Identity and Access Management Next Generation

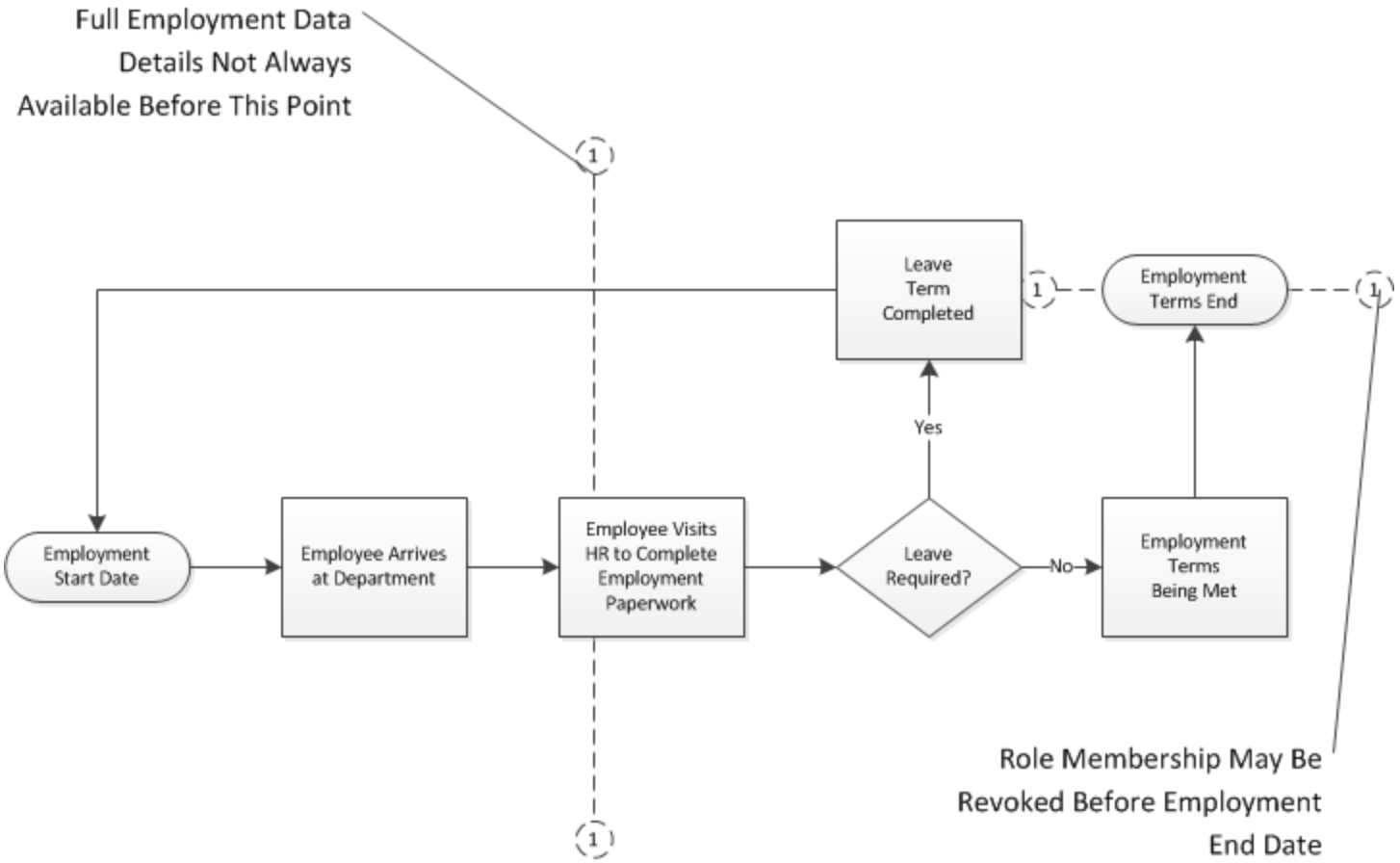
February 2014 Update to CTSC

ROLES

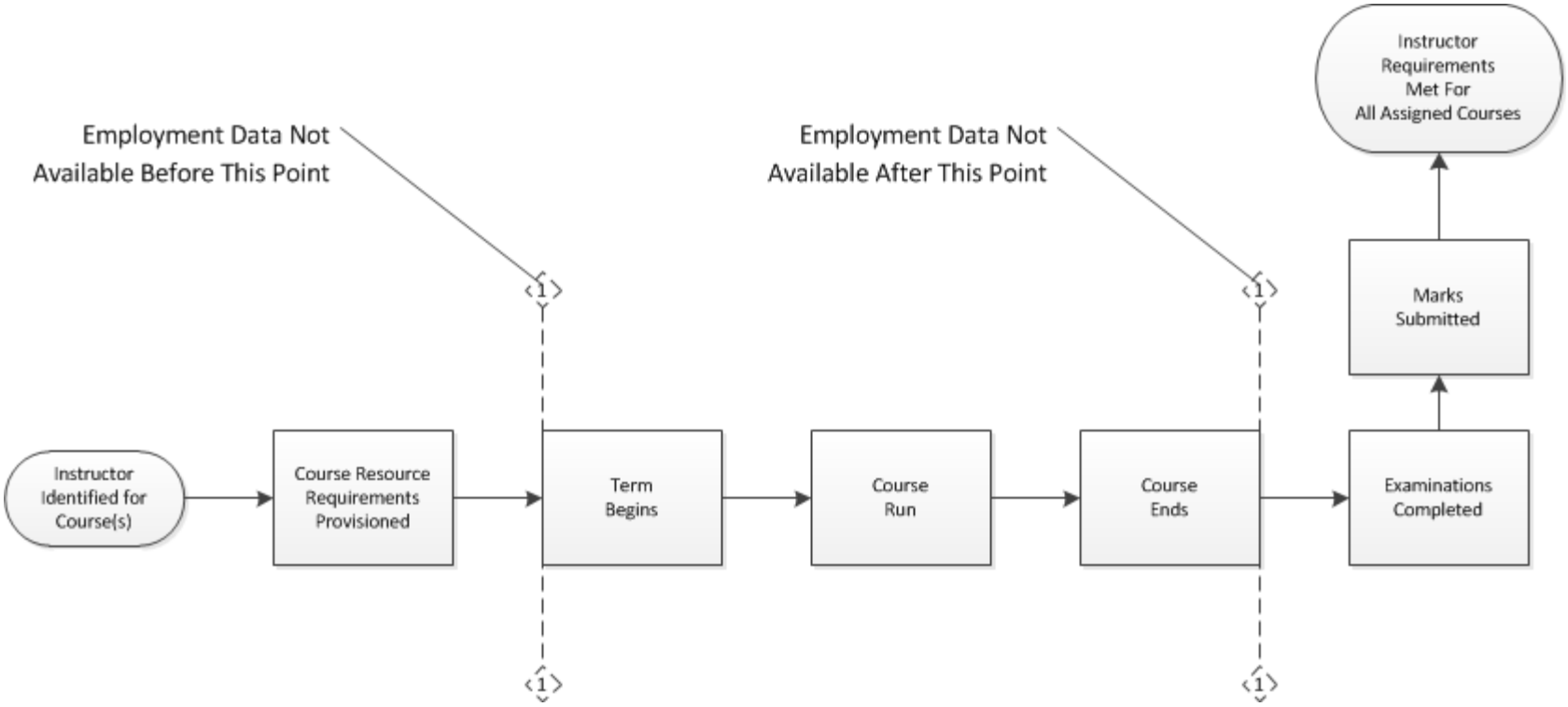
Discussing Roles

- Group formed in late 2013
- Representation from IST, AHS, Arts, Engineering, Environment, and Math
- Contribution #1: Role Inventory
- Contribution #2: Unique Role Lifecycles

Observation #1: Role Lifecycle



Role Lifecycle, Example #2



Conclusion

- Employment data is often insufficient to sponsor the full lifecycle of employee roles
- Administrators must have the ability to remove role membership manually, regardless of the presence supporting data

Observation #2:
Learner Role Membership

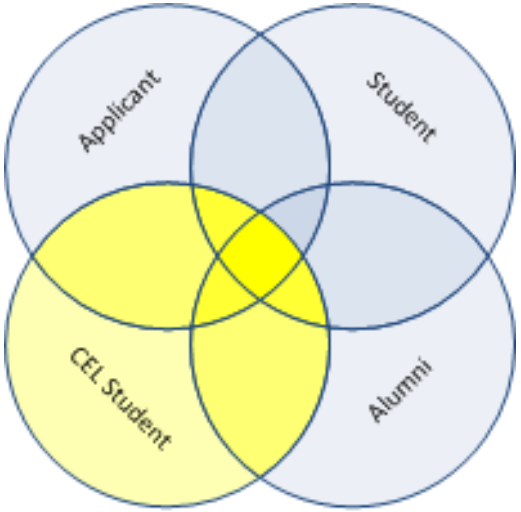
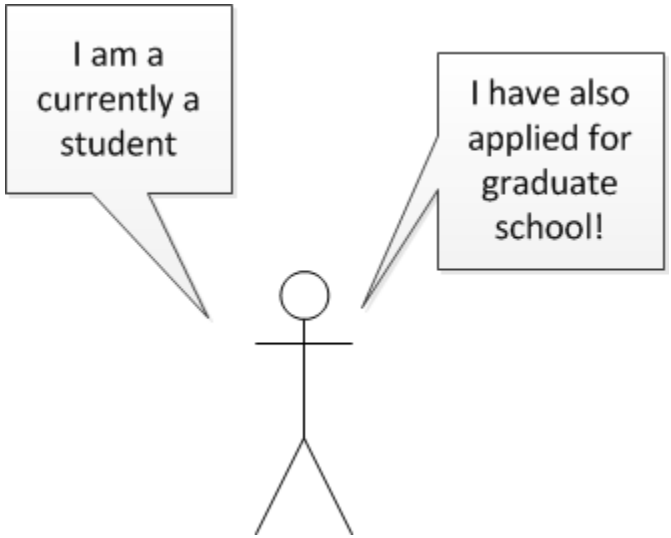


Diagram 1.1



Observation #2
Employee Role Membership

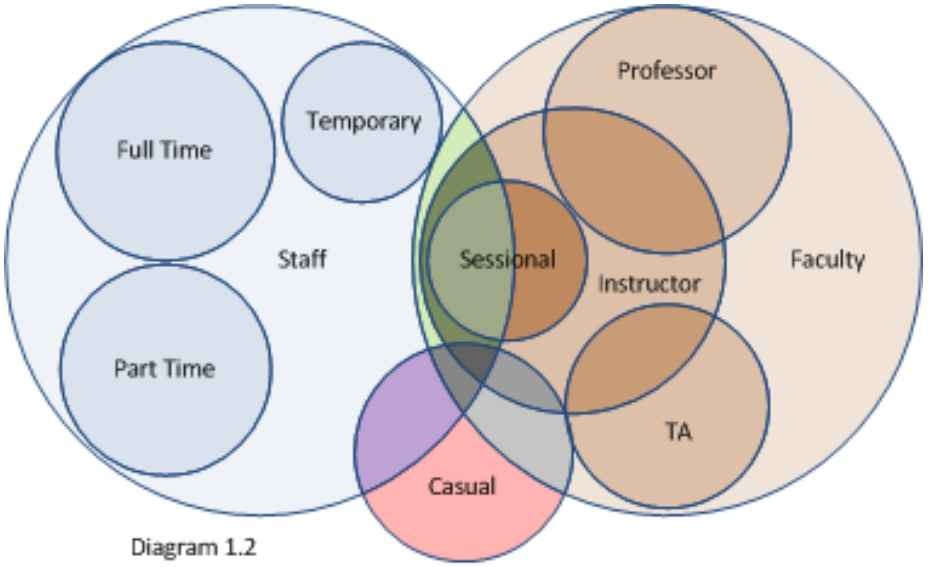
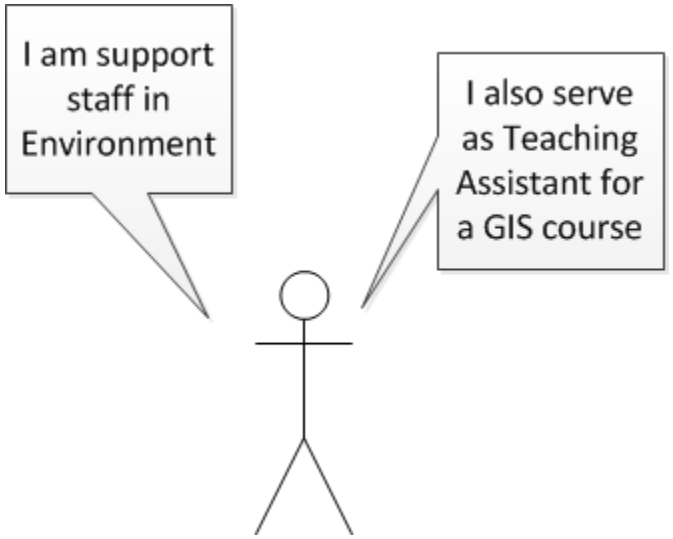
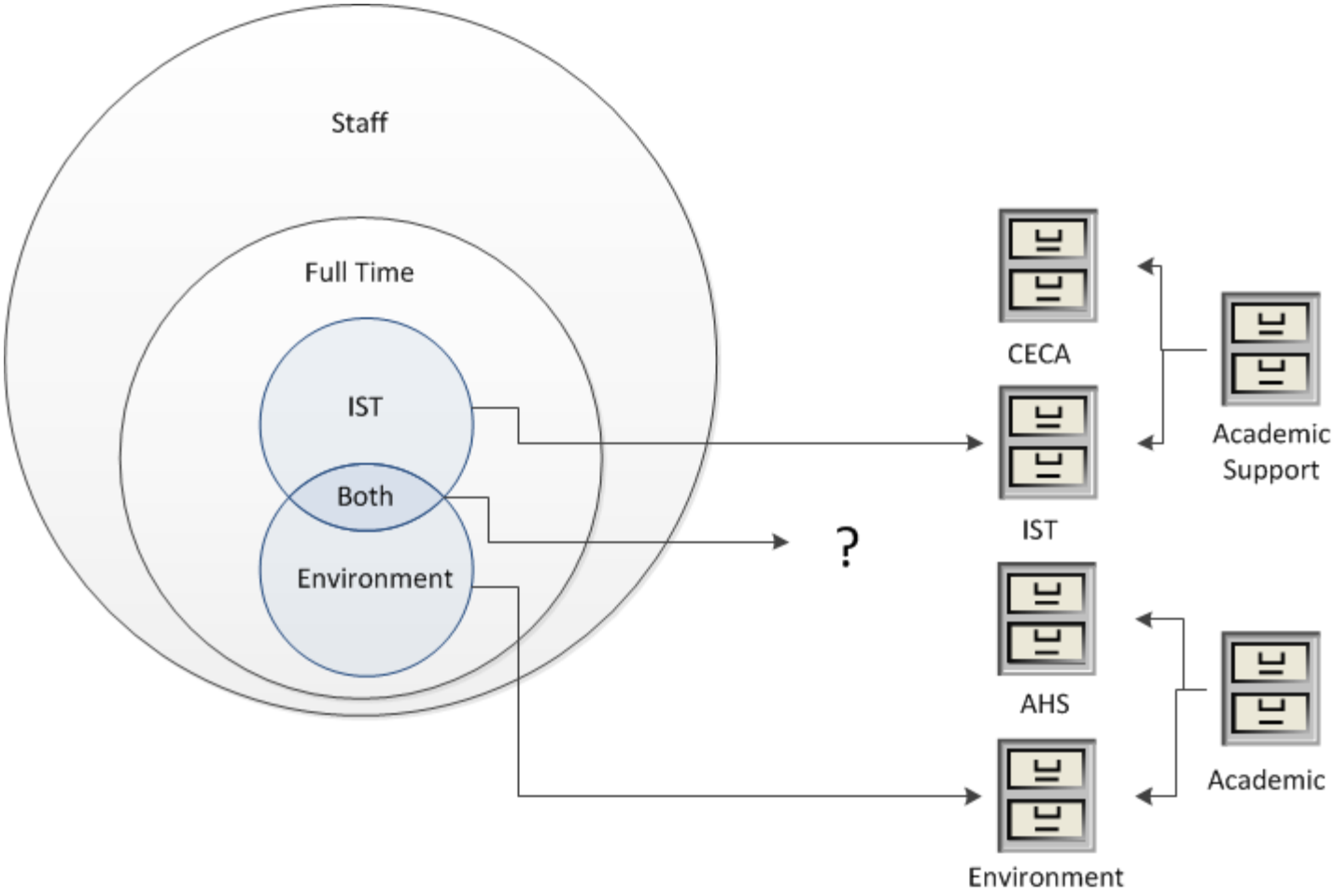


Diagram 1.2



Observation #2:
Role Membership: Making Choices



Observation #2
Role Collection Cross Appointment

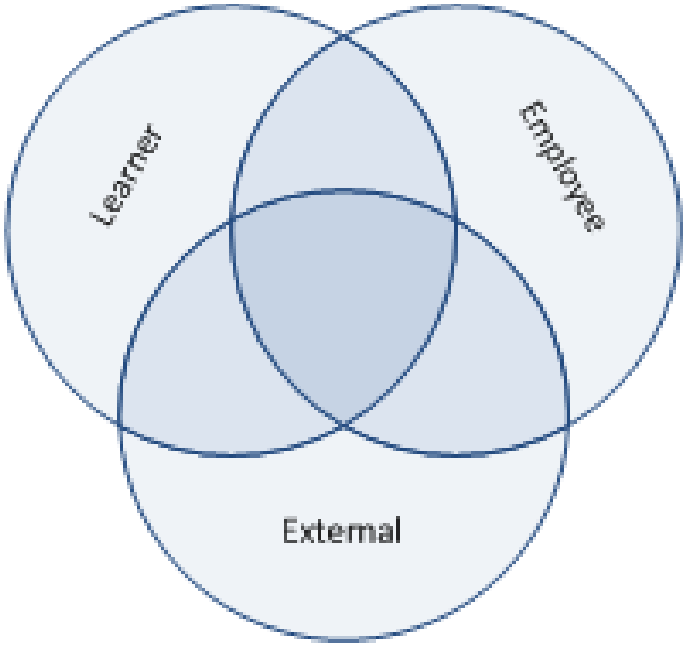
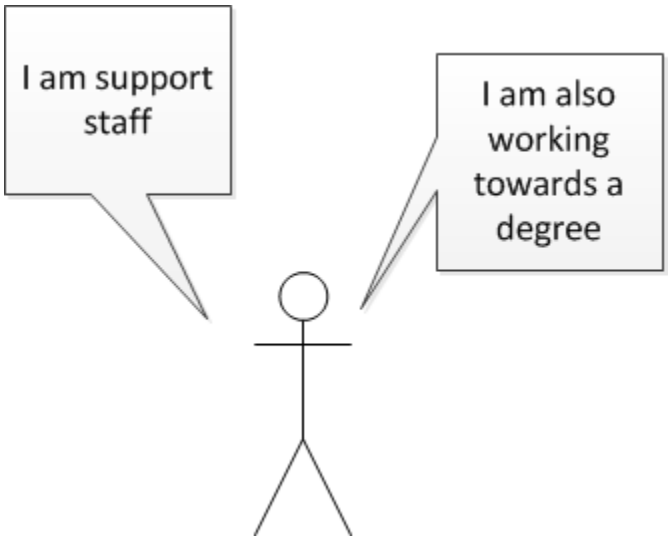


Diagram 1.4

Observation #2:
Role Collection Cross Appointment



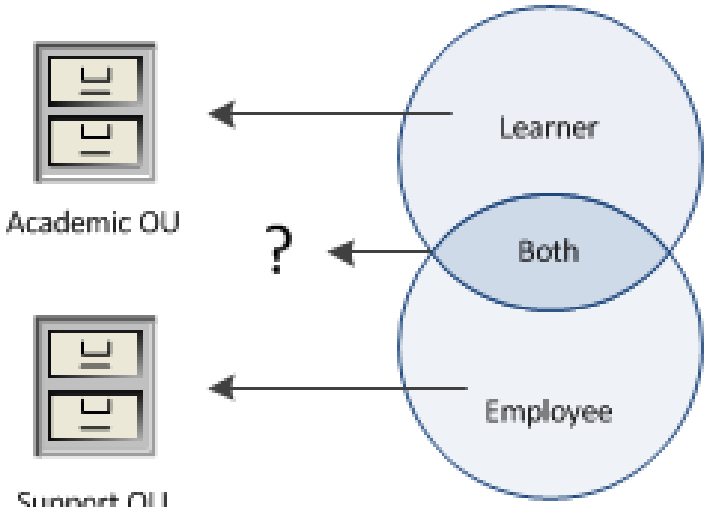


Diagram 1.5

Conclusion

- Both identity management and the campus infrastructure require the ability to express the complex relationships individuals have with the institution

RISKS

Risk Areas

1. Employee Terminations
2. Email Reliability and Security
3. SSO and the Cloud
4. Microsoft Technology Directions
5. Canadian Access Federation
6. Enabling Student Development

Employee Terminations

- Dept. heads want access to all resources, including email, to be discontinued at termination
- What happens when terminated employee is also a student?
- What happens when terminated employee is an alumnus?

Email Security

- Need to comply with CASL!
- Barriers to SPF/DKIM adoption:
  - Email forwarding
  - Email forgery
  - Mailservices creation mechanism
- Email in the Cloud
  - OK for students
  - Not for employees

SSO and the Cloud

- CAS adoption often requires custom development
- SAML is well established standard in Enterprise space
- E.g. Google Apps, Concur

Microsoft

- CLAIMS-based authentication
  - SAML
- Necessary for MS Azure

Canadian Access Federation (CAF)

- Shibboleth is standard in Higher Ed
- Based on SAML
- Identified as a priority for CUCCIO security group

Student/3rd Party Development

- Opendata is here
- What about PII?
- Password sharing is bad
- Need to manage owners' consent

ARCHITECTURE & DIRECTIONS

Implications

- Three security domains:
  - Learner
  - Employee
  - External
- Userid is not enough in a federated world
  - “userid@domain” is convention
  - Similar to email address
  - Confusion?

Possible Direction

- uwuserid@uwaterloo.ca
  - Employee collection
  - Email hosted on campus (CONNECT)
- uwuserid@mywaterloo.ca
  - Learner collection
  - Email could be hosted off-campus
  - Alumni email for life
- user@externaldomain.com
  - External collection
  - OpenID? Self-registration?

Edge cases in this model

- Applicants for academic admissions
  - "external" until matriculation
- Retirees
  - Email often cut-off
  - Access to Pension info?

SAML adoption

- CAS currently does “SAML-lite”
- Need to plan for full SAML support
  - If not CAS, then big change!
- On-line Expense project is first priority
- Need to consider timing:
  - CAF initiatives
  - Email in the cloud
  - Other strategic initiatives

Authorization Management

- SAML-based SSO is not enough
- Think “facebook” trust model
- OAUTH 2.0 protocol underneath

NEXT STEPS

First-half 2014

- Formalize functional requirements for Identity and Access Management
- Prioritize the following:
  - Replace Oracle Waveset
  - SSO with SAML support
  - Building OAUTH capability
- Determine multi-factor authentication strategy