Identity and the Cloud: Preparing Your Campus

EDUCAUSE 2010 Pre-Conference Seminar

The State of Identity Management

Self-assessment Questionnaire

Each entry below describes an aspect of identity management in three ways that that suggest a continuum from *basic* to *capable* to *advanced*, from *"just starting"* to *"battle scarred"* to *"been there, done that"*, from *clueless* to *clued-in* to *clue-full*, from *"I bought the book*" to *"I read the book"* to *"I wrote the book"*, from … well, you get the idea.

For each item, consider where your institution is today on a scale from 1 to 10. Observe that the 1 and 10 are sometimes extremes of the primitive past or dreams of a perfect future -- we expect everyone lives in the real world in between. Enter each score in the empty box to the right, subtotal each section, then compute your final total at the end.

This questionnaire is based on an identity management assessment tool developed by Lynn McRae, Stanford University, for the Internet2/Educause CAMP: Building a Distributed Access Management Infrastructure (**http://net.educause.edu/CAMP064**) and updated by John O'Keefe, Lafayette College.

1. Would there be a value for my institution to federate?

Cloud Resources

We rarely if ever look to the cloud to provide resources and services to the institution.	Some external applications and resources are of interest to us.	Leveraging as many cloud resources as is prudent is a key component of our IT strategy moving forward.

1	2	3	4	5	6	7	8	9	10	□

Internal support for cloud services

We have no support structure in place for cloud services, and must rely on our vendors completely.	We have limited support in place for users of cloud services.	We have a solid process in place to support external services that is tightly integrated with our internal support structures.

1	2	3	4	5	6	7	8	9	10	□

External Collaboration

Collaboration with other institutions and entities beyond our own is rare or non-existent.	There is some ad-hoc collaboration with institutions and entities beyond or own.	Collaboration beyond our institution is a key component to our educational and research missions.

1	2	3	4	5	6	7	8	9	10	□

Security of Identities and Authentication

We are comfortable permitting vendor access to BOTH our identity information AND authentication information.	We are comfortable permitting vendor access to EITHER identity information OR authentication information.	We are not comfortable releasing ANY authentication information and only releasing MINIMAL identity information to the vendor.

1	2	3	4	5	6	7	8	9	10	□

2. Current State of Identity Data

Coverage

Our identity management covers just the core community – faculty, staff and students as defined by source systems.	Our identity management includes faculty, staff and students, plus secondary sources like library patrons, conference attendees, hospital staff, etc..	We capture information about all people of interest to IT, schools, departments, central offices, libraries, etc.

1	2	3	4	5	6	7	8	9	10	□

Matching and Uniqueness

We get information from many sources; it's possible someone can be represented multiple times. This is difficult for us to detect except in reaction to service issues.	We have good central identity matching processes, but need to work to resolve identity issues mostly as needed.	We have strong partners and practices across campus and multiple systems that participate in detecting, avoiding and resolving identity issues.

1	2	3	4	5	6	7	8	9	10	

Enterprise reference data and definitions

We must deal with a variety of ways in which our systems handle common data like phones, addresses, buildings and locations, etc.	We have achieved a fairly high degree of uniformity of data of like type, through cooperation and multiple data mappings.	All descriptive data where applicable is governed by local, national and international standards and data definitions are shared across campus systems.

1	2	3	4	5	6	7	8	9	10	

Guests or weakly identified entities

We do not have a centrally supported guest login. This brings weakly identified people into our identity management system that are poorly tracked and managed over time.	We have policies to prevent the abuse of our identity infrastructure, and some infrastructure support for alternatives.	We have a centrally supported guest account infrastructure with policies that do not compromise core identity management.

1	2	3	4	5	6	7	8	9	10	

How fresh is your data?

We periodically gather information from sources on cycles that can vary from daily, to weekly or longer.	We regularly gather information from sources, generally no less than daily.	We have realtime or near-realtime connections to source and client systems that allow service and access changes to take effect in minutes -- on or off -- when data changes.

1	2	3	4	5	6	7	8	9	10	

3. Current State of IdM Infrastructure

Integration technologies

We gather information from sources with a mix of flat file transfer, reports, direct SQL access, and/or email.	We rely on batch processes but use consistent techniques with our clients and a common secured infrastructure.	We have realtime access to data, e.g., through LDAP, as well as an enterprise, message-based integration infrastructure.

1	2	3	4	5	6	7	8	9	10	

Identity Store

We have many (Student, Faculty, Staff, etc) that don't connect	We have many and some connect	We have a unified and central Identity Store

1	2	3	4	5	6	7	8	9	10	

SSO and Authentication

We have separate authentication credentials for access to different institutional services.	We leverage unified authentication for access to different institutional services.	We have implemented a single sign-on solution for access to different institutional services.

1	2	3	4	5	6	7	8	9	10	

4. Policies and Practices

Identity Management Roadmap

Identity Management Roadmap? We don't need no Identity Management Roadmap.	An Identity Management roadmap is under development.	An Identity Management roadmap is in place and being actively maintained.

1	2	3	4	5	6	7	8	9	10	

Account Provisioning Process

Our processes are manual, ad-hoc, and not documented or well understood.	We have a mix of formal processes and those created on an as-needed basis. Some are automated and some are not.	Our processes are established, automated, and documented.

1	2	3	4	5	6	7	8	9	10	

Account de-Provisioning process

There is little connection between central IT support for core infrastructure and business systems, and distributed school or departments system. There means many independently maintained shadow systems with poor data sharing and little automated updates from common sources.	We can make data available, through reports or directory lookups to more directly enable local systems, but actual reuse is inconsistent across campus.	We support collaborative work in schools and departments by enabling them to define and share information and privileges on their own. It is easy to access common enterprise data, either for realtime reference or for ongoing synchronization.

1	2	3	4	5	6	7	8	9	10	

Access rule consistency

IT staff may find themselves making access management decisions where business rules don't exist and no decision-making body exists.	Policies providing a framework for consistent access management decisions are in development or in place.	Business units base access management decisions on policies and the classification of the data being protected.

1	2	3	4	5	6	7	8	9	10	

Who gets to say who gets to say?

We don't have firm policies or guidelines governing who can manage privileges or groups. People are enabled "as needed".	We have general workplace guidelines that designate who can manage privileges and groups controlling access to services.	We have policies that establish responsibilities and a chain of authority for group and privilege management.

1	2	3	4	5	6	7	8	9	10	

Cohesiveness of effort

We have little or no development, test, and user acceptance environments, with no source system involvement.	We have development, test and user-acceptance environments, but inconsistent source system involvement, and problems with authentication/SSO.	We have end-to-end test, development, and user-acceptance environments with all sources and consumers, and cooperative processes for planning change.

1	2	3	4	5	6	7	8	9	10	

5. On the Road to IdP

eduPerson

We don’t have it or not sure what it is.	We have heard about it and/or partially implemented it.	We have fully implemented and leveraged eduPerson on our campus.

1	2	3	4	5	6	7	8	9	10	

Practices

Our practices are ad-hoc at best.	We have a mix of formal practices and those created on an as-needed basis	Our practices are established and publically posted.

1	2	3	4	5	6	7	8	9	10	

Federating Software

We don’t have it or not sure what it is.	We have heard about it and/or partially implemented it.	We have fully implemented and leveraged eduPerson on our campus.

1	2	3	4	5	6	7	8	9	10	

Staffing

We are stretched thin on staffing, especially with respect to Identity Management	We have some staffing efforts partly dedicated to IdM, but it is a best-effort and often these staff are pulled away to other projects.	We have staff dedicated to managing and growing our IdM infrastructure.

1	2	3	4	5	6	7	8	9	10	