

**VENDOR Name:**  
**REVIEWERS Name:**

**Category**  
**Functional Requirement**

	Person Registry		
Ref#	Scenarios	Use Case	Comments
1	Demonstrate ability to accept input via a) bulk load of flat file, b) message bus, c) exported web services interfaces		Student – 8,000
			Faculty/Staff – 8,000
			Alumni – 40,000
			Applicants – 35,000
			Affiliates – 1,000
2	Demonstrate ability to reconcile identities coming from multiple identity source systems	David was an undergraduate, is an alum, is a faculty member, is a staff member, and is a parent of a current student.	Describe standard fuzzy matching logic; describe how to add custom matching logic and criteria.
3	Demonstrate ability to manually handle resolution of duplicate identities	Merge two separate identities; split an existing entry (resulting from a bad match decision).	
4	Demonstrate how to implement associating multiple affiliations with a single person		How to:
			1. Define and manage attributes associated with each source system.
			2. Identify the primary owner of a field.
			3. Handle changes in attributes (eg name change)
5	Demonstrate ability to manually add a new person record	NA	Affiliate users
6	Demonstrate how an identity source is added/removed	NA	
7	Demonstrate how to associate identity proofing material with a user (e.g. scanned image of passport)		I-9 / LOA related

8	Demonstrate how a federated user is added to the Person Registry		Not a Brown identity, Federated users
9	Demonstrate how to implement a workflow for requesting a new user account, approving the request, and then adding the user		
10	Demonstrate how to do a regular comparison of the contents of the Person Registry and a production LDAP server.		
11	Demonstrate how to manage non-person identities		Departments, projects, events
12	Demonstrate the process for purging a set of records		Removing applicants who were denied admission
<b>Permissions Management</b>			
<b>Ref#</b>	<b>Scenarios</b>	<b>Use Case</b>	<b>Comments</b>
13	Demonstrate how to define/edit a Permission	All faculty, staff, students get email services.	See Glossary
14	Demonstrate the workflow to request, approve, and then manually grant a Permission to a specific subject (outside of the usual automated role/permission framework)	Only certain faculty and staff members in the Physics Department are allowed to update the Physics Department web site	
15	Demonstrate the temporary assignment of "a" permission to a different person		Delegation of certain permission
16	Demonstrate the process of managing who can manage permissions, including delegating management of a (set of) permission to a Subject		(scope = set of permissions; scope = target community eg a specific research group)
17	Demonstrate the process of replicating a set of permissions		Give User A has same permissions as user B
18	Demonstrate how to define that a Subject is eligible for a service but is not automatically provisioned for that service, and show how the subject would actually request and obtain such service		
<b>Roles and Role Provisioning</b>			

Ref#	Scenarios	Use Case	Comments
19	Demonstrate how Roles are	NA	How are roles created, and permissions associated; Organizational Context associated;
	created/maintained/removed, including associating a set of Permissions with the Role		
20	Demonstrate how to automatically assign a Role to a Subject, based on attribute information associated with the Subject		
21	Demonstrate how to manually assign a Role to a specific subject, outside of the automatic provisioning system		when the manual assignment conflicts with an existing Rule
22	Demonstrate how to manage hierarchies of Roles		A super-admin has all of the privileges of an admin, plus several additional privileges
<b>Groups Registry</b>			
Ref#	Scenarios	Use Case	Comments
23	Provide a quick overview of the functionality available with the Groups Registry		Non-functional question about the capacity of the Groups Registry
24	Demonstrate creating/managing rules to automatically maintain group memberships based on user attributes in the Person Registry	IdM must provide memberships for demographic groups, such as committed applicants or humanities graduate students.	How to manage the rules governing these processes?
25	Demonstrate using set arithmetic functionality to define the membership of Group A as the union of Groups B and C, and a list of specific individuals		We currently use all 3 logical operations, union, intersection, and complement.
26	Demonstrate real time replication of group memberships to production directories	Replicate group memberships to both isMemberOf and hasMember attributes (for people and groups) in LDAP.	
27	Demonstrate managing permissions, properties associated with a Group		Managing who can see that group exists, who can see group membership, who can manage where group gets provisioned to

28	Demonstrate various GUIs for managing group properties and memberships	(Properties) Create and set/reset a group property which controls whether a group is replicated to Google Groups.	We need to be able to add custom group properties.
29	Demonstrate Web Services interfaces for managing group properties and memberships		
30	Demonstrate how triggers/hooks can be associated with group changes (memberships, permissions, properties.)	Google group is created or removed when the group property for that is set or reset. Membership changes are replicated to the Google group.	
	<b>Using an External Groups Registry</b>		
<b>Ref#</b>	<b>Scenarios</b>	<b>Use Case</b>	<b>Comments</b>
31	Define a filter/Rule to push data to MACE Grouper	Update MACE Grouper in real time when demographic group memberships change.	How to manage the rules governing these processes?
32	Demonstrate using MACE Grouper as a Subject Source for Permissions	The list of people who can manage the Physics Department web pages is defined by the membership of a Grouper group.	
	<b>User Provisioning and De-provisioning</b>		
<b>Ref#</b>	<b>Scenarios</b>	<b>Use Case</b>	<b>Comments</b>
33	Provide an overview of how provisioning rules are written/maintained		
34	Demonstrate adding a new person to the Person Registry and causing that person to be granted a new family of permissions	John Doe submits an application to be a student at the university.	
35	Demonstrate adding a new Affiliation and causing a person to be granted a new family of permissions	Jane Doe, who is an Alum, is hired as a Faculty Member	The assumption is that Provisioning references Permissions created elsewhere in the IDM system.
			Demonstrate creating user objects in various systems, adding Jane to various Groups, and granting Jane various permissions

36	Demonstrate changing a person's attributes within a Business System (and, as a result, in the person registry), and triggering events to add and remove Permissions and Roles	a) Jane is an Academic Dept Mgr in Physics; she moves to the same position in Chemistry.	detect and remove permissions that had been manually granted to a person
		b) senior graduates, is no longer a student	remove group memberships (including opt-in groups), ability to access licensed content (specific value on entitlement attribute in ldap), and card access to dorm door
37	Demonstrate how marking an Affiliation type as "not active" disables certain permissions	Staff member leaves Brown, staff permissions are removed	variable grace periods for different affiliation types
38	Demonstrate user interface to manually provision/de-provision permissions to a Subject	Apply Overrides	
39	Demonstrate how to create a Rule to automatically assign a Role to a Subject		
<b>Audit / Compliance / Reporting</b>			
<b>Ref#</b>	<b>Scenarios</b>	<b>Use Case</b>	<b>Comments</b>
40	Demonstrate overall Audit capability	Who had permission X on date Y and why (e.g. from a role, rule, an override, etc)?	<ul style="list-style-type: none"> <li>Need configurable levels of detail</li> </ul>
			<ul style="list-style-type: none"> <li>What automatic maintenance features are available</li> </ul>
41	Demonstrate how to list all manual overrides		
42	Demonstrate creating a compliance rule		
43	Are any regulatory requirement rules embedded in the product?		
44	Historical data ad hoc reporting	Which people were classified as on-campus faculty one year ago?	
45	Provide a list of available canned reports		
46	Demonstrate how a custom report would be created		

47	Demonstrate how conflicting permissions would be reported for resolution		
	<b>Self Service</b>		
<b>Ref#</b>	<b>Scenarios</b>	<b>Use Case</b>	<b>Comments</b>
48	Demonstrate Self Service Capabilities	Account Activate	Current self service portal provides the following functionality:
		Account Maintenance	1. Account activate/Maintenance –
			a. New user provides 3 pieces of information (Name, DOB, ID)
			b. User accepts our acceptable use policies
			c. kicks off provisioning of accounts user is entitled to (typically Kerberos, active directory, Novell, Google Apps)
			d. Establishes passwords (sync'd for Kerberos, Active Directory, Novell)
			e. Updates flags in the service provisioning system
			f. Updates LDAP entry with email address
			g. password change for campus based systems
			h. password change for Google Apps
			i. directory attribute update (for attributes not fed by source systems)
			j. directory visibility update (modify whether on-campus/off-campus users can see certain attributes)
			k. request alternate email address (alias)
49	Demonstrate Admin Capabilities		Helpdesk - super user functions – ability to take action on behalf of an end user
	<b>Overview - Other</b>		
<b>Ref#</b>	<b>Scenarios</b>	<b>Use Case</b>	<b>Comments</b>
50	How does a user authenticate to the IDM system		
51	How are permissions managed within the IDM system		

52	How are custom connectors created		
----	-----------------------------------	--	--

[illegible]




[illegible]

[illegible]

[illegible]

[illegible]

--	--	--	--