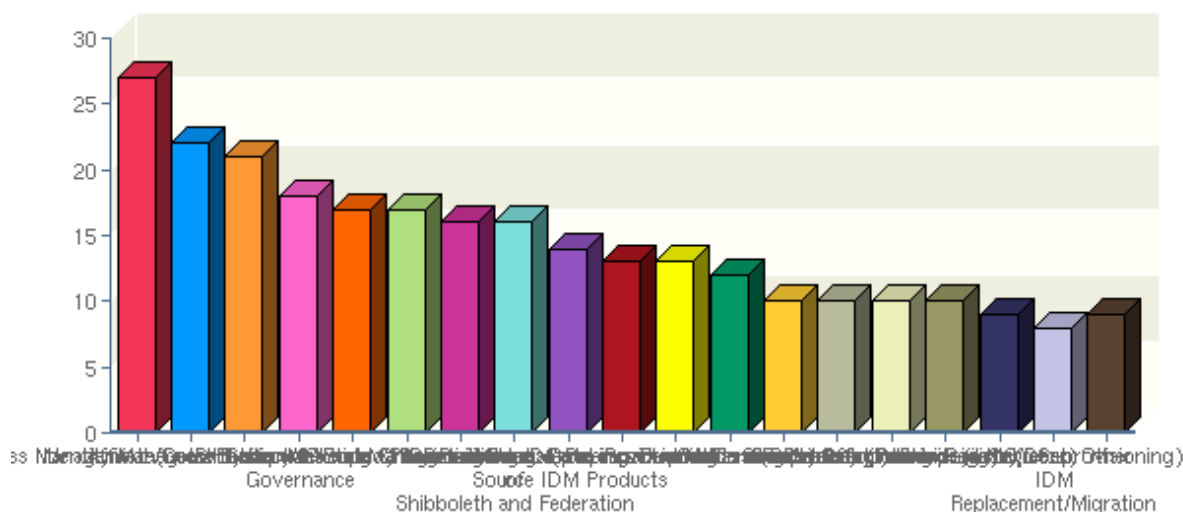


# Response Summary Report

December 13, 2010

1. The EDUCAUSE IAM - Tools and Effective Practices workgroup would like to gather, consolidate, and update resources on IAM practices in a way that will best serve IAM professionals in Higher Education. Resources might include things like documentation, "toolkits", and sample roadmaps. To help us focus our efforts, please select the top five topic areas below where up-to-date, well-organized, accessible resources would be most useful to you.

Please note: the survey will force you to select 5 topics.



Item	Count	Percent %
Privilege/Access Management (both local and federated)	27	50.94%
Affiliate/Guest Systems	22	41.51%
Identity Management Lifecycle/State Change	21	39.62%
IAM Governance	18	33.96%
Grouper/Group Management	17	32.08%
ID/Person Matching & Reconciliation/De-duping	17	32.08%
ID-Proofing	16	30.19%
Use of Shibboleth and Federation	16	30.19%
Open Source IDM Products	14	26.42%
Password Resets (and impact on InC-Silver/LoA?)	13	24.53%
Provisioning & De-Provisioning in a Federated context	13	24.53%
Assisting on-campus service providers (SPs) – e.g., libraries, LMS, etc.	12	22.64%
Dual/Multi-factor authentication	10	18.87%
Onboarding process (Provisioning)	10	18.87%
Password delivery methods (initial/reset)	10	18.87%
Person Registry	10	18.87%
Offboarding process (De-provisioning)	9	16.98%
Sun IDM Replacement/Migration	8	15.09%
Commercial IDM Products	6	11.32%
Open Registry	3	5.66%

2. Please write a brief description of the top 3 identity and access management business needs you are trying to address on your campus.

2a. IAM Business Need 1:

Item	Count	Percentage
Ability to assert higher LOA's for federal agencies	1	2.17%
Access Management	1	2.17%
Adding new resources (entitlements) to an existing IAM solution	1	2.17%
Affiliate creation and tracking	1	2.17%
Affiliate/Guest System including affiliate authentication	1	2.17%
Automated Deprovisioning	1	2.17%
Automated on/off boarding from an authoritative source UTOMATED PROVISIONIN/DEPROVIFING	1	2.17%
Better governance of IAM initiative	1	2.17%
centraliezed role based access controll	1	2.17%
Credentialing of affiliates	1	2.17%
De-provisioning	1	2.17%
Delivering a suitable system to cope with a relatively large number of guest/ affilliate accounts	1	2.17%
Designig and managing role-based privileges	1	2.17%
Encouraging vendor support for local SSO eg using Shibboleth	1	2.17%
Exception Accounts	1	2.17%
federated authentication	1	2.17%
Governance decision making	1	2.17%
Groups/roles	1	2.17%
guest systems	1	2.17%
How to do identity matching while at the same time, reducing our dependency on SSNs and other sensitive data.	1	2.17%
ID Card	1	2.17%
Identity Access Mangement Governance	1	2.17%
Identity Lifecycle	1	2.17%
identity management for distance education	1	2.17%
Identity vetting without requiring physical presence	1	2.17%
Implementation of a Registry	1	2.17%
InC Silver/levels of assurance	1	2.17%
Increased data quality in authoritative sources	1	2.17%
integration of SSO (shib) into suplier offerings (e.g. SAP)	1	2.17%
Lack of resources in a budget-constrained state university	1	2.17%
Merging existent identity info from multiple sources of record	1	2.17%
Migrate home grown IDM systems to open/supported architecture	1	2.17%
Need for strongly bound identifers in federated applications	1	2.17%
off site/remote ID proofing for password delivery	1	2.17%
Provisioning to applications	1	2.17%
reduce number of credentials	1	2.17%
reduced signon	1	2.17%
reducing users who have multiple logins, or are repeatedly prompted for sign on (improve end user experience)	1	2.17%
Removal of resources at the appropriate time	1	2.17%
Role- and rule-based provisioning in a post-Sun IDM world	1	2.17%
Single Sign On	1	2.17%
Single Sign-On to all applications	1	2.17%
Sun IDM replacement	1	2.17%
Timeliness of identity and affiliation feeds to service providers	1	2.17%
Timeliness of updates to systems of record as drivers if ID provisioning/ deprovisioning	1	2.17%
True single sign-on	1	2.17%

Item	Count	Percentage
A sane way to get databases of record into person registry, filtered by business rules	1	2.22%
add federated partnerships where valid	1	2.22%
Attribute release policy	1	2.22%
Auditing Access	1	2.22%
Automated Provisioning	1	2.22%
Better buy in from business units	1	2.22%
Business Unit acceptance of ID Proofing criticality	1	2.22%
Competition with resources for ERP projects	1	2.22%
Converging multiple roles of a person into one ID	1	2.22%
Create IDM infrastructure that eases/speeds new application deployments	1	2.22%
Creating a single, memorable identifier that resists change (non-name based)	1	2.22%
De-provisioning former employees	1	2.22%
Delegating group/ACL management (creation/update/delete) to sub-units and potentially any member of staff	1	2.22%
deprovisioning	1	2.22%
Efficient account and service provisioning	1	2.22%
Engagement of IAM Governance body(s) in decisions	1	2.22%
ensuring that user access is provisioned on day one to best of our ability	1	2.22%
eSSO	1	2.22%
Federation beyond WebSSO	1	2.22%
Funding for identity and security	1	2.22%
Group management	1	2.22%
Handling non-core users: vendors, non-undergrad students, other guests	1	2.22%
ID Merges	1	2.22%
Identity for Cloud Applications	1	2.22%
Identity Life cycle	1	2.22%
improved authN strength	1	2.22%
Improving onboarding of users (provisioning of services)	1	2.22%
Initial Provisioning of Services	1	2.22%
Lack of support from Oracle for Sun's IdM product	1	2.22%
level 2 LoA or higher in federated applications	1	2.22%
Lower helpdesk costs	1	2.22%
Management of non-person-related accounts, e.g. conference attendees	1	2.22%
More granular authorization control	1	2.22%
Password Delivery/Reset	1	2.22%
Password Management	1	2.22%
Privilege/Access Management	1	2.22%
privilege/access management in mixed directory environment - Enterprise Directory (Sun/Oracle) and Active Directory	1	2.22%
provisioning applications with IAM	1	2.22%
secure self service "forgot password" process	1	2.22%
Sharing/using authorization info	1	2.22%
Speed up granting of access to systems	1	2.22%
Stop successful phishing of our identities, by using more two-factor authentication for people with access to sensitive data.	1	2.22%
Streamlining identity info changes and corrections	1	2.22%
Successfully implementing open source IDM	1	2.22%
using single centralized management for on/off boarding of all enterprise related systems	1	2.22%

## 2c. IAM Business Need 3:

Item	Count	Percentage
Guest management	2	4.88%
Access rights approval delegation and attestation to appropriate business owners	1	2.44%
Accommodating multiple, simultaneous affiliations and transitions into and out of those affiliations	1	2.44%
affiliates/guests infrastructure to manage them	1	2.44%
Buy-in from leadership that Identity needs work	1	2.44%
Clustering and monitoring of Shibboleth IdPs	1	2.44%
Commerical IDM Product - Oracle IDM.	1	2.44%
De-provisioning	1	2.44%
Developing a consistent IdM strategy	1	2.44%
distributed management	1	2.44%
Economic solutions for comprehensive IAM products	1	2.44%
establish governance structure; make IAM a driving priority even if that means usurping other local priorities.	1	2.44%
Federation /Incommon	1	2.44%
federation with SAAS vendors	1	2.44%
Hybrid SSO	1	2.44%
IAM as cloud enabler	1	2.44%
IAM Governance	1	2.44%
Identity for Research Collaboration	1	2.44%
Implementing reduced sign-on and multiple layers of authorization	1	2.44%
Improve audit/reporting capabilities for compliance with internal and external requirements	1	2.44%
improved provisioning	1	2.44%
Improving password delivery (initial activation keys and on reset)	1	2.44%
Integrating existent provisioning systems with our person registry	1	2.44%
Manage access to library resources	1	2.44%
Managing culture change to use an IAM	1	2.44%
Need to deal with attribute providers that are not IdPs	1	2.44%
Privilege and access management	1	2.44%
product choice and migration strategy for Sun IDM replacement	1	2.44%
Providing a sufficiently secure password reset facility to our users	1	2.44%
Provisioning and Deprovisioning	1	2.44%
Provisioning/De-provisioning replacement	1	2.44%
Reduce account proliferation and the costs associated on campus	1	2.44%
Regulatory Compliance	1	2.44%
Replacing an existing, in-house web access tool with a "vendor" tool that uses standard protocols (e.g., Shibboleth, Oracle Access Manager)	1	2.44%
reporting/analytics	1	2.44%
Streamlining ldap directories and attributes	1	2.44%
Understaning and implementing effective group and authorisation solutions	1	2.44%
Unified initial trust process for all constituents	1	2.44%
unify identity and access policies for campus to enable internal trust agreements/federation	1	2.44%
Vendors not supporting Shibb or CAS	1	2.44%