Governance and the Student Life Cycle (panel discussion)

Dennis Skovsted, University of Minnesota
Karen Hanson, University of Wisconsin
Beth Cate, Indiana University
Andrea Beesing, Cornell University
Keith MacIntosh, Pima Community College

Dean Woodbeck, Internet2 (scribe)

******

Tasks forces, data steward teams, IdM advisory groups – universities give them different names, but the concept is the same. For effective governance and policies for IdM systems, it is essential to develop a team approach and include stakeholders from many different campus areas: registrar, IT, HR, student services, financial services, and others.

Identity management can also mean identity cards and smart cards, which means also involving the campus police and facilities representatives. Campuses also talk about “cradle to endowment” relationships, which means involving staff from the alumni and fundraising offices, as well as athletics.

It seems you can’t cast a wide enough net when it comes to IdM governance.

Here are some of the main points and themes that emerged from this panel discussion.

Centralize the IdM Database

Campuses have gone through cycles of centralization and decentralization of IT services. One result may be separate IdM systems for different constituents – such as a student system and a separate alumni system – and various departments or schools may operate their own IdM systems.

For an effective IdM system and to have an effective SSO system across campus, all identity records need to reside in the same location.

- Cornell has all records in PeopleSoft, which has greatly simplified parts of the IdM management function.
- Pima Community College uses Banner as its authoritative source for its IdM system.
- Wisconsin has used PeopleSoft since 1999 and is now replacing a homegrown IdM system with the Oracle Identity and Access Management Suite.
• Minnesota has a number of separate systems, but it looking toward a “cradle to endowment” philosophy, with all constituents – from students to alumni to season ticket holders – in one identity system.

Governance by Involvement
It is essential to involve campus stakeholders in the process of developing policies and procedures that relate to IdM governance. Data stewards must be a part of this process.

• Cornell has several advisory and policy groups that guide the IdM process and decisions:
  o IdM advisory group
  o Administrative systems priorities committee
  o IT data management council
  o IT security council (defines requirements for secure systems and propagates those throughout campus). The IdM manager frames the issues for the group to address.
  o Data stewards group – responsible for data that requires protection

• The multi-campus Indiana University system has several levels of involvement, as well.
  o A committee of data stewards, including legal counsel and auditor, have the responsibility to review old policies and develop new policies related to access management. An access management subcommittee is looking at several systems, including HR and student information, to map who needs access to what information. These efforts will culminate in a set of practices and policies for a role-based IdM system.
  o An IdM task force has formed to frame the challenges, issues, and opportunities for the IdM system. The long-term goal for this body is to feed into the policy-making process and, ultimately, a governance structure for identity management.

• The University of Wisconsin established an IdM Leadership Group (IMLG) In 2004, charged with demystifying IdM on campus and developing an enterprise-wide approach to identity management issues. Key to effectiveness of such a committee is including high-level positions at the table (facilities, police, library, HR, registrar and others). Among the committee’s responsibilities and outcomes:
  o Seeking efficiencies, and strategic policies and procedures, in part by define IdM processes, roles and responsibilities, and documenting how decisions are made.
Assumed the responsibilities of, and eliminated disparate committees, such as a security committee and a photo ID committee.

Created an appropriate use policy for the existing directory system and created a template for creating new NetIDs.

Working at eliminating the number of ID cards on campus, such as merging door access and photo ID cards. With the advent of a new photo ID card, the committee is developing policies and practices to define who has access to the photos.

Governance by involvement can be a messy procedure. You can expect those coming to the table to bring their own agendas. One of the first tasks, when spinning up the group, is to educate them about IdM and the main campus-wide issues. You need to get them to focus on the policy issues.

Multiple Roles

Things can get tricky when an individual has multiple roles. Some institutions address this by having a primary affiliation, with a set of business rules associated with those roles reflected in the enterprise directory. If an individual’s primary role is “staff,” that is what rules, subject to FERPA, in some situations.

FERPA and Privacy

In the situation in which an employee takes a class, regardless of their primary affiliation with the university, their student records are protected by FERPA.

When using a federation to provide services, the IdM system needs to account for cases in which a student has a privacy block on certain data. An ideal system would allow individuals to approve the release of information and attributes. This will involve some education, because blocking the release of certain attributes may prevent access to a service or, at least, hinder some personalization or other features.

On the flip side, open records laws may prevent university staff and faculty from blocking certain information. One university had a situation where a faculty member was being stalked and wanted to suppress certain information that is deemed public (the names, times and locations of courses being taught). Under most open records laws, at state institutions, all of that information is public.

Balancing Security and Convenience

A key challenge is educating people about the need to balance security and convenience. Users need to understand why additional security measures become more important (required password changes, prompting for security questions) and IT people need to understand user needs for simplicity.

International Issues

International programs and campuses present another layer of complexity for governance. Distributing user IDs and passwords can become complicated if a country
does not have a reliable mail system (or if they do not receive mail from the U.S.). Laws and privacy protection varies from country to country. Having a representative from the international programs office on the data stewards committee may help in identifying potential pitfalls.

**Governance for Exceptions**

Each campus on the panel discussed the ways in which they accommodate exceptions to identity management policies and procedures. Most of these involve guest accounts for research associates or others with short-term access needs.

- At Wisconsin, accounts for loosely affiliated individuals are the responsibility of the office that has the responsibility for the particular person in question.

- Minnesota uses a "sponsored account" in which a guest must have a sponsor who becomes accountable for that ID. When someone gives an ID to a volunteer, the person giving the ID is responsible.

- Indiana, like many universities, has people on the network that are not faculty, staff or student, and have had accounts for years. People become entrenched and want to keep their accounts. The concept is to make these accounts the responsibility of the appropriate campus stakeholder, then educated those stakeholders as to the risks associated with such accounts and the resources required to continue to support the accounts.

- Cornell’s approach is to get business rules into policy and identity those who have authority to issue NetIDs. There is a push to have even loosely affiliated IDs entered into the ERP system, so that all those with Cornell IDs can be accounted for.