

Identity and Access Management

CIO Advisory Community

October 22, 2009

1:30 – 2:30 PM

Agenda

1. Identity & Access Management Program Overview

- a) Current State
- b) Program Vision
- c) Future State
- d) Components
- e) Activities to Date

2. Small Group Discussions:

- a) Active Directory
- b) Password Requirements
- c) White Pages

3. Report Back & Wrap Up

What is Identity and Access Management?

- A combination of business processes, technology, and policies used to manage information about a person throughout the lifecycle of his or her affiliation with OSU.
- Information is used to provide individuals with the right access to the resources they need and for which they are approved.

Identity and Access Management Current State

People

- Few understand process, technology, or integration
- Incomplete view of person's OSU affiliation
- Many user IDs / logins
- No governance
- Most authorization pre-reqs manually verified
- Multi-day process to gain or remove user access
- Little communication among IT staff and across business units
- Many skeptics

Process

- Numerous processes that are complex and confusing
- Not well-documented, defined, or communicated
- Lack of transparency
- Most requests via email with manual provisioning
- Manual reporting
- Fragmented ownership
- Compliance manually tracked (Sarbanes Oxley)
- Reactive to unauthorized access

Technology

- Duplicate entries and errors
- Fragmented
- Overall lack of flexibility and scalability
- Home grown systems
- Many active directories and data repositories
- No system redundancy
- Overall lack of development and testing environments
- Little data synchronization across systems
- Limited or no integration of digital or physical access

Single Points of Failure Across Categories

Identity and Access Management Vision

Students, faculty, staff, alumni and other members of the extended university family must have an intuitive way to find and utilize pertinent information and resources in a streamlined environment that protects confidentiality and intellectual property, promotes security of physical assets, and encourages multi-institutional collaboration.

Identity and Access Management Future State

People

- Fewer user IDs/passwords
- Same day start/stop
- User self-service
- Single view of person's OSU affiliation: identity, pre-reqs, credentials, attributes
- Governance in place
- Broad understanding of technology and capability
- Seamless integration among distributed & central IT staff
- Awareness of source data integration & error impacts

Process

- Simple, defined standards & procedures
- Roles based provisioning
- Workflow enabled
- Enhanced audit and reporting capabilities
- Central standards and local control
- Transparency
- Regulatory compliance
- Separation of duties

Technology

- Interoperable and scalable
- Industry standard software
- Single repository with defined source system(s)
- Appropriately redundant
- Synchronization across systems (real time amap)
- Integrated digital and physical access control
- Fewer active directories and license fees
- Unauthorized activity alerts

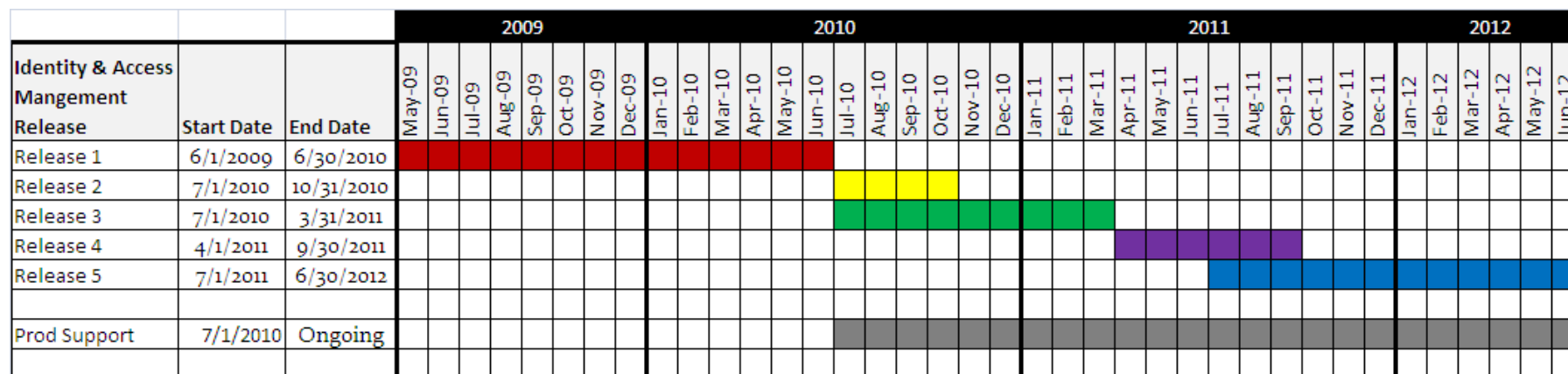
Greater Efficiency, Effectiveness, Business Agility

IdM Program Components

- Auditing & Reporting
- Authoritative Sources
- E-mail Schema
- Affiliate Changes (refers to existing affiliates; includes bio/demographic changes, affiliation type change)
- Federation
- Multi-Factor Authentication
- New Affiliate (includes system access)
- University White Pages
- Password Management (includes self-service, password policy, and simplified sign-on)
- Production Support (includes addressing duplicate ID issues and improving business processes associated with management of identities)

IdM Program Release Schedule

Identity & Access Management Release	Start Date	End Date
Release 1 – Foundation	6/1/2009	6/30/2010
Release 2 - Buckeye Pass Model & White Pages	7/1/2010	10/31/2010
Release 3 – Enterprise Access and Lifecycle Management	7/1/2010	3/31/2011
Release 4 – Federation & Audit Management	4/1/2011	9/30/2011
Release 5 – Distributed Systems & Production Support	7/1/2011	6/30/2012
Production Support - Ongoing Operations	7/1/2010	<i>Ongoing</i>



Release 1: Foundation Project (June 2010)

Deliverables	University Benefits	Unit Benefits
<p>November, 2009</p> <ul style="list-style-type: none"> Document business processes and technical requirements. <p>December, 2009</p> <ul style="list-style-type: none"> Recommend business process changes. Conceptual design of IDM System. <p>January, 2010</p> <ul style="list-style-type: none"> Implementation of business process changes starts. <p>May, 2010</p> <ul style="list-style-type: none"> Create target enterprise active directory structures. <p>June, 2010 (Foundation implementation)</p> <ul style="list-style-type: none"> Password self-service resets and changes. Universal password rules in effect across systems. Automated password synchronization for select enterprise systems (e.g., central email, Carmen, Kerberos). Automate provisioning & de-provisioning for select enterprise systems. Replace current IdM software with a vendor supported solution. Identity repository in place. Identity data for affiliates with name.n identifiers repaired and loaded. Implement reporting and auditing capabilities. Connect Find People to IdM repository. 	<ul style="list-style-type: none"> Password reset calls reduced by ~75% (currently 22% of CIO Help Desk calls). Annual savings ~\$400K. Faculty, staff and student able to reset passwords on demand. Service increase: from 77 hr/wk Help Desk availability to ~125 hr/wk unassisted, a 62% increase. Provisioning and de-provisioning occur real time. Service increase: from minimum of 24-48 hours to immediate Fewer central systems and staff supporting identity and access management (from ~5.5 oCIO FTE to ~3 FTE). Annual savings \$250K. Reduce current duplicate ID issues, and streamline processes to mitigate creation of duplicate IDs. (From minimum of 8 FTE to 2 FTE.) Annual savings \$600K. Industry best practices enabled (e.g., standard application of password rules, fewer passwords to remember, automated auditing, intrusion alerts, 360° view of individual's affiliation). Cost avoidance: \$243/identity breached Establish foundation (business rules, configuration, technology) to reduce authoritative sources for OSU identity data. Service increase: sets the stage for role-based provisioning and other future benefits. 	<ul style="list-style-type: none"> Reduced calls to local Help Desks. (Estimate 75% reduction in password reset calls). Total annual savings across units ~\$300K. Faculty, staff and students can have necessary enterprise system access on Day 1. Productivity gain: \$1M (~25K employees with avg salary of \$17/hr, 2 hours productivity gain), plus guests Toolset to quickly connect local systems to IdM services. Utilization of central repository of ID data to populate local systems (in place of data entry, in some cases). Consistent, accurate identity data across all systems ensures data integrity and requires less staff time to focus on identity issues. (Annual savings of \$600K reported in prior column) <div data-bbox="1507 1219 1866 1317" style="background-color: #cccccc; padding: 5px; text-align: center;"> <p>Total Release 1 Cost Savings: \$2.55M/year</p> </div>

Activities to Date

- Established program charter and governance structure
- University constituents defined technical requirements; validated with Technical Advisory Group
- Completed review of IdM software marketplace
- Prioritized components into release schedule
- Collaborated with David Pike and Unified Communications team on Active Directory recommendation
- Began process validation and requirements gathering for IdM components
 - 24 of 34 sessions completed

Small Group Discussions

Enterprise Active Directory

- What are the challenges & obstacles for your unit to achieve this?
- What can the OCIO do to make this successful?
- What can your unit do to make this successful?

Password Requirements

- Do these seem like the right password requirements?
- Missing anything?
- What do we need to be aware of in implementing?

White Pages

- What are the desired features, functions and services?

Discussion Facilitator:

Brian Keller

Discussion Scribe:

Chad Wulf

Discussion Facilitator:

Keith Kidner

Discussion Scribe:

Kristina Torres

Discussion Facilitator:

Joyce Wagner

Discussion Scribe:

Diane Owens

Small Group Report Back

- Share the top 3 discussion points from your small group discussion.
- Note items to share during Report Back to full Advisory Community.

Wrap Up

- Next Steps:
 - Incorporate your input into requirement gathering and process validation documentation
 - Analysis of requirements (November)
 - Recommendations (November/December)
 - Conceptual Design (December)
 - Design & Begin Implementation (January)
- All session materials posted at cio.osu.edu/advisory (by Oct 30)

Contact Information

- **Program Team:** ids@osu.edu
- **Program Director:** owens.3@osu.edu
- **Web Site:** cio.osu.edu/projects/ids