IAM Committee
Meeting Notes
9/12/2016

Attending: Cam Beasley, CW Belcher, Michael Bos, John Chambers, Graham Chapman, Cesar de la Garza, Seth Feder, Fred Gilmore, Brian Hurdle (for Bill Bova), Alison Lee, Ty Lehman, Andy Loomis, Jason Mayhew, Darin Mattke, Mike McIntosh (for Tiffany Yanagawa), Charles Soto, Karen Weisbrodt

Absent: Tim Fackler, Shelley Powers, Steve Rung

IAM: Kenneth Dunbar (Contractor – KPMG), Joel Guajardo, Rosa Harris, Marta Lang, Mario Leal, Aaron Reiser, Andrew Russell

1. **New IAM Committee Members – Introduce (All)**

Due to the membership changes with the new fiscal year, meeting attendees went around the room and introduced themselves.

2. **IAM FY '16 – '17 Planning – Review (CW Belcher)**

The planning for the new fiscal year is not yet ready for review. The estimates have been completed but additional review is needed at the ITS Applications director and CIO level. The team anticipates having the fiscal year plan available for review by the committee in time for the next meeting.

Part of the delay is due to a service review that ITS is undergoing in order to better understand what services cost to maintain so that governance can make better decisions about which services to support and prioritize.

Q: Are there any concerns that this service review will impact the IAM service portfolio?
A: All IAM services are common good and not fee-for-service. During the last review five years ago, most of the portfolio was marked as critical and campus governance agreed. Since then, the campus has brought on a new executive team so there will be some work necessary to confirm standing.

3. **Group and Role Management "Standard Model" & Use Cases – Discuss (Joel Guajardo)**

Reference presentation.

Joel: Task 6 of the IAM Modernization Program (IAMMP) deals with group and role management. The team conducted numerous stakeholder interviews both to bring awareness of this effort and new functionality to campus and also to elicit use cases.

Kenneth: The standard model mentioned in the presentation will help to standardize the group and role models and the associated terminology. The standard model defines a set of access requests and support functionality associated with those requests. The objective of this effort is to onboard new applications and functionality of roles as consistently as possible. The service model was derived from

stakeholder interviews about the roles and applications of interest to those stakeholders. Next steps will include prioritizing use cases, roles, and applications.

Q: Is there an intent to provide groups and roles functionality during Phase 1 of the project or will the initial analysis be completed and implementation scheduled for a later time?
A: The plan is to implement basic groups and roles functionality to support early adopters in Phase (by February 2017). Groups and roles functionality will be enhanced over subsequent releases during Phase 2.

Q: Have any particular roles been prioritized as a result of ASMP?
A: No, but the prioritization effort has not yet started.

In the diagram of IAM Standard Model Functionality, the dark blue ovals represent access requests and the light blue ovals represent support or maintenance activities. Joiners will include new students as well as new employees. Leavers will include terminated employees, retiring employees, and graduating students. Movers represent individuals changing jobs or taking on additional jobs, i.e. for a new department. In this document, the SNOW abbreviation refers to ServiceNow.

Reporting includes reporting on group membership, who has access to what service, what access an individual has, and who has a particular role. Certification refers to the review of individuals in particular roles or access. Reconciliation will pull information from applications into the system and correlate that information with an identity in order to either supplement a view of the identity or in order to identify discrepancies. Role maintenance involves building and changing access definitions.

In the Functionality by Phase timeline diagram, white represents an initial limited functionality release while the solid dark and light blue indicate full functionality.

Q: What is the projected timeline for each of the represented phases?
A: Phase 1 is expected to finish in February 2017. Phase 2 will take 15-18 months after the completion of Phase 1. Phase 3 will take about 9 months after.

Q: Have you identified any pilot customers?
A: Not yet. The work on prioritizing use cases will inform the selection of early adopters.

Q: Will certification be conducted up-front or will it be an ongoing process?
A: The goal is to have certification be done up-front but also provide re-certification on a customizable frequency, or as-needed. Some roles may require re-certification every six months and others may require re-certification every 12 months. Getting a full picture of what people have access to is dependent on getting the central repository of information up and running.

Q: Is that prerequisite why certification isn't scheduled until phase 3?
A: Yes. As applications are brought on there will be an initial reconciliation. That will be built into the pilot. However, feedback from the IAM Committee is welcome and the team recognizes the strong desire of committee members to have at least limited reconciliation functionality available earlier than proposed. The team has noted this feedback and will ensure that it is prioritized accordingly.

Q: Is there an opportunity to take advantage of instrumented certification? For example, automatically provisioning access upon the completion of a prerequisite compliant training class?
A: Yes. Workflows check business rules prior to running. It would be feasible to set up a business rule to have the system check something (e.g. UTLearn) before giving somebody a role or, alternatively, alert when somebody obtains a role for which they do not meet the prerequisites.

Comment: Certification is particularly important with regard to HIPAA compliance. This work is already being done, but it would be better if this was conducted via a central repository. It would be particularly helpful to have audits available earlier, if possible.

Joel: The next step is to finalize the criteria for determining early adopters. This criteria will be applied to the interview notes and gathered information, allowing applications to be ranked. Then, the IAM Committee will be solicited for approval of early adopters. The goal is to have this information ready for committee approval by the October 2016 meeting.

The presentation includes two appendices. The first is a consolidated list of identified use cases. The second provides descriptions of the standard model categories.

4. **Other Initiative Updates**
   a. **IAM Team Staffing (Mario Leal)**

Phone screens for the IT Manager position are currently being scheduled. Four phone screens have been conducted for the Software Developer/Analyst position and another three have been scheduled. The team is currently reviewing applications for the Quality Assurance position. The applicant pool for the Business Analyst position has been narrowed and the team is currently making selections for phone screens.

Q: Based on the aforementioned service reviews, is there a concern that hiring may stall?
A: So far, the team does not anticipate the service review impacting hiring.

   b. **IAM Integrations (Mario Leal)**

   Start (Aug 1): 26
   +4 New: (AWS – Concur, CMS Hosting, Eloqua, Project 2021)
   -4 Completed: (Cisco WebEx, EverFi, StarRez, Virtual EMS)
   -2 Cancelled: (edX, LibCal)
   End (Aug 31): 24

The new reporting format is above. The integrations team is beginning to find its groove. There are some slowdowns on assessing questionnaires, due to resource constraints.

   c. **Directory Services Roadmap (Mario Leal)**

Work on peer institution benchmarking has stalled due to peer institutions, like UT Austin, beginning their new school years. This effort will be restarted this week. In addition, the team is soliciting research from Gartner, Inc. The team still aims to complete this work by the end of September.

d. Legacy Authorization Roadmap (Mario Leal)

Details are still being gathered and the overall plan is being built. A deployment plan for retiring position-based authorizations in Apollo has been developed. The team plans to start implementing this plan in October and completing work by April 2017. The plan will be published when it has been finalized.

e. Two-Factor Authentication / Duo Implementation – Update (Mario Leal)

The Shibboleth upgrade on August 16 did not go as planned and had to be rolled back. The team is working on understanding the issues and remediating. The deployment is now re-scheduled for September 29.

The target date for Toopher retirement is September 26. Support gaps have been closed and work on a communication strategy is ongoing. Duo currently has about 25,000 campus users.

Q: Will communications be targeted to Toopher users who have not yet registered for Duo?
A: Yes.

Action Item: When attempting to assist a faculty member, a committee member encountered some confusing documentation. This issue will be resolved offline.

Q: Are there plans to expand the use of multifactor authentication beyond the UT VPN?
A: Certain applications already require multifactor authentication. It is possible to protect specific functions within an applications.

Comment: One feature that was really appreciated in Toopher which isn't present in Duo is the ability to automate authentication based on geolocation.

The team has proposed that feature to the vendor as a future enhancement.

Q: How would the committee feel about protecting the email system with multifactor authentication?
A: This would probably not be ideal, but the suggestion is understandable given recent security incidents on campus. Multifactor authentication would not have prevented the recent incident. Further, integrating multifactor authentication into multiple native clients would be extremely challenging. Regarding the recent security incident, the Information Security Office (ISO) is currently working on mitigation strategies.

f. IAM Modernization Project / SailPoint Implementation (Marta Lang)

Reference handout.

The team is working with KPMG to improve performance. The project is behind on a number of deliverables, so the team is analyzing how to best correct and re-baseline to make the deadlines more realistic.

Q: Is the technical architecture development using tools selected by ASMP?
A: Yes, the team is using some of those tools, such as Artifactory.

g. Lightweight Authentication (Rosa Harris)

The team is still working on contract negotiations. The team is also working on developing an informational flier which will be sent to the Customer Steering Committee and the IAM Committee for review and feedback. Those parties will also be solicited for input on branding for the service.
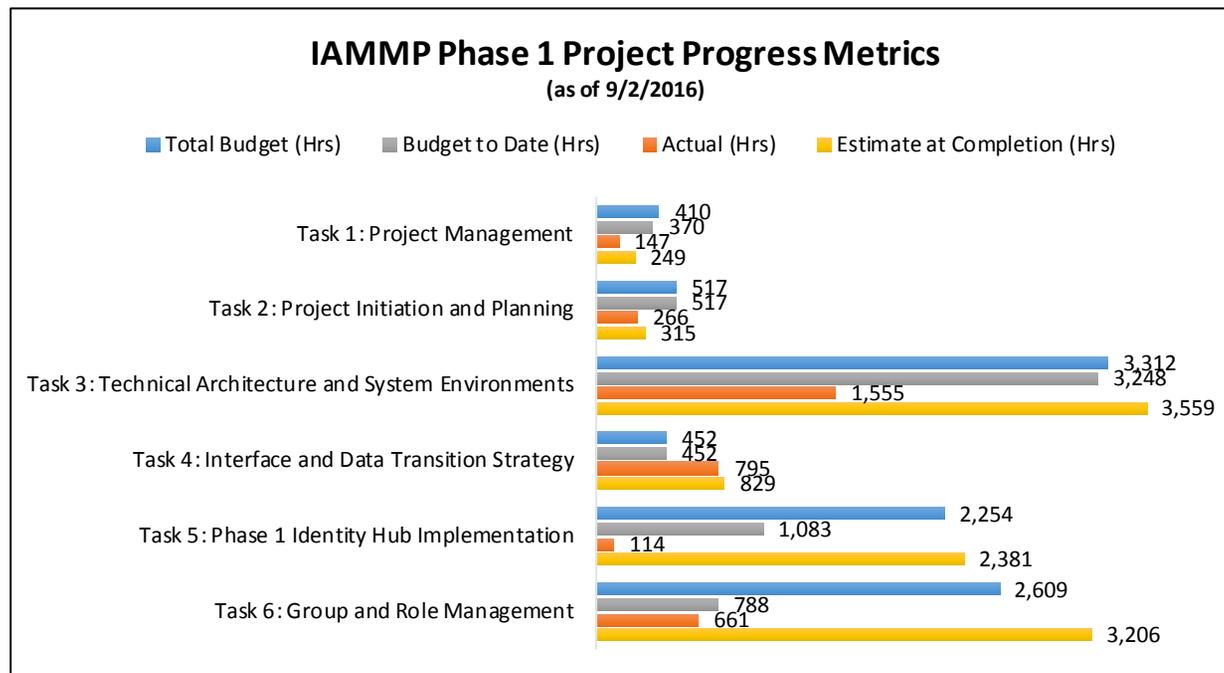
Items for Management Attention

- Corrective measures are in progress to address issues with KPMG's performance, with a focus on overcoming resource challenges and improving the delivery of quality and value. Weekly project management issue reviews are expected to continue until issues are addressed accordingly.
- The project schedule is being reassessed based on delays of key deliverables. Rebaseline expected to be complete by the end of September 2016.

Executive Summary

The following six tasks are in progress:

- Task 1: Project Management – Project Managers are working towards a rebaseline analysis. The Communication Plan is in project management review.
- Task 2: Project Initiation and Planning – The Deployment Plan and Training Plan were approved. The Comprehensive Test Plan is under review.
- Task 3: Technical Architecture and System Environments – The Technical Architecture Design Blueprint was approved. The team is making progress to build out a number of environments for the Technical Architecture Build deliverable. The team has begun testing and building the Technical Architecture Testing deliverable.
- Task 4: Interface and Data Transition Strategy – The Interface and Data Transition Interface and Data Transition Strategy is in revision as final edits are addressed.
- Task 5: Phase 1 Identity Hub Implementation – The Phase 1 Identity Hub Design Blueprint deliverable has begun, focusing first on the Workday integration.
- Task 6: Group and Role Management – The team is interviewing key stakeholders and drafting use cases. The team has created a framework for the categorization of use cases to support prioritization and implementation.

IAMMP Phase 1 Project Progress Metrics
(as of 9/2/2016)

Legend: ■ Total Budget (Hrs) ■ Budget to Date (Hrs) ■ Actual (Hrs) ■ Estimate at Completion (Hrs)

Task	Total Budget (Hrs)	Budget to Date (Hrs)	Actual (Hrs)	Estimate at Completion (Hrs)
Task 1: Project Management	410	370	147	249
Task 2: Project Initiation and Planning	517	517	266	315
Task 3: Technical Architecture and System Environments	3,312	3,248	1,555	3,559
Task 4: Interface and Data Transition Strategy	452	452	795	829
Task 5: Phase 1 Identity Hub Implementation	2,254	1,083	114	2,381
Task 6: Group and Role Management	2,609	788	661	3,206

	Deliverable Status				
Project Task Area	Deliverable	Deliverable Name	Status	Planned Finish	Actual Finish
Task 1: Project Management	D1.1	Project Work Plan	Complete	3/21/2016	3/14/2016
	D1.2.1	Q1 Quarterly Status Report	Complete	4/25/2016	4/29/2016
	D1.2.2	Q2 Quarterly Status Report	Complete	7/25/2016	7/29/2016
	D1.2.3	Q3 Quarterly Status Report		10/24/2016	
	D1.2.4	Q4 Quarterly Status Report		1/30/2017	
	D1.3	Risk and Issue Register	Complete	3/21/2016	3/17/2016
	D1.4	Change Control Process	Complete	4/4/2016	4/11/2016
	D1.5	Communication Plan	Behind	7/18/2016	EC: 9/23/2016
Task 2: Project Initiation and Planning	D2.1	Application Development and Configuration Standards	Complete	4/18/2016	4/8/2016
	D2.2	Project Kick-off Meeting	Complete	2/29/2016	2/29/2016
	D2.3	Comprehensive Test Plan	Behind	6/6/2016	EC: 9/30/2016
	D2.4	Deployment Plan	Complete	4/25/2016	7/22/2016
	D2.5	Training Plan	Complete	5/23/2016	8/26/2016
Task 3:Technical Architecture and System Environments	D3.1	Technical Architecture Approach	Complete	5/2/2016	5/20/2016
	D3.2	Prototype Environment(s)	Complete	5/2/2016	4/18/2016
	D3.3	Technical Architecture Requirements	Complete	5/16/2016	6/10/2016
	D3.4	Technical Architecture Design Blueprint	Complete	6/20/2016	8/26/2016
	D3.5	Technical Architecture Build	Behind	8/8/2016	EC: 10/10/2016
	D3.6	Technical Architecture Testing	Behind	8/22/2016	EC: TBD
	D3.7	Technical Architecture Training	Behind	8/29/2016	EC: TBD
	D3.8	Technical Architecture Deployment Playbook	Behind	8/22/2016	EC: TBD
	D3.9	Technical Architecture Deployment		9/12/2016	
	D3.10	Technical Architecture Operations and Maintenance Plan		9/26/2016	
Task 4: Interface and Data Transition Strategy	D4.1	Interface and Data Transition Strategy Requirements	Complete	5/9/2016	6/3/2016
	D4.2	Interface and Data Transition Strategy	Behind	5/23/2016	EC: 9/23/2016
Task 5: Phase 1 Identity Hub Implementation	D5.1	Phase 1 Identity Hub Design Blueprint	Behind	8/1/2016	EC: TBD
	D5.2	Phase 1 Identity Hub Build		9/6/2016	
	D5.3	Phase 1 Identity Hub Test	Behind	10/24/2016	EC: TBD
	D5.4	Phase 1 Identity Hub Training	Behind	10/31/2016	EC: TBD
	D5.5	Phase 1 Identity Hub Deployment Playbook		10/10/2016	
	D5.6	Phase 1 Identity Hub Deployment		10/31/2016	
	D5.7	Phase 1 Identity Hub Operations and Maintenance Plan		11/14/2016	
Task 6: Group and Role Management	D6.1	Group and Role Management Use Cases	Behind	8/22/2016	EC: 9/30/2016
	D6.2	Group and Role Management Requirements	Behind	9/6/2016	EC: TBD
	D6.3	Group and Role Management Design Blueprint		9/26/2016	
	D6.4	Group and Role Management Adoption Plan		11/7/2016	
	D6.5	Group and Role Management Build		10/24/2016	
	D6.6	Group and Role Management Testing		11/21/2016	
	D6.7	Group and Role Management Training	Behind	12/12/2016	EC: TBD
	D6.8	Group and Role Management Deployment Playbook		10/24/2016	
	D6.9	Group and Role Management Deployment		12/12/2016	
	D6.10	Group and Role Management Operations and Maintenance Plan		12/19/2016	