What is Identity & Access Management (IAM)?

IAM enables the right individuals to access the right resources at the right times for the right reasons

For an end user (student, employee, etc.), this means:
Getting accounts provisioned in the correct systems, and getting access to the correct features/ data within those systems, all in a timely manner (automated to the greatest extent possible).

For a manager, this means:
Knowing which systems his/her direct/indirect reports have access to, being able to request more/less access as needed, and being able to audit access over time.

IAM is an ecology of:

- Digital identities, and processes related to identity lifecycle management
- Identity management registry (Fischer Identity)
- Password management tools
- Directories (e.g. AD, OpenLDAP)
- Access and authentication tools (e.g. CAS, Shibboleth)
- Support providers' and service owners' roles and responsibilities
- Security
- Governance and training

IAM initiative resources

The IAM project has many campus stakeholders. The departments that are contributing the bulk of the implementation resources are listed here.

Functional/business teams:

- ADMS – Office of Admissions
- FA – Faculty Affairs
- GRAD – Graduate Studies
- HRIS – HR Information Systems
- REGS – Office of the Registrar

Technical teams:

- ADS – Application and Data Services
- CMT – Creative Media Technologies
- EADS – Enterprise Apps and Data Services
- ESYS – Enterprise Systems
- ISEC – Information Security
- ITCS – IT Client Services
- ITSS – IT Support Services
- NOP – Network Operations

What does the IAM initiative mean for CSU, Chico?

Implementation of the Fischer Identity solution represents the next step in the University's ongoing IAM initiative. Fischer was selected via campus RFP in 2015.

Phase I objectives:

- Create a new set of affiliations and roles, aligned with CO definitions as much as possible
- Create an entitlements catalog that indicates when/how users get accounts/access in target systems based on their affiliations/roles (Phase I targets include LDAP, AD, Bb Learn, Google Apps, and O365)
- Create new group structures within LDAP/AD directories to store affiliations/roles
- Install and configure the Fischer Identity application
- Automated account provisioning and de-provisioning
- Password management
- Install and configure DUO multifactor authentication for users with elevated Fischer access
- Create new governance procedures for the management of identity/access data
- Decommission homegrown Registry (as a follow up)
- Decommission current password management tools (as a follow up)

Phase I should begin to address the following security audit findings:

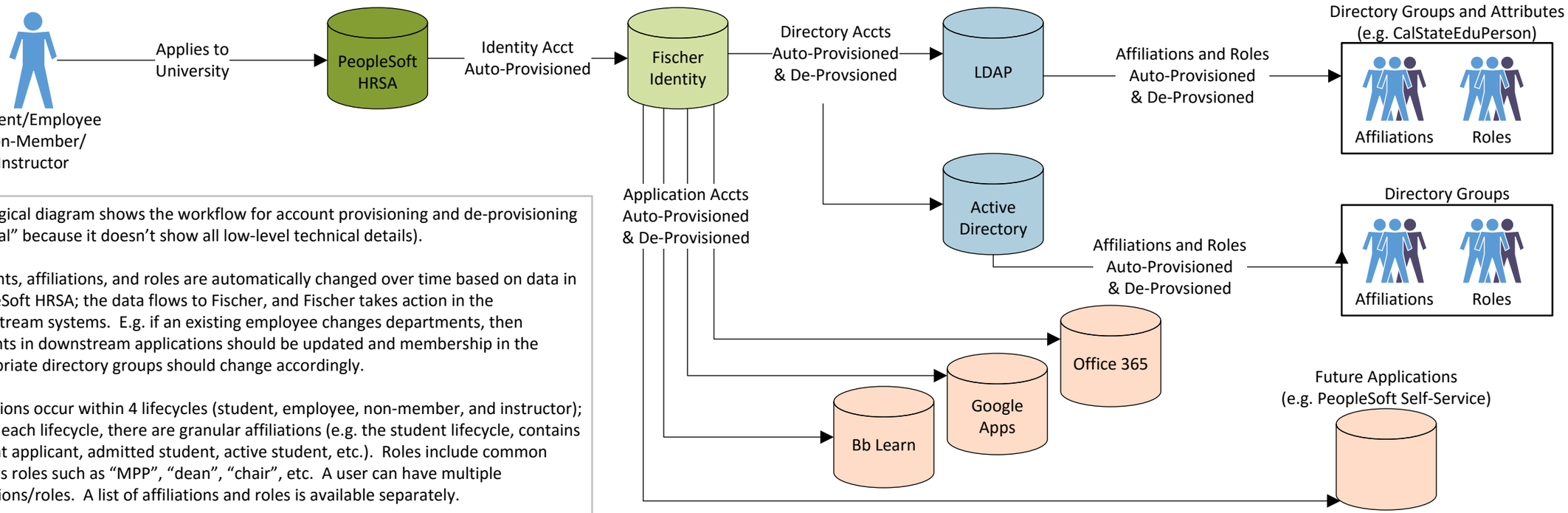
- 2008 CO Audit -18.0 - Password Standards
- 2012 Advisor Assessment - 01.1 - Access Control DB Access
- 2008 CO Audit - 20.0 - Granted Privileged Access
- 2012 Advisor Assessment - 01.0 - L1 Access Control
- 2012 Advisor Assessment -01.2 - Access Control- DB Access Review
- M&I Assess. - 03.1 - Level 1 Data Protection
- 2008 CO Audit - 15.0 - User Access Control
- 2008 CO Audit - 21.0 - Adjust Desktop Access Rights
- 2008 CO Audit - 17.0 - Network Access
- M&I Assess.-05.3 -Application, System & Privileged Service Password Management
- 2008 CO Audit - 08.0 -Sharing of Accounts
- 2012 HIPAA Assessment - 08.0 - Access Control (session timeout)
- M&I Assess.-05.1 - Identity Management
- M&I Assess.-05.2 - Account Auditing & Review (Users, Servers, Firewalls, Databases, Applications)
- 2008 CO Audit - 07.0 - Employee Separation

IAM Initiative Contacts

Questions about the IAM initiative can be directed to any of the following:

- Andy Miller, Co-Sponsor, EADS
- Mark Hendricks, Co-Sponsor, ISEC
- Wendy Bentley, Project Manager, EADS

IAM - Account Provisioning and De-Provisioning

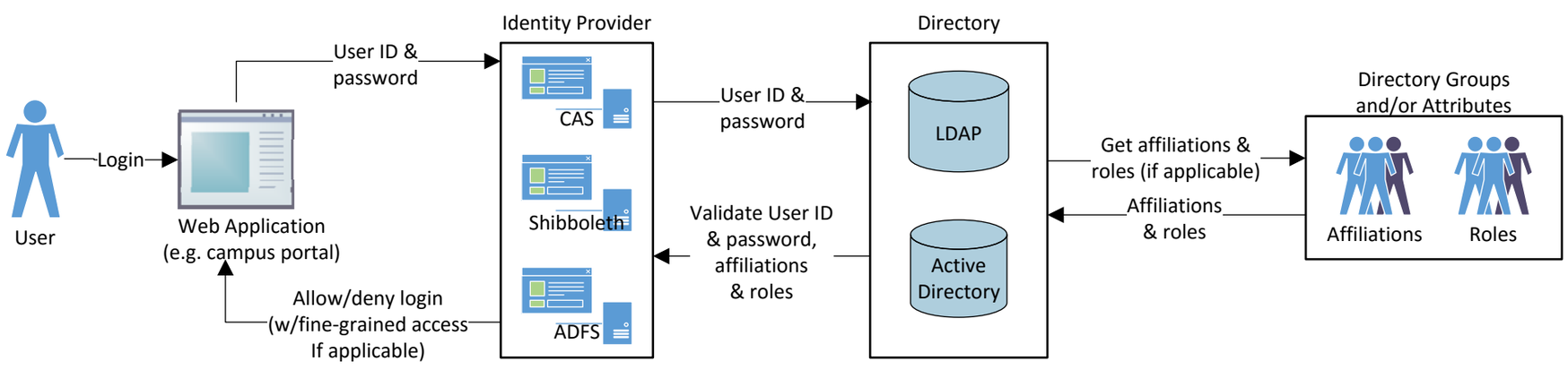


This logical diagram shows the workflow for account provisioning and de-provisioning ("logical" because it doesn't show all low-level technical details).

Accounts, affiliations, and roles are automatically changed over time based on data in PeopleSoft HRSA; the data flows to Fischer, and Fischer takes action in the downstream systems. E.g. if an existing employee changes departments, then accounts in downstream applications should be updated and membership in the appropriate directory groups should change accordingly.

Affiliations occur within 4 lifecycles (student, employee, non-member, and instructor); within each lifecycle, there are granular affiliations (e.g. the student lifecycle, contains student applicant, admitted student, active student, etc.). Roles include common campus roles such as "MPP", "dean", "chair", etc. A user can have multiple affiliations/roles. A list of affiliations and roles is available separately.

IAM - Authentication and Access (i.e. Login)



This logical diagram shows a login to a typical web application (again, "logical" because it doesn't show all low-level technical details). When the user enters his/her User ID and password, those credentials are passed to an identity provider, and then they are verified against a directory.

Fine grained access in an application (e.g. access into specific features/screens, fields within a screen, data elements, etc.) can be allowed or denied based on the user's affiliation(s) and/or role(s).

IAM – Road Map

Objectives:
- Assess campus identity and access processes/tools/usage
- Engage campus stakeholders
- Recommend new processes

Supporting documents:
- Identity and Access Management Assessment for Implementation.docx
- Chico State - IAM Assessment FINAL v1.0 _ 11.06.2014.pdf

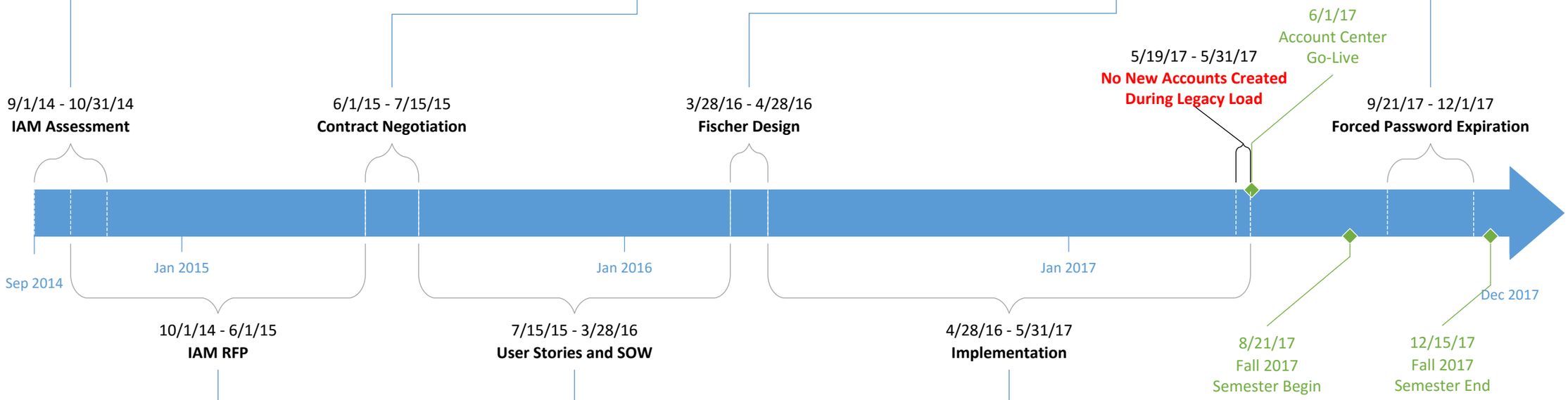
Objectives:
- Finalize selection of Fischer as RFP winner
- Procurement/security review of Fischer contract
- Soft schedule implementation dates

Supporting documents:
- Fischer Master Software Licensing Agreement.pdf

Objectives:
- Translate user stories into technical design

Supporting documents:
- Chico Affiliations and Services.xlsx

Objectives
- Force password expiration for all accounts
- All users update their PW recovery info (SMS/text phone number, email address, security questions)



Objectives:
- Write/post a public RFP for a new IAM tool

Supporting documents:
- Chico IAM RFP.docx
- IAM Update for Systems Security Meeting, May 2015.pptx

Objectives:
- Document the user stories which explain the features that we intend to implement and how we do business; the user stories essentially act as the design guide
- Engage campus stakeholders
- Finalize SOW (statement of work) for Fischer's professional services for implementation

Supporting documents:
- Chico Affiliations and Services.xlsx
- 2016-03-02-SOW-Final-Chico.pdf

Objectives:
- Automated provisioning/deprovisioning accounts into Fischer, LDAP, Active Directory, Blackboard Learn, Office 365, and Google Apps
- Automate user affiliations (and group membership) within student, employee, non-member, and instructor life cycles
- Accommodate management of user 'level of assurance' (LOA)
- Password management

This roadmap is not intended to spell out low-level project details/timelines. Low-level details/timelines are stored in TeamDynamix, and are available upon request.