What is Identity Management?

“Identity management is the set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities.”
-- The Burton Group

Identity and Access Management (IAM) relates to:
- Identity proofing – the process for verifying someone’s identity before issuing them an ID/password
- Authentication – when a person signs on to a network or attempts to access a resource, the process of comparing the offered NetID and password with the identity system/directory.
- Authorization – after a person is authenticated, the process of providing access to services for which that person is authorized (and preventing access to services for which the person is not authorized).

An IAM system includes both policies and governance (which involves a broad range of people from across the campus) and the technical software and hardware provided by IT. An effective and efficient identity system will provide the authority and responsibility to make additions, changes and deletions to the appropriate department or office and not leave everything in the hands of IT.

Federations

A federation is an association of organizations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions. Through the use of a federation, authentication is done at the home institution (identity provider) and the authorization is done by the owner of the resource (service provider).

Federated identity management involves the management and use of identity information across security domains, e.g. between individual universities. It deals with issues such as interoperability, liability, security, privacy and trust.

Advantages of a Central IAM System

- Scalability
- Agility: Deliver new services, quick changes in population
- Reduce complexity
- Improved user experience
• Audit and security

Institutional Benefits

• Budgetary and Resource efficiencies
  o Shared or federated authentication for common system applications.
  o Reduced staff requirements.
  o Increased security by focused experts.
  o Reducing duplication.
  o Provisioning of account faster—do it once vs. multiple services.

• Consolidated implementation of policy.

• Provisioning of roles (contractors, guest speakers, non-traditional, etc)

• Role change and new implementations – more efficient.

• Enhanced security and privacy measures
  o Consolidation of logging.
  o Reduction of departmental based/single service databases.
  o Fewer passwords and credentials to manage.

• Ensuring compliance
  o FERPA/HIPAA
  o Federal and State legislation (use of SSN)

• Improved troubleshooting procedures; Reduced time to resolve problems (with common directory, and documentation of roles and services).

• Ease of use by customer.

• Enhanced partnership building between IT and Data/Source Custodians.

• New opportunities for online service providers and third-party vendors.

Challenges

Policy
Who sets policy for IAM?
Who gets to use the IAM system and its attributes?
  • Who approves new populations/roles and services?
  • Appropriate use of IAM (reporting?)
  • Who grants access and to whom (source data custodian?)
  • Third-party requests
Technology needs policy decisions in order to proceed with development paths-
access controls within the IAM application(s).
Security and privacy assurances.
  FERPA, HIPAA
Documentation
**Governance and Leadership**
Identify and engage Stakeholders
- All about the people, not the technology.
- Establish need, buy-in, work collaboratively.
- Know what you want to gain/problem to solve.
- Technologists and functional folks together.
Charter a “governance” team.
Assist with setting policy and procedure
- Charge sub-teams (policy and implementation teams; administrative operations council)
Determine priorities and next steps.
Assess resource needs.
Roles and Expectations – who is responsible for what

**Privacy and Security**
Do you know where your data is?
Many consumers of data:
- Local “shadow” systems storing data on unprotected servers.
Consuming from data warehouse, directory service, instructor and student supplied info.
- Local portals and supporting authentication databases.
- Manual manipulation of data.
- Unauthorized sharing of data. “oh, I have access to that data, let me send you a file”
Ensuring privacy of student data is at the core of our mission.
Central tracking of access.
They all have true business needs.

**Education and Training**
Instead of restricting the data, teach consumers to use and care for the data.
Teach responsibility.
FERPA
Facilitate campus awareness and understanding of the importance and value of IAM.

**Role of the Registrar’s Office**
- Role Definitions
- Privacy
- Policy/Security
- Identity Proofing
- Leadership
- Process
- Education and Training
Key Issues

Each participant was asked to identify a key issue, related to identity management, that they face in their work. Some items emerged as key issues for a number of people. The most frequently mentioned items became the basis for four break-out discussion groups:

1. Identity proofing
2. Role-based authorization
3. Governance
4. Student Lifecycle

Participants joined the group that most closely matched their key issue or held the most interest for them. The groups were asked to keep track of the discussion and report back to the larger group.

Group Report-outs

Identity Proofing

- Changes in FERPA will stop people from using social security numbers and/or date of birth (personally identifying info) will break some business processes.
- Have a basic person record – tag attributes onto that for provisioning/access levels/levels of authentication.
- What are the attribute standards for federating?
- After a person is identity-proofed, there are issues around storing the information. For most of these types of documents, it is not necessary to store a copy of the document itself, but to track and confirm that someone has checked the document.
- If a student ID card is used for financial transactions, the associated number must be protected and proofing should be similar to that used by banks.
- Two-factor proofing is coming.

Role-Based Authorization

- What are the definitions for the roles? Coarse-grained authorizations might be assigned by the university. Finer-grained access might be assigned to an individual.
- Policy/governance are key in defining the services that are available, based on an individual’s role(s) and, particular, in determining who should have that role. It must be decided whether such decisions will be made centrally, or depend on the specific application.
- Roles/groups can be created centrally, but the data steward or application owner should determine the roles/groups having access.
- Provisioning/deprovisioning is based on affiliation. When is a student no longer a student?
- What is the time frame for deprovisioning (wait for a year?). Is there a need for more fine-grained affiliations?
Does deprovisioning need to happen, or should access be limited instead (based on roles)? Does it depend on the service or application?

**Governance**

- Define which issues you want to tackle first.
  - Look at industry standards
  - Proper use of ID info
  - Data governance
  - Move to single identity store
  - Centrally managed consolidated list of roles
  - Documenting and controlling identity feeds between services/systems
- IAM is about providing services to students while protecting resources of the institution
- View the lifecycle and services and develop policies around that.

**Student lifecycle**

- Identify stages of the cycle and the services to provide at each stage.
- Stakeholders/application providers need to be involved in the decisions along the way.
- Having a common language is helpful.
- At what stages will provisioning and deprovisioning occur for various services, as well as for the portal?