IAM Governance

Terms

For the purposes of this topic (and the referenced documents) the following terms are defined:

Governance

> *This is a fairly broad area even within IT. The focus of the term for this space is specifically on Identity and Access Management Governance, which may be a standalone set of committees and working groups in large institutions, a single committee of a larger IT Governance structure, or a subset of topics or priorities addressed by a single Governance body.*
>
> *The purpose of IAM Governance is to establish or endorse policies that communicate stakeholder agreement or direction on how subjects or identities are to be represented and what services they are entitled to access. Additionally, they may evaluate proposed IAM projects and set priorities depending on the makeup and charter of the governance committee(s).*
>
> *Data Governance is closely related to IAM and in many cases is handled by the same committees. Controls around data security, access to data, release of data (e.g. identity data attributes) are all either directly or indirectly impacted by Identity and Access Management.*

Policy

> *A policy is typically described as a principle or rule to guide decisions and achieve rational outcome(s). The term is not normally used to denote what is actually done, this is normally referred to as a procedure. In IAM a policy frequently establishes the way subjects are classified such as distinct "affiliate populations" with the university and what services they might receive. Additionally, policies deal with student and employee lifecycles, security around password management, etc. IAM Systems can be thought of as the technical "implementation" of IAM Policies and Business Practices.*

Stakeholder

> *Stakeholders are typically anyone impacted by an action. Whether that's the creation of new user accounts or the assignment of a subject to a group that enables access to a resource. Usually, stakeholders have the authority to make decisions about the people, data or resources they're responsible for. IAM Governance is usually made up of key stakeholders from various departments or campus organizations directly impacted by an IAM System - e.g. Registration & Records, HR, Admissions, Legal, Library Services, Internal Audit, IT, Business and Academic systems, etc.*

Overview (problem description)

***** See Notes from ACAMP 2010 - IAM Governance Session**

While Identity Management has always had an underlying need for a governance body to make decisions on policy around who should have accounts, how often to force a password change or what resources or applications can be accessed by an authenticated user, IAM Governance has become much more "critical" in the last few years as the scope of this field has expanded to include "Access Management". Centralized authorization capability or at least the value-added feature(s) of assigning roles, groups and entitlements to subjects has pretty much required that institutions form groups of stakeholders to decide what "roles" are defined or how affiliates are classified, and subsequently what services these different populations get access to. Even though the decision of who/what gets access is usually left up to the resource owner, the decision is more frequently being based on attributes provided by an Identity and Access Management System (IAMS).

This site will highlight how some universities have implemented IAM Governance to provide guidance and support (Policies) to the technology implementors of IAM components and systems, in an effort to provide a framework and tools (presentations, peer institution examples, etc.) to assist those institutions struggling with implementing their own IAM Governance.

Use Cases (examples)

Use cases in the context of IAM Governance is a bit different than in other topic areas. The approach taken here is to list situations where there is a need to have some stakeholder group authorize or endorse a Policy or policy (formal or informal) or Business Practice, needed to implement some aspect of an Identity and Access Management System (IAMS).

1. In order to assign an "affiliation value" (e.g. alumni, contractor, vendor, parent, library patron, researcher, guest, spouse, etc.) to certain populations of subjects that are not considered traditional members of the community - students, faculty and staff - a governance group of stakeholders (HR, Registrar, Audit, Safety, Legal, Library, Graduate School, Alumni Affairs, etc.) must establish a list of Affiliate values. Subsequently, resource and application owners need to decide which affiliate groups can have access to their services and what privileges they have. These policy decisions will then be incorporated into the IAM provisioning "rules" for populating roles, groups and entitlements related to these services.
2. When a student leaves the university, their accounts and access to applications and services remain active until the help desk is notified they have left (e.g. withdrawn, expelled, graduated). In order to tighten up the security of these "open" accounts the university administration has requested that student accounts be automatically disabled when they leave. The details of what and when leaving "means" need to be defined and established as policy so that it can be technically implemented within the IAM system, and that the responsibility for this decision is owned by the Stakeholders of the Governance committee making the policy and not IT.
3. (Similar situation to #2, but the subject is an Employee who is terminated or retires). Again, the Governance body needs to define "when" access is disabled and for "what" services. If the employee needs to retain access to payroll information (to obtain W2 information for tax purposes) but

not have any access to Library Services, that needs to be decided upon so de-provisioning of access to the restricted services can take place according to what the policy states.

4. Federated Identity Management (FIM) involves multiple institutions trusting each other to abide by a set of established practices. In the case of Identity Providers, a limited set of attributes about subjects are released to Service Provides so that they may determine whether the subject should be allowed access to the resource. The attribute release policy (ARP) of an institution - "which" attributes get released - needs to be established or endorsed by an IAM Governance Committee, particularly if there is a "default" set of attributes that are released to any service provider in the federation.

Regulations

Some IAM Governance decisions are driven by regulatory requirements such as FERPA, HIPAA, Sarbanes-Oxley, PCI-DSS, Federal and State Privacy Laws, etc. These regulations may be in conflict with Academic goals and governing bodies frequently have to make decisions around the appropriate course of action.

Case Studies and White Papers

1. Penn State Governance Council (Online Content)
2. University of Southern California IAM (Online Content)
3. University of Southern California EDUCAUSE 2008 presentation on Data Governance and IAM (.pdf presentation)

Tools

-

Links

- **Identity Management Governance - CAMP 2011** Presentation Slides (.pdf), Notes from Panel Discussion (.pdf)