

Identity Management in Higher Education, 2011

Mark Sheehan

May 2011

EDUCAUSE 2011 STUDY OF IDENTITY MANAGEMENT

Contents

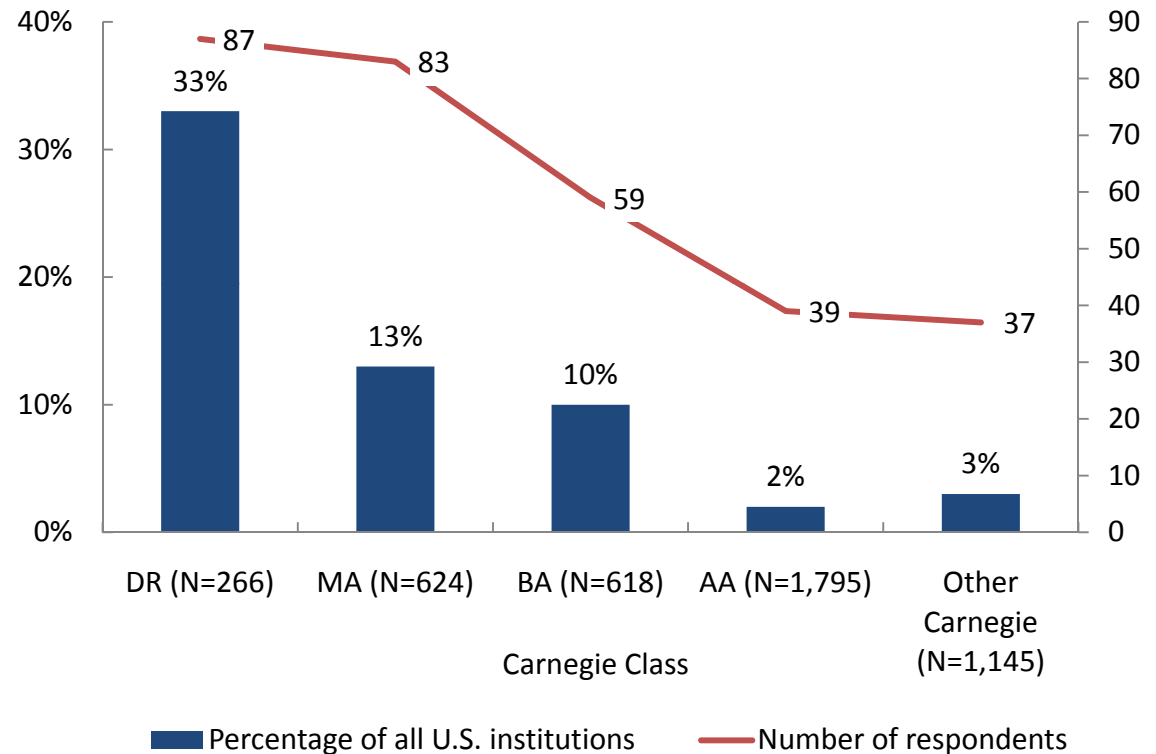
- Survey Respondents
- Motivators and Challenges for ID Management initiatives
- Benefits of ID Management
- Initiating and Funding ID Management projects
- Five Core Elements of ID Management
- Key Outcomes

Source: Sheehan, Mark C. and Cedric Bennett, with Pam Arroway, Susan Grajek, Judith A. Pirani, and Ronald Yanosky, *Identity Management In Higher Education, 2011* (Research Study, Vol. 1). Boulder, CO: EDUCAUSE Center For Applied Research, 2011. Available from <http://www.educause.edu/ecar>.

SURVEY RESPONDENTS

2010 Survey Responses

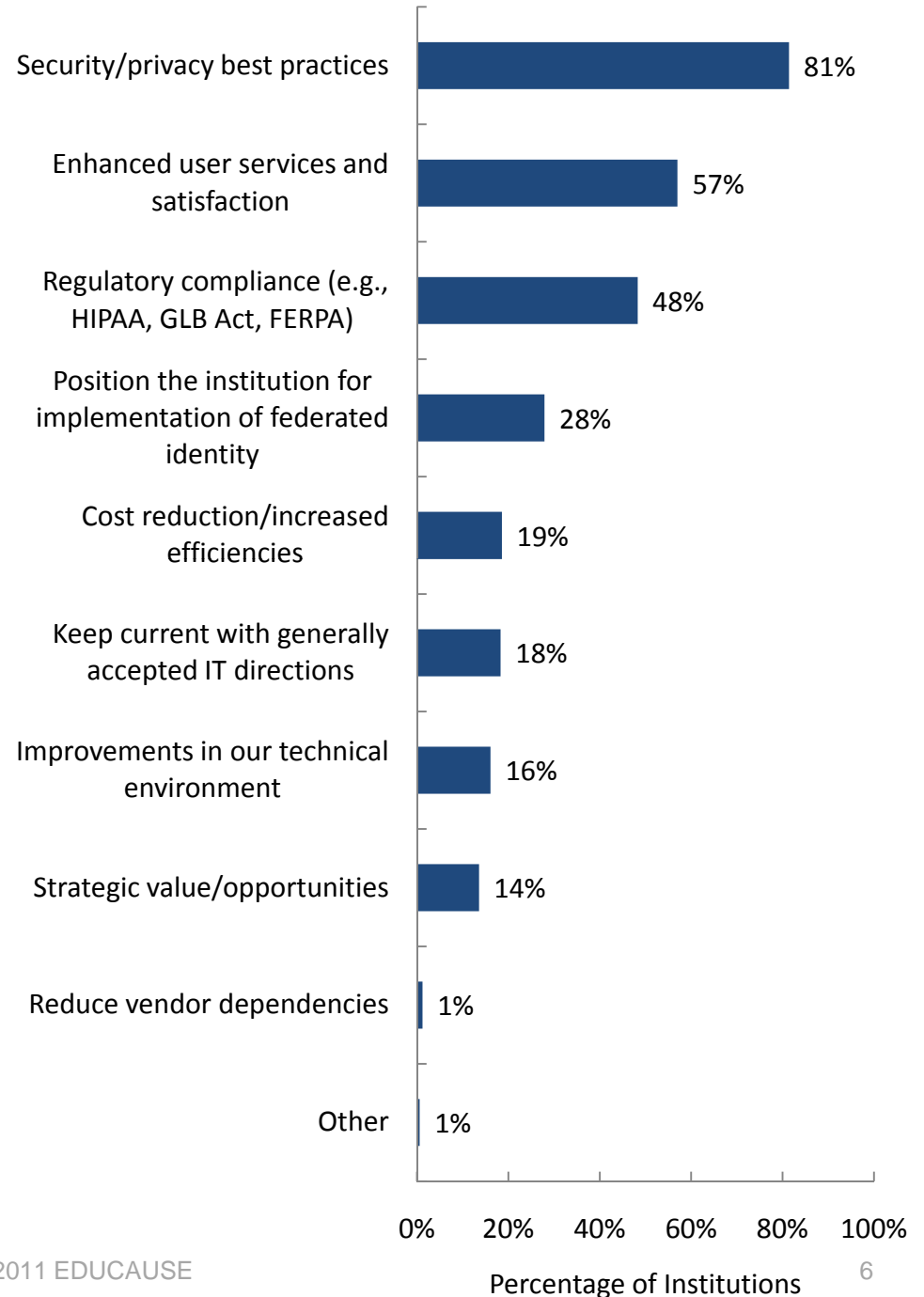
- 1,726 invitations
- 323 respondents
 - 18.7% response rate
- Doctorals overrepresented
- Associate's institutions most underrepresented
- Reprises 2005 study
 - 403 respondents in 2005
 - 137 responded to both surveys



MOTIVATORS AND CHALLENGES FOR ID MANAGEMENT INITIATIVES

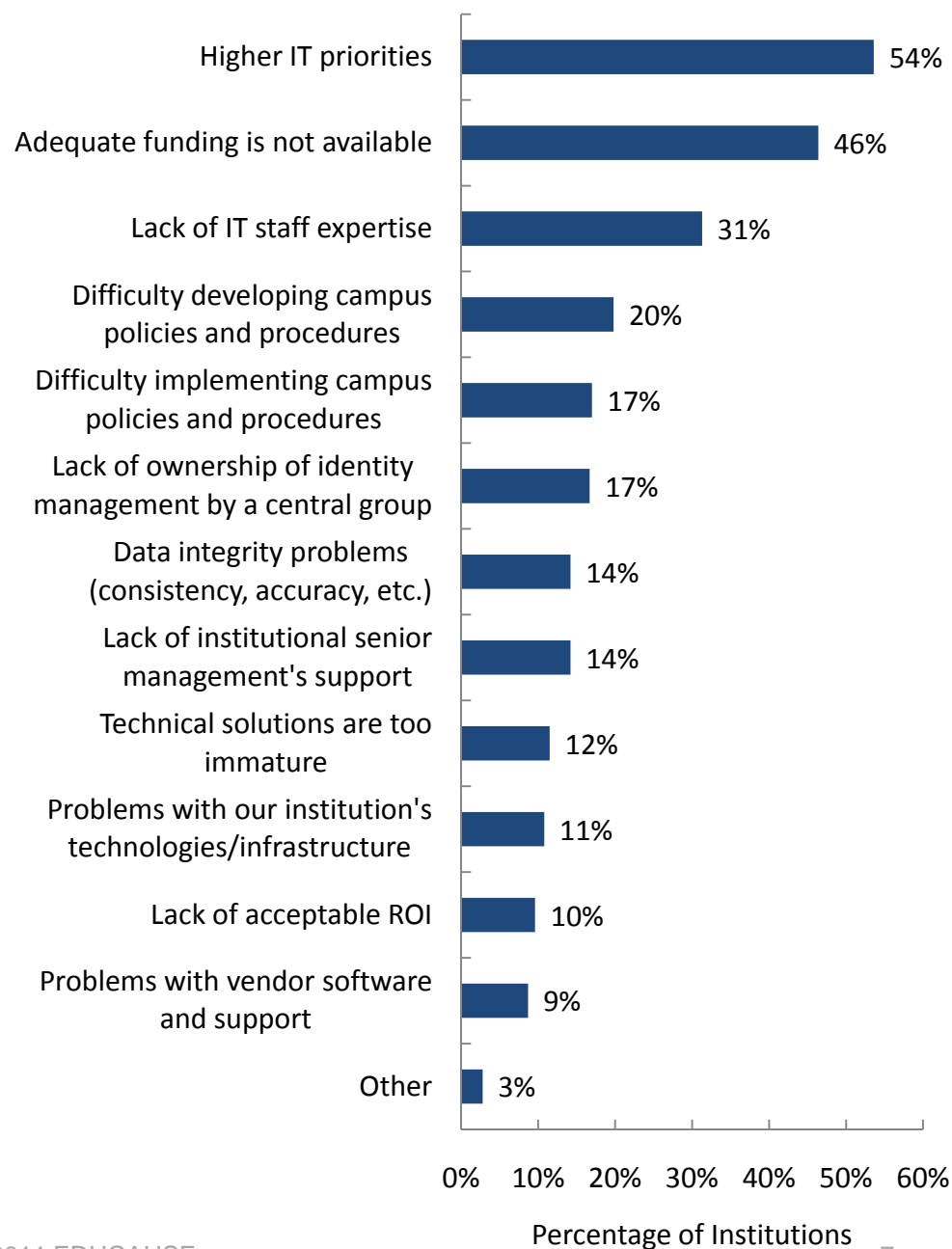
MOTIVATORS FOR PURSUIT OF IDENTITY MANAGEMENT

- Security and privacy remain the primary motivator for IdM.
- Positioning the institution for federated identity was selected 1.7 times as often in 2010 as in 2005; no other motivator varied significantly by year.
- Doctoral and liberal arts (BA) institutions were each twice as likely as others to select cost reduction/ increased efficiency as a top motivator and one-third as likely to select keeping current with accepted IT directions.



CHALLENGES TO PURSUIT OF IDENTITY MANAGEMENT

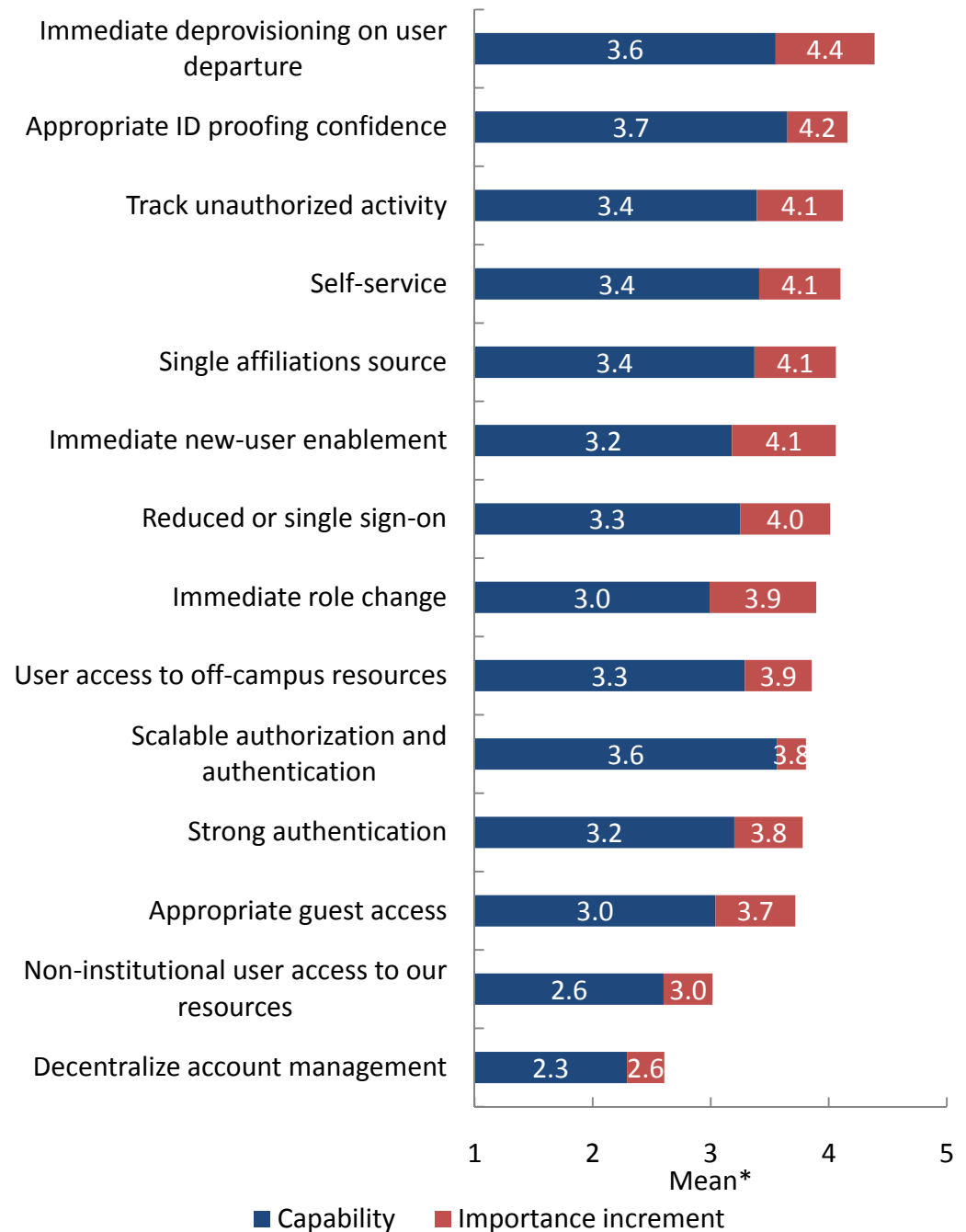
- Most of the top challenges are organizational rather than technical.
- Difficulty developing campus policies and procedures was selected half as often in 2010 as in 2005.
- Two technical challenges were selected half as often in 2010 as in 2005: immaturity of technical solutions and problems with vendor software and support.
- The rain falls equally on all parades: challenges did not vary meaningfully by Carnegie class or institution size or control.



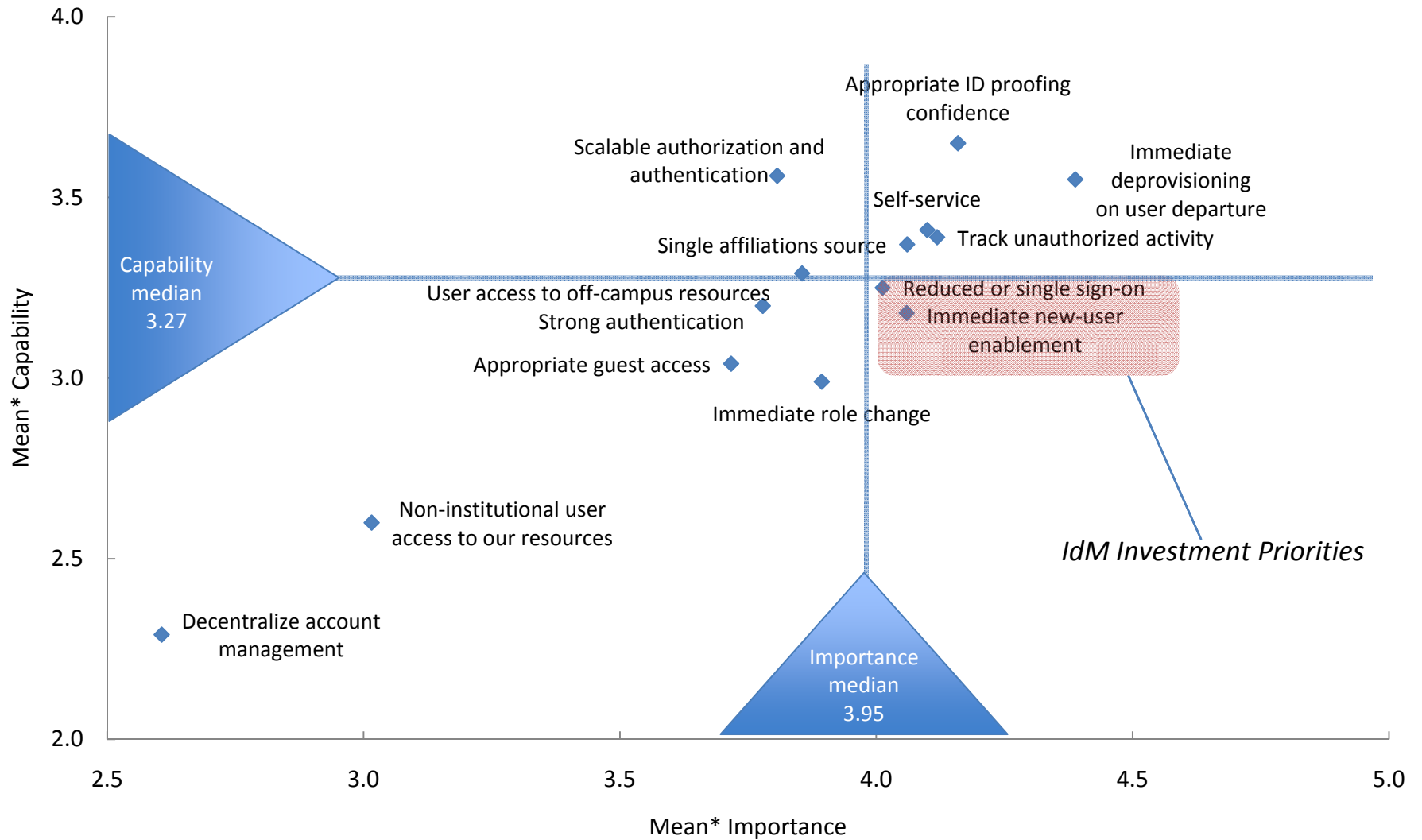
BENEFITS OF ID MANAGEMENT

IDENTITY MANAGEMENT BENEFITS

- Mean importance of benefits exceeded mean capability by 0.3 to 0.9 points.
- Performance is improving: in the longitudinal sample, mean “capability gap” between importance and capability was 1.0 points in 2005 and only 0.6 points in 2010.
- Capability scores were averaged for each institution to yield a composite “capability score,” one of this study’s primary measures of IdM success.



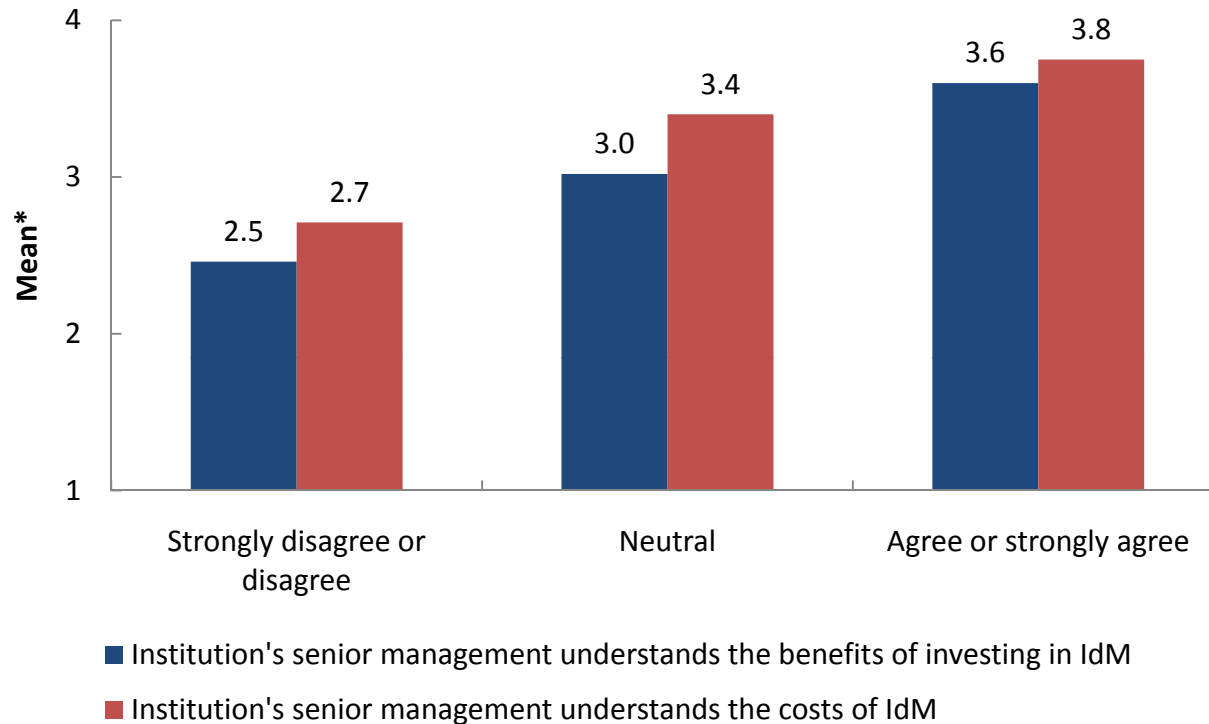
IDM BENEFIT CAPABILITY, BY BENEFIT IMPORTANCE



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

INITIATING AND FUNDING ID MANAGEMENT PROJECTS

RESOURCES FOR IDM TRACK WITH SENIOR MANAGEMENT UNDERSTANDING



*Scale: 1=strongly disagree, 2=disagree, 3=neutral, 4=agree, 5=strongly agree

- In both years, where senior management understood IdM costs and benefits, mean agreement about resource provision was at least a full point higher.
- Those agreeing that senior management understood the benefits of IdM increased by 43% from 2005 to 2010; those agreeing it understood the costs more than doubled.

COORDINATING IDM PROJECTS

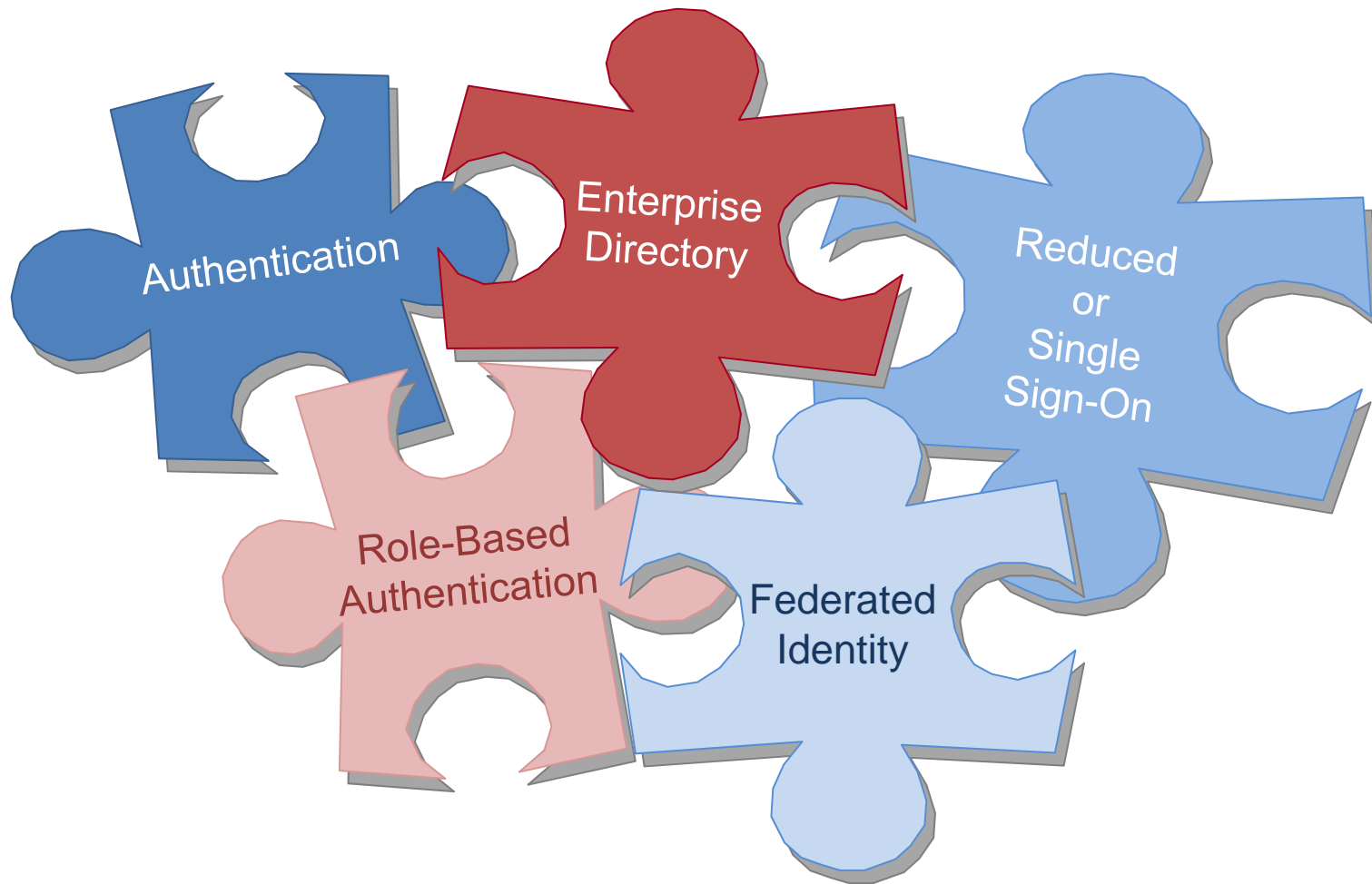
IdM projects became more focused between 2005 and 2010.

In 2010:

- They were 50% more likely to stand alone, 25% less likely to be bundled with security projects and 33% less likely to be bundled with portal projects.
- They were equally likely to be funded through one-time campus budget allocations but 60% less likely to have their funding bundled into other project budgets such as an ERP.
- They were about half as likely to be sponsored by IT administrators other than the CIO or chief information security officer.

FIVE CORE ELEMENTS OF ID MANAGEMENT

FIVE CORE IDENTITY MANAGEMENT ELEMENTS



FIVE CORE ELEMENTS OF IDENTITY MANAGEMENT

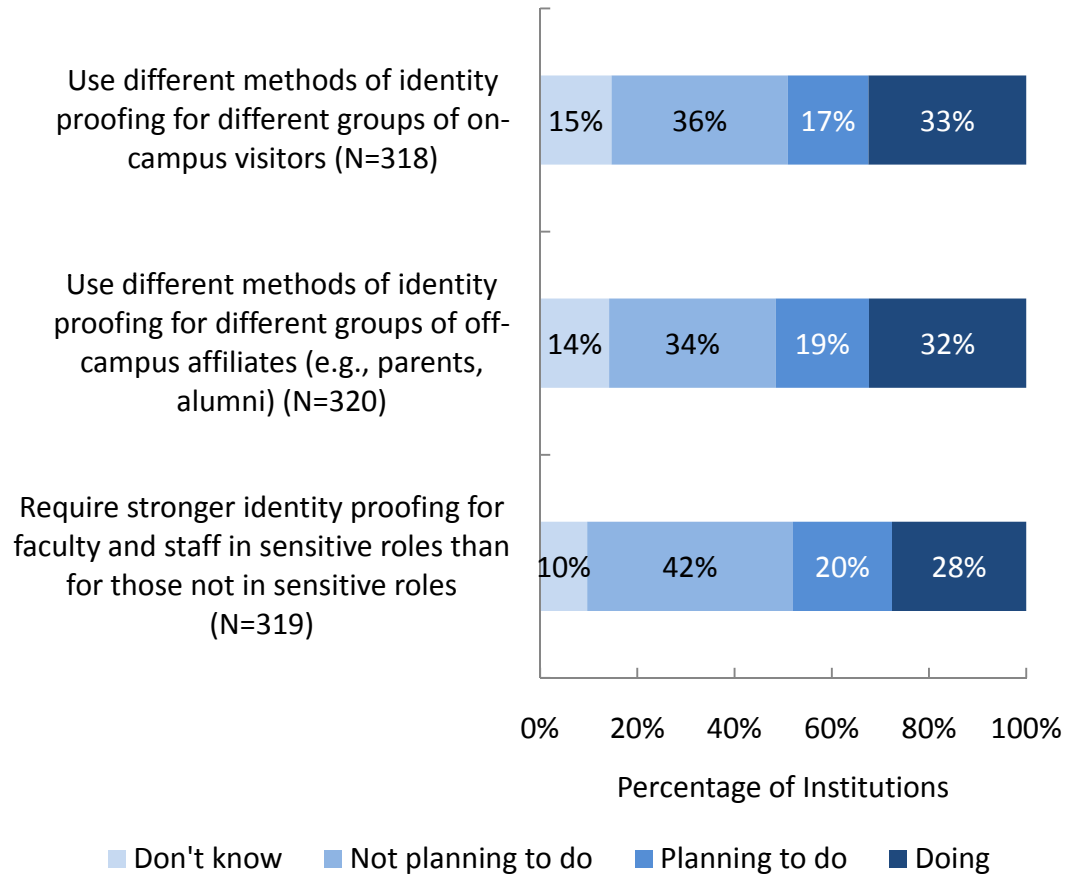
- **Authentication:** Are you who you say you are? By authenticating with trusted credentials, you let networks, systems, and applications know you can be trusted.
- **Enterprise Directory:** Does your institution have a single, authoritative repository of information about IT resources and their users? An enterprise directory will provide one.
- **Reduced or Single Sign-On:** How many usernames and passwords must you juggle to access the IT resources you need? Reduced or single sign-on technologies can help keep that number manageable.
- **Automated Role- or Privilege-based Authorization:** What do you need IT resources for? In complex IT environments, the process of empowering users to carry out their roles can benefit from automation.
- **Federated Identity:** Do you need to use IT resources that another institution maintains and protects? An identity federation lets you use locally assigned credentials to gain access to remote resources.



Identity Proofing:

- Relatively few institutions are engaged in these activities.
- Larger numbers are not planning to become engaged in them.
- Higher standards for users in sensitive roles are least common.

Differentiated Identity Proofing for Constituencies

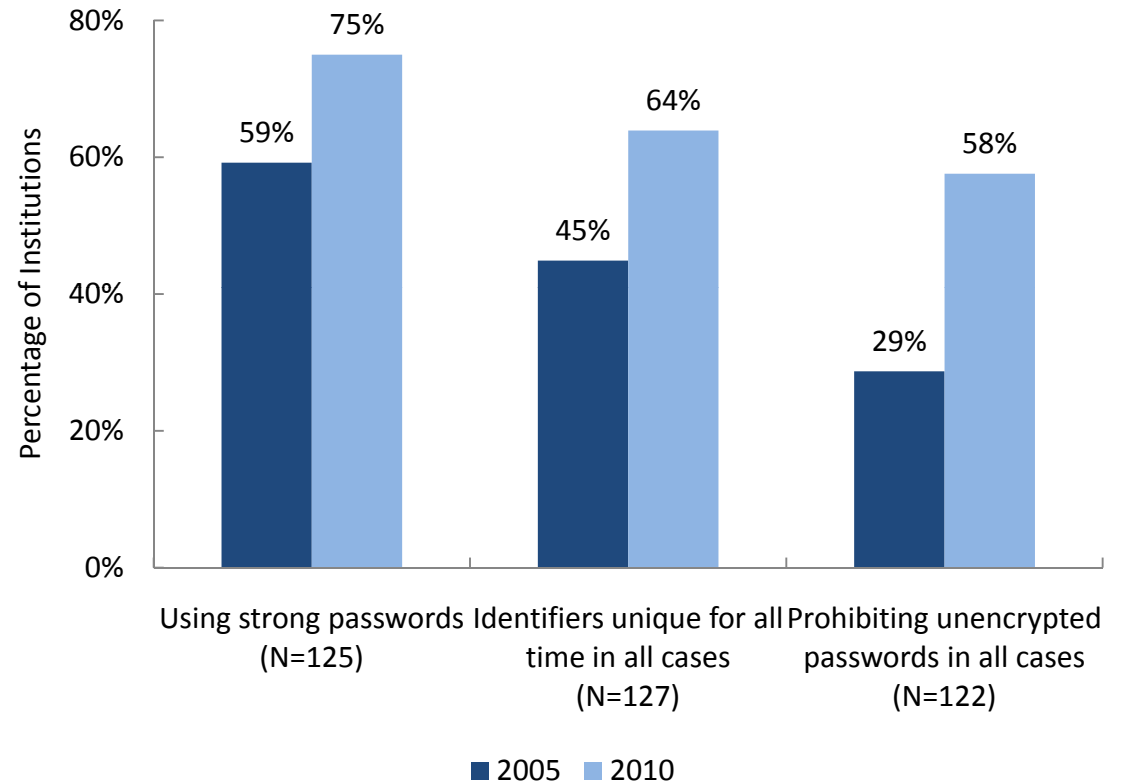




2010 Saw Progress In:

- Use of strong passwords
- Use of “unique for all time” identifiers
- Prohibiting transmission of unencrypted passwords

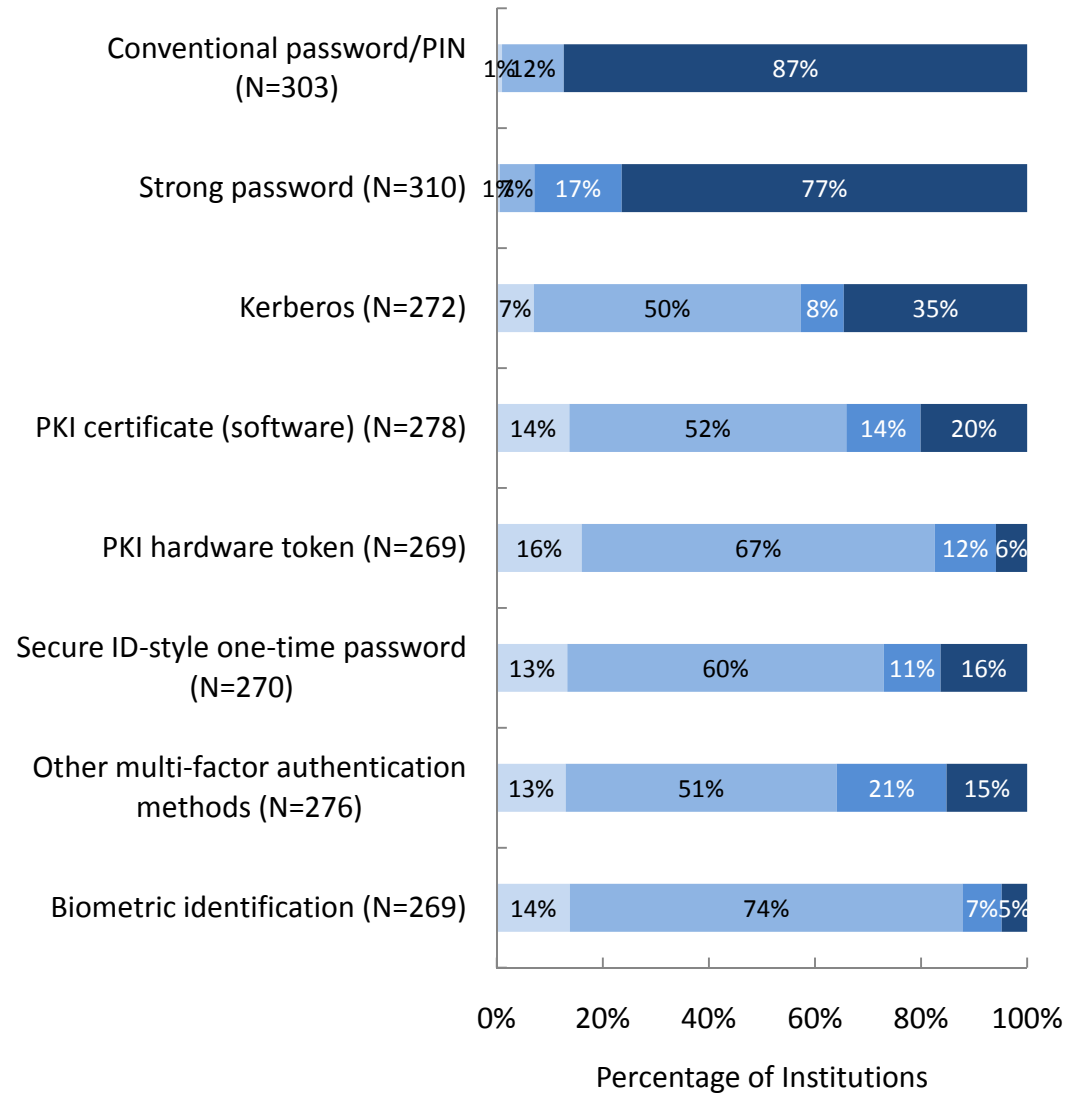
Progress In Application of Identifier Policies and Practices





- Passwords remain the primary authentication method.
- Kerberos is used by a third of respondent institutions (and by more than half of doctorals).
- Strong passwords and multi-factor methods other than biometric ID are relatively often planned.

Authentication Methods In Use



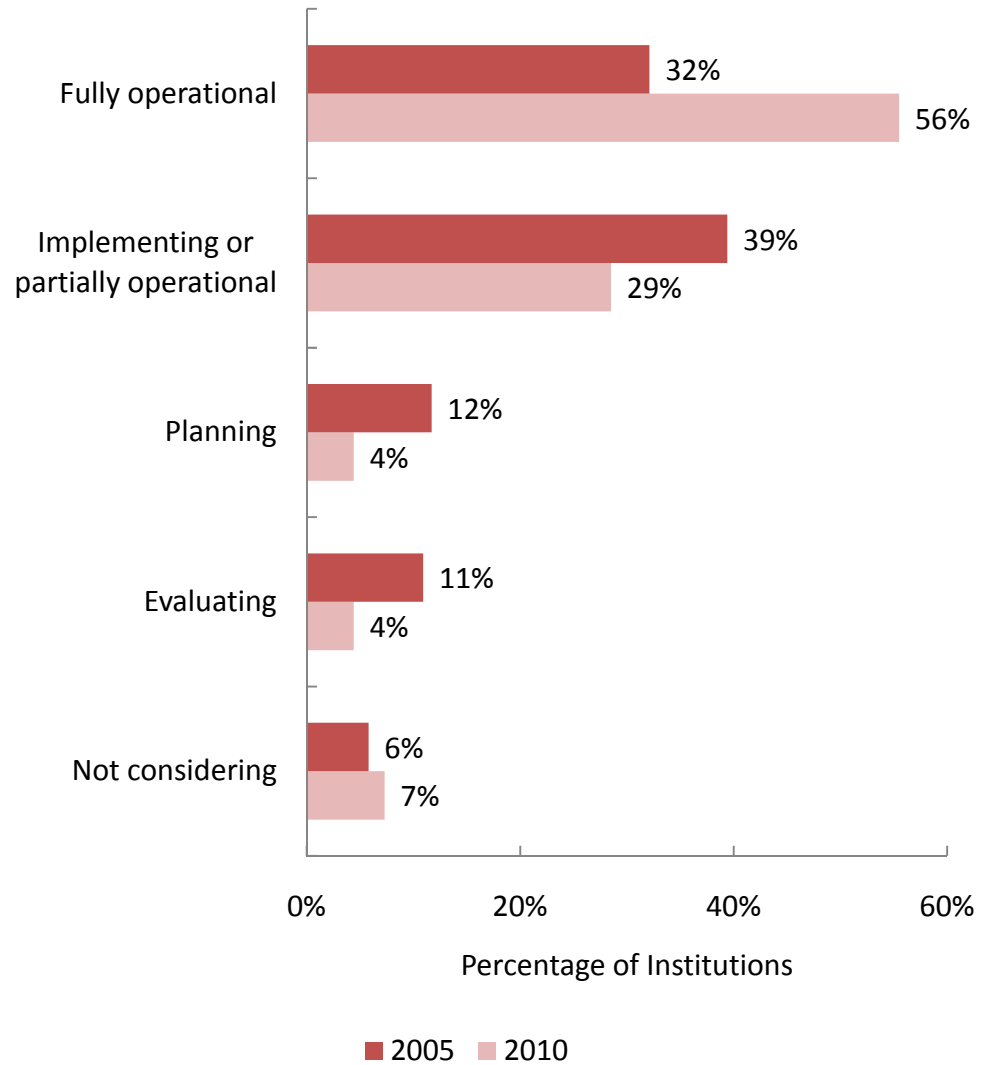
■ Don't know
 ■ Not planning to use
 ■ Planning to use
 ■ Using



Enterprise Directory:

- Fully operational implementations (FOIs) nearly doubled between 2005 and 2010.
- Larger institutions more often reported FOIs.
- EDs are used most for authentication and authorization and to store affiliation and group information, and less often for other functions.

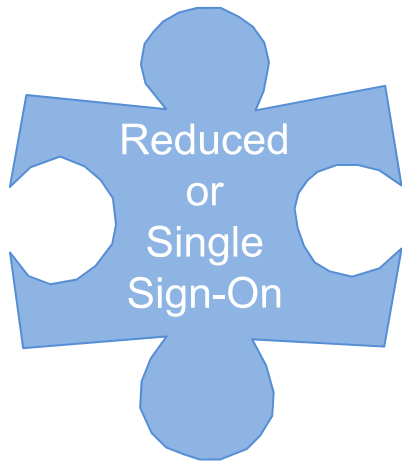
Stage of Implementation of Enterprise Directory, by Year (N=137)





Enterprise Directory Approaches (multiple responses allowed)

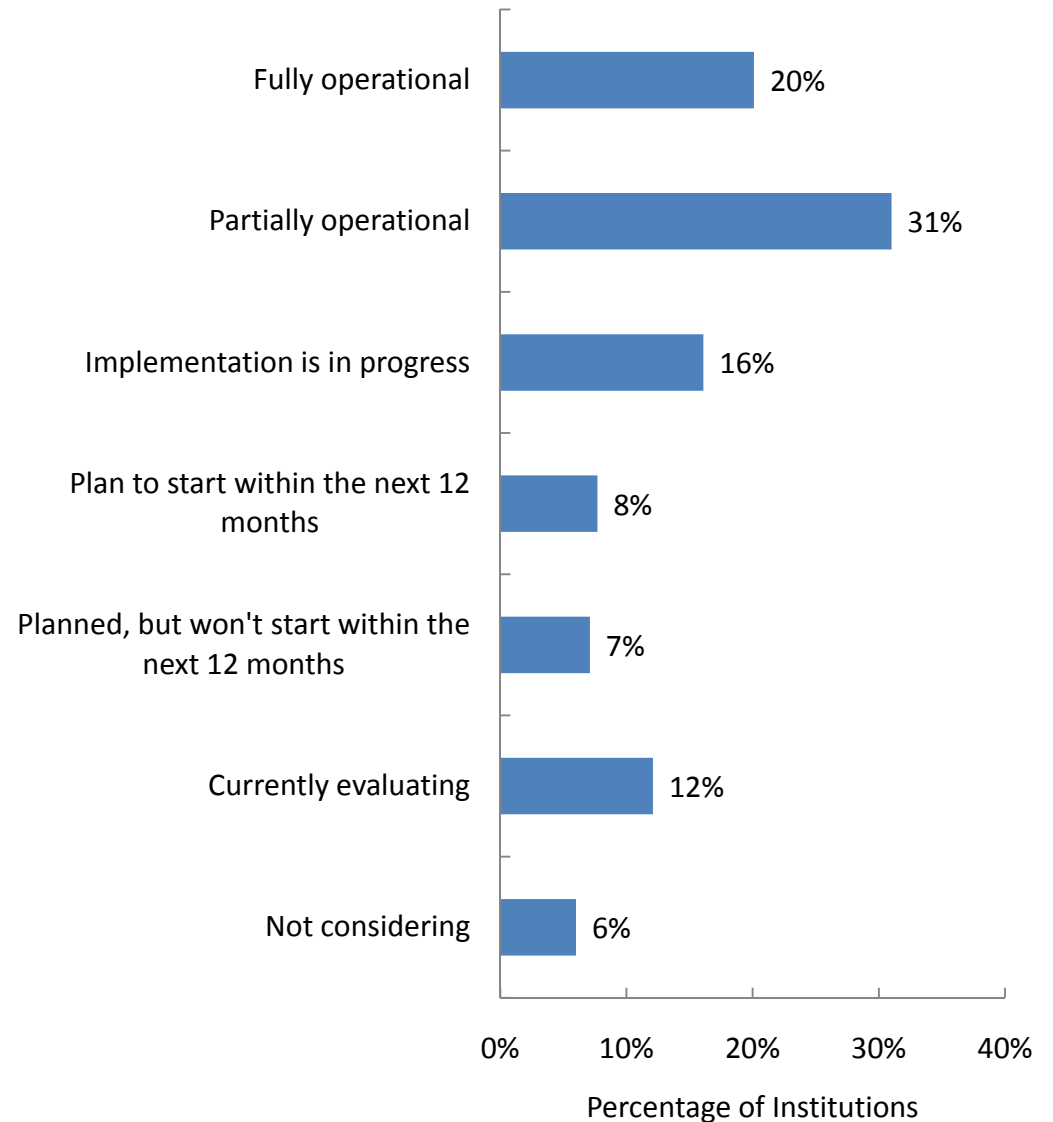
- A **network operating system** approach was in the top three for all Carnegie classes (<50% only for doctorals).
- Doctoral institutions (40%) were more likely than any other Carnegie class (9%-33%) to approach ED as a stand-alone system using **commercial vendor software**.
- Stand-alone, **open-source** 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.

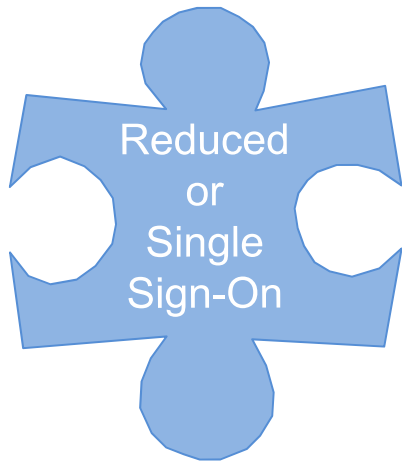


Reduced or Single Sign-On:

- Half of respondents report at least partially operational implementations of RSSO,
- There was no significant change in stage of implementation from 2005 to 2010.
- Stage of implementation was more advanced among larger institutions and doctorals than among smaller, less complex ones.

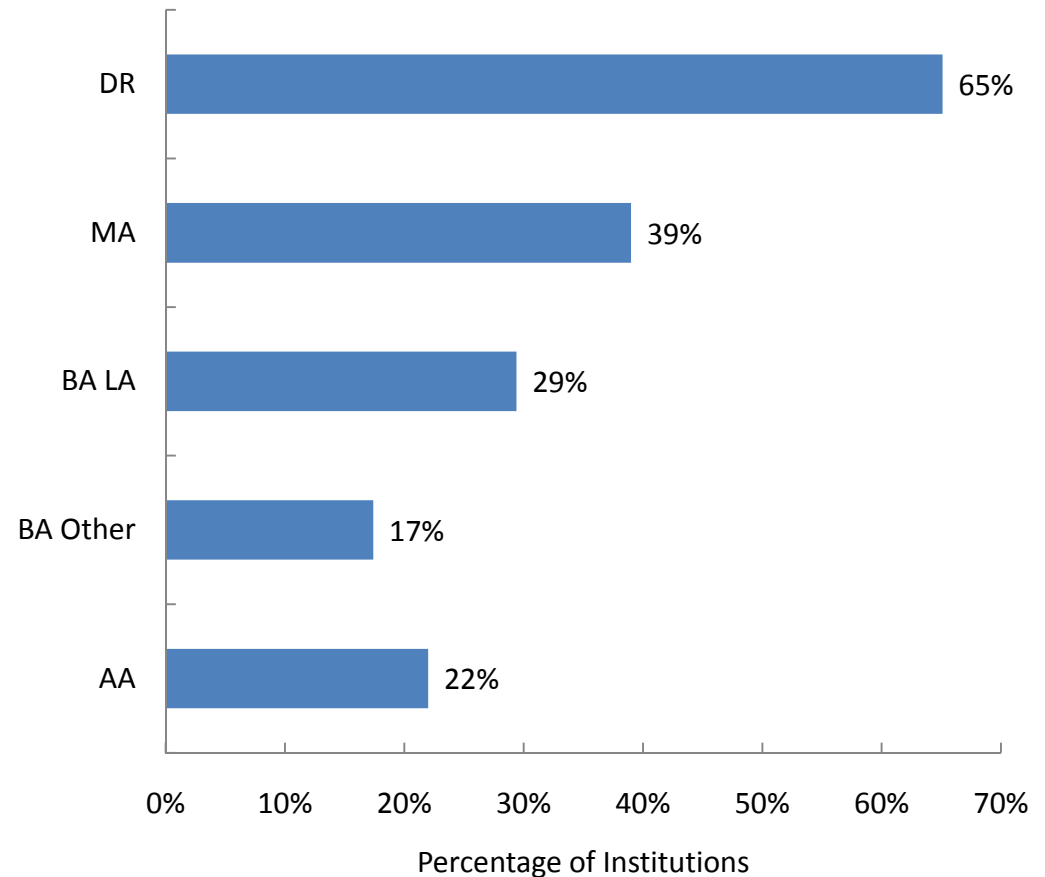
Stage of Implementation of Reduced or Single Sign-On
(N=323)

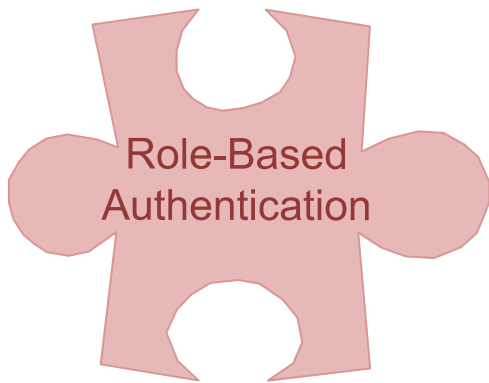




- Open-source software such as Kerberos, CAS, or PubCookie was most frequently selected as an RSSO approach (41.4%).
- Doctorals were most likely to select open-source software as an approach.
- Commercial vendor (e.g., RSA, Aladdin) and homegrown software were selected by about a quarter of respondents.

Selection of Open-Source Software As an Approach to Reduced or Single Sign-on, by Carnegie Class (N=254, Excludes Respondents Not Considering RSSO)

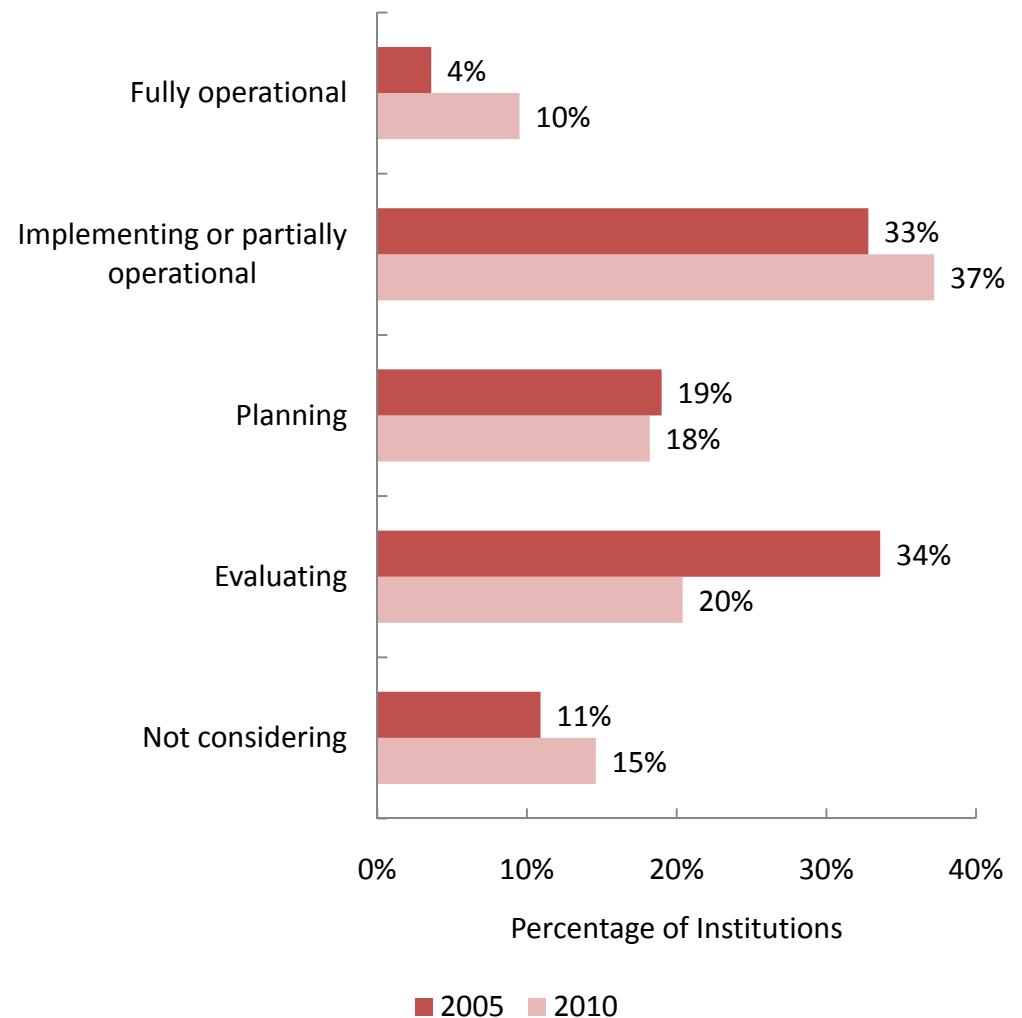


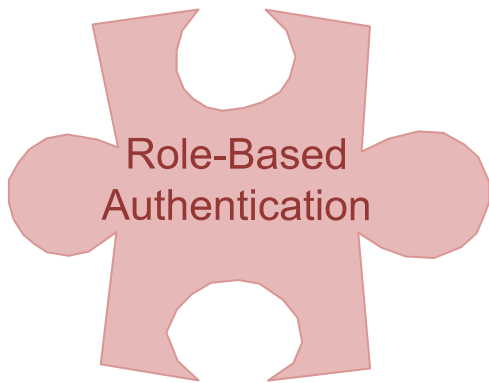


Role-Based Authentication:

- Implementation activity increased from 2005 to 2010; FOIs more than doubled.
- In 2010 doctoral and master's institutions were most likely to have FOIs, followed by associate's and then bachelor's institutions.
- Stage of implementation differed significantly but not greatly with institution size.

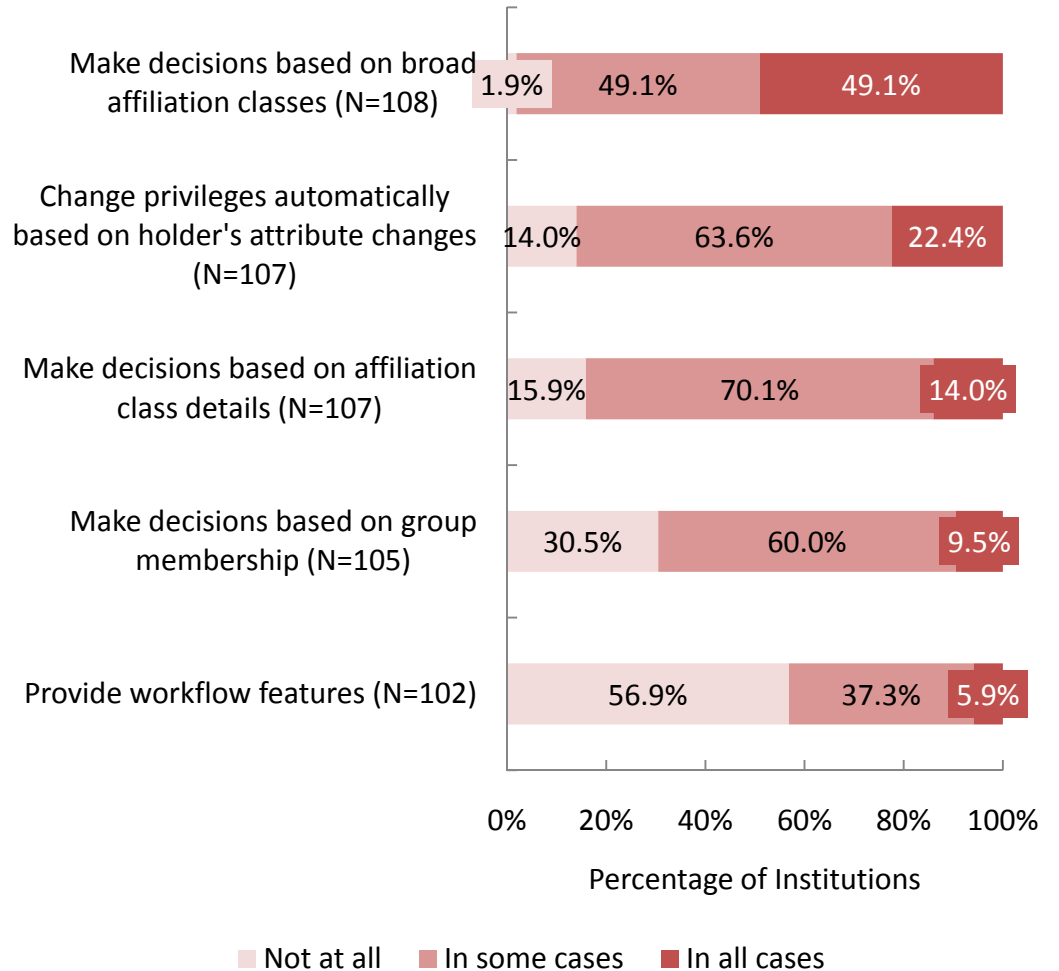
Stage of Implementation of Role-Based Authorization, by Year (N=137)

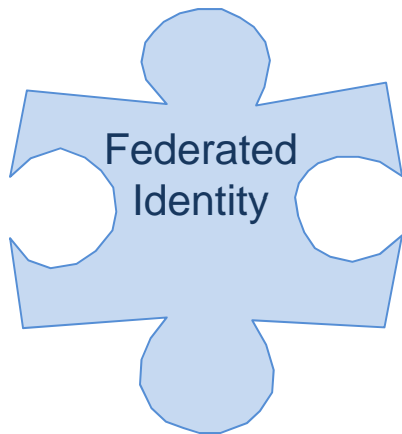




- Where automated role-based authorization is in place, it is applied most often for broad affiliation classes.
- Ability of the institution's role-based authentication environment to make privileging decisions based on fine-grained roles or affiliations in all cases was seven times as common at public 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)

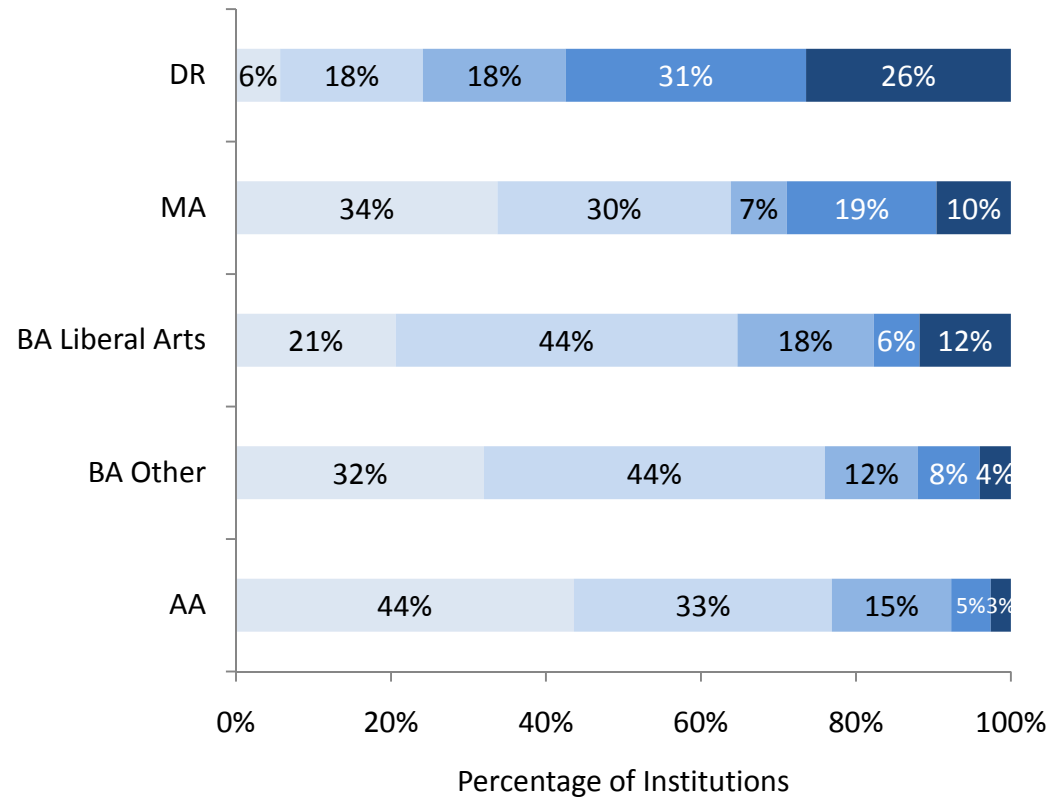


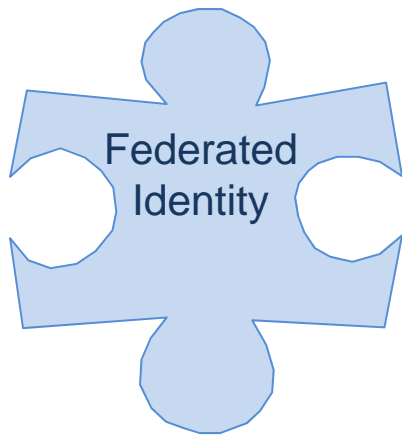


Federated Identity (FID)

- Doctoral institutions were more than twice as likely as other Carnegie classes to have fully operational FID solutions in place and were much more likely to have implementations underway.
- 53% of respondents agreed or strongly agreed that over the next 12 months, demand for cloud computing resources would increase need for FID services.

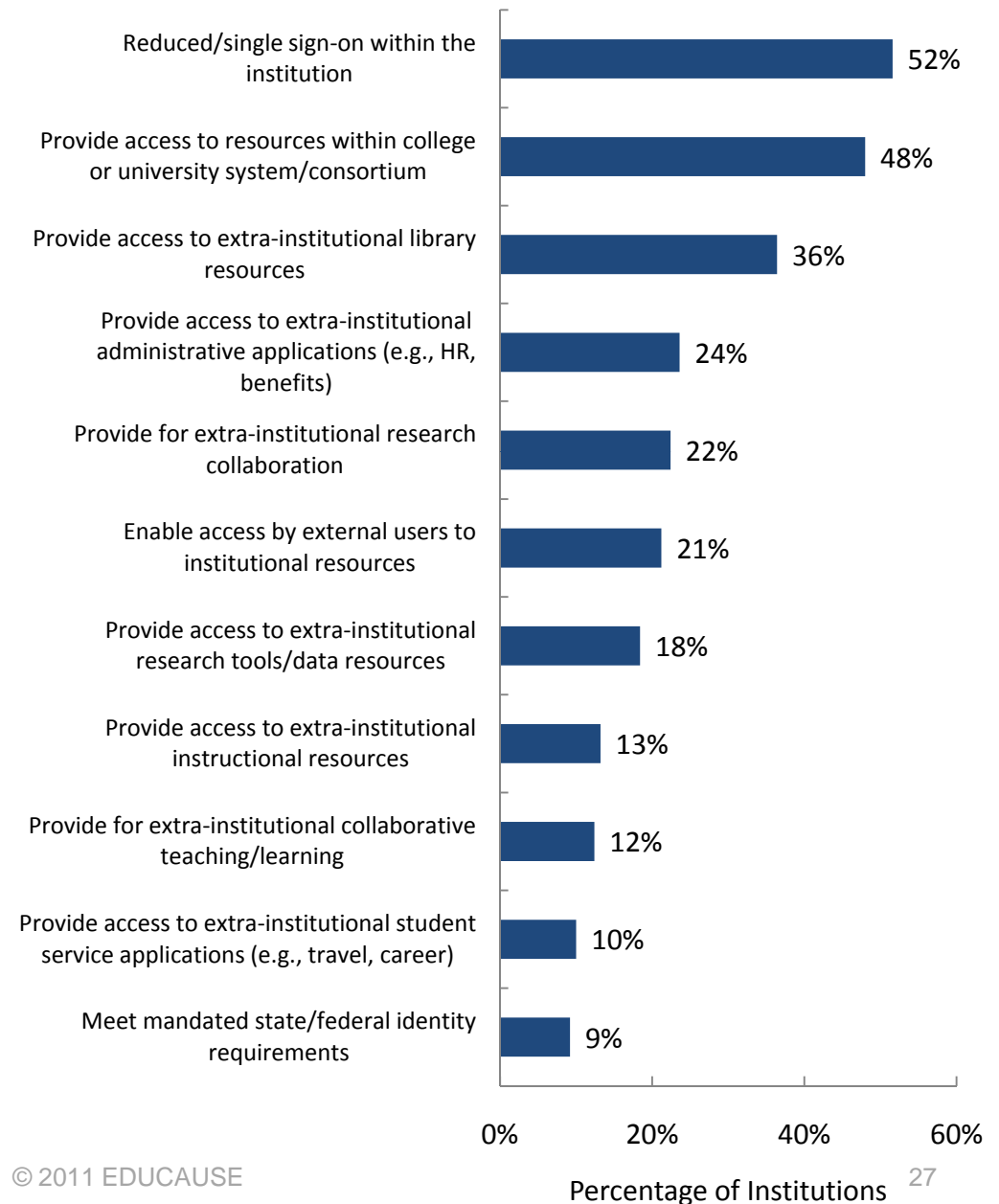
Stage of Implementation of Federated Identity, by Carnegie Class (N=268)





- 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.

Top Motivators for Evaluation or Implementation of Federated Identity (N=250, Up to Three Responses Allowed)

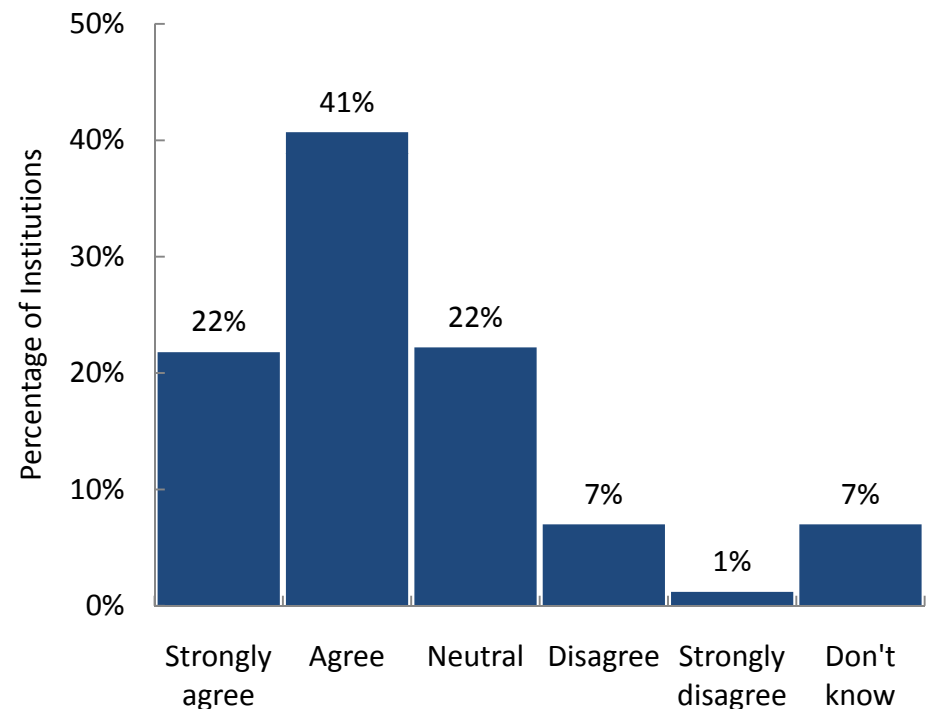


KEY OUTCOMES

OUTCOME: GETTING EXPECTED VALUE FROM IDM PROJECTS

- Most institutions agreed they were getting the value they expected from IdM projects.
- Among those that didn't agree, the majority were neutral on the question or didn't know the answer.
- Only 8% of respondents disagreed at some level.
- Mean agreement did not change significantly between 2005 and 2010.
- In neither year did mean agreement did not vary significantly by Carnegie class, institution size, or institutional control.

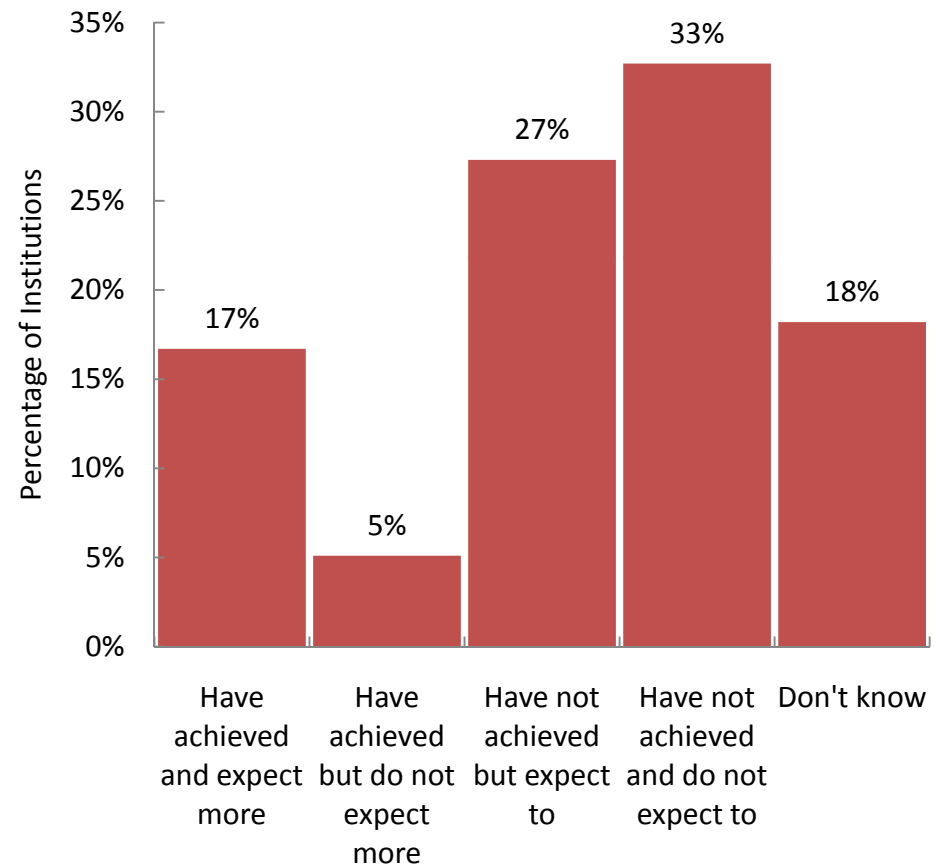
Institution Is Getting Expected Value from Identity Management Projects (N=226, Institutions Engaged In Projects)



OUTCOME: MEETING EXPECTATIONS ABOUT COST SAVINGS FROM IDM PROJECTS

- Nearly 1 institution in 5 didn't know if it had achieved cost savings from its IdM projects.
- Just over 1 institution in 5 had achieved cost savings from IdM projects but many of those did not expect more.
- Among those that had not achieved savings, slightly more than half did not expect to do so.
- Responses did not change significantly between 2005 and 2010.
- In neither year did mean agreement did not vary significantly by Carnegie class, institution size, or institutional control.

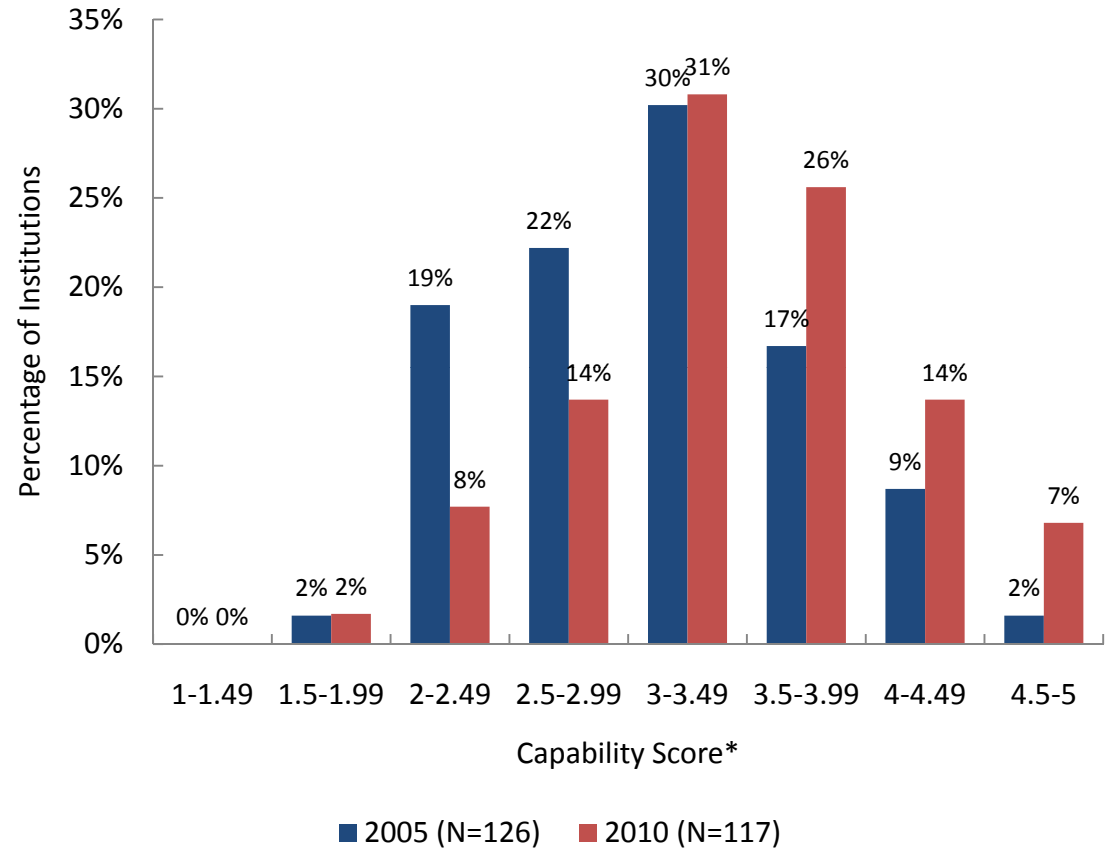
Meeting Expectations about Identifiable Cost Savings from Identity Management Projects (N=225, Institutions Engaged in Projects)



OUTCOME: IDENTITY MANAGEMENT CAPABILITY SCORE

- To compare institutions, for each one, we calculated its mean reported capability to deliver the 14 IdM benefits; we called the result the institution's "capability score."
- Capability score improved significantly between 2005 and 2010.
- In neither year did capability score vary significantly by Carnegie class, institution size, or institutional control.

Identity Management Capability Score, by Year



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

READINESS AND IDM OUTCOMES

- A number of IdM readiness activities are significantly associated with IdM capability score.
- Each appears to boost capability score by between 0.2 and 0.8 points on our five-point scale.

READINESS ACTIVITY	Capability Score Boost*
Monitoring a set of IdM-related metrics	0.8 point
Having IdM-related policies in place	0.5 point
Documenting campus data custodians/owners	0.5 point
Providing for recovery of identity services in disaster recovery plan	0.5 point
Conducting an inventory of campus identifiers	0.4 point
Conducting a risk assessment of data access security and privacy practices	0.4 point
Providing sufficient resources for IdM	0.3 point
Developing a documented plan for IdM	0.2 point

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