Business and Process Requirements

Business Requirements mapped to downstream Process Requirements

IAM

UC Davis

IAM-REQ-1 Authorization Capabilities

The system shall enable authorization capabilities that align user's affiliations and associations to a wide range of applications and systems.

Relationships:

IAM-REQ-106 Assign Roles Based on User Attributes
IAM-REQ-109 Authorization Rules
IAM-REQ-110 Auto-Assignment of Roles
IAM-REQ-112 Mandatory Roles
IAM-REQ-95 Recommended Roles Interface
IAM-REQ-116 Role Bundling
IAM-REQ-91 Third Party Access Management
IAM-REQ-92 Third Party Role Management
IAM-REQ-96 User Role Request

IAM-REQ-8 Limit Access to Restricted Data

The system shall limit access to restricted information to privileged users and processes.

Relationships:

IAM-REQ-47 Encrypt Transport and Storage of Sensitive Data
IAM-REQ-25 Identify Restricted Information
IAM-REQ-78 Multiple Interface Views
IAM-REQ-59 Provide Views of Identity Info
IAM-REQ-93 Third Party Attribute View
IAM-REQ-90 User Search Interface

IAM-REQ-10 Activity Logging

The system shall log all IAM activities.

Relationships:

IAM-REQ-27 Log System Activities
IAM-REQ-118 Report Retention Policies

IAM-REQ-11 Report Generation

The system shall allow reports to be generated and viewed by authorized personnel.

Relationships:

IAM-REQ-29 Deliver Reports as Appropriate
IAM-REQ-28 Generate Reports as Appropriate
IAM-REQ-27 Log System Activities
IAM-REQ-118 Report Retention Policies
IAM-REQ-117 Target System Report Constraints
IAM-REQ-26 Track Access to Restricted Information

IAM-REQ-12 Auditing Capabilities

The system must support auditing capabilities.

Relationships:

IAM-REQ-32 Audit Non-Target Specific Data
IAM-REQ-31 Audit Target Specific Data
IAM-REQ-29 Deliver Reports as Appropriate
IAM-REQ-28 Generate Reports as Appropriate
IAM-REQ-27 Log System Activities
IAM-REQ-118 Report Retention Policies
IAM-REQ-117 Target System Report Constraints
IAM-REQ-26 Track Access to Restricted Information

IAM-REQ-14 Privacy Protections

The system shall maintain privacy protection for identity and other confidential data.

Relationships:

IAM-REQ-47 Encrypt Transport and Storage of Sensitive Data
IAM-REQ-73 Identify Privileged User Types
IAM-REQ-25 Identify Restricted Information
IAM-REQ-62 Limit System/Process Access to Restricted Info
IAM-REQ-61 Limit User Access to Restricted Info
IAM-REQ-49 Meet FERPA Requirements
IAM-REQ-46 Meet UCD Campus IT Usage Policy
IAM-REQ-45 Meet UCDHS Use Agreements
IAM-REQ-78 Multiple Interface Views
IAM-REQ-48 Obscure Sensitive Data Entered
IAM-REQ-59 Provide Views of Identity Info
IAM-REQ-74 Self-Service View of Identity Info
IAM-REQ-26 Track Access to Restricted Information

IAM-REQ-15 Multiple Password Policies

The system shall accommodate password policies for all affected source and target systems.

Relationships:

IAM-REQ-75 Accommodate Multiple Password Policies
IAM-REQ-79 Password Reset Questions
IAM-REQ-80 Password Reset Questions Interface
IAM-REQ-76 Self-Service IAM Password Reset
IAM-REQ-77 Self-Service Target System Password Reset

IAM-REQ-19 Role Assignment and Provisioning Actions

The system shall use roles to provision user accounts and provide access to resources across multiple computer systems and applications.

Relationships:

IAM-REQ-106 Assign Roles Based on User Attributes
IAM-REQ-113 Auto-Approval of Roles
IAM-REQ-110 Auto-Assignment of Roles
IAM-REQ-112 Mandatory Roles
IAM-REQ-95 Recommended Roles Interface
IAM-REQ-116 Role Bundling
IAM-REQ-99 Role Definition and Policies
IAM-REQ-100 Role Expiration
IAM-REQ-102 Role Expiration Extensions
IAM-REQ-101 Role Notifications
IAM-REQ-107 Role Ownership
IAM-REQ-103 Role Usage Guidelines
IAM-REQ-105 Roles May Define Multiple Permissions
IAM-REQ-104 Roles May Provision Multiple Systems
IAM-REQ-23 Support Immediate Access Requests
IAM-REQ-114 Third Party Bulk Role Management
IAM-REQ-92 Third Party Role Management
IAM-REQ-96 User Role Request

IAM-REQ-35 Accommodate Externals

The system shall provide Identity and Access Management for externals from both the Health System and Campus, reusing any existing functionality whenever possible.

Relationships:

IAM-REQ-33 Externals' Registration Interface
IAM-REQ-34 Externals' Sponsors
IAM-REQ-36 Interface to Manage Externals
IAM-REQ-38 Maintain Externals' Identity Info
IAM-REQ-37 Reconcile Externals with Existing Affiliates

IAM-REQ-120 Privileged Users

The system shall empower an organization of authorized IAM privileged users who provide identity vetting for members of the community, as well as assistance for end-users for common IAM interactions such as password resets or group management.

Relationships:

IAM-REQ-159 Help Desk Interface
IAM-REQ-25 Identify Restricted Information
IAM-REQ-78 Multiple Interface Views
IAM-REQ-91 Third Party Access Management
IAM-REQ-93 Third Party Attribute View
IAM-REQ-94 Third Party Password Reset
IAM-REQ-92 Third Party Role Management
IAM-REQ-26 Track Access to Restricted Information
IAM-REQ-90 User Search Interface

IAM-REQ-121 Person Repository

The system shall provide a Person Repository capable of containing all members of the UC Davis community, for use as an authoritative source of identity information for applications deployed for use at UCD.

Relationships:

IAM-REQ-111 Account Name Retention
IAM-REQ-57 Define and Locate Identity Info
IAM-REQ-115 Identity Suspense Interface
IAM-REQ-55 Interface to Resolve Identity Conflicts
IAM-REQ-58 Maintain and Store Identity Info
IAM-REQ-38 Maintain Externals' Identity Info
IAM-REQ-56 Match Resolution Processes
IAM-REQ-59 Provide Views of Identity Info
IAM-REQ-37 Reconcile Externals with Existing Affiliates
IAM-REQ-54 Uniquely Define Users

IAM-REQ-122 Group and Org Hierarchy Management

The system shall provide a Group Manager tool and other tools to support group management and organizational hierarchies for their use in approval workflows, creating and maintaining institutional groups and ad hoc groups. (Some administrative tools will also require group management.)

Relationships:

IAM-REQ-98 Accommodate Organizational Hierarchies
IAM-REQ-149 Group Approvers
IAM-REQ-141 Group Owners
IAM-REQ-140 Groups Admin Interface
IAM-REQ-136 Groups API
IAM-REQ-146 Groups Containers
IAM-REQ-137 Groups DB Access
IAM-REQ-145 Groups Hierarchy
IAM-REQ-139 Groups LDAP Access
IAM-REQ-142 Groups Logging
IAM-REQ-147 Groups Membership APIs
IAM-REQ-143 Groups Privileged Users

IAM-REQ-144 Groups Reports
IAM-REQ-148 Groups Structure APIs
IAM-REQ-151 Groups Workflow Constraint
IAM-REQ-138 Groups WS Access
IAM-REQ-119 Role Approver Groups
IAM-REQ-163 Virtual Organization Management

IAM-REQ-123 New IAM Processes

The system shall support new policies and procedures to govern IAM processes and activities including delegation of authority and role management.
Relationships:

IAM-REQ-124 Auto-Provisioning

The system shall provide a mechanism to automatically provision and de-provision accounts and authorizations on integrated systems.
Relationships:

IAM-REQ-110 Auto-Assignment of Roles
IAM-REQ-100 Role Expiration
IAM-REQ-6 Timely, Role Aligned Authorization Enabling

IAM-REQ-125 Self Service PW Reset

The system shall provide a mechanism for self-service password reset for integrated applications.
Relationships:

IAM-REQ-76 Self-Service IAM Password Reset
IAM-REQ-157 Self-Service Password Reset Interface
IAM-REQ-77 Self-Service Target System Password Reset

IAM-REQ-126 Self Service Access and Role Requests

The system shall provide a mechanism to facilitate self-service provisioning and role change requests for integrated applications.
Relationships:

IAM-REQ-71 Auto-Assign Account IDs
IAM-REQ-53 LOA Self-Service Interface
IAM-REQ-95 Recommended Roles Interface
IAM-REQ-116 Role Bundling
IAM-REQ-158 Self-Service Account Creation Interface
IAM-REQ-74 Self-Service View of Identity Info
IAM-REQ-96 User Role Request

IAM-REQ-128 ESSO

The system shall implement, and integrate with IAM, an Enterprise Single Sign-On (ESSO) system available across all UC Davis departments with the goal of reducing the number of credentials (user name/password) a user must remember, while maintaining the integrity and accountability of the user credentials.
Relationships:

IAM-REQ-162 ESSO Support for EPIC

IAM-REQ-129 Federation Services

The system will provide federation services for all UC Davis users.
Relationships:

IAM-REQ-130 InCommon Silver (LOA)

The system must comply with InCommon Silver requirements for those community members who require it, as it pertains to 1) Registration and Identity Proofing, 2) Credential Issuance, Management and Technology, and 3) Identity Information Management.

Relationships:

IAM-REQ-7 Comply with InCommon Level of Assurance
IAM-REQ-53 LOA Self-Service Interface
IAM-REQ-52 Process LOA Vetting
IAM-REQ-50 Support Users/Accounts of Varying LOA
IAM-REQ-51 User LOA Vetting

IAM-REQ-131 Software Integration Infrastructure

The system shall be scalable, reliable, and securely designed, allowing integration with multiple source and target applications requiring minimal configuration and repeatable results.

Relationships:

IAM-REQ-39 Contact Info for Target System Owners
IAM-REQ-160 EPIC Integration
IAM-REQ-162 ESSO Support for EPIC
IAM-REQ-161 HSAD Integration
IAM-REQ-156 Kuali Rice Integration
IAM-REQ-153 Real-Time Availability
IAM-REQ-154 Self-Service Availability
IAM-REQ-87 Support De-Provisioning of Common Applications
IAM-REQ-86 Support Provisioning of Common Applications
IAM-REQ-155 System Maintenance Supportability
IAM-REQ-152 Target Supportability

IAM-REQ-132 Virtual Directory

The system will provide a Virtual Directory service available to UC Davis applications.

Relationships:

IAM-REQ-133 Hardware Infrastructure

The system's infrastructure components must meet business objectives in a scalable, reliable, sustainable manner.

Relationships:

IAM-REQ-44 Adequate Storage
IAM-REQ-42 Infrastructure for High Availability
IAM-REQ-43 Infrastructure for Reasonable Response Time
IAM-REQ-153 Real-Time Availability
IAM-REQ-154 Self-Service Availability
IAM-REQ-155 System Maintenance Supportability
IAM-REQ-152 Target Supportability

IAM-REQ-134 Approval Workflows

The system shall provide workflows for approval of access requests, which includes email based notifications and a web interface for approval of requests.

Relationships:

IAM-REQ-98 Accommodate Organizational Hierarchies
IAM-REQ-164 Approval Types
IAM-REQ-113 Auto-Approval of Roles
IAM-REQ-83 Delegate Approval Authority
IAM-REQ-84 Delegate Authority to Group
IAM-REQ-119 Role Approver Groups

IAM-REQ-135 Operational Support

The system shall support the needs of a post-live operational support model that addresses customer support and ongoing IdM maintenance.

Relationships:

IAM-REQ-41 Administrative Interfaces

IAM-REQ-24 Delegation of Approvals and Role Management

The system shall allow role approvers and owners the ability to "delegate" their authority for all or some of their roles to another individual.

Relationships:

IAM-REQ-83 Delegate Approval Authority
IAM-REQ-84 Delegate Authority to Group