**Identity Management Practices – What services can the Institution provide if we……**

The business of attracting, recruiting, admitting, registering and generally providing services for and on behalf of students is, today, delivered electronically and dependent upon the “network”. Often, the information and services rendered are tailored specifically for an individual and its (information) release may well be protected by federal or state regulation and/or minimally by institutional policy. Thus, assurance that the individual is “who they say they are” is critical in order to provide a network-based service while remaining “compliant”. Connecting the physical person (student) to their associated digital record within the institution’s electronic environment and assessing the strength of that connection is the essence of “Identity Proofing” and the associated Level of Assurance.

Identity-Proofing practices can and do vary across institutions and have evolved based upon the business processes, culture, and technical environment of each college or university. Each institution offers a buffet of virtual services and often wishes to enable access to specific individuals or groups IF it is deemed SAFE; that is, displaying/releasing the information is complaint with known regulations and the practices used to establish identity are deemed “reasonable”.

However, what practices are “reasonable” to ensure that the credential is being used by the person it was (thought to be) issued to? How should digital “credentials (e.g., IDs and Passwords) be delivered to clients and does the delivery mechanism affect their robustness? What information or service presents a “high risk” to the institution if compromised or released inappropriately? The institutional may need to assess the risks associated with the introduction of a new information service, but well established business practices constrain them from adopting the “best” IAM practices. How can these administrators perform a risk assessment within their identity management domain? What if the institution only deals with their clients remotely and needs to provide their services quickly?

The purpose of this exercise is to provide an inventory of IAM practices(e.g., identity proofing techniques, standards (e.g., LoA), credential delivery practices, applicable regulations, information services, the level of risk associated with each service and use case examples (affiliation with the institution) that provide a means of performing an IAM assessment. In other words, matching the services and their associated risks to IAM and security practices that support them. This may be done in a variety of ways but a good analogy/model is the password entropy spreadsheet or by placing certain variables into an iPhone app (wheels) and seeing if the combination is “valid”. .

Capturing the thoughts of the January 15th InC-Student meeting and M&M’s deliverable.

* We want to list Services provided to campus
* Then apply a “risk” (L,M,H) associated with the service or data
* Then gauge the LoA required for accessing the Service
* Then (possibly) the population or affiliate type - matched against the Service

Narrative or write-up would include a description of the above …

**Purpose of the Exercise:**

*To come up with a methodology for determining whether an individual should have access to a Service, based upon their affiliation with the university and the university’s LoA that the credential being used to “access” the service was appropriately tied to the individual. (Is the university CONFIDENT ENOUGH, that the user of the credential is the person it was assigned to)?*

1. Should the **affiliate** type (e.g. Prospect, Student, Alumni) have access to the **Service**?
2. Does the **Risk** of exposure or “data release” require an elevated **LoA**? (and if so – what level?)
3. Does the **Credential** being used by the individual have the required **LoA** tied to it? (Which means was it issued and “tied” to an individual after the appropriate amount of document vetting and ID-Proofing was performed)?

**STEPS to Develop this Application/Table/Webapp:**

1. List all [*insert appropriate scoping term - e.g. university, Enterprise, major, etc.*] Services to be captured by this process
2. Create columns for all **affiliates** defined for the university (the scope of this task should ideally include all affiliates that are issued any type of login credential)
3. **Assign** a level of **RISK** to the data associated with the **Service**, mapped across all **affiliates** (in most cases the RISK level will be the same for all, but depending on the service it may vary). Many of these “cells” may be blank if the affiliate type should never have access to the service.
4. **Map** a **LoA** to the **RISK** level
5. Define the **Credential** required for each **LoA** including:
   1. Strength of the credential (PWD strength, 2-factor, 3-factor, Biometric, etc.)
   2. Vetting procedure (documentation required and extent of verification – background checks, references, etc.)
   3. ID-Proofing required (Government issued ID – 1,2,3)
6. Ensure that each member of the university has a **LoA** tied to each **credential** (preferably only one?) assigned to them.
7. **Configure** each **Service** to only allow access by users with the correct (allowed) **affiliation** type and a credential with the required **LoA**. (Either by the credential itself – Cert may contain required information - or by **entitlement** attributes)