kuali. days 2011
EMPOWERING THE COMMUNITY

Help Shape the Future of Open Source Identity and Access Management for Higher Education

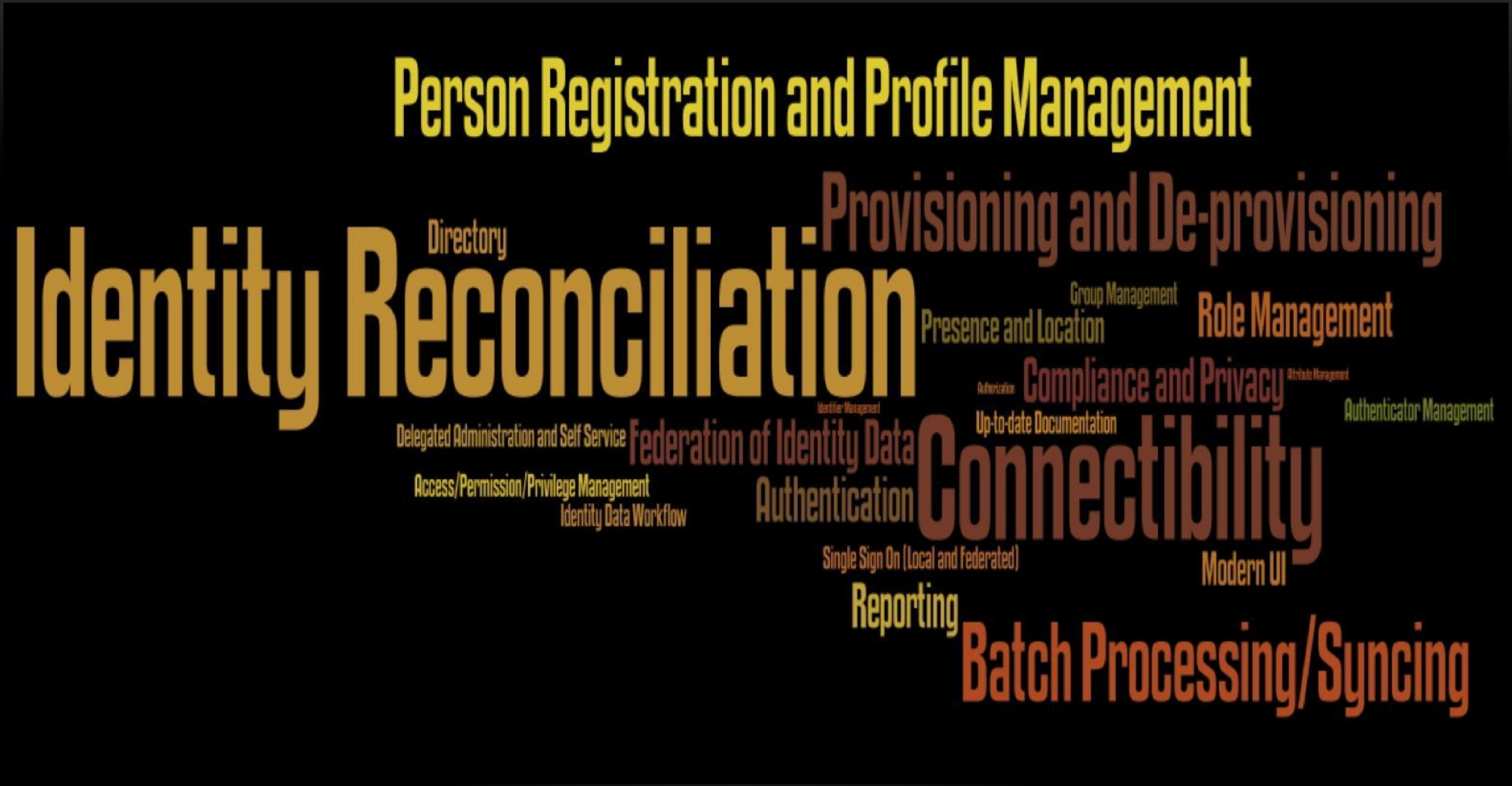
Presenter(s):	Candace Soderston
	Matt Sargent
	Bill Yock
Date:	November 16, 2011
Time:	2:30 to 3:30 pm

Introductions

What topics do you hope we get time for during this hour?

And we’ll start with a few questions for you!

Facets of Identity Management



Person Registration and Profile Management

Provisioning and De-provisioning

Directory

Identity Reconciliation

Group Management

Presence and Location

Role Management

Authorization

Compliance and Privacy

Attribute Management

Authenticator Management

Identifier Management

Up-to-date Documentation

Delegated Administration and Self Service

Federation of Identity Data

Connectibility

Access/Permission/Privilege Management

Identity Data Workflow

Authentication

Single Sign On (Local and Federated)

Modern UI

Reporting

Batch Processing/Syncing

kuali. days 2011

EMPOWERING THE COMMUNITY

Questions:

- What is the single-most important requirement you would look for in an identity and access management solution?

- What software tools do you use in managing identities and access?

- What do you like most about these tools? What do you like least?

Staff at 12 Universities Responded to an IDM Survey before Kuali Days 2011

Within Kuali community:

- Lehigh University
- MIT
- Ohio Northern University
- University of Connecticut
- University of Maryland
- University of Southern California
- University of Washington

Outside Kuali community:

- Carleton College *
- Duke University *
- Rensselaer Polytechnic Institute *
- University of Iowa *
- University of Saskatchewan *

*(* = Outside Kuali community)*

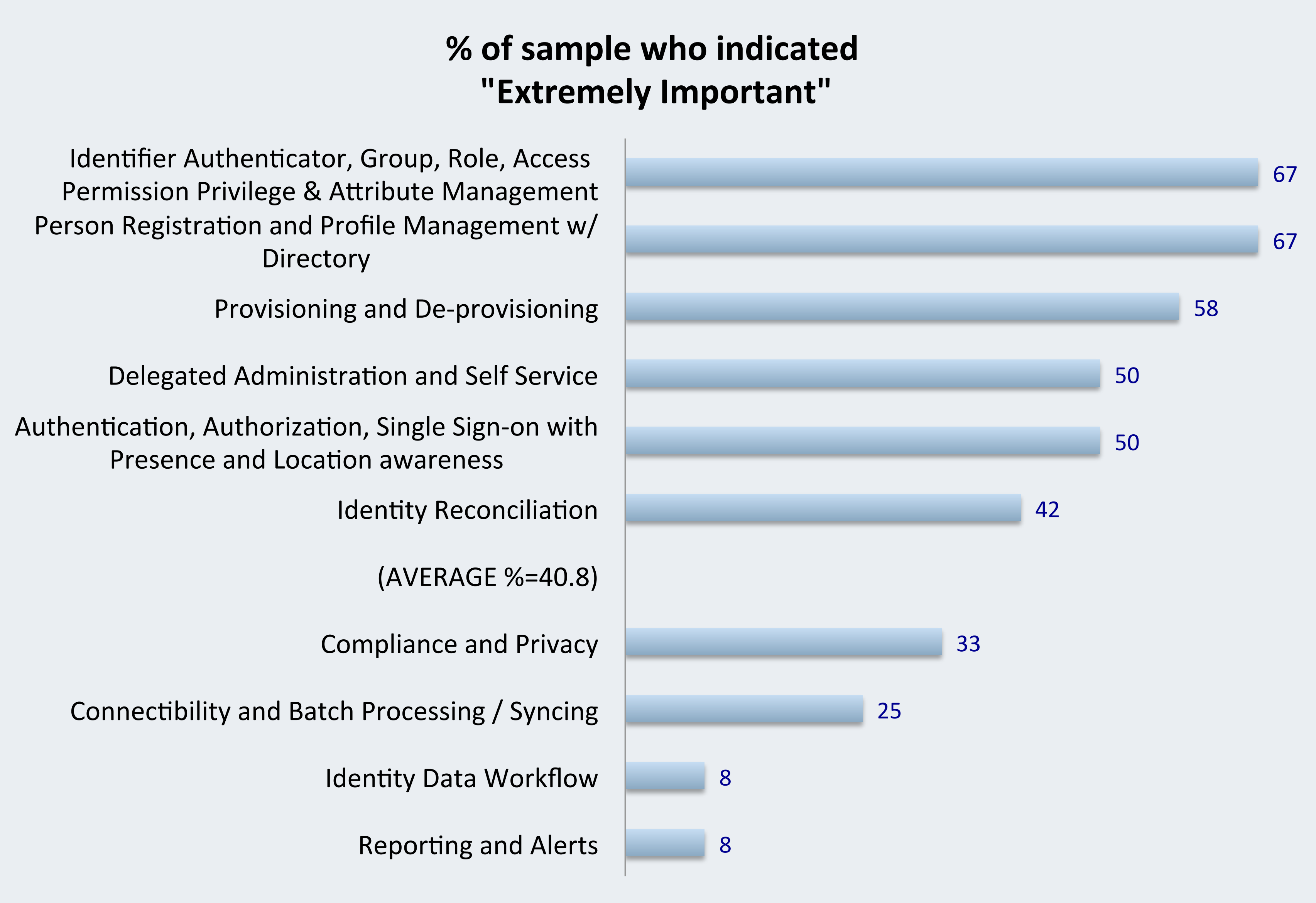
Identity and Access Management Survey

- Results For Discussion -

They rated 10 Potential Investment Areas:

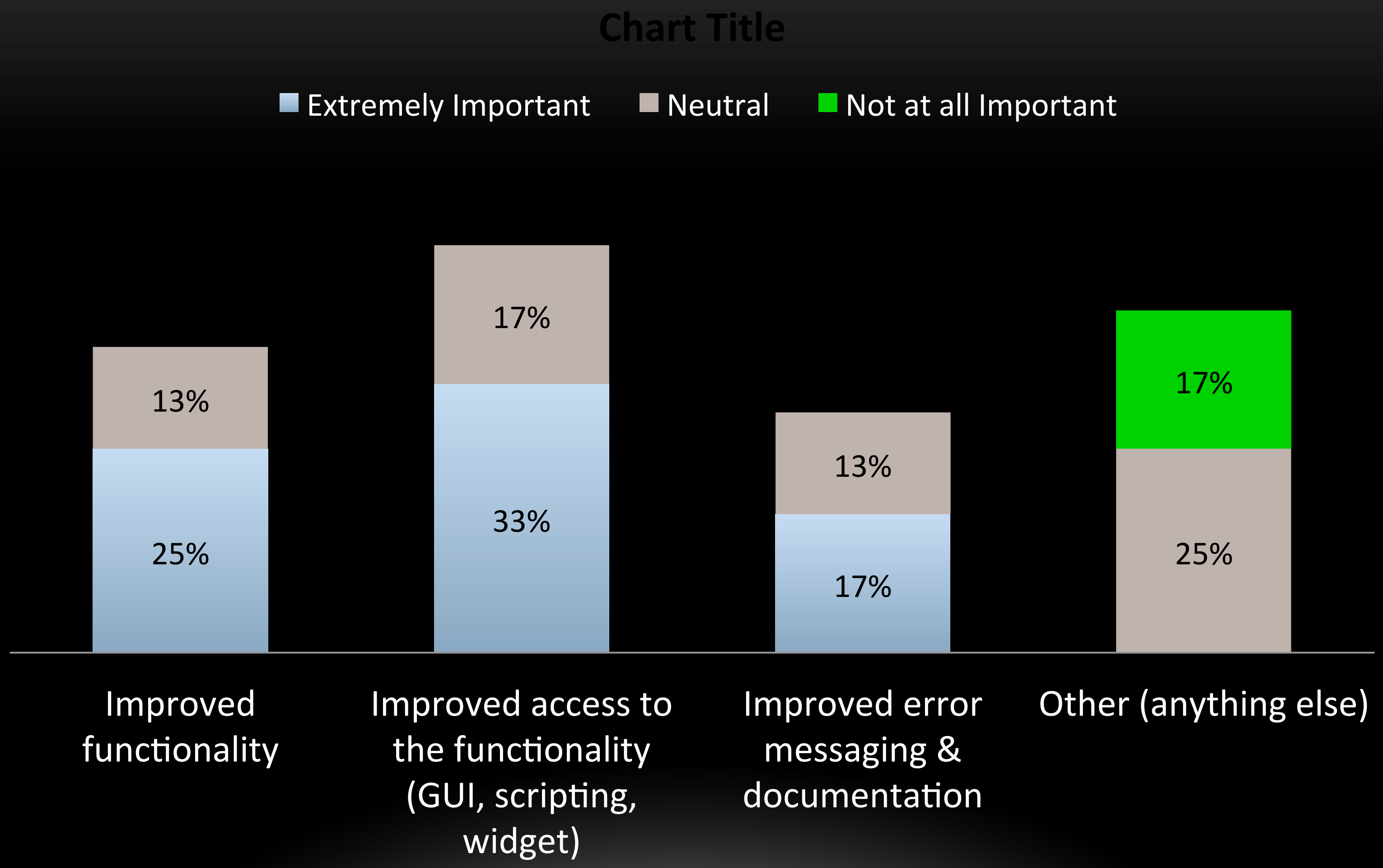
- Person Registration and Profile Management w/Directory
- Identity Reconciliation
- Compliance and Privacy
- Identity Data Workflow
- Identifier Authenticator, Group, Role, Access/Permission/ Privilege, and Attribute Management
- Delegated Administration and Self Service
- Reporting and Alerts
- Provisioning and De-provisioning
- Connect-ability and Batch Processing/Syncing
- Authentication, Authorization, and Single Sign-on with Presence and Location awareness

Do These Results Represent You?



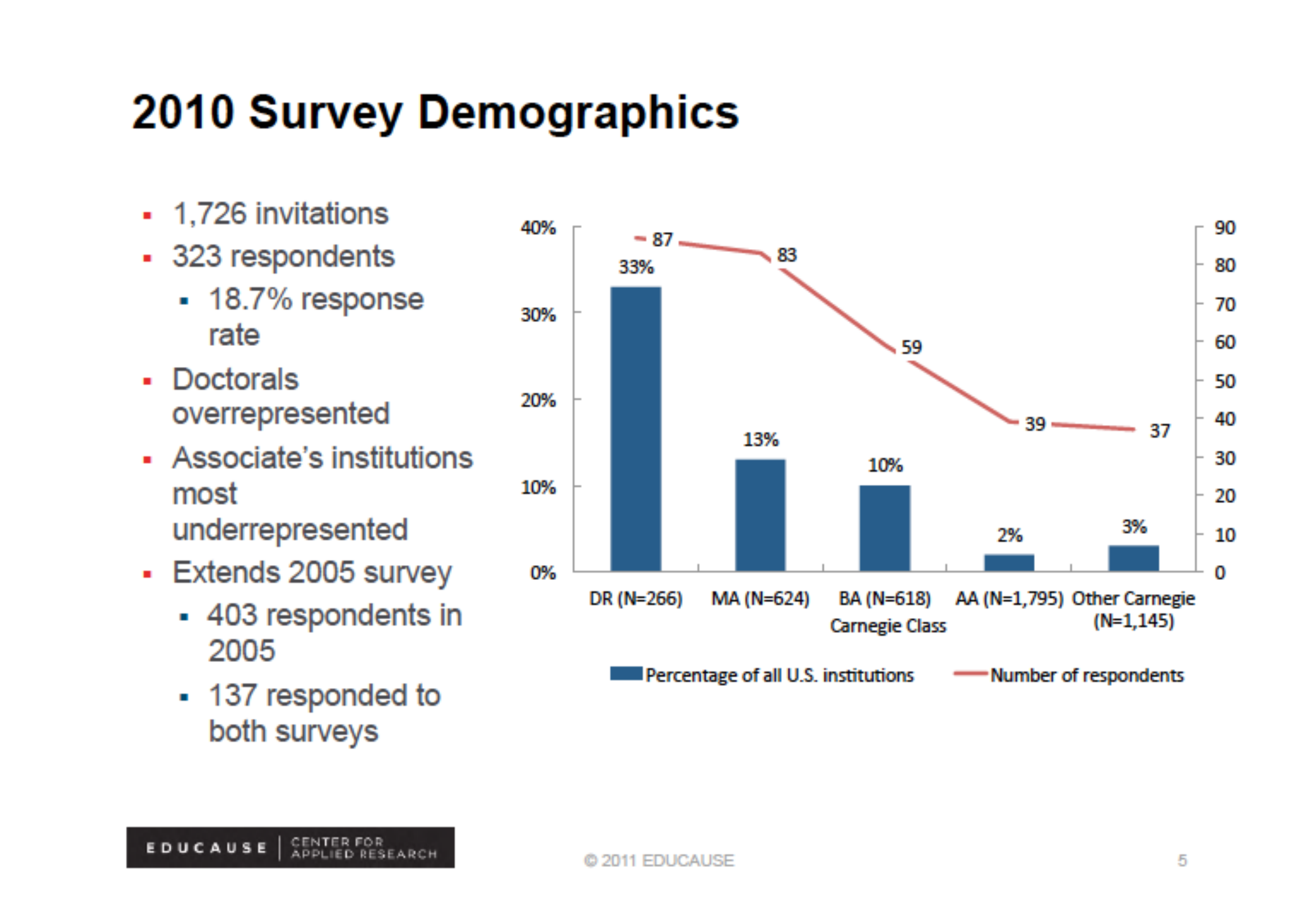
% of sample who indicated "Extremely Important"

For the task areas you identified as most in need of improvement, please rate the types of improvements you would like:



Other Data You May Be Interested In

(Large study by Mark Sheehan, et.al.)



2010 Survey Demographics

- 1,726 invitations
- 323 respondents
  - 18.7% response rate
- Doctorals overrepresented
- Associate's institutions most underrepresented
- Extends 2005 survey
  - 403 respondents in 2005
  - 137 responded to both surveys

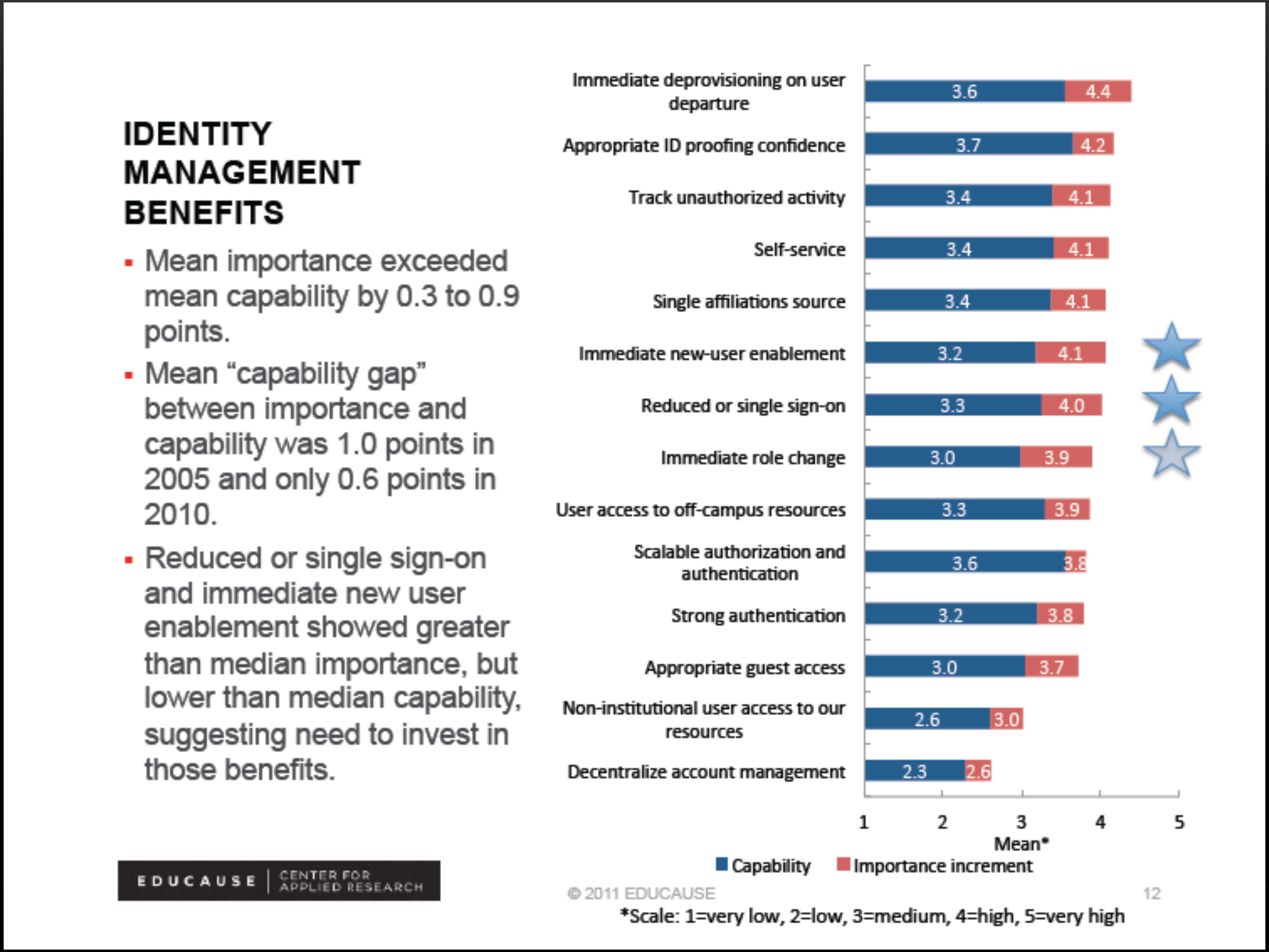
EDUCAUSE | CENTER FOR APPLIED RESEARCH

© 2011 EDUCAUSE

5

See ECAR's 2011 Study of Identity Management in Higher Education (recorded July 13, 2011 at http://www.incommon.org/iamonline/)

Focus Increasing on Identity Management?



IDENTITY MANAGEMENT BENEFITS

- Mean importance exceeded mean capability by 0.3 to 0.9 points.
- Mean "capability gap" between importance and capability was 1.0 points in 2005 and only 0.6 points in 2010.
- Reduced or single sign-on and immediate new user enablement showed greater than median importance, but lower than median capability, suggesting need to invest in those benefits.

Immediate deprovisioning on user departure 3.6 4.4
Appropriate ID proofing confidence 3.7 4.2
Track unauthorized activity 3.4 4.1
Self-service 3.4 4.1
Single affiliations source 3.4 4.1
Immediate new-user enablement 3.2 4.1
Reduced or single sign-on 3.3 4.0
Immediate role change 3.0 3.9
User access to off-campus resources 3.3 3.9
Scalable authorization and authentication 3.6 3.8
Strong authentication 3.2 3.8
Appropriate guest access 3.0 3.7
Non-institutional user access to our resources 2.6 3.0
Decentralize account management 2.3 2.6
1
2
3
4
5
Mean*
■ Capability ■ Importance increment

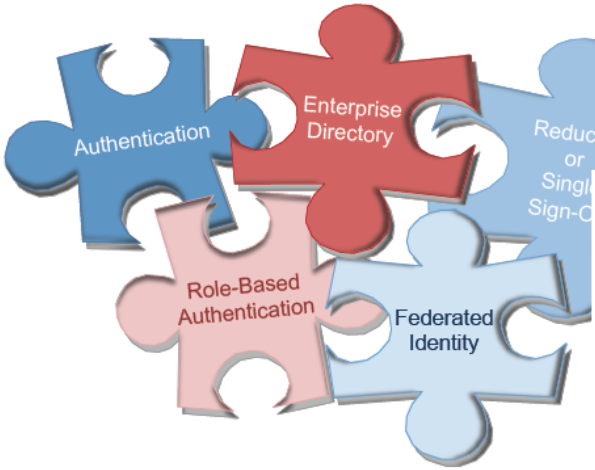
EDUCAUSE | CENTER FOR APPLIED RESEARCH

© 2011 EDUCAUSE

*Scale: 1=very low, 2=low, 3=medium, 4=high, 5=very high

See ECAR's 2011 Study of Identity Management in Higher Education (recorded July 13, 2011 at http://www.incommon.org/iamonline/)

FIVE CORE IDENTITY MANAGEMENT ELEMENTS



EDUCAUSE | CENTER FOR APPLIED RESEARCH

Enterprise Directory Approaches
(multiple responses allowed)

- A network operating system approach was in the top three for all Carnegie classes (<50% only for doctorals).
- Doctoral institutions (40%) were more likely than any other Carnegie class (9%-33%) to approach ED as a stand-alone system using commercial vendor software.
- Stand-alone, open-source ED systems were in the top three approaches selected by doctoral (33%), BA-liberal arts (29%), and other bachelor's (9%) institutions.
- All classes but doctorals and BA-liberal arts institutions often (>20%) selected "part of vendor-supplied application software (e.g., ERP)" as a top-three approach.

EDUCAUSE | CENTER FOR APPLIED RESEARCH

Comments?

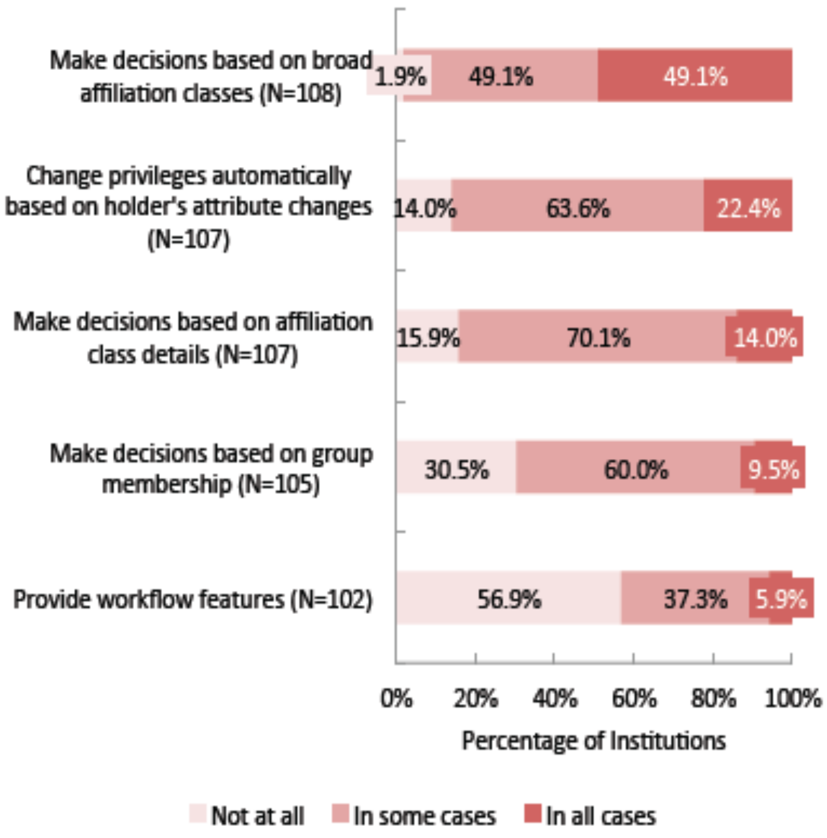
See ECAR's 2011 Study of Identity Management in Higher Education (recorded July 13, 2011 at http://www.incommon.org/iamonline/)

FIVE CORE IDENTITY MANAGEMENT ELEMENTS

EDUCAUSE | CENTER FOR APPLIED RESEARCH

- Where automated role-based authorization is in place, it is applied most often for broad affiliation classes.
- Ability of the institution's role-based authentication environment to make privileging decisions based on fine-grained roles or affiliations in all cases was seven times as common at public institutions as private ones; no other ability varied by Carnegie class, institution size or institutional control.

Abilities of Institution's Role-Based Authorization Environment (Partially or Fully Operational Implementations Only)



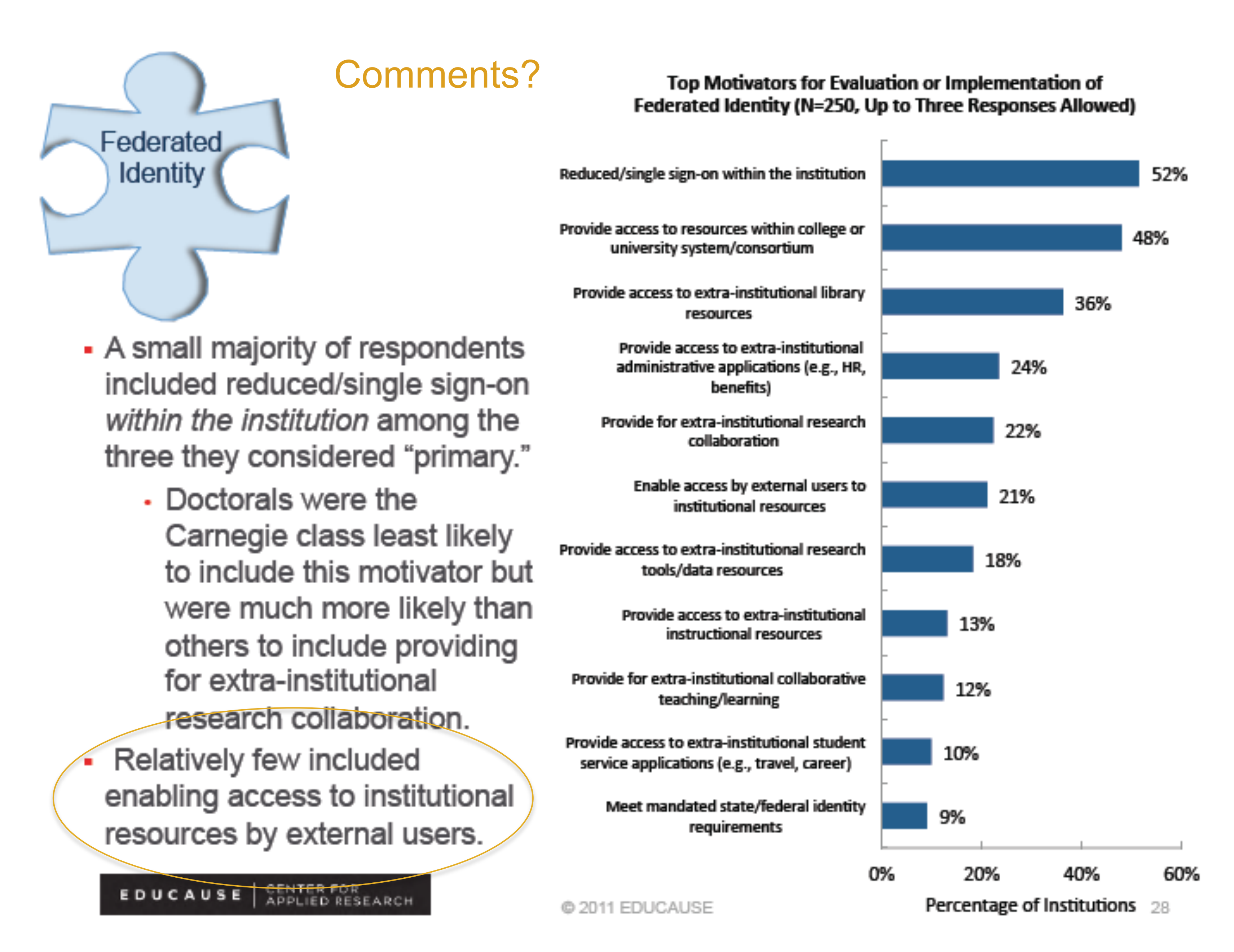
Comments?

EDUCAUSE | CENTER FOR APPLIED RESEARCH

© 2011 EDUCAUSE

27

See ECAR's 2011 Study of Identity Management in Higher Education (recorded July 13, 2011 at http://www.incommon.org/iamonline/)



Comments?

- A small majority of respondents included reduced/single sign-on *within the institution* among the three they considered "primary."
  - Doctorals were the Carnegie class least likely to include this motivator but were much more likely than others to include providing for extra-institutional research collaboration.
- Relatively few included enabling access to institutional resources by external users.

EDUCAUSE | CENTER FOR APPLIED RESEARCH

© 2011 EDUCAUSE

See ECAR's 2011 Study of Identity Management in Higher Education (recorded July 13, 2011 at http://www.incommon.org/iamonline/)

OK – Let’s Shift Gears!

Work on
An Open Source Identity Management Solution For Higher Education?

Open Source IdM for Higher Ed (OSIdM4HE)

(a working code name)

1. The OSIdM4HE Joint Development Proposal
2. Drivers leading to the OSIdM4HE Proposal
3. Benefits and Key Differentiators of OSIdM4HE
4. What is the Status of the OSIdM4HE
5. Proposed OSIdM4HE Startup Governance Structure
6. How to participate in OSIdM4HE

Joint Development Proposal

- Many Higher Ed Institutions (and their community efforts like Jasig, Internet2, Kuali, etc.) have been building Identity and Access Management (IAM) solutions largely disconnected from each other.

- OSIdM4HE is a proposal to Join Forces to collaborate and create a diverse and comprehensive suite of IAM solutions.

Drivers Leading to the Proposal

- Commercial vendor contract lock ins, forced migrations
- Many different commercial products, hard to compare, hard to integrate
- Commercial products do not meet all Higher Ed requirements, costly customizations
- Significant expertise in this problem space within Higher Ed communities
- Considerable Higher Ed development already underway (Kauli KIM, Jasig CAS, Jasig OpenReg, Internet 2 Grouper, Internet2 Shibboleth, etc.)

Benefits and Key Differentiators

- Backed by proven, established Open Source Leaders
- A well coordinated and focused development effort by Higher Ed
- Ability to accelerate development efforts by targeting and maximizing resources of contributing members
- Lower Cost of Ownership (No licensing fees, community support, no binding vendor contracts)
- The best minds in the Higher Ed sector solving the problems together
- Able to leverage, build on and reconfigure existing code bases (Kauli KIM, Jasig CAS, Jasig OpenReg, Internet 2 Grouper, Internet2 Shibboleth, etc.)

What is the Status of the Proposal?

- Many volunteers met over the summer of 2011 to document current state and identify gaps in an overall IAM suite
- Four subcommittees formed: Registries, Provisioning, Access Management, Strategy and Organization
- A “Coordination Agreement” document was drafted which includes:
  - ✓ Product Vision and Reference Architecture
  - ✓ Governance Framework and Development Principles
  - ✓ Common Configuration and Deployment Requirements
- Proposal being reviewed by many interested parties

kuali days 2011
EMPOWERING THE COMMUNITY

Proposed Startup Governance Structure

- Initial work to begin around Registry and Provisioning
  - ✓ Identity matching and resolution in the Registry
  - ✓ Registry-to-Provisioning engine interfaces
- Kuali Rice targeted as "Caretaker" for Registry work and Internet2 MACE targeted as "Caretaker" of Provisioning work
- Caretaker organizations provide coordination and logistical support of development work and agree to long term support
- Caretakers for Access Management and Authentication still being discussed
- A startup Coordination Committee to be appointed by consensus of the initial contributing members

How to Participate

- Review and sign the "Coordination Agreement" acknowledging vision and strategy
- Review and sign the "Memorandum of Understanding" for the Registry - Identity Matching work
- Contribute resources towards the Registry – Identity Matching work
- Assume institutions already contributing to Higher Ed communities (Kuali, Internet2, Jasig, etc.) will make additional targeted contributions towards OSIdM4HE

Other Topics of interest -
(from flip chart generated by the group)

- Group Discussion
- Q & A

Get Involved!

OSIdM4HE Initiative

Visit	https://spaces.internet2.edu/x/HpeKAQ
Contact	osidm4he-info@internet2.edu

Kuali Rice Information

Visit	http://kuali.org/rice
Test Drive *(login as admin)*	http://demo.rice.kuali.org
Download	http://kuali.org/download-form
Get Involved	http://kuali.org/membership https://wiki.kuali.org/display/KULRICE/Collaboration
Contact	rice.info@kuali.org

Appendix

The following slides contain other data from the Kuali IdM Survey - for optional viewing.

Definitions

Person Registration and Profile Management w/Directory

A single, central registry with tools for adding and managing person and non-person entities

Identity Reconciliation

Tools for administering and limiting the number of potential duplicate entries in a registry. Including tooling for identifying (matching) and consolidating (merging) duplicates

Compliance and Privacy

Tools to ensure information being collected adheres to various local and federal compliance and privacy handling laws, and to track access to these data

Identity Data Workflow

Structured processes for approval and notification of all aspects of identity management

Identifier Authenticator, Group, Role, Access/Permission/Privilege, and Attribute Management

Tools for defining, administering, and managing person, security, and access management attributes

Definitions continued

Delegated Administration and Self Service

Rich tools for centralized and self-service management for validation and updating of personal information

Reporting and Alerts

Reports and alerts for critical monitoring of all aspects of identity management

Provisioning and De-provisioning

Automated, real-time tools to expedite the setup or removal of access and permissions

Connect-ability and Batch Processing/Syncing

An infrastructure for communication and collaboration with existing IdM solutions as well as the ability to easily import, process, or sync data from external applications

Authentication, Authorization, and Single Sign-on with Presence and Location awareness

Tools and attachment points for the management and monitoring of identities and access

What is the most important requirement you would look for in an open source identity and access management solution?

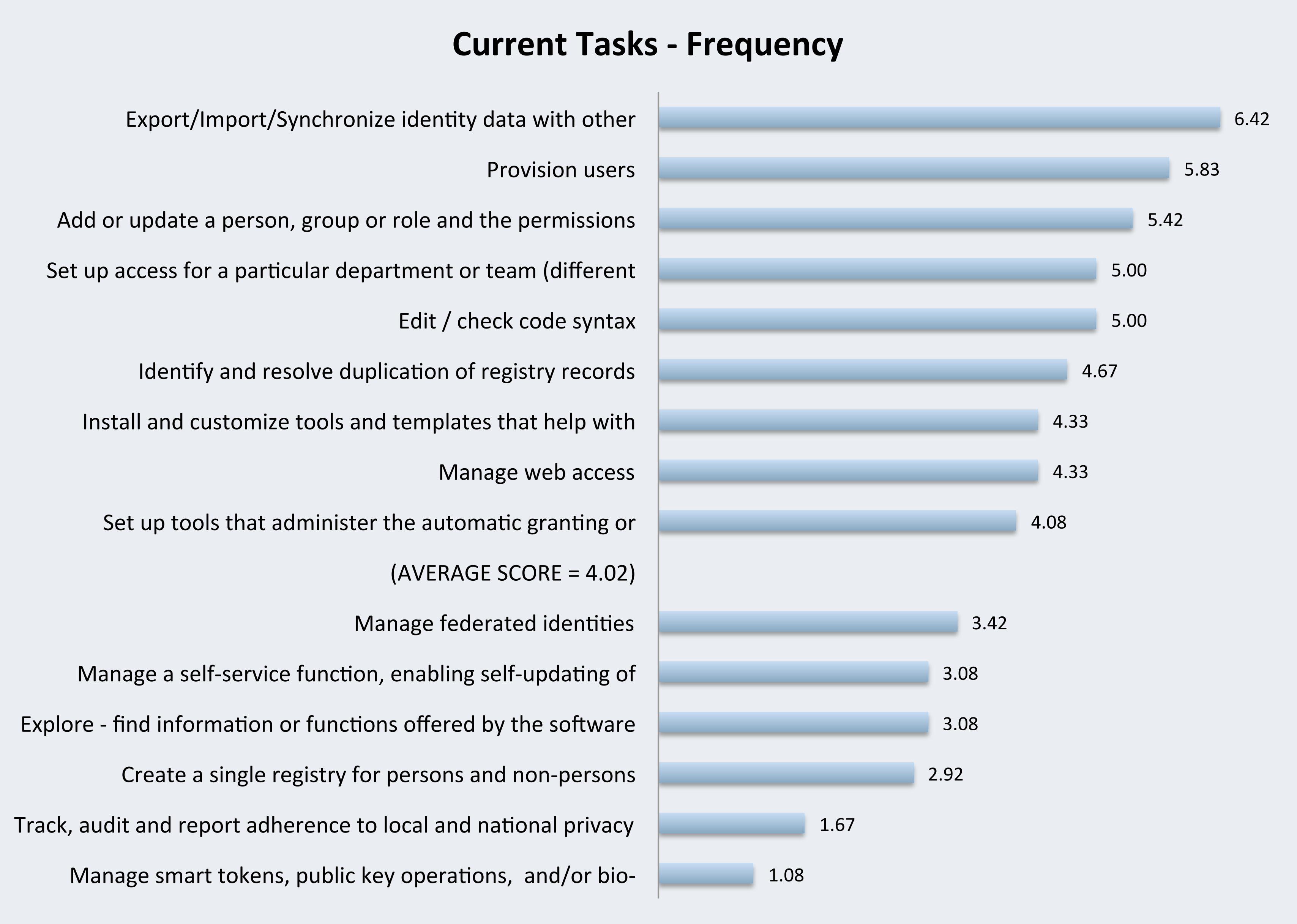
Within Kuali community:

- open standards
- good documentation and getting started guides
- The ability to customize it to meet the needs of our business practices and work flows.
- Clean service interfaces
- Identity merge/match functionality is the most important capability.
- Federation

Outside Kuali community:

- Ease of access from other systems using standard protocols
- Ease of getting setup and going. Match to our existing functionality.
- Workflow that is easy to maintain, in which complex logic can be embedded, and where the steps can invoke either interactions with people or with agents.
- Ability to de/provision flexibly and reliably in heterogeneous systems based on rich business rules defined in the solution.
- Improved functionality over existing system - migration must be a step forward - moving backwards or even sidewise in function is a lose.

Do These Results Represent You? *(cont)*



WHAT CURRENT TASKS ARE MISSING FROM THE LIST?

Within Kuali community:

- Design and implement new functions
- Integrate these IDM tools into a new business application
- Scheduled tasks that handle triggering date-driven provisioning/deprovisioning functions, and other functions that are handled in a batch-mode.
- weekly - Document requests for Identity data and coordinate review with appropriate data stewards
- Three things:
  - - looking up users to see who they are (daily)
  - - Compiling reports of users (from lists of university NETIDs) broken down by department, college
  - - determining if a Student is paying the STF fee (daily)

Outside Kuali community:

- Periodic review and attestation of role assignment by the people with the correct authority; for example, the bursar needs to periodically view and sanction who has access to financial data in the data warehouse.
- Design and implement new functions

What other tasks are you NOT able to do today through the IDM tools that you wish you could?

Within Kuali community:

- Automated user account provisioning
- We currently have limited password maintenance and security question functionality with the off the shelf product. We have created our own system for handling this to be in compliance with our security policies.
- Two things:
  - Delegate authorizations (our tools don't do that)
  - Impersonate people for testing and debugging
- Three things:
  - - generate reports from lists of university NETID's
  - - centralized storage for individuals and groups, based on university NETID and the university group service
  - - Allow the Support Org members to manage the storage of a person in the NETID domain that is under their umbrella

Outside Kuali community:

- Automating the creation and management of non-person objects. (And … More of a feature than a task) Better detection of, and recovery from, the temporary inability to contact a remote resource.

SOFTWARE TOOLS USED TODAY

Within Kuali community:

- MS Windows Active directory, pubcookie, Likewise Enterprise, Beyondtrust
- Oracle Identity Manager
- Shibboleth, Aleph patron database
- 389 Directory Server (LDAP)
- Internally developed Person Registry, Groups processing. Shibboleth for authorization.
- ldap, homegrown authorization system, CAS, kerberos, homegrown id system
- Home grown as follows:
    - Moira db to create kerberos principals and manage groups for both email and authorization,
    - MailMan to manage email groups,
    - homegrown ID service to match people and assign university IDs,
    - X509 personal certificates for web authentication,
    - Touchstone (Shibboleth) to do federated access,
    - Roles Service to manage and check authorizations and roles,
    - LDAP for exposing information

SOFTWARE TOOLS USED TODAY *(CONT)*

Outside Kuali community:

- Sun Identity Manager (changing soon), and lots of home-grown programming both internal and external to SIM.
- University's LDAP-enabled Enterprise Directory; Active Directory; Spring-LDAP for accessing LDAP directories; Grouper for group management
- Internally developed (in Oracle)
- In house developed system
- Home grown as follows:
  - Mainframe PL/I batch identity feed,
  - Microsoft Forefront Identity Manager,
  - custom perl, PowerShell and VBS scripts,
  - custom .NET/C# software for provisioning and identity management frontend web app,
  - Shibboleth Identity Provider/Service Provider,
  - Heavily modified CAS 1 SSO implementation.

What do you like most about your tools?

Within the Kuali community:

- Open source
- Flexible. Efficient. Supportable by a small team. Based on open standards.
- CAS, kerberos and ldap are industry standards and work well with our open source applications.
- supports consortial operations; Shibboleth is a standard with wide support
- We use university NETID's everywhere, its great to have a common username across all university services
- Centralizing process of assigning roles and determining resources based on this assignment.
- The matching logic integrated into the university's ID assignment process The structure and simplicity of the Roles Service

Outside the Kuali community:

- They meet our specific needs. We can make changes as needed
- The flexibility of our tools is fairly good, we have a lot of different things to use for different tasks at our disposal.
- Good fit for our needs
- We are able to express the fairly complex logic that goes into managing identities, roles and access permissions.
- Ability to get canonical identity information from official University sources; ease of configuration of Spring-LDAP module

What do you like least about your tools?

Within Kuali community:

- homegrown solutions are limited and outdated and need to be replaced
- LDAP is not equal to IdM
- Not well documented and therefore reliant on a few experts
- complex environment which is difficult to debug
- Changing the web interface is not easy. We have a lot of real estate used for built-in fields we don't use
- There is no centralized storage for users and no way to share files in a native drive-letter mapped way that leverages NETID and university groups membership
- Batch (nightly) feeds for most data integration (except university ID and Roles which are real time services).
- Too many ways to authenticate... (1) X509 personal certificates, (2) Kerberos user name & Password, (3) Touchstone's internal account creation. Difficult for non-core (i.e. departmental) applications to plug into these services so they often don't bother to.

What do you like least about your tools? *(cont)*

Outside Kuali Community:

- Some of it is written in dated technologies. We do not have enough resources to catch up on some needed changes
- Some older tools need revision, some tasks areas poorly supported.
- Sometimes there are multiple sources of information for the same identity; interface I have to Grouper is difficult to use
- Implementation of business rules in multiple systems is a huge problem.
  - Would like to have the bulk of the rules implemented in just one place. The *(lack of)* interconnectedness of our tools causes difficulty in making any kind of change.
  - We don't have a great way to enforce access management broadly other than with Active Directory groups, thus we have a problem with token size due to the huge number of groups in AD. Some kind of policy/enforcement management engine (XACML?) would probably help.

WHAT DO YOU LIKE LEAST ABOUT YOUR TOOLS? *(CONT)*

Outside Kuali community, continued:

- This is a long list *(related to SIM ,AD, LDAP, Moodle)*:

1. 1) Managing non-person objects (such as course objects in LDAP, AD and Moodle) is essentially the same sort of task as managing identities. The managing of the objects and the managing of access to the objects needs to be coordinated. But out of the box, SIM does not really support anything but user objects.
2. 2) SIM has a proprietary rule language which is not as facile at expressing complex logic as most general-purpose languages.
3. 3) Some of the primitive operations do not match up with our needs and are difficult to replace. Example: when an identity no longer needs an AD user object, we do not immediately delete the AD user. Instead, we disable it, rename it and move it off to the side for a period to avoid "dangling SIDs." It's not particularly easy to capture a "delete" event and replace the processing.
4. 4) Workflow is key in so many ways. SIM has a workflow engine, but it has many shortcomings.
5. 5) Database access is also key to provisioning. SIM has two database connectors. The simple one covers a lot of situations but not all. The more complex one has no documentation, useful examples or training, making it very difficult to use.
6. 6) The lack of good vendor support and lack of access to source code makes for a bad combination.

(Optional) What questions about your IdM creation and management experience and requirements did we NOT ask, that you wish we did?

(And what would be your answer to these!)

Outside Kuali community:

- Federation and othe related: We are running a locally developed, mature IdM system. Being able to take feeds from, and provide feeds to other systems is very important. Ability to manage roles, and delegate control based on roles is key to our success.
- Life cycle management of "guests" is very important, as well as being able to accommodate deficiencies in enterprise systems (ie - our HR/Payroll system does not have an accurate "end date" for employees - we have an employee "overlay" on the data feed from banner to correct this).