Access Management Survey Questions

The Identity and Access Management (IAM) Technical Architect Group (TAG) was formed by Kevin Morooney, the vice provost for information technology at Penn State, in July 2009. The primary responsibilities for this group are to gather stakeholder requirements, turn these requirements into technical requirements documents, design, architect and prototype solutions, and support integration and implementation, as outlined in the IAM Final Report and Recommendations.

As an IAM stakeholder, you are critically important to the development of a successful IAM implementation at Penn State. As such, we would like to ask for your assistance with defining the requirements for Access Management, as outlined in Strategic Recommendations 4 and 7, of the IAM Final Report and Recommendations. For additional details on Access Management, refer to the Access Management Overview available in the Resources section of the IAM Community site.

The IAM TAG team has developed a survey to solicit your input for Access Management. Please take a moment to complete the survey. Feel free to skip any question you are unable to answer. Likewise, we invite other staff with your area who may have valuable insights to the challenges related to IAM. Please have those staff members contact iam@psu.edu to partake in the survey.

As you complete the survey, you may encounter use cases that you feel are relevant. A use case is a situation or scenario whose consideration could help define the Access Management requirements. Please include these use cases along with the responses to the survey. For your reference, we have examples of IAM use cases available on the IAM Community Site.

One of the core concepts of Identity and Access Management is the management of access rights to resources (content/services) - ensuring they are appropriately and efficiently granted, auditable, and updated or removed when circumstances change. The purpose of this survey is to solicit your input on several aspects of access management. The areas are:

- access control via groups, roles and/or attributes
- policy engine - access control via business rules
- compliance - auditing, reporting and/or monitoring activities to meet regulatory requirements
- use case - describe challenges that are not addressed by current survey offering

If you are interested in taking the survey, please submit a request to iam@psu.edu. Shortly after your request is received, an invitation to take the survey will be sent to you. Survey responses must be submitted by Friday May 14, 2010.
**Group Access**

Currently groups can be used to control access to content, services and other resources. In this case a group is a collection of people that exists in the Penn State Directory, based on Lightweight Directory Access Protocol.

- **Class Groups** – A class group contains all of the students registered for a particular course, location and section. The information for a course group is based on student enrollment activity in Integrated Student Information System. A group is created for each course, location and section. When a student adds a course, he/she is added to the group. Conversely, when a student drops a course, he/she is removed from the group. The instructor(s) of record for the course are also members of the groups and have administrative rights to add/remove users manually (via the User Managed Group (UMG) interface, https://umg.its.psu.edu/). The UMG interface allows users to create and manage groups of users, as well as restrict access to this group to a number of Web-based services.

- **Standing Groups** - A standing group is based on data that is provided from IBIS (Integrated Business Information System); its membership is updated daily. Some examples include:
  - psu.facstaff - contains all full-time Penn State faculty and staff at all campus locations
  - staff.up.cis - all ITS employees
  - psu.up.faculty – all faculty members at University Park
  - psu.up.staff – all staff members at University Park
  - all of the other campus locations have two groups like the UP ones

- **User Managed Groups** - Groups that can be managed by users, via the UMG site located at https://umg.its.psu.edu/.

Examples of content/service are:

- **Content** - Web-based content located in one's Penn State Access Account Storage Space; via https://protected.personal.psu.edu/ an individual can control who has access to content stored in his/her PASS.

- **Service** - The ITS Downloads site, https://downloads.its.psu.edu/, which uses groups to control access to downloads that are only available to Penn State faculty and staff.

**Question**

*The IAM TAG is investigating solutions to enhance the existing functionality provided by groups. What are some of your requirements and/or enhancement requests for utilizing groups in your application(s)?*
Roles
Roles are used to group University members together and specify access restrictions via attributes. Some examples are:

- Financial Roles - Currently, financial roles are used within Penn State's Workflow application to control access and determine the routing of forms within the system. Workflow is Penn State's Web-based hosting system for University academic, administrative, and financial management processes, specifically pertaining to review approval needs. An example of a financial role is a financial officer role. This role has a defined set of attributes that determine the characteristics of the role. An example of a form within Workflow is the Termination (TRMN) form.
- Academic Roles - This role permits for the ability to review/approve Undergraduate Education Travel Request (UGTR) and Sabbatical Request for Leave (SABB) forms via Workflow.
- Human Resource Roles - This role permits for the ability to review/approve Termination in Workflow.
- Notification Roles - This role is used by Penn State's Housing and Foods (HFS) to, for example, notify users about purchases made via eBuy.

Question
The IAM TAG is currently investigating solutions to enhance the existing functionality. What are some of your requirements and/or enhancement requests for utilizing roles in your application?

Attributes
An attribute is a name/value pair that exists in the Penn State Directory. An example is the common name (cn) attribute. It has a name, cn, and can have multiple values. Attributes can either be single-valued or multi-valued. A single-valued attribute can only hold one value; an example is the displayName attribute. A multi-valued attribute can hold multiple values; an example is the cn attribute mentioned above. Some other examples of attributes are:

- Person's Affiliation
- Department
- Administrative Area

Question
The IAM TAG is currently investigating solutions to enhance the existing functionality. What are some of your requirements and/or enhancement requests for utilizing attributes in your application?
Central Access Management Services
Currently there is not a consistent central mechanism by which users may access groups, roles and/or attributes that reside in Penn State's Directory. In most cases, one typically needs to either develop the software or purchase a solution in order to interface with the Directory.

Question
If such a central mechanism can be developed, what are your requirements for it? (For example, Web-based services/applications in your area that would need to rely on such a mechanism).

Compliance
Ensuring that only authorized users are granted access to content/services for which they have been granted access is an important aspect of access management. Several key components are:
• reporting mechanisms for displaying authorized users and their privileges
• auditing of the addition/deletion of users and/or privileges
• monitoring access to content/services

Question
What are your requirements for auditing, reporting and/or compliance monitoring related to access services?

Central Policy Engine
A policy engine provides centralization of access controls based on business rules. This service separates the business rules from the application code providing consistent policies across the organization, easy maintenance of the business rules and auditing/monitoring of all changes. An example is controlling access to a document so that only faculty in a particular department are granted access. The central policy engine could have a rule that would check to determine if a person meets the requirements for access and returns via a service a yes/no as to whether or not the person may have access.

Question
If a central policy engine could be developed that will allow you to apply business rules to control access to content/services what are some of your requirements for such a service?
Priorities
Rank by importance the features you would like to see implemented or select the features you would like to have implemented

1. A **group** is a collection of people, which can be used to control access to content, services and resources.
2. A **role** is used to group University members together and specify access restrictions.
3. An **attribute** is a name/value pair that can be used control access to content, services and resources.
4. **Central Access Management Services** is a consistent, central mechanism used to access groups, roles and/or attributes.
5. **Compliance** is insuring that only authorized users are granted access to content/services for which they have been granted access.
6. A **central policy engine** provides centralization of access controls based on business rules.

*Please number each box in order of preference from 1 (most important) to 6 (least important):*

- Groups
- Roles
- Attributes
- Central Access Management Services
- Compliance
- Central Policy Engine
- Other (list here)

Administrative Data Access
Integrated Student Information System (ISIS) is the centralized student system that manages records for all Penn State Students at all Penn State locations. Integrated Business Information System (IBIS) is the electronic business system that manages financial and human resources data. Two-factor authentication is required to access either system.

**Question**

*Do you have any recommendations for improving the process for granting access to higher risk services and/or protected data? Some examples include:*

**IBIS**
**ISIS**

**NOTE:** Please answer this question based on the current functions of your job. For example:
- Data Steward - an administrator or designee who is responsible for Computerized Institutional Data
• Access and Security Representative (ASR) - an individual, usually an administrator of a major University office (e.g., college or campus) or designee, who coordinates requests from administrators, faculty and staff within the unit for access to: University Institutional Computer and Network Resources; specific production capabilities; Computerized Institutional Data; and system development, processing and communications tool
• End-User - any individual who uses University Computer and Network Resources

**Additional Information - Use Cases**

Do you control access to content or services via a method that is not acknowledged in the groups, roles and/or attributes questions? If so, please provide a brief description about how you control access.

Do you have additional comments and/or use cases (example of problems)?