

IAM Committee
Meeting Agenda
3/14/2016

Attending: Thomas Beard, Cam Beasley, CW Belcher, Michael Bos, Bill Bova, John Chambers, Fred Gilmore, Ty Lehman, Andy Loomis, Shelley Powers, Steve Rung, Karen Weisbrodt

Absent: Graham Chapman, Tim Fackler, Cesar de la Garza, Alison Lee, Darin Mattke, Charles Soto

IAM: Joel Guajardo, Rosa Harris, Justin Hill, Marta Lang, Aaron Reiser

1. IAM Team Staffing – Update (CW Belcher)

In the last month, the IAM Team has hired five new employees. The team has a Software Developer Trainee who is projected to complete training in May. The team still has five vacancies, and has been looking at the possibility of using a recruiter that has a contract with UT System that we can leverage.

Q: What is the recruiter's record of success?

A: This recruiter has not worked with UT Austin yet, but has worked with other UT System component institutions. The IAM Team will be reaching out to those component institutions for their feedback.

Q: Is the hiring trouble IAM experiencing specific to the Software Engineer and Senior Software Engineer roles?

A: Yes, but it also includes the Software Developer/Analyst roles.

Rosa Harris has accepted a Project Manager role on the team, so her previous Business Analyst position is now open.

The IAM Team is building an operations group within the team, which will provide Tier III technical support, manage ticket queues, perform basic maintenance, and keep systems up and running. The team has hired two Information Analysts to help build out this group. The operations group will also align and unify operational processes and procedures across all IAM systems, leveraging ITIL concepts and standards where appropriate. The team is currently reviewing IAM systems to assess their readiness for transition to the operations group. We expect to transfer most operations duties to the new group by this July.

2. IAM Roadmap – Spring 2016 Update (CW Belcher)

See Handout.

There are only a few major changes to the Roadmap since the last update. The Roadmap reflects better estimates for the IAM Modernization Program (IAMMP) Phase 1. The Duo implementation has been elongated due to some technical challenges with UTLogin and Shibboleth integration, but progress is being made (including release to VPN this morning). Grey bars have been added to reflect UTLogin enhancements and UTLogin v12/13 upgrade, since they are on the horizon and planning has not yet begun. The enhancements include high priority initiatives such as OAuth (a different authentication

mechanism commonly used in federated environments) which is needed by the TAI team for the Enterprise Service Bus (ESB), integration of Duo with UTLogin SAML, and Realm Policy Manager (RPM) improvements.

Q: Given that MuleSoft needs OAuth, will MuleSoft still be able to meet their project deadlines?

A: Yes. MuleSoft will be using LDAP authentication via the uTexas Enterprise Directory (TED) as a workaround.

Q: When Mulesoft transitions from LDAP to OAuth, will the transition be invisible to users?

A: The transition may not be invisible, but we will work with the ESB team to minimize disruption.

Once OAuth is in place, that will pave the way for supporting OpenID Connect. The ultimate goal is for UTLogin to support a variety of identification and authentication technologies.

Regarding the line item for the UTLogin upgrade, the version of OpenAM at were are currently using will go out of support at the end of the calendar year. There are two versions that the team could potentially upgrade to, so there will need to be an assessment undertaken to determine which version to move to.

Q: Regarding the listed TRAC replacement, and the roadmap in general, if other major pieces such as Workday wind up shifting their timelines, how will that affect the IAM Roadmap?

A: In general, the IAM Team will make every effort to stick to the IAM Roadmap though some projects may have to adapt to changing external timelines. For example, if an external project is delayed, that may allow the IAM Team to direct their efforts to a long-term integration rather than a short-term bridge solution.

3. Two-Factor Authentication / Duo Implementation – Update (Justin Hill)

As of this morning, the UT VPN is protected by Duo. The Help Desk reported that the release has been very smooth and that they have encountered no major issues. Approximately 2700 users have enrolled as of this morning. Hard tokens have been delivered and are ready to be assigned as needed.

The timeline for the Duo integration with UTLogin has been pushed back to May 8 and the integration with Shibboleth has been pushed back to June 7, both due to technical hurdles. The transition for Financial Information Systems (FIS) and Payroll are still scheduled to begin in May, however that will be dependent on the successful completion of the UTLogin integration.

4. Other Initiative Updates

a. IAM Integrations (Justin Hill)

The integration process has been defined and operational management of the IAM Integration process will transition from Mario Leal to Justin Hill. An additional Software Engineer will be cross-trained on integrations to help process the backlog, and other avenues for adding capacity are being explored. Three integrations are current in progress and 24 are in the backlog.

b. IAMMP / SailPoint Implementation (Marta Lang)

See handouts.

Since the previous meeting, the KPMG SailPoint integration team has arrived and are on the ground working with the team. The formal project kickoff was on February 17. The project is deliverable-based, where the project has been structured into tasks where deliverables will roll up into major tasks. One of the major accomplishments to date is that the project plan has been baselined.

Task 2, Project Initiation and Planning, includes important deliverables needed at the outset of a project including determining a testing approach, developing application coding and development standards, etc. Task 3, Technical Architecture and System Environments, establishes the technical environment, the technical approach, prototype environments, and includes technical training for the team. Task 4, Interface and Data Transition Strategy, addresses the approach for managing change to IAM systems while the rest of the university is in transition. This strategy will identify where the team will use short-term “bridges” versus long-term integrations, and where those approaches will change at different points in the project timeline. Task 5, Phase 1 Identity Hub Implementation, addresses implementation of the strategy that comes out of Task 4, though the term “Identity Hub” may be renamed depending on the approach taken in the strategy. Task 6, Group and Role Management, deals with implementation of group and role management functionality in SailPoint, including certain use cases that will help in the transition from Apollo. The Project Management task (Task 1) is ongoing throughout, and extends past the end of Task 6 to account for approvals and other project management tasks needed at the completion of Phase 1.

Q: You stated that the project kickoff was February 17, but the timeline shows that work began on January 20?

A: The informal kickoff was January 20 and the formal kickoff was February 17. Additionally, we have built two points into the timeline at the end of May and end of September to determine if deliverable dates need to be re-baselined.

Q: It appears that the end of Task 4 is overlapping with the beginning of Task 5. Is that due to resources freeing up?

A: Task 5 is dependent on Task 4. This overlap reflects defining requirements and communicating those requirements to campus to solicit feedback.

Q: When will the planning for Phase 2 start?

A: The hope is for planning to begin this summer and to ensure that there is not a gap between Phase 1 and Phase 2.

Q: Does Task 6 include an approach to OHSC replacement?

A: That has yet to be determined, but OHSC roles are one of the early adopter use cases the team is considering. Some of the existing OHSC roles will transition to Workday while others will likely be managed by SailPoint. The IAM team has been talking to the Workday team about organizational hierarchy and how the transition from the current organizational hierarchy will work.

The IAM Committee will serve as the Customer Steering Committee for IAMMP. The CSC charge document was handed out to the group. An electronic version will be provided to the committee for review and comment.

c. Directory Services Roadmap (CW Belcher)

A survey was sent to the technical community asking for feedback about directory services on campus. The survey is open until the end of March, and committee members are encouraged to have their technical staff fill out the survey. The team is looking for feedback from those experienced with using TED and AD, as well as those with less or no experience with directory services.

Q: Does the team want CSUs to submit a response for the entire CSU?

A: IAM is okay with getting multiple responses from different parts of the group.

d. Lightweight Authentication (Rosa Harris)

The original scheduled response date for the Lightweight Authentication RFP was March 2, but the deadline was extended to March 8 by vendor request. The project team has received and is reviewing 6 vendor responses. The review will be completed by Friday, April 1. The team met with purchasing to discuss dates for vendor oral presentations in May. The goal is to finalize the purchase by mid June.

e. Authorization Roadmap (Joel Guajardo)

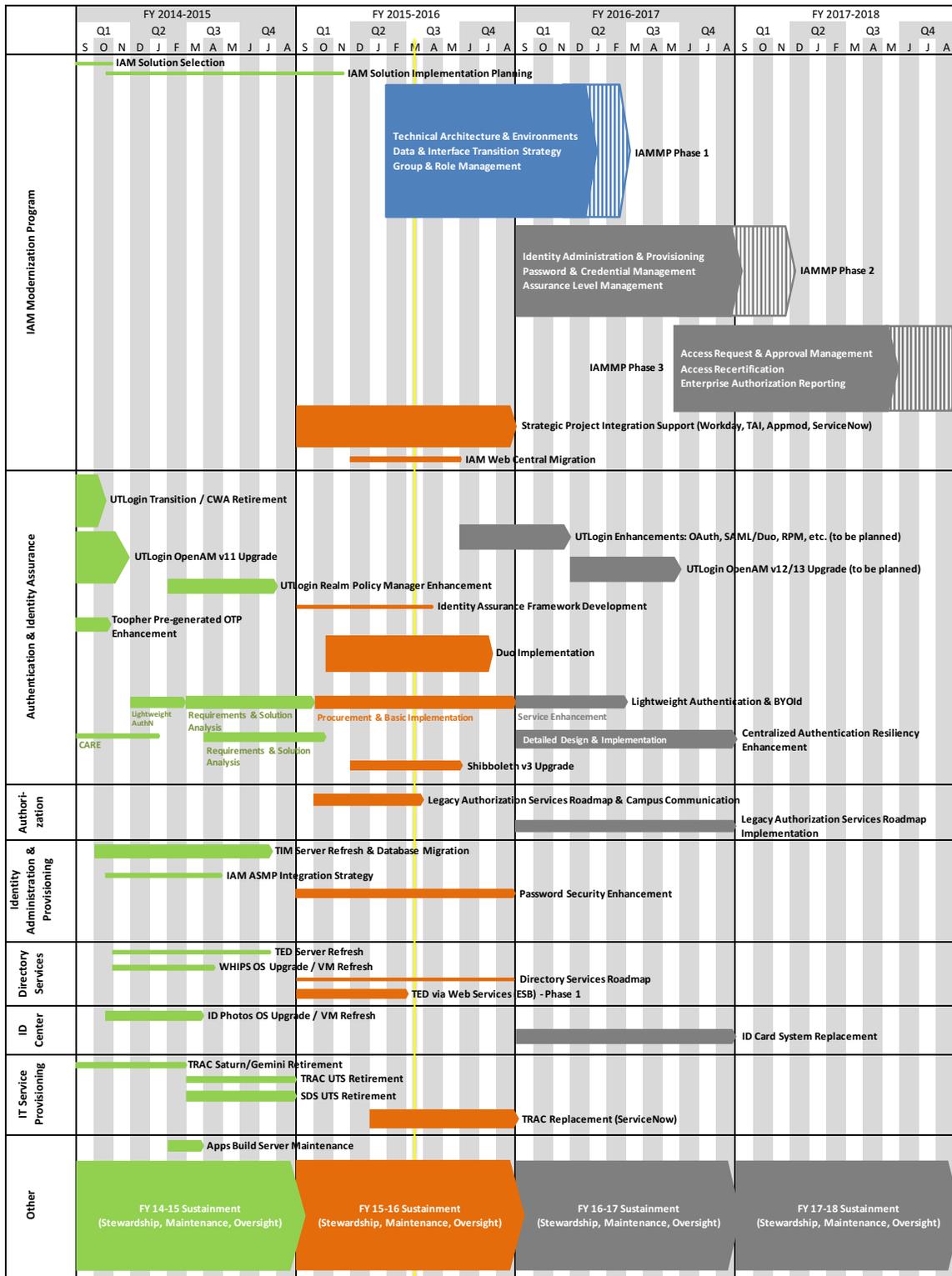
All but one of the customer interviews have been completed for major users of Apollo position-based management. These customers have provided good feedback which will help determine the requirements and approach of the project. The team will be arranging discussions with major stakeholders for OHSC in the near future.

IAM Roadmap Overview

Status Legend:

- Complete (Green bar)
- In Progress (Orange bar)
- Planned (Blue bar)
- Future (Grey bar)

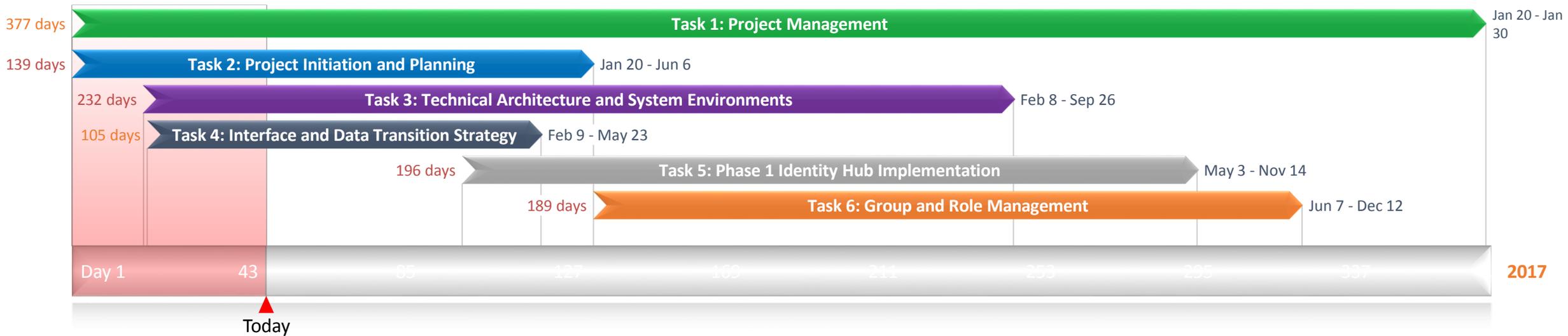
Bar Height Indicates Level of 1 FTE



IAM Roadmap Initiative Descriptions

IAM Modernization Program	<ul style="list-style-type: none"> ✓ IAM Solution Selection (Complete): Select and procure new IAM software to support and enable the roadmap goals. ✓ IAM Solution Implementation Planning (Complete): Complete high-level planning for the implementation of the software selected in the IAM Solution Selection project. <p>IAMMP Phase 1: Establish new technical architecture and environments for SailPoint; Develop data and interface transition strategy; Implement group and role management.</p> <p>IAMMP Phase 2: Implement identity administration and provisioning, password and credential management, and assurance level management functionality.</p> <p>IAMMP Phase 3: Implement access request and approval management, access recertification, and enterprise authorization reporting functionality.</p> <p>Strategic Project Integration Support: Support authentication and identity data integration with University strategic projects, including Workday, TAI, ASMP application modernization, and ServiceNow.</p> <p>IAM Web Central Migration: Migrate IAM web site content off of the end-of-life Web Central platform.</p>
Identity Assurance and Authentication	<ul style="list-style-type: none"> ✓ UTLogin Transition / CWA Retirement (Complete): Transition Central Web Authentication & Fat Cookie customers to UTLogin and retire the CWA/FC authentication system. ✓ UTLogin OpenAM v11 Upgrade (Complete): Upgrade UTLogin to the current version of OpenAM software to address bugs, implement session management enhancements, and stay current with vendor support. ✓ UTLogin Realm Policy Manager Enhancement (Complete): Enhance the UTLogin RPM to allow delegated administration of sites on shared hosting environments like UT Web and Windows Web Hosting. <p>UTLogin enhancements (to be planned): Add OAuth capability, integrate Duo with UTLogin SAML, implement customer-requested enhancements to RPM, implement architectural improvements to reduce maintenance complexity and enable server virtualization.</p> <p>UTLogin v12/13 Upgrade (to be planned): Upgrade UTLogin to current version of OpenAM software to address bugs, implement policy management enhancements, and stay current with vendor support.</p> <p>Identity Assurance Framework Development & Implementation: Implement a framework to assist campus departments in assessing risks and selecting an appropriate level of assurance to mitigate those risks.</p> <ul style="list-style-type: none"> ✓ Toopher Pre-generated OTP Enhancement (Complete): Add the ability to use pre-generated one-time-passwords (OTPs) with Toopher. <p>Duo Implementation: Implement two-factor authentication using the Duo Security solution.</p> <p>Lightweight Authentication & BYOID: Implement a lightweight identifier and authentication service and integrate with external identity providers (Bring Your Own Identity).</p> <p>Central Authentication Resiliency Enhancement: Improve the resiliency of central authentication services by leveraging off-campus hosting.</p> <p>Shibboleth v3 Upgrade: Upgrade the Shibboleth federated authentication solution to the currently supported version.</p>
Authori-zation	<p>Legacy Authorization Services Roadmap & Campus Communication: Define the transition and retirement roadmaps for Apollo, OHS Contacts, and DPUSER Department Contacts systems and communicate with campus stakeholders.</p> <p>Legacy Authorization Services Roadmap Implementation: Implement transition and retirement roadmaps for Apollo, OHS Contacts, and DPUSER Department Contacts systems.</p>
Identity Administration & Provisioning	<ul style="list-style-type: none"> ✓ TIM Server Refresh & Database Migration (Complete): Retire out-of-warranty servers and migrate to virtual server infrastructure and enterprise Oracle service. ✓ IAM ASMP Integration Strategy (Complete): Define high-level plan for maintaining required integrations while source systems and IAM system are being replaced. <p>Password Security Enhancement: Improve the security of EID password storage infrastructure.</p>
Directory Services	<ul style="list-style-type: none"> ✓ TED Server Refresh (Complete): Retire out-of-warranty servers. ✓ WHIPS OS Upgrade / VM Refresh (Complete): Migrate to supported OS version and refresh virtual server infrastructure. <p>Directory Services Roadmap: Document new and evolving TED use cases and requirements and plan approach for addressing</p> <p>TED via Web Services (ESB) - Phase 1: Implement an initial set of TED services on the ESB (public directory information lookup, group membership lookup, confidential directory information lookup).</p>
ID Center	<ul style="list-style-type: none"> ✓ ID Photos OS Upgrade / VM Refresh (Complete): Migrate to supported OS version and refresh virtual server infrastructure. <p>ID Card System Replacement: Modernize ID Card System and remove mainframe dependency.</p>
IT Service Provisioning	<ul style="list-style-type: none"> ✓ TRAC Saturn/Gemini Retirement (Complete): Retire use of out-of-warranty servers. ✓ TRAC UTS Retirement (Complete): Migrate TRAC functions off end-of-life UTS service. ✓ SDS UTS Retirement (Complete): Migrate SDS functions off end-of-life UTS service. <p>TRAC Replacement (ServiceNow): Replace TRAC functionality with ServiceNow.</p>
Other	<ul style="list-style-type: none"> ✓ Apps Build Server Maintenance (Complete FY14-15): Maintenance and enhancements required to support ITS Applications software build and testing infrastructure.

IAM Modernization Program, Phase 1 Project Timeline



Monday, March 14, 2016