

## **IAM Committee**

### Meeting Notes

3/13/2017

**Attending:** Cam Beasley, CW Belcher, Michael Bos, Bill Bova, Tim Fackler, Seth Feder (for Dash Ballarta), Fred Gilmore, Ty Lehman, Darin Mattke, Karen Weisbrodt, Tiffany Yanagawa

**Absent:** John Chambers, Graham Chapman, Cesar de la Garza, Alison Lee, Andy Loomis, Jason Mayhew, Shelley Powers, Steve Rung, Charles Soto

**IAM:** Rosa Harris, Justin Hill, Aaron Reiser, Autumn Shields

#### **1. IAM Roadmap – Update (CW Belcher)**

Reference handout.

In progress and recently completed efforts:

- Phase 1 of the IAM Modernization Program (IAMMP) – SailPoint IdentityIQ implementation
- IAM Integrations – Working with campus areas to integrate new software to make use of IAM authentication services
- Sustaining work on UTLogin – Improving reliability and adding new functionality, specifically OAuth
- Transition to Duo for two-factor authentication – Transition is complete and the busiest season for two-factor authentication, W-2 claiming, went smoothly this past January
- Legacy Authorization System Roadmap (LASR) – Planning a roadmap for customers who currently use Mainframe-based authorization systems such as Apollo and the Organizational Hierarchy System Contacts (OHSC).
- Directory Services Roadmap – On hold due to resource constraints. Will reassess this summer.
- TRAC Replacement Project – IAM team is working with the ServiceNow team to restart transition of services from TRAC to ServiceNow.

**Q:** Where does the implementation of the Legacy Authorization Roadmap stand?

**A:** The team is currently implementing changes to legacy systems to make sure they will continue to function when Workday goes live.

**Q:** A lot of effort was made last year on the Identity Assurance Framework. How is that being used?

**A:** During the IAM Integrations process, customers complete a risk assessment that leverages the Identity Assurance Framework to help determine the appropriate authentication mechanisms for their services.

**Q:** Previously, it was stated that TRAC needed to be transitioned by July. Is that no longer the case?

**A:** Correct. One of the main drivers of the July deadline was to avoid having to retrofit TRAC to work with Workday Financials. Since the Workday go-live has been delayed, the team will have more time to transition services out of TRAC.

**Q:** Has Shibboleth been incorporated into UTLogin to use Duo?

**A:** Shibboleth is a separate service from UTLogin, but both support Duo for two-factor authentication.

**Q:** Are you considering merging UTLogin and Shibboleth?

**A:** Most likely not, since Shibboleth allows for more fine grained customization, which is necessary for some third-party vendor applications. The team is considering having Shibboleth hand off authentication to UTLogin to allow Shibboleth and UTLogin to operate in the same Single Sign-On (SSO) environment. Shibboleth is well-supported by InCommon with an active enhancement effort, so Shibboleth remains a viable product at this time.

In the original IAM Roadmap, Identropy performed an assessment of our maturity across six sets of criteria. Since then, we have made some improvements in various areas of maturity. (Reference handout.) Target states reflect where we are moving toward and indicate which phase on IAMMP corresponds to that level of maturity. This graphic serves as a snapshot of where we were, where we are, and where we are headed.

**Q:** What has been the biggest impediment to increase maturity?

**A:** The major hurdles have been resourcing and the length of the procurement process.

**Q:** Was the updated assessment completed by the IAM Team?

**A:** Yes, it was completed making use of the existing scoring rubric.

As planning for Phase 2 of IAMMP begins, there will be discussions about the prioritization of resources. Since the original Roadmap was developed a number of years ago, the Committee may need to reassess the priorities based on the changing state of IT on campus. The bulk of the planning is expected to take place this summer. The team will also need to look into what capabilities are available in SailPoint and how those capabilities might be leveraged to realize operational efficiencies.

## **2. 2016 Authentication Service Incidents Analysis – Update (CW Belcher)**

This item has been deferred to the next meeting due to illness.

## **3. Other Initiative Updates**

### **a. IAM Team Staffing (CW Belcher)**

There has been a lot of recent progress on the hiring front. Two new outside hires started at the end of February: a Software Developer/Analyst who will be primarily assisting with IAMMP and a new Business Analyst/Quality Assurance Tester to help out with testing. The new Identity Management lead and IAM Operations manager are internal hires.

There are currently two vacancies on the IAM team: a Software Engineer and an IT Operations Analyst. The team is currently waiting on approval to post these openings.

**Q:** Are there any opportunity for improving efficiencies?

**A:** The recently-created IAM Operations team has been investing a lot of time in automating processes

which can be automated, which has resulted in significant efficiency improvements. There is a need to reduce the maintenance tail for products, which the team will accomplish by moving toward more standard implementations with fewer customizations.

**Q:** Given the resource constraints, will your team be available to help with a large number of upcoming integrations?

**A:** Yes, the team has a number of engineers trained to assist with integration tasks. If you are aware of a big upcoming integration, contact the team early so we can learn more about your particular needs and to ensure that we can best support you.

**b. IAM Integrations (Justin Hill)**

- i. Start (Feb. 1): 27
- ii. +4 New: (DEM-AWS, iLab, Stache, Workplace by Facebook)
- iii. +1 Reopened: (Load Balancing)
- iv. 1 Completed: (Thousandeyes)
- v. 0 Cancelled: ( )
- vi. End (Feb. 28): 31

On average there are 2.5 integration requests per month, but there were nine new requests in January and four new requests in February. The team is working on processing these and is hopeful to have some requests completed soon.

**c. Legacy Authorization Roadmap (CW Belcher)**

As mentioned in a previous item, work on the LASR wiki is ongoing to help customers learn about how legacy authorization use cases will be supported in the future environment.

**d. IAM Modernization Program / SailPoint Implementation (CW Belcher)**

Reference handout.

The project schedule for Phase 1 is being re-baselined to align with the team's revised approach to completing the build and testing tasks. Re-baselining is complete for Task 5 (Identity Hub implementation) and will be completed for Task 6 (Group and Role Management) by next month's meeting.

Task 3 (Technical Architecture Implementation) work is nearly complete, pending final resolution of several testing items.

Task 5 build activities are in progress. Knowledge transfer from KPMG to the IAM Team is underway and training materials are being developed in parallel with the build activities. The second round of Workday testing has been completed. There will be at least one more round of testing with the Workday team.

The Task 6 design has been drafted and is being reviewed. Drafting of the Group and Role Management Adoption Plan is also in progress.

The team projects completing Phase 1 activities in September, though production implementations with the Group and Role Management early adopters will likely begin earlier than that depending on what is appropriate for each early adopter.

# Identity & Access Management: Strategic Roadmap Update

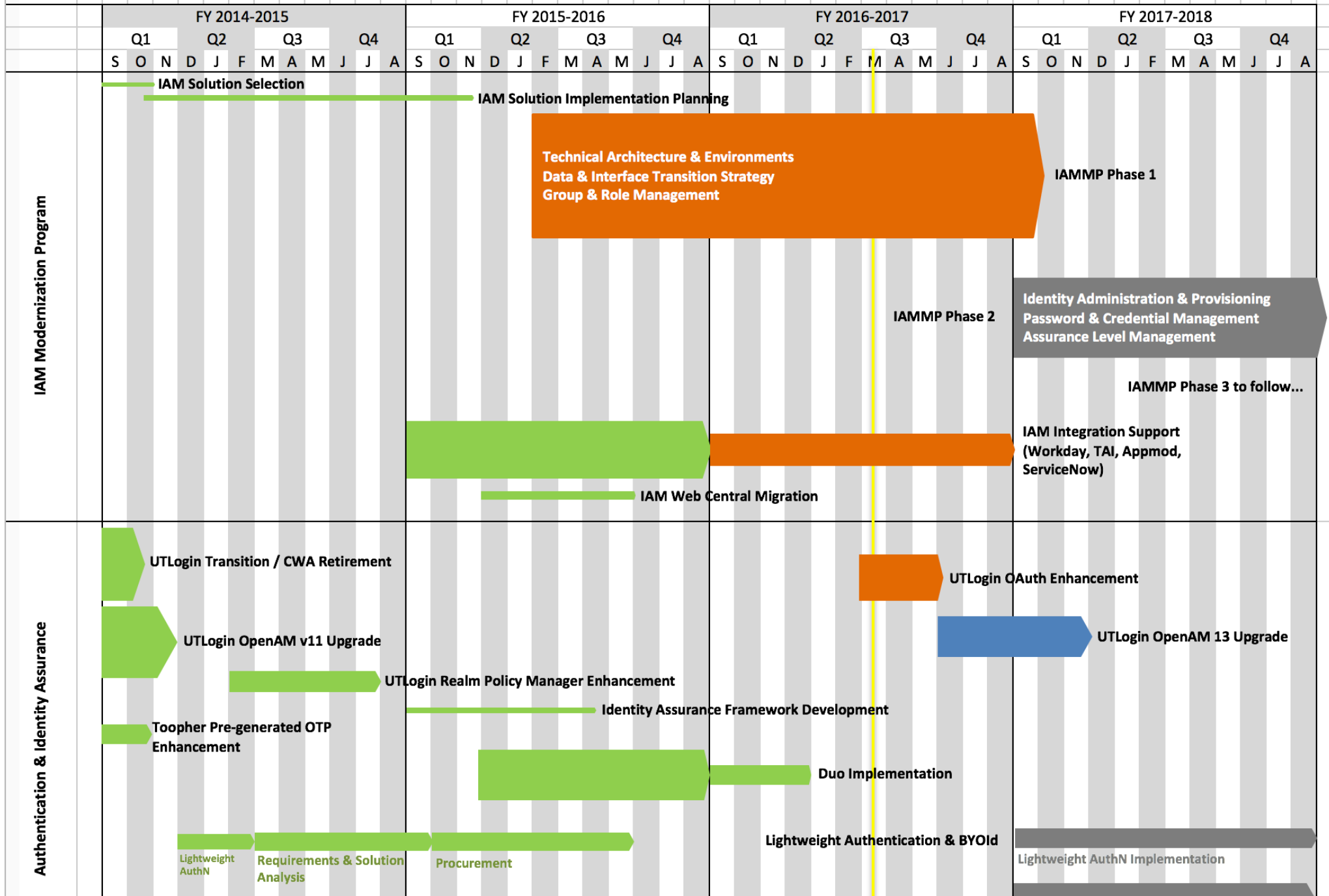
March 2017

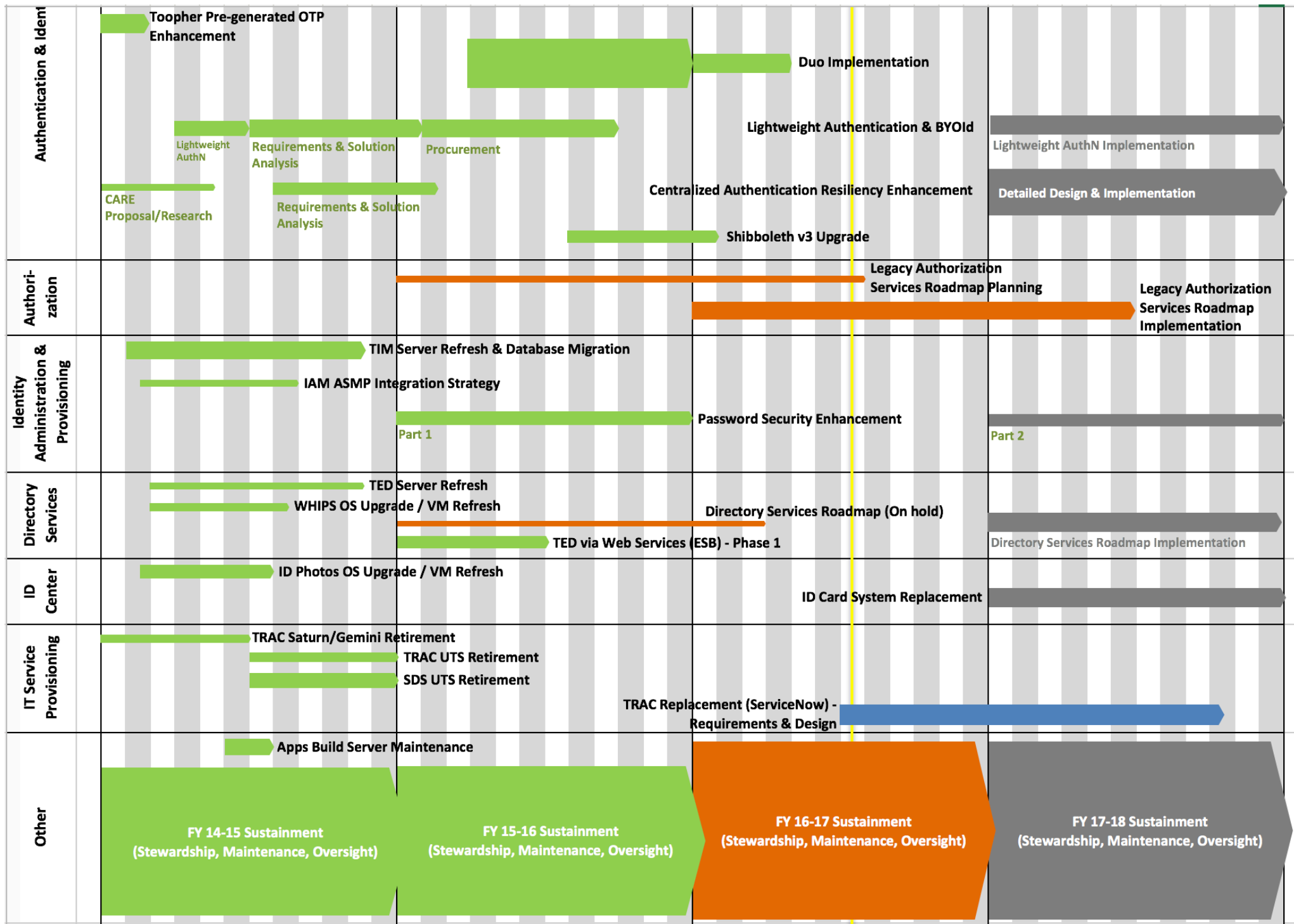
# IAM Roadmap Overview

Status

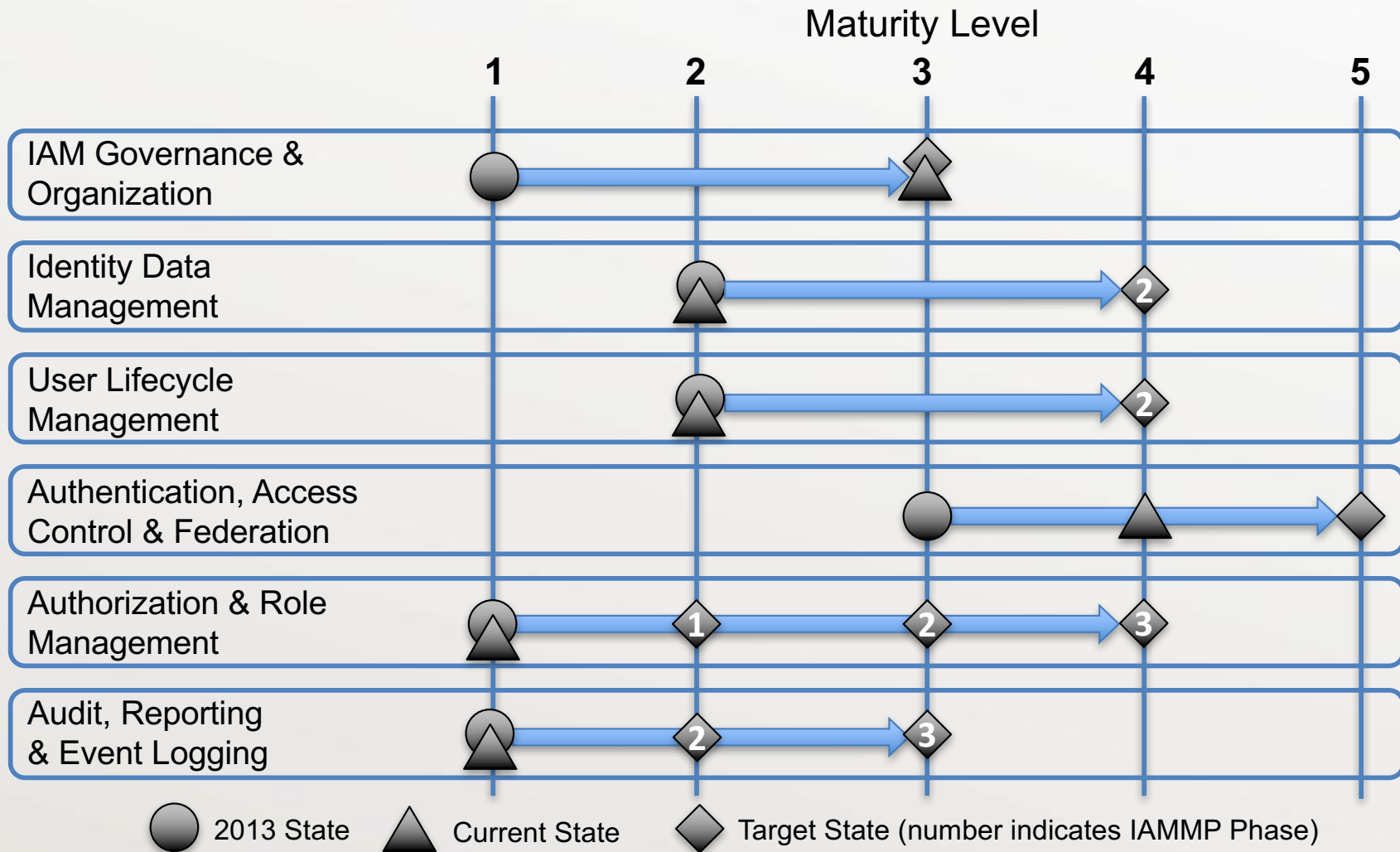
- ▶ Complete
- ▶ In Progress
- ▶ Planned
- ▶ Future

Bar Height Indicates Level of 1 FTE





# IAM Capability Assessment





# IAM Capability Assessment Rubric

Capability	Scoring Rubric
IAM Governance & Organization	<ul style="list-style-type: none"> <li>• 5 = Formal IAM Governance is serving the needs for visibility for all stakeholders</li> <li>• 4 = IAM Governance is part of a larger IT governance framework and manages with metrics and SLAs</li> <li>• 3 = IAM Governance is part of a larger IT Governance framework and includes formal subcommittees</li> <li>• 2 = IAM Governance is formal but is not part of a larger IT governance framework</li> <li>• 1 = IAM Governance is informal</li> </ul>
Identity Data Management	<ul style="list-style-type: none"> <li>• 5 = All accounts &amp; roles centrally provisioned and reconciled</li> <li>• 4 = Centralized account &amp; role provisioning processes in use</li> <li>• 3 = Internal accounts provisioned, roles local in applications</li> <li>• 2 = Single registry exists, some provisioning is automated</li> <li>• 1 = No single registry of users</li> </ul>
User Lifecycle Management	<ul style="list-style-type: none"> <li>• 5 = User lifecycle is managed centrally, request and approval processes are segregated and captured</li> <li>• 4 = Most lifecycle processes are centralized, approvals are generally captured</li> <li>• 3 = Most lifecycle processes are centralized, approvals are generally out-of-band</li> <li>• 2 = Identity is created centrally, but remaining lifecycle processes decentralized</li> <li>• 1 = Identity Management processes are tribal knowledge</li> </ul>
Authentication, Access Control & Federation	<ul style="list-style-type: none"> <li>• 5 = Federated single sign-on</li> <li>• 4 = Single sign-on with strong authentication</li> <li>• 3 = Single sign-on, static password</li> <li>• 2 = LDAP directory authentication, static password</li> <li>• 1 = Local username, local static password</li> </ul>
Authorization & Role Management	<ul style="list-style-type: none"> <li>• 5 = Business roles are defined and leveraged for (de)provisioning and transfers</li> <li>• 4 = Business roles are defined and leveraged for (de)provisioning</li> <li>• 3 = Centralized group management processes exist and are widely leveraged</li> <li>• 2 = Centralized group management processes exist but are not widely leveraged</li> <li>• 1 = Authorization processes are decentralized and not coordinated</li> </ul>
Audit, Reporting, & Event Monitoring	<ul style="list-style-type: none"> <li>• 5 = Risk-based access recertification cycles exist with quality control measures in place</li> <li>• 4 = Risk management framework used to establish appropriate recertification cycles</li> <li>• 3 = High-risk access is periodically recertified in an automated system</li> <li>• 2 = Access recertification tools exist but are not widely used</li> <li>• 1 = Access is not routinely audited or recertified</li> </ul>

# Identity and Access Management Modernization Program (IAMMP)

## Phase 1 Status

Monday, March 13, 2017

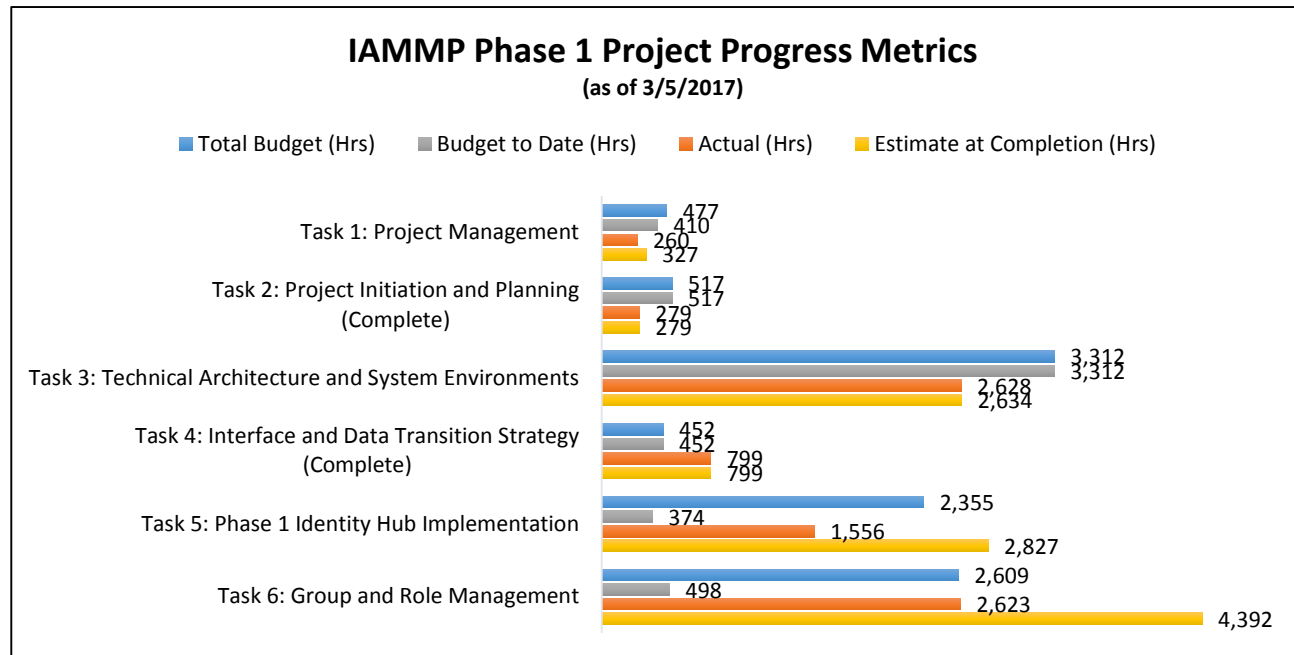
### Items for Management Attention

- The rebaselining of the Phase 1 schedule is in progress.

### Executive Summary

The following four tasks are in progress:

- Task 1: Project Management – No updates. The next quarterly report is due in April.
- Task 3: Technical Architecture and System Environments – The Technical Architecture Testing deliverable is being revised to address gaps in requirements traceability.
- Task 5: Phase 1 Identity Hub Implementation – The Phase 1 Identity Hub Build, Training, and Deployment Playbook deliverables are in progress. The second round of Workday integrations testing has been completed successfully, and detailed test planning for the remainder of Phase 1 Identity Hub Testing is in progress.
- Task 6: Group and Role (G&R) Management – The G&R Design Blueprint has been submitted for project manager review. All Adoption Plan deliverable items are in progress.



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	Complete	10/24/2016	12/2/2016
	D1.2.4	Q4 Quarterly Status Report	Complete	1/30/2017	1/20/2017
	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
Task 2: Project Initiation and Planning	D1.5	Communication Plan	Complete	7/18/2016	12/2/2016
	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	Complete	6/6/2016	10/7/2016
	D2.4	Deployment Plan	Complete	4/25/2016	7/22/2016
Task 3: Technical Architecture and System Environments	D2.5	Training Plan	Complete	5/23/2016	8/26/2016
	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	Complete	8/8/2016	12/2/2016
	D3.6	Technical Architecture Testing	Behind	8/22/2016	EC: 3/17/2017
	D3.7	Technical Architecture Training	Complete	8/29/2016	2/6/2017
	D3.8	Technical Architecture Deployment Playbook	Complete	8/22/2016	12/2/2016
	D3.9	Technical Architecture Deployment	Complete	9/12/2016	12/13/2016
Task 4: Interface and Data Transition Strategy	D3.10	Technical Architecture Operations and Maintenance Plan	Complete	9/26/2016	1/20/2017
	D4.1	Interface and Data Transition Strategy Requirements	Complete	5/9/2016	6/3/2016
Task 5: Phase 1 Identity Hub Implementation	D4.2	Interface and Data Transition Strategy	Complete	5/23/2016	9/16/2016
	D5.1	Phase 1 Identity Hub Design Blueprint	Complete	8/1/2016	1/20/2017
	D5.2	Phase 1 Identity Hub Build	In Progress	<del>9/6/16</del> 4/14/17	EC: 4/21/17
	D5.3	Phase 1 Identity Hub Test	In Progress	<del>10/24/16</del> 9/15/17	
	D5.4	Phase 1 Identity Hub Training	In Progress	<del>10/31/16</del> 4/28/17	
	D5.5	Phase 1 Identity Hub Deployment Playbook	In Progress	<del>10/10/16</del> 5/12/17	
	D5.6	Phase 1 Identity Hub Deployment		<del>10/31/16</del> 5/19/17	
Task 6: Group and Role Management	D5.7	Phase 1 Identity Hub Operations and Maintenance Plan		<del>11/14/16</del> 6/2/17	
	D6.1	Group and Role Management Use Cases	Complete	8/22/2016	12/5/2016
	D6.2	Group and Role Management Requirements	Complete	9/6/2016	1/6/2017
	D6.3	Group and Role Management Design Blueprint	Behind	<del>9/26/16</del> 3/10/17	EC: 4/7/17
	D6.4	Group and Role Management Adoption Plan	In Progress	<del>11/7/16</del> 6/2/17	
	D6.5	Group and Role Management Build		<del>10/24/16</del> 7/7/17	
	D6.6	Group and Role Management Testing		<del>11/21/16</del> 9/15/17	
	D6.7	Group and Role Management Training		<del>12/12/16</del> 9/1/17	
	D6.8	Group and Role Management Deployment Playbook		<del>10/24/16</del> 7/21/17	
	D6.9	Group and Role Management Deployment		<del>12/12/16</del> 9/15/17	
D6.10	Group and Role Management Operations and Maintenance Plan		<del>12/19/16</del> 9/22/17		
Task 7: Optional Post Implementation Support	D7.1	Optional Post Implementation Support			