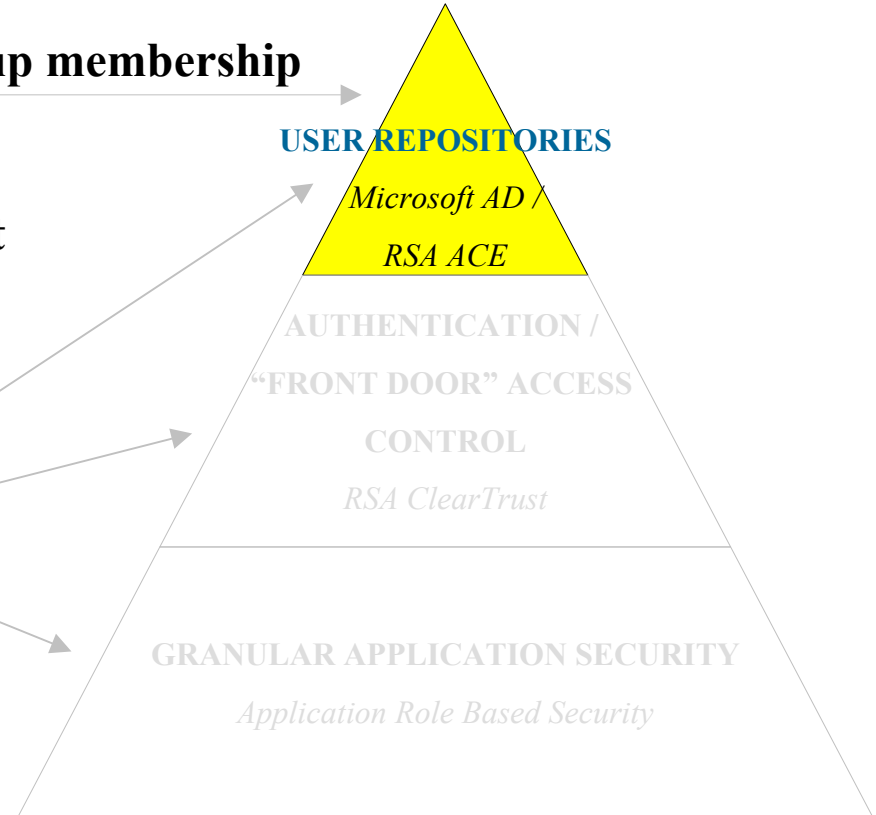
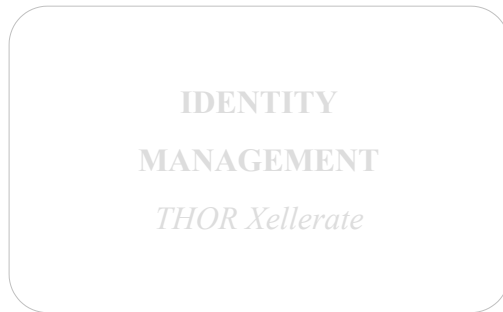
# I&AM @ Accenture – User Repositories



END USER



- User repository – single & two factor authentication
- Active Directory group membership
- User attributes
- Account management



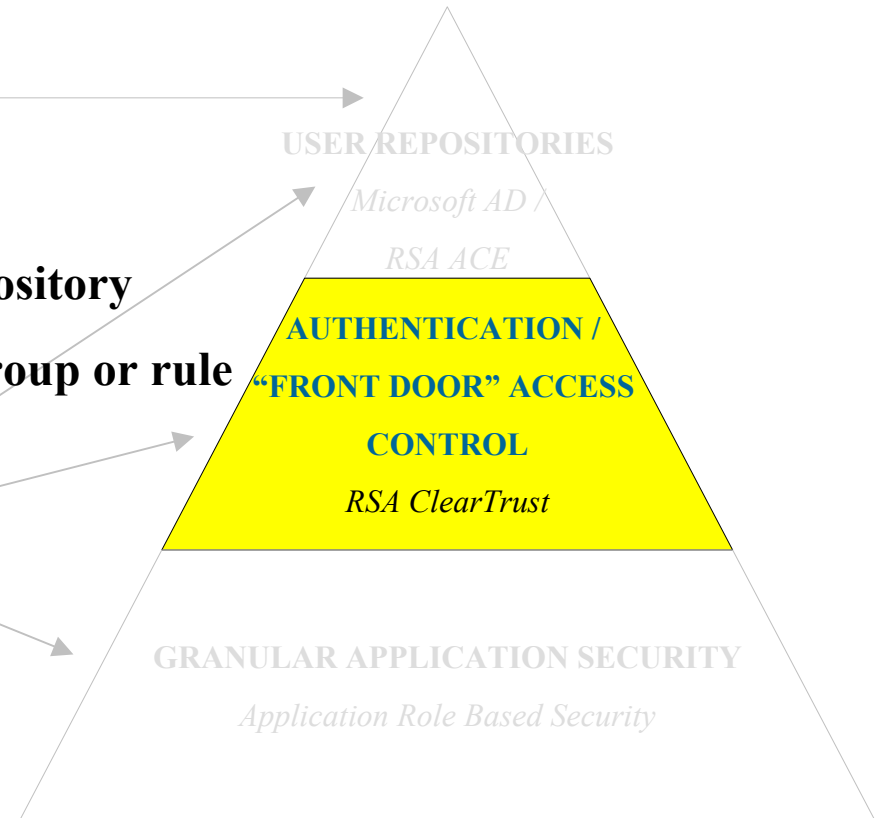
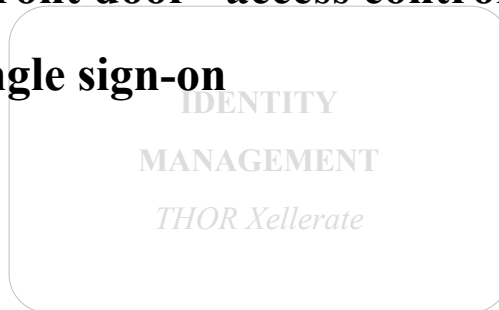
# I&AM @ Accenture – Authentication / Authorization



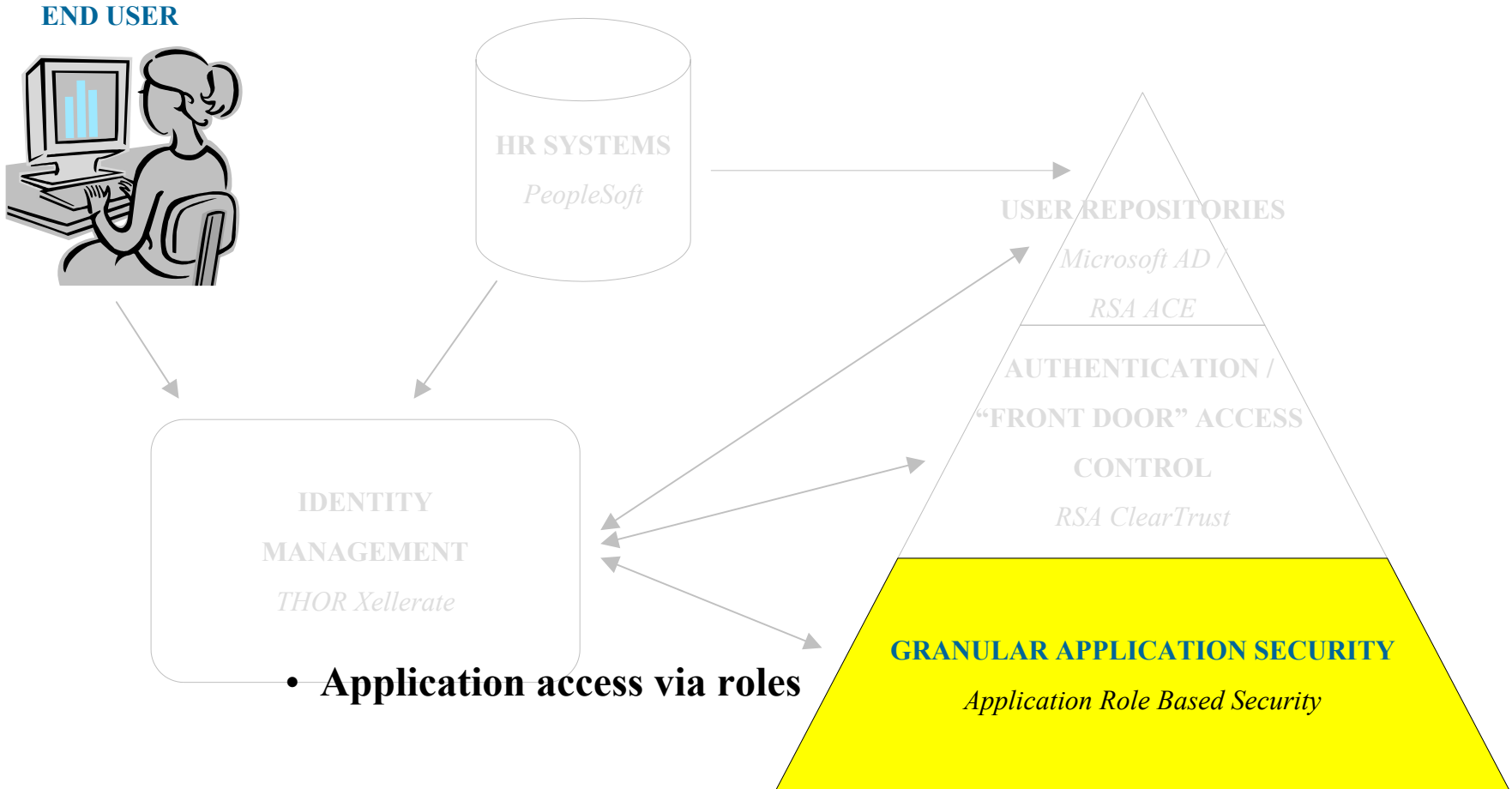
## END USER



- User Authentication – app to user repository
- “Front door” access control via AD group or rule
- Single sign-on



# I&AM @ Accenture – Application Level Access Control





# IDENTITY MANAGEMENT ACTIVITIES COMPLETED

# Self Service PW Reset



## Business Case

- Time to develop – ~4 months with 3 developers
- Currently realizing a 62% reduction in Help Desk calls
- 3 year Internal Rate of Return of 41%
- Payback period on investment of ~19 months
- Provides the base infrastructure to build out additional provisioning workstreams

## Control Benefits

- *Provides a systematically standardized, auditable process replacing current manual Help Desk PW reset process*
- *Mitigates social engineering risks*
- *Reporting of successful, unsuccessful resets*

# SecurID Token Provisioning



## Business Case -

- Savings of estimated \$100k from not upgrading existing WebExpress
- Restructured process from what was a 7 screen registration, with an unacceptable failure/dropout rate, to only 1 screen.
- Time to develop – 4 months with 3.5 developers

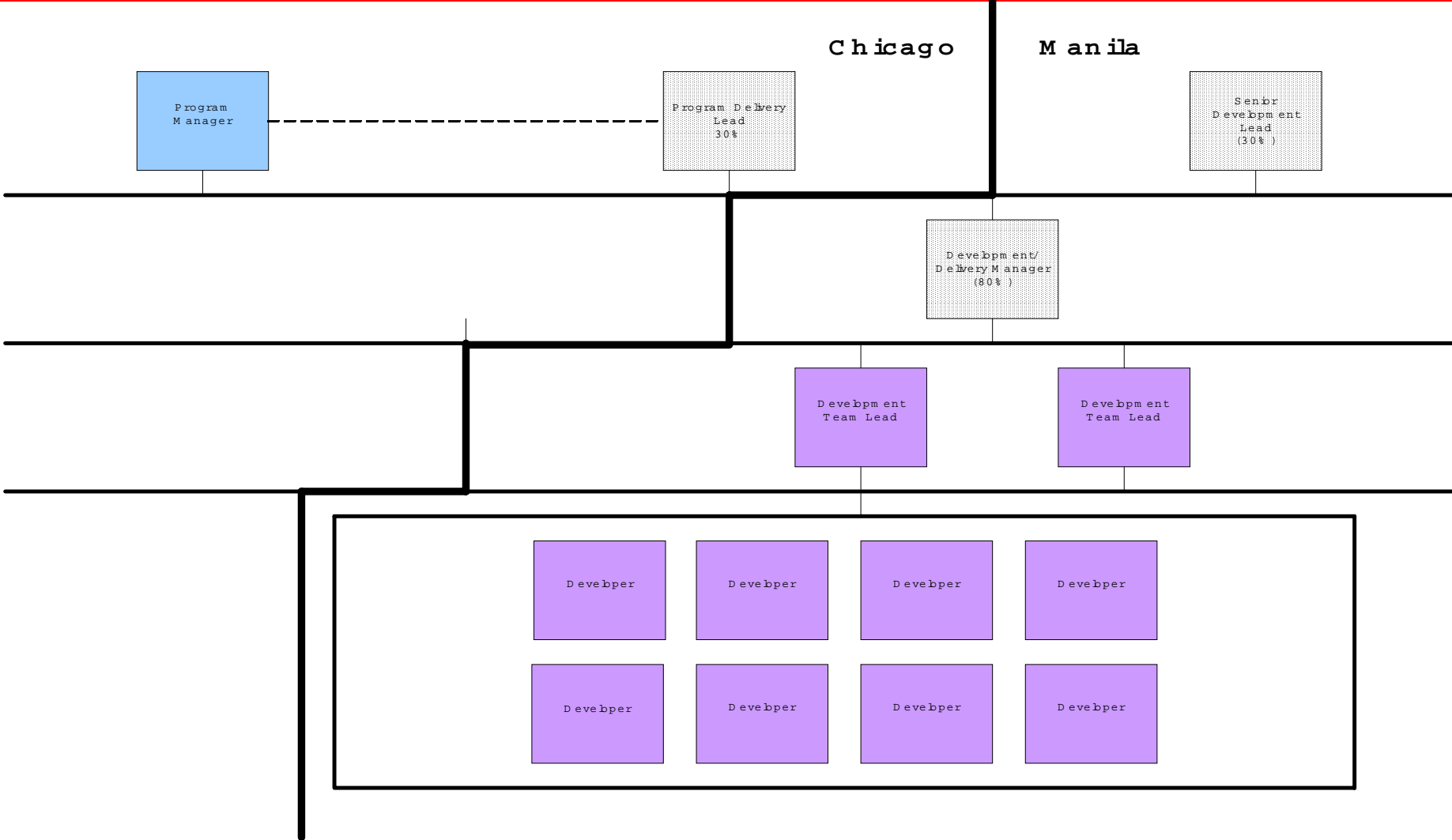
## Control Benefits -

- *Provides standardized, auditable process replacing Help Desk PIN resets*
- *Mitigates social engineering risk for PIN resets*
- *Reporting of successful, unsuccessful registrations / resets*



# IMPLEMENTATION OF SELF SERVICE FUNCTIONALITY

# Our Implementation Team



# Governance Model



**As the Identity & Access Management program has many different customers, we formed an I&AM Steering Committee.**

- Executive-level committee made up of members of Help Desk Services, Directory Services, Information Security, CIO Technical Architecture, and Accenture's Security Practice.
- Membership will change based on development activities, organizational shifts, etc.
- Monthly meetings, geared towards decision making, not simply status updates.

# Requirements / Design



- Worked with teams that were operating current processes to identify requirements.
- Reviewed requirements with Thor PS organization, and Accenture's Security Practice
- Passed requirements, along with subject matter experts (SME) comments, to our Manila development center for detailed design development
- Held final sign-off meeting with development, program management and customer prior to moving into build.

## Build / Test



- SMEs available to assist build; brought in as necessary
- SME code review
- User acceptance test with small team – “friends/family”
- Pilot with ~10% of intended population; selected by GU
- Pilot lasted six weeks
- Monitored and reported on key success metrics
- Significant issues addressed prior to global rollout

# Change / Communications



- Developed support materials for Operations teams and Help Desk
- Developed end user support materials for posting to our internal user support website
- Communicated release of Self-Service processes globally
- Monitored service take up: verification questions, resets, token registrations
- Help Desk instructed to redirect requests to Xellerate where applicable.

# Ongoing Operations



- Help Desk trained to handle common questions
- Help Desk trained to redirect to self-service where appropriate
- Reporting metrics accumulated and presented to Steering Committee
- Technical operations support: % of developer time earmarked for operations; infrastructure support designed in-line with application hosting model.



# UPCOMING IDENTITY MANAGEMENT ACTIVITIES

# Active Directory Account Provisioning



## Business Case -

- Provisioning Active Directory accounts for Non-Accenture users
- Consolidate all provisioning activities into single solution
- Intertwine provisioning activities to eliminate redundancy

## Control Benefits -

- *Provides standardized, auditable process*
- *Logging of business needs for access levels*
- *Increased account lifecycle management*

# Application Level Access Control



## Business Case -

- Elimination of manual security admin activities – account maintenance, **access level reconciliation**
- One process can be leveraged by multiple applications (process cloning)

## Control Benefits -

- *Provides standardized, auditable security administration process*
- *Automatic rogue account identification*
- *Segregation of Duties checks across multiple applications*
- *Centralized “who has access to what” reporting: user or group*

# Web Access Control



## Business Case -

- Centralized “Front door” access control
- Ability to quickly react to changing access requirements to groups of users – affiliated companies, Accenture workforces, contractors, etc.

## Control Benefits -

- *Ensure appropriate access rights; sometimes contract driven*
- *Enhances centralized “who has access to what” reporting*

# Affiliated Company Account Synchronization



## Business Case -

- Cannot load users of some Affiliated companies into Accenture HR systems
- Synchronization will enable use of Accenture resources as if they were merged into Accenture HR systems

## Control Benefits -

- *Provides standardized, auditable process*
- *Provides real-time updates on employment status / attributes*
- *Enables use of self-service tools*



# LAUNCHING YOUR I&AM PROGRAM

# Launching I&AM



- Justify investment by anchoring to ROI of self-service PW reset
- Internally market IRR and control achievements
- Scale application provisioning based on control benefit and any cost savings
- Don't migrate processes just for migration sake
- Become good friends with your Sarbanes-Oxley program manager!



# LESSONS LEARNED

# Lessons Learned – End User Perspective



- Consistent look and feel of all communications
- More detail is better in the communications even if it makes the comm a little longer
- Active support of all sponsors, champions, leads, etc for supporting and enforcing end-user activities
- Pilot, Pilot, Pilot and then Pilot some more
- Users will find things that you never saw before – have good support/response plans in place
- Provide detailed job aids/information/self help
- Have escalation channels/processes in place for questions/concerns raised by end-users
- No matter how clear the directions are, a percentage of the users will call Help Desk for support
- A percentage of users not do what you ask them to – be prepared to identify and address those users

# Lessons Learned – Support/Technical perspective



- Don't underestimate learning curve required by your internal development team
- Get consultants (**Accenture's Security Practice, for example**) or your vendors Professional Services organization involved early on in your planning – before detailed design
- Work closely with Help Desk – daily meetings at the beginning of rollout
- Be prepared to update support docs/web sites/etc numerous times
- Keep necessary support groups involved in all activities
- Prepare reports before go live – they will be critical for ongoing troubleshooting and understanding where issues are occurring
- Make sure plenty of time is given for support teams to be fully trained on the new processes
- Make sure vendors are fully engaged in processes and have skin in the game
- **Celebrate and market your successes**



**What questions do you have?**