Understanding IAM – Functional Categories and Components

- **Identity Management**
  - Identity Governance Administration (IGA)

- **Accountability**
  - Access Reports

- **Audit Reporting**
  - Logging and Auditing

- **Authentication**
  - Single Sign-On (SSO)

- **Authorization**
  - Access Control (AC)
Goals

IAM Riverside (Identity Governance)
- Move from old technology built locally to an enterprise level tool
- Create a canonical identity that addresses identity issues now and in future (i.e. Lived Name)

Password Management & Access Governance
- Move from technology built locally to an enterprise level tool (MyAccount)
- Develop more capability for password management
- Implement and streamline automatic provisioning of access

Access Management
- Move from technology built locally to an enterprise level tool (EACS)
- Develop more modern capability for access management i.e.
  - Guest federation
  - Independent of UCPath

Develop a Robust Foundation to Mature IAM
Current State

Identity Life Cycle
- Enterprise Directory
- Legacy IAM Database
- Legacy EDIR Scripts
- Identity Database
- MyAccount
- Legacy IAM Scripts
- Legacy EDIR Scripts

Provisioning Fulfillment
- Identity Database
- Legacy IAM Scripts
- Legacy EDIR Scripts

Workflow
- Legacy IAM Scripts
- Legacy EDIR Scripts
- Identity Database

Environment Administration & Interfaces
- Entitlements Management
- Access Request
- Data Stores
- Authentication
- Audit
- Policy & Role Management
- Access Certification
- Reporting & Analytics
IAMRiverside Timeline

- **March**: Workshops
- **April**: Initial Design
- **May**: Final Design
- **June**: Fischer Implementation
- **July**: UAT
- **Aug**: Prod Env Set up
- **Sep**: Support Post Go-Live
- **Oct**: N/A
- **Nov**: N/A
- **Dec**: N/A
- **Jan**: N/A
- **Feb**: N/A
Other Campus Stakeholders

- CSC
- SOM
- UNEX
- APO
- Staff Development (HR)
Future Provisioning Process

1. Department Authorized Person
   - IAMRiverside Person Account Request

2. Shared Service Center
   - Fill out the New Hire Template in UCPath (provide the NetID)

3. IAMRiverside
   - Matching Process
   - Provision the identity

4. Process the accounts (LDAP record, UCR email, access to wireless, VPN, DUO based on the request)

5. UCPath
   - Send 1-280 to UCR

6. Keep ID and disable the accounts (LDAP record, UCR email, access to wireless, VPN, DUO)

7. Populate attributes of the NetID with data from 1-280 and adjust roles (audit and verify roles etc.)

8. Process New Hire Template