One of the goals of the new IAM model will be to automate the provisioning of access to resources and applications—reducing the time it takes for new users to gain access, while at the same time ensuring the access granted is appropriate and meet security and standards and policy. Basic access could be provisioned (granted) in initial broad strokes based on Affiliation. As the affiliation is further defined through the use of roles and attributes, additional more finely tuned access can be automatically granted as well. The timely updating of directory services is critical the success of timely and automated provision.

The new model for affiliations and related statuses and attributes will give the University the ability to define relationships (that may include certain inherent rights for access) in a way that did not exist before. Assigned Roles in WebRAT as well as the new departmental identity will all dovetail with the new affiliations, and other current data sources to help to clearly describe an individual’s relationship with the University in a very specific context—creating an identity profile or view of each person. Access should be able to be automatically provisioned and de-provisioned as that profile changes.

One individual’s profile may look like the following:

Staff Employee – currently employed [Assigned automatically through the hiring process]
Admin area 056 [Assigned automatically through the hiring process]
Departmental Identity Housing & Food Services [Assigned automatically through the hiring process]
Role – Financial Officer [Assigned by human intervention using WebRat approval process]

Another individual’s profile may look like the following:

Student – currently enrolled [Automatically assigned when accepted]
College of Communications [Assigned when accepted to the college]
Major of Media Studies [Assigned when enrolled in the major]
Currently Schedule Classes/Sections: Speech Communications 100, Astronomy 101, ... [Automatically assigned in the course enrollment process]

The examples above are simplistic and do not attempt to outline actual relationships but are meant to convey the concept of an identity profile. However, it is reasonable to assume that certain levels of access to university-wide and departmental resources and applications could be granted based on this type of model. The access rights would be dynamic and could also change automatically based on changes as the individual moves through the cycles inherent with employment or enrolment in the University. Different business processes including hiring, promotion/job change, enrollment, registration for classes, and others would update the profile—directly and automatically impacting the provisioning of access to certain resources and applications. Departmental workflow would also play a part in the building and updating of the profiles.
Not all provisioning will occur automatically. There will be certain scenarios, resources, applications, that will continue to be provisioned manually based on a request to a data steward/applications provider and a related evaluation of the request and decision to either grant or deny access. These types of instances would normally be at the departmental level. Examples would include access to special research data/applications, and departmental applications where access is granted on a case-by-case basis or where the granularity required to make the access decisions it not represented in the broader identity profile.

Even when taking into consideration the continued need for manual provisioning, the new IAM model offers the potential to significantly enhance the current provisioning by increasing the efficiency based on input from current business processes that are already in place. If successfully implemented the University would realized increased productivity, a higher level of customer satisfaction, and greater security through more timely de-provisioning of access when circumstances change.