IAM Committee
Meeting Notes
8/10/2015

Attendees: Cam Beasley, CW Belcher, Michael Bos, David Burns, John Chambers, Graham Chapman, Alison Lee, Ty Lehman, Darin Mattke, Shelley Powers, Steven Rung, Charles Soto, Kim Taylor, Karen Weisbrodt

Absent: Greg Baker, Cesar de la Garza, Fred Gilmore, Ed Horowitz

IAM Team Members: Justin Czimskey, Josh Kinney, Marta Lang, Aaron Reiser

1. **FY 15-16 Committee Membership and Chair/Co-chair Selection – Discuss**

Decision: Committee approved Ty Lehman as committee chair. Michael Bos volunteered to be co-chair, committee approved.

Committee agreed to reach out to Dell Medical School again to see if they are available to send a representative. McCombs volunteered to yield its spot on the committee for Natural Sciences or Liberal Arts if they would be interested in joining to represent large schools. The committee also indicated a desire to reach out to Academic Technology Support (ATS).

2. **Two Factor Authentication – Update**

Salesforce is redirecting development resources away from Toopher, meaning no product updates for the next year, making it very difficult to use the Toopher product to meet the UT System two factor authentication mandate and provide the enterprise-level support needed for the UT Austin environment. The IAM team has completed a high-level two-factor authentication solution assessment (including industry analysis, peer institution consultation, and fit-gap analysis against our two-factor authentication requirements). The next step is to conduct a proof-of-concept of the leading solution from the assessment to validate that it meets our key requirements.

Regarding compliance with the UT System mandate for two factor authentication, an exception request has been submitted to extend UT Austin's deadline through the end of spring break.

Q: Were the assessment criteria adjusted based on lessons learned from the previous implementation?
A: Yes, the assessment criteria were informed by lessons learned over the past year with our current two-factor authentication system.

Q: Do we know how much it will cost and how it will be paid for?
A: We have an estimate on cost. Source of funding is to be determined.

3. **IAM Staffing Issues – Update**

Dustin Slater will be assuming leadership of the Middleware and Common Applications (MCA) team in ITS Applications, taking over the position vacated by Cooper Henson. This is a great opportunity for Dustin, but leaves a big gap on the IAM team, bringing IAM up to 5 vacancies.

The ITS Applications director, Julienne VanDerZiel, has completed a salary survey process and recommended salary adjustments for a number of IAM staff to better align them with market rates, which should reduce attrition rates in key technical roles. These recommendations have been approved by the CIO and CFO and will be effective 9/1, assuming overall approval of the UT Austin budget.

Q: Will IAM leadership be reposting Dustin's vacated position as-is?
A: A manager position will be posted, but the details of the posting are still to be determined.

4. **IAM Project Planning for FY 2015-2016**

Reference handout.

Every year, each team in ITS Applications goes through a service planning process for the upcoming fiscal year to estimate sustainment hours (system patching, bug fixes, customer support, product management, etc.) and project/development hours for the team.

This year, there are 33 FTEs-worth of potential work for the team, but only 16.5 FTEs are available to do this work, which will require creative approaches to augmenting available resources as well as some hard choices about which projects will be prioritized in FY2015-2016.

Q: Does the 16.5 FTE calculation include vacancies?
A: Yes. The IAM Team has 19 authorized FTEs but taking into account current and future vacancies, only 16.5 FTEs are available.

Q: Have the projects listed under "Other Projects" been evaluated to determine if the IAM Team is the best group to own the projects? Some of these projects might be well-suited to the portfolios of other teams.
A: As we work on the roadmap, we can evaluate projects that might be handed off to other groups.

Q: Regarding the gap between FTEs needed to complete projects and FTEs available, is this an issue unique to the IAM Team or is this an issue which also affects other teams within the ITS Applications portfolio?
A: Each year there are more potential projects than available resources, but this year is especially difficult for the IAM team since there are so many "must-do" projects related to University priorities such as ASMP and multi-factor authentication that are competing for resources with the IAM Roadmap projects.

As a next step in the planning process, the impact of deferring projects will be documented to aid project prioritization. In addition, a proposal for augmenting resources to address additional projects will be developed.

5. **Identity Assurance Framework – Update**

Reference handout.

As the risk associated with an electronic application increases, assurance in the identity of its users should increase. The university currently has a two-tier assurance level system: base and "upgraded." This two-tier system is no longer meeting the needs of the university. Stakeholder interviews have identified the need for both lower-level assurance (e.g., engaging with donors) and higher-level assurance (e.g., two-factor authentication use cases).

The IAM Team is developing a framework to help campus units determine the appropriate level of assurance for a system or function on a five-tier scale of identity assurance. The Identity Assurance Framework is aligned with (but not yet equivalent to) the federal e-authentication framework and InCommon Assurance profiles. To obtain InCommon certification will require future enhancements to our identity systems and processes.

Q: Where did the five levels come from?
A: The federal government uses four levels, 1 through 4. Penn State added a fifth level (level 0) to their structure for very low assurance. We adopted the Penn State approach considering the need we have for a very easy-to-use lightweight authentication option.

Q: Once the Identity Assurance Framework is created, how will the framework be enforced? Will the Information Security Office continue to handle enforcement, or should governance be involved?
A: Departments are the best judges of their use cases, business needs, and risks. The IAM team will be working to provide education and outreach to campus units so they have the knowledge and resources they need in order to make good, educated decisions regarding authentication and information security.

6. **Other Initiative Updates**
    a. **SailPoint Implementation Statement of Work**

Vendor responses are due today. So far two responses have been submitted. The information in these responses will be sent out for review and evaluation within the next few weeks.

    b. **Lightweight Authentication & BYOId**

Three vendor demos were conducted over the past few weeks. The customer steering committee will be engaged later this month to determine next steps.

    c. **Apollo Roadmap**

Documentation of high-level Apollo uses cases is complete. Documentation for use cases for other legacy authorization systems (DPUSER Department Contacts and OHS Contacts) are in progress.

    d. **CARE Project**

Interviews with eight peer institutions have been completed. Work has begun on a research summary to be presented to the customer steering committee, which will present a high level design and budget analysis. The project has been re-baselined due to resource constraints.

Q: Is Dell Medical School part of the CARE CSC?
A: Not at this time, but based on your recommendation we will look into adding them.

e. IAM Integrations

19 integrations are in progress from ASMP and other application modernization activities across campus. A formal process is being developed to incorporate a standard IAM questionnaire, making sure that important questions are answered, and then providing assistance during implementation.

FY15-16 IAM Service Planning Update

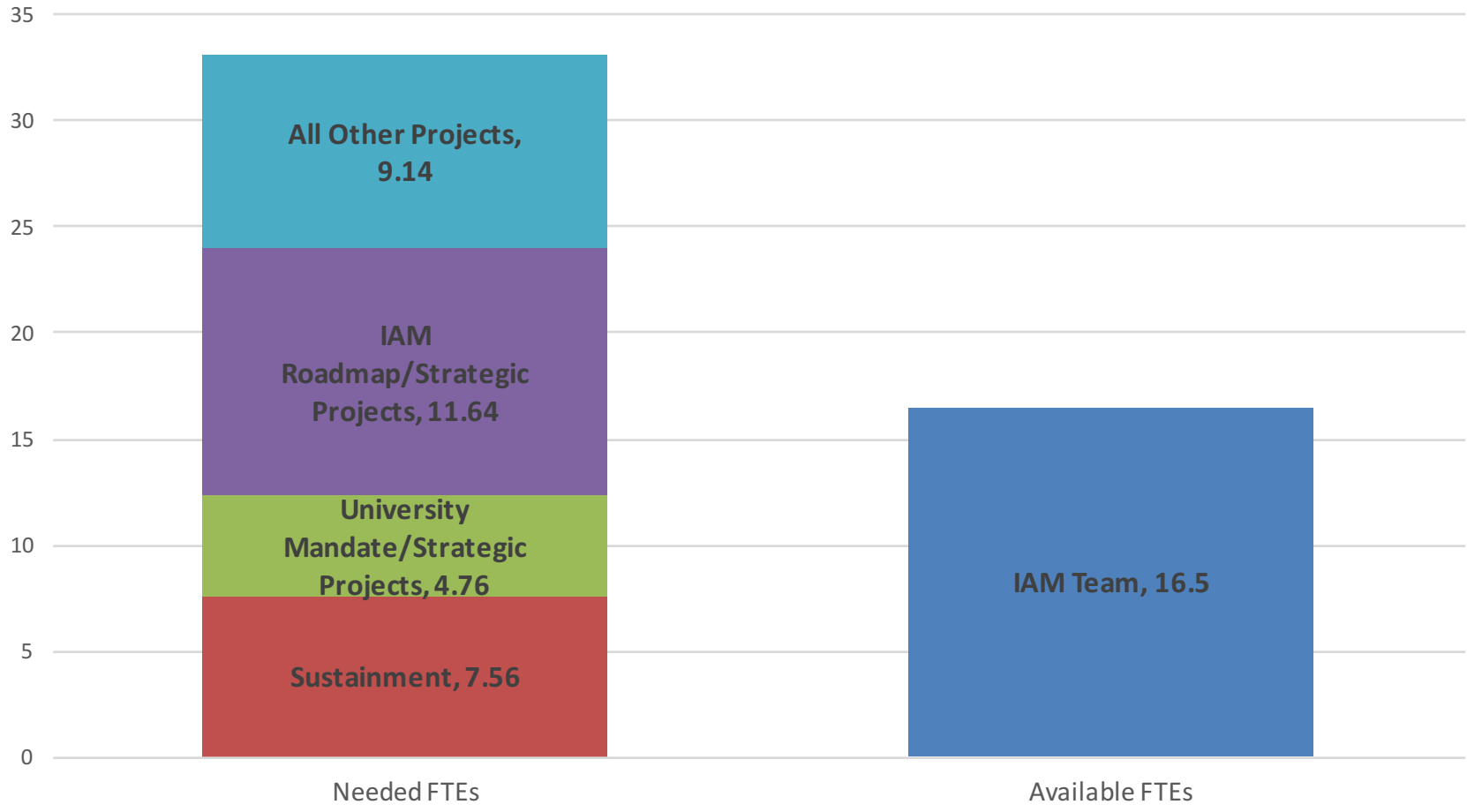
IAM Committee

August 10, 2015

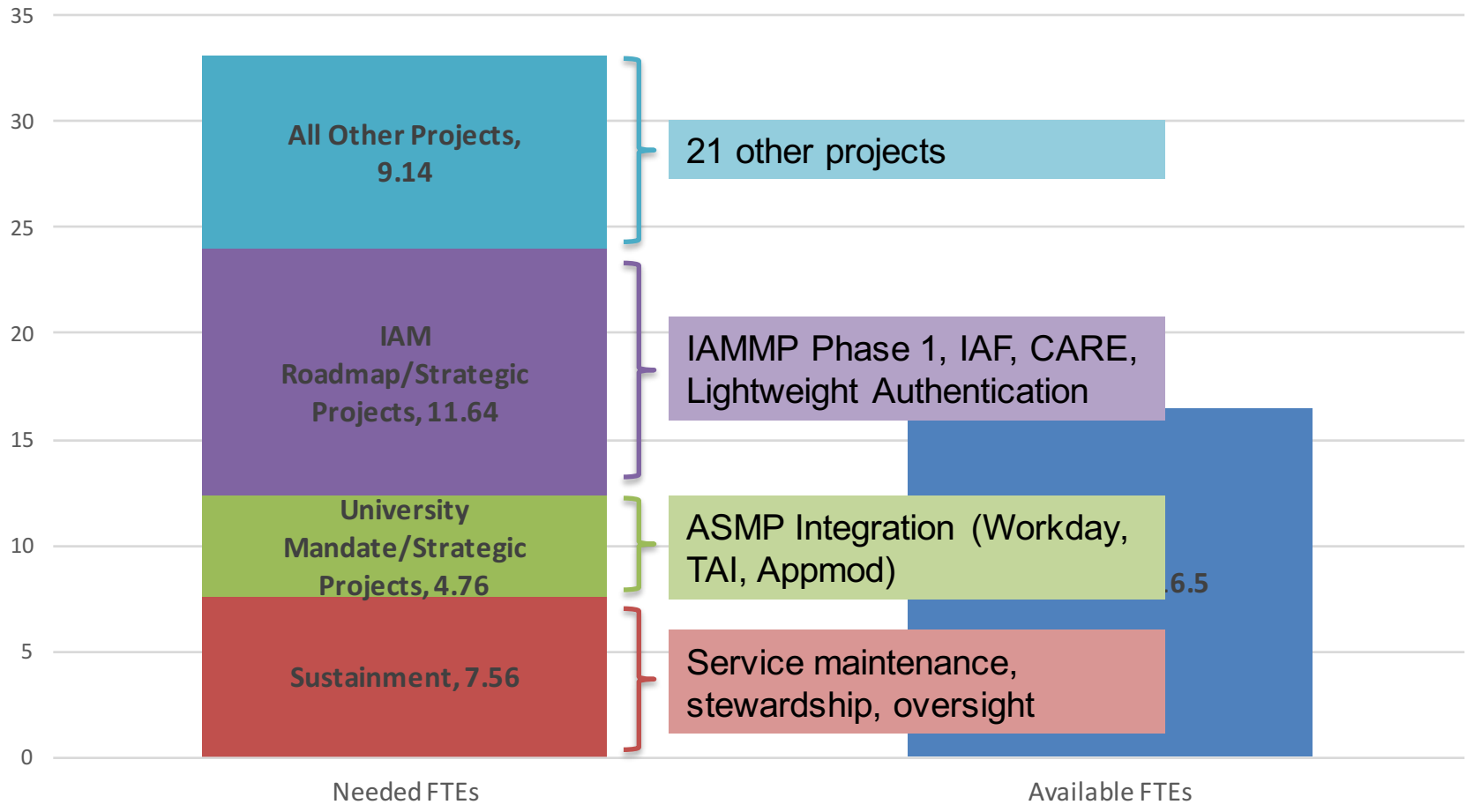
Service Planning Process

- ✓ Estimate FY15-16 sustainment hours for all services based on historical data
- ✓ Estimate FY15-16 project hours for all in-progress or potential projects
- ✓ Estimate available resources
- Prioritize projects and determine which can be included in FY15-16 plan ← **We are here**

FY15-16 Potential Projects & Available Resources



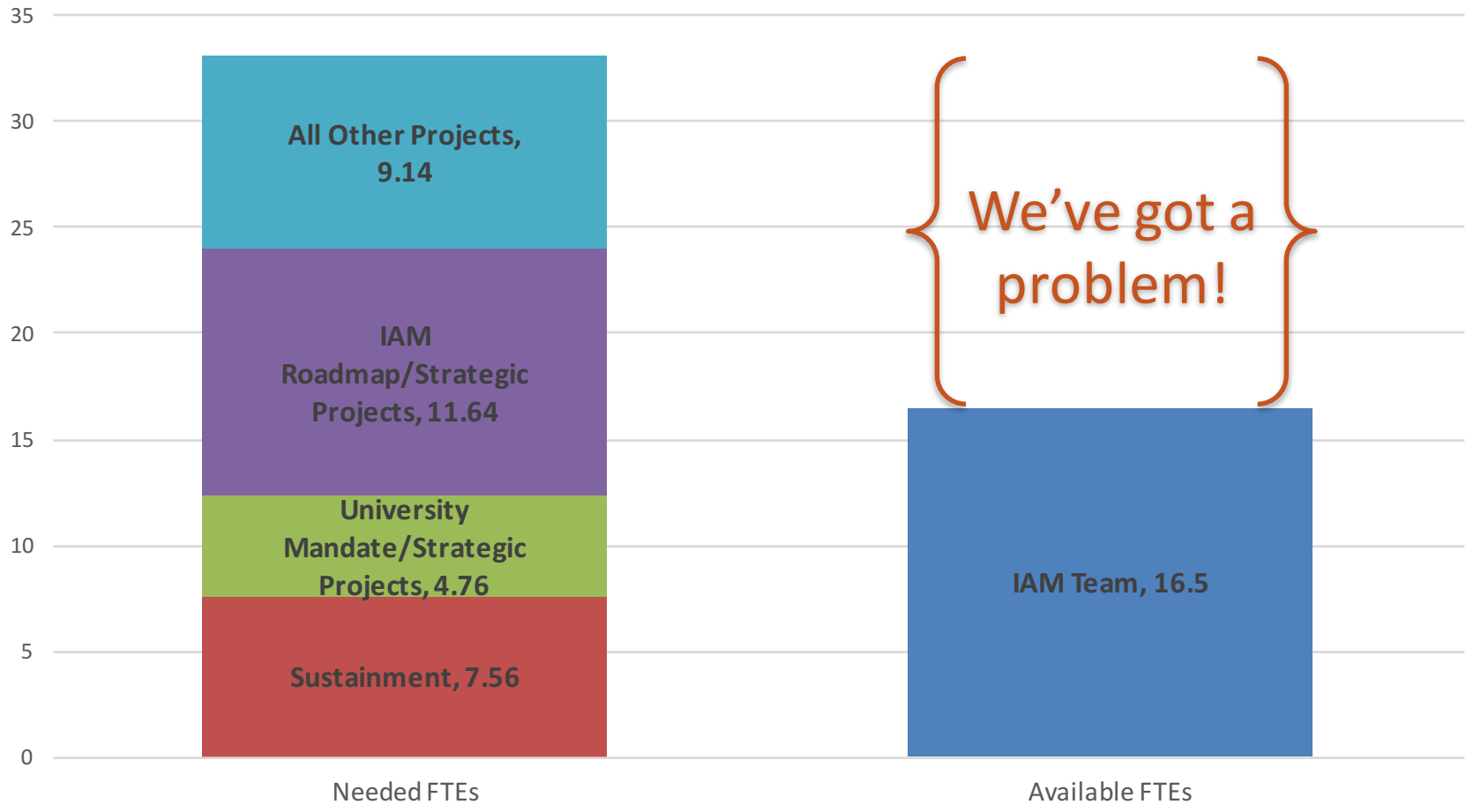
FY15-16 Potential Projects & Available Resources



“Other” Projects

- Password hash remediation
- Shibboleth SSO
- Shibboleth v3 upgrade
- OpenAM v12/13 upgrade
- UTLogin logging rearchitecture
- Toopher admin tool retirement
- Apollo roadmap implementation
- OHS Contacts roadmap implementation
- DPUSER Department Contacts roadmap
- TAI alpha user participation
- Directory Services roadmap
- UTLogin writeable user store
- TED web services
- TED replication model fix
- ID Card System replacement
- ID Photo Gateway rearchitecture
- Student Photo Roster replacement
- TRAC replacement
- SDS replacement
- IAM server maintenance automation
- IAM Request automation

FY15-16 Potential Projects & Available Resources



Available Resources

- IAM team has **19** authorized FTEs
- But current and future vacancies will reduce resource pool by ~**2.5** FTEs
- Leaving ~**16.5** available FTEs for FY15-16

Resourcing Options

- Delegate more work to Sailpoint integrator (and other project consultants)
- Add permanent staff to address structural staffing deficit in Authentication service area
- Add temporary staff to support key projects

Next Steps

- Assess and document impact of not doing each potential project
- Confirm project priorities with key stakeholders and ITS leadership
- Develop staff augmentation proposal to address must-do projects
- Finalize FY15-16 service plan

FY15-16 IAM Service Planning Update

IAM Committee

August 10, 2015

Identity Assurance Framework Update

IAM Committee

August 10, 2015

Identity Assurance Background

- As the risk associated with a system goes up the level of assurance in the identity of its users should also go up
- The current two-tier assurance system (base and “upgraded”) no longer meets the needs of the University
- Both lower and higher levels of assurance are needed for low-risk and high-risk transactions

Identity Assurance Framework

- Provides a 3-step process to help campus departments:
  1. Assess risks
  2. Determine recommended level of assurance (level 0 through 4)
  3. Identify appropriate authentication options
- Aligned with federal e-authentication framework and InCommon Assurance profiles (additional work will be needed for Silver compliance)

Levels of Assurance

Level Number	Level of Assurance	Identity Vetting & Authentication
Level 0	Very Low	Self-asserted identity data Lightweight authentication
Level 1	Low	Some vetting of identity data Lightweight authentication
Level 2	Moderate	In-person identity proofing Complex password
Level 3	High	In-person identity proofing Complex password Two-factor authentication
Level 4	Very High	Additional identity proofing Complex password Hard token two-factor authentication

Step 1: Assess Risks

- Rate the potential risk of an authentication failure across 6 risk areas (none, low, moderate, high):
  - Reputation and standing of the University
  - Financial loss or University liability
  - Harm to University programs or public interest
  - Unauthorized release of sensitive/confidential data
  - Civil or criminal violations
  - Personal safety
- Determine if UT System two-factor authentication mandate applies to the application

Step 2: Determine Recommended Level of Assurance

Risk Area	No Risk/NA	Low Risk	Moderate Risk	High Risk
Reputation	Level 0	Level 1	Level 2	Level 3
Financial	Level 0	Level 2	Level 3	Level 4
Program Harm	Level 0	Level 2	Level 3	Level 4
Data Release	Level 0	Level 2	Level 3	Level 4
Civil/Criminal	Level 0	Level 2	Level 3	Level 4
Personal Safety	Level 0	Level 3	Level 4	Level 4

If system allows remote updates to employee banking, tax, or financial information, or allows remote administrative access to systems that contain confidential University data, Level 3 will apply.

Step 3: Identify Appropriate Authentication Options

LoA	Valid Credentials	Authentication Options
Level 0	• Lightweight Identity • UT EID	• Lightweight Authentication • UTLogin • Shibboleth • LDAP (TED/AD)
Level 1	• Lightweight Identity w/ Vetting • UT EID	• Lightweight Authentication • UTLogin Shibboleth • LDAP (TED/AD)
Level 2	• Upgraded UT EID	• UTLogin • Shibboleth • LDAP (TED/AD)
Level 3	• Upgraded UT EID -AND- Two-Factor Authentication	• UTLogin • Shibboleth
Level 4	• *TBD*	• *TBD*

Next Steps

- Complete draft of Identity Assurance Framework document and review with stakeholders
- Develop questionnaire to help departments determine required Level of Assurance for their applications
- Plan LoA implementation steps and develop roadmap to Silver compliance

Identity Assurance Framework Update

IAM Committee

August 10, 2015