This research study is available online at the ECAR Web site (www.educause.edu/ecar). The content of this study is restricted to authorized ECAR subscribers and to those who have separately purchased this study. The username and password below are required to gain access to the online version and are to be used only by those who may legally access the content.

Username: ERS0602
Password: IDMGMT412
Identity Management in Higher Education: A Baseline Study
EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.

The mission of the EDUCAUSE Center for Applied Research is to foster better decision making by conducting and disseminating research and analysis about the role and implications of information technology in higher education. ECAR will systematically address many of the challenges brought more sharply into focus by information technologies.

Copyright 2006 EDUCAUSE. All rights reserved. This ECAR research study is proprietary and intended for use only by subscribers and those who have purchased this study. Reproduction, or distribution of ECAR research studies to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior written permission is granted by EDUCAUSE. Requests for permission to reprint or distribute should be sent to ecar@educause.edu.
Contents

Foreword .............................................................................................................................................. 5

Chapter 1 Executive Summary ............................................................................................................. 9
Methodology • Key Findings • Conclusion

Chapter 2 Introduction ....................................................................................................................... 19
The Rising Significance of Digital Identity • Digital Identity in the Spotlight • What Do
We Mean by Identity Management? • IdM in Higher Education • Establishing a Baseline
for Higher Education IdM

Chapter 3 Methodology and Respondent Demographics .................................................................. 27
Research Approach • Overview of Respondents • Study Organization

Chapter 4 The Institutional Context for Identity Management ............................................................... 33
Importance of IdM Benefits and Capability • The IdM Capability Gap • Motivations to
Pursue IdM • IdM Challenges • Security and Regulatory Compliance • Perceptions of
Senior Management Understanding and Support • IdM Resources • IdM Readiness:
Metrics, Documentation, Policies, and Planning • Planning for IdM: Making the Case
and Making a Plan • Summing Up

Chapter 5 Establishing Identity and User Authentication ...................................................................... 57
Creating and Maintaining Identifiers • User Authentication • Summing Up

Chapter 6 Enterprise Directories, Sign-On, and Authorization .............................................................. 71
Enterprise Directories, RSSO, and RBA: A Comparative Overview • Enterprise Directories
• Reduced or Single Sign-On • Role-Based Authorization • Sourcing Approaches to
Enterprise Directories, RSSO, and RBA

Chapter 7 Federated Identity .................................................................................................................. 95
Institutional Need for a Federated Identity Solution • Federated Identity Implementation
and Approaches • Identity Federations • Summing Up

Chapter 8 Identity Management Projects ............................................................................................. 103
IdM Project Activity and Strategies • Spending and Staffing • Project Sponsorship and
Participation • IdM Project Challenges • IdM Solutions • Summing Up
Identity Management

Chapter 9  Identity Management Outcomes: What Matters .................................................. 125
           Value and Cost Savings • IdM Capability and Cost Savings: What Matters • Summing Up

Chapter 10 What’s in Store for Higher Education Identity Management? .......................... 135
           Higher Education IdM Ambitions: What’s on the Table? • Government and Regulatory
           Drivers • Academic and Business Drivers • Toward a New Paradigm: User-Centric IdM
           • Moving Forward • Conclusion

Appendix A Institutional Respondents to the Online Survey ........................................ 145
Appendix B Interviewees in Qualitative Research .......................................................... 151
Appendix C Glossary ....................................................................................................... 155
Appendix D References .................................................................................................. 163
Foreword

Identity and authenticity. Was that Sartre? Who are you, really, and is that real?

When the first four nodes of the ARPAnet were first powered up, communiqués sent between UCLA, UC Santa Barbara, the University of Utah, and the Stanford Research Institute were communications between known, select, and trusted colleagues in academia. Indeed, the early history of internetworking and network communication is a history of nearly clanlike trust—that is, a history of bilateral and then multilateral understandings based on membership in a rather small academic fraternity of scientists, computer specialists, their graduate assistants, and other “usual suspects.” These early days witnessed the emergence of a pioneer mentality wherein friends rushed to the aid of friends to limit network outages, restore service, and repair damaged bit streams. The concept of network citizenship was unnecessary because those on the network in those early days truly were the members of a community. Engineering the Internet to establish and affirm identity and authenticity was an unnecessary extravagance and, perhaps, even an insult.

Of course, the network grew and evolved: from four nodes, to scores of nodes, to hundreds of nodes, to millions of nodes. Today, with more than one billion people onboard, the Internet is a part-time home to young children and to elders, and it spans every geographical frontier in nearly every language. While it remains a medium of vital scholarly communication and exchange, it is also a robust environment for economic commerce, a social network of growing importance, and a mass medium for the exchange of ideas, music, literature, and film. It is also—as satirized on The Daily Show of February 16, 2006—home to “sexual predators and sexual prey.” Indeed, with more than one billion denizens, the Internet is the frontier of the postmodern era—a source of nearly unimaginable wealth (in terms of community, content, and commerce) and of equally unimaginable peril. When astute political cartoonist Peter Steiner (1993) observed that “On the Internet, nobody knows you’re a dog,” he anticipated and underscored the magic and the misery of the original nondecision to engineer the management of identity into the Internet.

It is now universally understood that the Internet is potentially humankind’s most important mass medium to date. Internet commerce has grown by double digits for more than a decade and shows no signs of abating. The number of people and devices attached to the Internet continues to grow. While the sales of traditional (e.g., 15-year-old)

©2006 EDUCAUSE. Reproduction by permission only.
media such as music CDs decline steadily, sales of (and illegal downloads of) digital music over the Internet rise. In many instances, the Internet has become the venue of choice—or at least of the first instance—for scholarly, business, and news publication. Students, and other young people, redefine social life via social networking sites such as Friendster, Facebook, and MySpace. More and more of our personal and professional lives exist as digital resources, discoverable on the open Internet. And concomitantly, Internet crime rises at double-digit rates; identity fraud and other identity crimes are daily occurrences; and spoofing, spamming, phishing, and other new terms of dark art have been added to our vocabularies, our watch lists, and our CIOs’ sources of sleeplessness.

In many ways, the management of identity becomes—in a post-9/11 world—a bridge that links cyberspace and the “real world,” as campus security officers struggle to determine how identities are to be established, asserted, acknowledged, and accepted, and how authorizations (for building access, parking, lab access, and so on) are to be established, monitored, and enforced. As we move into an era of imbedded intelligence, I worry about our ability to ascertain the identity of sensors and the authenticity of the data that streams in from them. Can we believe that shock waves of 7.0 on the Richter scale are indeed being experienced off the coast of Monterey, because that is what sensor data is telling us?

The need for rigor in the establishment and safeguarding of identity has become manifest among the leadership of higher education’s IT community. We get it. We see that the failure to manage identity in the end imperils all that the Internet has become and will constrain the promise of what the Internet has yet to become. Worse, the failure to manage identity effectively threatens to drive commerce, scholarship, innovation, and community out of the open Internet and into secure and stovepiped private networks—digital clubs with secret handshakes. Lest we think that managing identity is only about defending perimeters and vouchsafing resources, it is important to note that good identity management has the potential to lower administrative costs (reduced help desk costs; self-service passwords; automated, aggregated audit reporting; and so on), increase end-user productivity (reduced time to provision new employees, grant access to systems), and enhance IT productivity.

Identity management (IdM) is therefore a new term of art and one that indeed stirs the embers of Jean-Paul Sartre, Albert Camus, and others. The leaders and early practitioners of IdM talk about the “trust fabric” as something that can be stitched together. Burton Group, an ECAR partner and leading researcher and advisor in domains that include IdM, defines IdM as the business processes and infrastructure that are required to create, maintain, and use digital identities. The insertion and placement of business processes into this definition is thoughtful and essential, for once again, while it may be the information technologists who will lead their institutions into an understanding of a critical new area of institutional capability and need, in the end, the owners of a host of college and university processes will need to debate and reform institutional processes and policies; they will ultimately determine the extent of institutional success or failure in this important arena.

The management of identity and campus security has become top-of-mind for higher education’s top IT leaders. In fact, IdM and IT security replaced the ever-present topic of funding as the topic considered most likely to become “much more significant” in the most recent EDUCAUSE survey of current issues (Maltz, DeBlois, & EDUCAUSE Current Issues Committee, 2005). For this reason, ECAR added the study of identity and access management...
to its research agenda in 2005 and is pleased to present Ron Yanosky’s findings here. As an inherently conservative (culture of evidence, you know) organization, ECAR positions this study as a baseline study. IdM indeed is an evolving area of practice, and we know too well that the results of a careful nine-month study may, in the context of a changing art form, be immediately dated on release. We are also mindful that in forging ahead with this study, we made conscious decisions to bound its scope. We understand the management of identity to consist of

◆ authentication,
◆ reduced or single sign-on (RSSO),
◆ enterprise directory services,
◆ authorization and access controls, and
◆ federated identity.

We made (educated) assumptions about the state of practice in these areas, and these assumptions, in turn, fueled priority decisions about our research. In most cases, our research bears out our assumptions. In some cases, it does not. We assumed that progress would be greatest in the areas of authentication, RSSO, and enterprise directories. We also assumed that authorization and federated identity would reflect the least progress and the least standards-based practice. As a consequence of these assumptions, we asked more questions about areas we assumed to be in motion and fewer questions about areas closer to the presumed leading edge of adoption. Therefore, we present a report that we believe will be of enormous value to most in higher education, but perhaps less so to those practitioners who may be leading the rest of higher education. Finally, baseline study phraseology implies that more studies will follow, and that is certainly our intention. Assuming this report is well received (you will tell us) and that IdM remains an area of topmost concern, we will investigate it again, particularly as today’s leading practices begin to be embedded in the work of many institutions.

As always, the report that follows comprises the hard work of many people, under the leadership of Ron Yanosky. Ron is an accomplished storyteller (historian) and tells here a compelling and interesting story that in many ways is the story of a work in progress. It is another story of how a professional community (the higher education IT community) identifies a need and sets about addressing that need before the broader community (the institution, higher education generally) fully comprehends the need and certainly before institutions bring new resources to bear. In many ways, this is a story of vision and commitment within higher education’s IT community.

The story that unfolds ahead is also one of risk—that is, the risk that technical innovation will once again outpace policy and process innovation. The reader is urged to remember Burton Group’s definition of IdM as inclusive of process reform and therefore is admonished to build the case for inclusion of others at the institution who will need to participate in reforming policies and processes. Adding to both the risk and the drama of this story, going forward, is the important interplay that will unfold between the need for ever-higher levels of assurance (perhaps defined in government regulation); the capacity of our infrastructures, middleware, and applications; and the values of our institutions. This study’s data confirms what most of us would suspect: while there is an increasing regulatory interest in biometric authentication and rising technical capacities to scan fingers, retinas, and other body parts, the adoption rate and interest in future adoption of these techniques and technologies among survey respondents are low. This example likely anticipates a variety of tensions that will mount between regulatory drive, technical capacity, and institution culture and values. Concepts like identity, authenticity, and trust are deeply personal and value laden.
Ron’s analysis and craftsmanship of a fascinating story is anchored in good data. ECAR Fellow Gail Salaway deserves the credit for the original research design and for producing a survey that simply asks the right questions. Once again, it took a village to fashion an ECAR study, and Ron had plenty of remarkable help. Dan Blum of Burton Group; Kathy Carmichael of SunGard Higher Education; Ken Klingenstein of Internet2; Ann West of the National Science Foundation’s middleware outreach effort, the NSF Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium; and Steve Worona, Director of Policy and Networking Programs at EDUCAUSE, merit special thanks. Gail’s work on the survey that underpins this study was crafted in consultation with Gary Augustson, vice provost for information technology, The Pennsylvania State University; Mark Franklin, PKI lab project leader, Dartmouth University; John Grosen, director, infrastructure services, North Dakota State University; Carrie Regenstein, executive director of computing services at Carnegie Mellon University; Barry Ribbeck, director of systems, architecture, and infrastructure, Rice University; John Voloudakis, regional practice leader, Higher Education Consulting Services, BearingPoint; David Wasley, infrastructure planner, University of California Office of the President; and William Weems, assistant vice president for academic technology, University of Texas Health Sciences, Houston.

The EDUCAUSE staff is also part of our community, and our ability to conduct this research depends on their provision of myriad services big and small. The EDUCAUSE team is always there when you need them, and their commitment to excellence is evident in all that they do. Toby Sitko works with a talented production team and with a committed cadre of editors and typographers to ensure that the aesthetics of an ECAR study are in proportion quality-wise to the analysis and writing that goes into them. Thank you!

Finally, ECAR, while now enjoying the support of nearly 400 college and university subscribers, continues to depend on the generous support of a small and dedicated cadre of corporate sponsors. Datatel, HP, Oracle, and SunGard Higher Education not only provide financial direct support of ECAR but are also generous with their advice and skilled resources. Former ECAR Fellow John Voloudakis and his colleagues Todd Facemire and Brian Fuller at BearingPoint, for example, made early, ongoing, and instrumental contributions to the project, as did Kathy Carmichael of SunGard Higher Education.

This study of IdM reminds us that the opportunities and challenges posed by networked information demand responses that are at once technological and cultural in nature. The story of IdM in higher education is ultimately another story of people—people on the outside and inside of our academies, most with good intentions, some with sinister motives, and others with good intentions but incomplete knowledge of or attention to good practice. These people, good and bad, converge in, on, and around our virtual commons, which we have optimized for communication and the free exchange of scholarly ideas. In the end, higher education’s potential to provide sustainable and efficient compliance, to achieve operational effectiveness, and to provide foolproof security for its stakeholders and their information assets will depend on the creativity, vigilance, investment, and technical sophistication of our IT leaders on one hand, and on new processes, policies, and collaboration among institutional subunits on the other. IdM, too, is everyone’s responsibility.

Richard N. Katz
Boulder, Colorado
Executive Summary

Knock, knock. Who’s there?

Those of a certain age and background who hear those words will brace themselves for a weak, punning punch line. But the question is a serious one for higher education administrators. Today, about a billion people are equipped to come knocking at the online resources that colleges and universities have spent so much effort building. Most who do will come with legitimate purposes, some with malicious ones. It’s more important than ever to know: who is there?

This study’s roots lie in the spreading realization that our online environments have outgrown the ability to answer that question with assurance and precision. Information systems have used passwords and other means of user identification for a long time, but for generations their main defense was the implicit assumption that systems were only really usable by a small circle of people whose IT skills were rare and whose good intentions could usually be taken for granted. Batch and client-server systems carried out transactions for the masses while keeping them at arm’s length.

But the explosion of Internet usage in the 1990s vastly increased access to systems while also encouraging the expansion of online self-service to ever more sensitive domains. Viruses, hacking, and other unpleasant phenomena soon showed that not all Internet users were trustworthy. Not much later, a new phenomenon—the accidental or malicious exposure of digitized personal information involving thousands or millions of persons at a time—fed growing public fears of “identity theft.” It became increasingly clear that the Internet’s lack of native user identity mechanisms was a severe weakness and that the mechanisms built into older back-end systems were neither scalable nor interoperable enough for the new IT reality. Along with the generally heightened security consciousness that followed the September 11, 2001, attacks, these developments have made identity and data privacy the subjects of intense regulatory concern.

Security concerns, however, are not the whole story. IT organizations have also struggled to scale their transaction systems to meet the huge new volume of online users and to realize new capabilities not easily served by existing identity systems, such as opening access to digital content collections, automating the exchange of information with business partners, and creating collaborative networks.

In this context, technologists began to promote a comprehensive approach to “identity management.” Rather than treating user
identity as an afterthought, as the Internet does, or as the local concern of application business logic, as most legacy systems did, identity management (IdM) takes a holistic approach in which identity attributes are abstracted and standardized for seamless and secure exchange throughout the online environment. What’s more, IdM recognizes that identity issues are ultimately a matter of business and academic policy, not just a piece of the technology infrastructure. In the definition this study uses, developed by Burton Group, IdM is “the set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities” (emphasis added).

Higher education institutions have been keenly aware of the rise of identity issues and indeed have been in the forefront of the discussion. The 2005 EDUCAUSE Current Issues Survey of higher education IT administrators ranked “security and identity management” as the second most important issue (after IT funding) to resolve for strategic success—and the 2006 survey named it as the most important issue (Maltz, DeBlois, & EDUCAUSE Current Issues Committee, 2005; see also the forthcoming report in EDUCAUSE Quarterly, Vol. 29, No. 2). Discussions with ECAR clients and members of the higher education community at large amply confirmed these findings. This interest, combined with corresponding interest and activity in the vendor community, led us to pursue this empirical study of higher education’s IdM activity.

If IdM has become a classic IT “hot topic,” however, not much is known about how higher education is using or planning to use it. Hypothesizing (correctly, as our results confirmed) that experience with fully operational IdM would not be widespread among our respondents, we designed this study to establish a baseline of technology adoption, business practice, and resource allocation. The core IdM functions we examined include

- **Establishing identity**, the process of associating a physical person with verified identity information prior to the issuance of digital identifiers and the creation of a user account.
- **Authentication**, the process of gaining confidence that the person using a digital identity is the person who is qualified to use it.
- **Authorization**, the process of determining a specific person’s eligibility to gain access to an application or function, or to use a resource.
- **Enterprise directory**, a central institutional lookup repository that holds data regarding the institution’s people and services, informing authentication and authorization processes.
- **Reduced or single sign-on (RSSO)**, a method of authentication that lets a user log into a network and, for a period of time, have his or her credentials passed to the requested applications, enabling the use of the resource without requiring separate authentication for each one.
- **Federated identity**, the management of identity information between members of a federation. A federation is an association of organizations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions.

As summarized in the key findings below, besides looking at the adoption of technologies related to these functions, we examined the importance respondents saw in IdM benefits and their ability to deliver them; the motivations that drive them to adopt IdM and the challenges they face; the policies and plans they are preparing to support IdM; how they are organizing IdM projects and what resources and staff they are dedicating to them; and the factors that influence good outcomes in IdM investment and capability.
Methodology

ECAR pursued a multipart research approach to this study, including
◆ a literature review to identify issues and establish the research questions;
◆ consultation with a select group of individuals representing organizations involved in IdM, including the NSF Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium, Internet2, EDUCAUSE, and several higher education institutions and vendor organizations, for the purpose of identifying and validating research questions;
◆ a quantitative survey of 403 higher education institutions among the EDUCAUSE membership base; and
◆ postsurvey qualitative interviews with 36 executives and IT staff members involved in IdM, representing 24 institutions.

Participants in the quantitative Web-based survey consisted of 379 U.S. and 24 Canadian institutions, of which 60 percent were public. Survey respondents consisted largely of CIOs (64 percent) and other IT managers (30 percent).

Key Findings

We found that our respondent institutions were deeply involved in IdM activities. They told us they thought its benefits were important, and they were almost unanimous in at least considering adopting its major technologies. At the same time, we found that experience with fully operational IdM technologies was relatively rare, and many institutions seem to be struggling with finding the resources for IdM projects and making IdM an institutional priority. We found as well that much of the critical policy, planning, and measurement work supporting IdM initiatives remains to be done. Here, we integrate and summarize our findings.

Importance of IdM Benefits and Capability to Deliver Them

Respondents clearly regarded IdM benefits as important overall, giving security and user service benefits the highest ratings. We presented them with a list of 14 practical benefits commonly attributed to IdM and asked them to rate each one’s importance to their institution on a scale of 1 (very low) to 5 (very high). Six items garnered mean ratings at or above the level of high (= 4) importance, and only two were at or below the level of medium (= 3) importance (see Figure 1-1). Security-related items such as tracking unauthorized activity and deprovisioning user accounts when users leave dominated the top slots, while core-community service improvements such as fast new-user enablement and RSSO were close behind.

Respondents were more guarded, however, when rating their institution’s ability to deliver the same benefits (see Figure 1-1). In every case, capability to deliver rated lower, usually by about one level of the 5-point scale. The existence of this “capability gap” suggests a widespread sense among respondents that they are not delivering IdM services at a level commensurate with their importance. The ambitious plans for adopting IdM technologies that we discovered, reported below, imply that institutions see pressing unmet needs that they plan to fulfill. However, it is also possible that some institutions are “satisficing”—that is, tolerating suboptimal performance because the political or financial costs of optimizing are too high.

Motivations and Challenges

As with the benefit importance results, we found that security and user service were the dominant motivators driving IdM adoption. More than 80 percent of respondents named security/privacy best practices as one of their top three motivators, and 61 percent
chose enhanced user services and satisfaction. As one interviewee told us, “Security is a very big issue these days, and is the primary driver for our IdM work.” Regulatory compliance came in third, while few or no respondents chose a strategy of early adoption or the desire to reduce vendor dependencies. Although the top motivators were ranked almost identically among different Carnegie classes, master’s and associate’s institutions tended to emphasize technical improvements and cost efficiencies among midrange motivators, while doctorals stressed the strategic value of IdM and positioning for federated identity.

Somewhat surprisingly, given the high place of security and regulatory compliance in the motivation rankings, respondents generally rated the security of their central data, networks, and applications high (4.0 on a scale of 1 to 5) and their compliance with regulations higher still. This may be an effect of optimistic self-reporting of performance, but it also suggests that many respondents, though concerned with security and regulatory issues, see them as manageable.

Asked about the challenges they face pursuing IdM at their institutions, respondents painted a picture of tight resources and the complexity of getting agreement about IdM policies. Over half cited higher IT priorities among their top challenges, and 39 percent named the unavailability of adequate funding. Difficulty developing campus policies and procedures and lack of IT staff expertise were each selected by just under 30 percent. Among respondents who told us their IT budgets had declined in the last three years, nearly half named inadequate funding as a top-three challenge, while only about one in five of those with rising budgets did so.

**Senior Management Understanding and Support**

ECAR studies commonly find that senior management support is a factor in producing good outcomes for IT initiatives, and our IdM study was no exception. Institutions that gave
higher ratings to their senior management’s understanding of IdM and their willingness to address related policy issues tended to report higher overall IdM capability and resource sufficiency for IdM.

We found, however, a mixed bag of respondent perceptions about senior management attitudes. Slightly over half agreed or strongly agreed with the statement that their senior management “is willing to address the policy issues related to identity management,” but only about 40 percent felt the same way about the statement that senior management “understands the benefits of investing in identity management.” Respondents were most pessimistic about the statement that senior management “understands the costs of identity management”: over half disagreed or strongly disagreed, while only 17 percent agreed or strongly agreed. This contrast between understanding of benefits and costs may reflect reticence or incomplete understanding on the part of senior management—or the failure of IT units to build a compelling case (or both). But aligning both kinds of understanding will be a key challenge for institutions attempting to mobilize the financial and political resources needed to realize their IdM ambitions.

**Readiness for IdM Activity**

Organizations that advise enterprises on IdM strategies commonly tell them to prepare the ground with attention to the many policy issues, data definitions, metrics, and business rationales that contribute to IdM success. To see how well institutions are readying themselves for IdM initiatives, we asked about the status of their activities in these “soft infrastructure” areas.

On the whole, we did not find that respondent institutions were currently well prepared for ambitious IdM ventures. There were some bright spots: slightly over half reported completing policies in the key areas of establishing identity and user authentication, and most of the rest were working on them. But in other areas, completed work lagged, though there was much in-progress and planned activity. About one-third of respondents said their institutions had documented campus data custodians, and about one-fourth had completed an inventory of campus identifiers. Only 15 percent said that they had documented data definitions and reconciled differences between different data sources. Despite the role of security as a motivator for IdM, only 13 percent had completed a risk assessment of data access security and privacy practices. Much of the completed work was concentrated disproportionately in doctoral and large institutions. Nearly three-quarters of institutions with 25,000 or more FTE students had finished documenting data custodianship, for example, which was more than double the rate among those of 15,000–25,000 students and over triple the rate at institutions of 2,000 or fewer students.

With roughly one-third of respondents in progress with the documentation activities mentioned above, and most of the rest planning to undertake them, this situation could improve considerably. These plans, however, need to be considered in light of the IT priorities and budget constraints mentioned in our IdM challenges data. But there is good reason to pay attention to the policy side of IdM: we found that completion of certain policy and documentation activities correlated with both higher overall reported IdM capability and the likelihood of realizing cost savings from IdM projects.

**User Authentication**

When it comes to authentication—the process of verifying that a person is who he or she claims to be—our respondent institutions rely overwhelmingly on passwords. Ninety-one percent reported using conventional passwords or PINs to authenticate users for network access, and 55 percent said they
used strong passwords (that is, passwords using formulation rules, forced reset dates, and other techniques to make them harder to guess, compute, or misuse). Another 24 percent said they plan to use strong passwords in the future.

Beyond these common authentication methods, however, use and planned use dropped dramatically. Slightly more than one in four reported using the Kerberos network authentication protocol, with doctoral institutions more than twice as likely as the other Carnegie categories to use it. Though security experts increasingly recommend multifactor authentication methods (those employing two or more factors of identification, such as a hardware token combined with a password) at least in some situations, only 28 percent of respondents said their institution used at least one such method, and more than 60 percent of those not using them either said they had no plans for them or didn’t know their plans. Among such technologies, the most commonly reported were SecurID-style one-time passwords, at 13 percent of all respondents.

With increasing pressure for multifactor authentication coming from sources such as the federal government’s E-Authentication Initiative, which requires multifactor methods for some defined levels of assurance, and from federal banking industry regulators, resistance to such methods may decrease over time. For now, however, we found that most institutions have few arrows in their network authentication quivers, and a majority of respondents have no firm plans to change.

**IdM Technology Adoption**

We asked detailed questions about institutions’ adoption of three key IdM technologies: enterprise directories, reduced or single sign-on (RSSO), and automated role-based authorization (RBA). Figure 1-2 shows the distribution of responses among the stages of adoption we specified, ranging from “not considering” to “fully operational.”

Enterprise directories emerged as easily the most widely adopted IdM technology, with more than half of respondents reporting either a partially or fully operational enterprise directory. RSSO and RBA had about the same level of partially operational respon-
dents as enterprise directories—about one in four institutions each—but they were much less likely to be reported as fully operational. For RSSO and enterprise directories, adoption levels tended to be more advanced as Carnegie highest-degree levels and institutional size increased. We also found that institutions that had implemented data warehouses and student portals tended, in each case, to report more advanced stages of adoption for all three technologies.

We found a great deal of ongoing or planned implementation activity that will keep many institutions involved in IdM adoption issues. Altogether, more than 60 percent of respondents told us that they were either in progress with an implementation of at least one of the technologies or had plans to implement one or more in some time frame. When those currently evaluating the technologies are included, the percentage of institutions that are “in the game” but not yet operational reaches 61 percent for RSSO, 57 percent for RBA, and 40 percent for enterprise directories. Adding to the level of planned activity, a majority of those with operational enterprise directories told us that they expect to add functionality in the future.

The applications most commonly reported as using enterprise directories were classic central infrastructure services such as e-mail directories and network operating systems, and enterprise applications such as course management systems, library systems, and student information systems. Only slightly more than one in four institutions reported that any departmental systems used the enterprise directory, underscoring the decentralized nature of many campus IT environments. The dominant technologies in use or planned for use in enterprise directories were Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory, each claiming well over half of all respondent institutions with operational enterprise directories.

Federated Identity

Federated identity lets entities in different IT domains share user attribute information, making resources from the entire group available to users who are known and authorized in only one domain. Using a standards-based, loosely coupled approach to interoperability, federated identity can expose library content, customer account information, research data, and many other kinds of resources within frameworks of trusted federation partners.

We found that most institutions envision a need to participate in a federated identity solution in some time frame, but only about one in seven sees a need now. About 30 percent of doctorals reported such a need, nearly three times the rate of the next highest Carnegie category (associate’s institutions). “Don’t know” answers were relatively high for this question (23 percent), indicating the technology’s newness. A high growth rate for federated identity adoption is suggested by the one in four respondents who told us they anticipated a need within the next two years, but overall we found no clear time frame that looked like a potential “tipping point” for explosive growth.

Seeing a need does not equate to implementing a federating technology such as Internet2’s open source Shibboleth solution or the more corporate-oriented Liberty Alliance technology. Among those who said they see a need now, 42 percent reported implementing a federating technology, though another 29 percent said they plan to. While our question did not specify a particular solution, interviewee comments made it clear that respondent interest is overwhelmingly in Shibboleth rather than some other federated identity product.

Participation in identity federations such as InQueue or InCommon was quite limited, reflecting the early stage of development among higher education federations. Fewer than 4 percent of respondents reported be-
longing to each of these federations, with some overlap between them. Though planned participation was higher than current participation, nearly three out of four respondents told us they had no plans now to take part in either of these federations.

**Project Activity and Strategies**

Engagement in IdM efforts or projects was nearly ubiquitous among our respondents: 89 percent reported being active in this way. The rate rose from 74 percent among institutions of 2,000 or fewer students to more than 96 percent at those of 8,000 or more students. About one-third of project-active respondents said that their IdM projects were organized as a formal project, and another 22 percent said they were considering doing so.

This activity is often bundled with other projects. In fact, six of 10 respondents reported to us that they bundled IdM project work with a security, portal, enterprise resource planning, or other implementation project—about double the number that reported a stand-alone IdM project.

Despite these bundling strategies, we found much evidence that at most institutions IdM is an “inside baseball” activity for the IT unit. By far the most common funding source cited for IdM projects was the annual central IT budget; nearly three of four respondent institutions named it. Bundling with other campus projects, at 27 percent, was the second most named funding source, though this number was only about half the percentage of those mentioning bundling as an implementation strategy. Only about three in 10 respondents told us that their IdM projects had any kind of non-IT sponsorship (for example, a functional area executive), and virtually all of these also mentioned some kind of IT sponsor, usually the CIO. Institutions that had organized their IdM projects as a formal initiative were about twice as likely to say they had a non-IT sponsor.

As if to emphasize the IT-centric nature of most IdM project work, only about one-third of respondents reported having an oversight committee for their IdM projects. This figure rose to over 60 percent, however, among institutions that say they anticipate $500,000 or more of central IT spending on IdM projects in the next three years. The most common role cited for oversight committees was advisory; only about a third of such committees were said to have the power to set policy, and only 17 percent were reported to adjudicate conflicts.

**Resources, Spending, and Staffing**

We found respondents about evenly divided in their perceptions about the sufficiency of IdM funding at their institutions, though leaning slightly toward pessimism. Thirty-six percent disagreed or strongly disagreed with the statement that their institution was providing the resources needed for IdM, while the remainder were about equally divided between those who were neutral and those who agreed or strongly agreed. Institutions with more aggressive technology adoption strategies and those that said creating competitive advantage was their institutional IT goal tended to report higher agreement that they were getting needed resources.

Anticipated central IT spending on IdM projects over the next three years was, on the whole, quite modest. Nearly half of respondents said they expected to spend $100,000 or less, and three-fourths said they would spend $500,000 or less. Since about 14 percent said they didn’t know what they would spend, this leaves about 11 percent planning to spend $500,000 or more. Most of these anticipated spending under $1 million. Spending in the $500,000 or more bracket was dominated by doctorals and institutions of 15,000 or more students.
These figures should be understood as a lower bound to what would certainly be higher expenditures were all internal and external spending considered. Our question did not attempt to capture all institution spending comprehensively, leaving out routine nonproject spending and spending not controlled by central IT (such as expenditures by departments, schools, or special project offices). It is also possible that some respondents did not consider bundled projects in which IdM work was being done as “IdM projects,” and so did not report spending on IdM within those bundled projects, even if controlled by central IT. Also, when we asked interviewees to confirm their spending responses, some told us that they had included all internal and external spending, but others told us that they did not include staff costs, just external goods and services. All but one of our interviewees, however, did confirm their spending responses.

Even with these caveats, our conclusion remains that anticipated central IT spending on IdM projects over the next three years is modest enough to challenge the aggressive adoption plans many respondents report. We found little evidence for a pending wave of “big bang” IdM projects, and the multimillion-dollar IdM projects that some product and services firms promote will be relatively rare among our respondent base.

We found a corresponding modesty in IdM project staffing. About 14 percent of project-active institutions reported no central IT staff dedicated to IdM projects, and 58 percent said they had either one or two FTE staff. Though staffing levels tended to rise with institutional size, even among institutions of 15,000 or more students slightly over half reported two or fewer FTEs.

**Value and Cost Savings**

Our project-active respondents gave a strong if not quite overwhelming endorsement of the value of IdM investment. Asked how strongly they agreed with the statement that their institution was getting the expected value from money spent on IdM projects, six of 10 agreed or strongly agreed, and another 26 percent were neutral. Most of the rest said they didn’t know, leaving only a small sliver (2 percent) of disagreement.

We got more mixed and nuanced responses when we asked about expectations of cost savings. Only 10 percent of respondents told us they had achieved cost savings from their IdM projects, though another 27 percent said they expected to in the future. The largest group, over 40 percent, said they had not and didn’t expect to.

Why the contrast between high agreement about getting value and few reports of cost savings? Recall that among top motivations to pursue IdM, our respondents most often named security and user service issues; only about 18 percent cited cost savings or greater efficiencies as a primary motivator. “The goal is first to make the system secure, and then save people’s time,” said one interviewee. “I don’t know how you put a dollar amount on that, but I’m sure it’s valuable.”

Still, we were able to find some factors associated with an increased rate of reported cost savings. Cost savers were more likely to agree that senior management at their institutions understood IdM costs, to agree that their institution provided needed resources, and to generally have more aggressive technology adoption strategies.

**Conclusion**

Though we found our respondents’ agendas crowded with activity, it would be more accurate to say that we found most of them standing at the threshold of IdM rather than practicing it. Interest in IdM is very high, and respondents acknowledge the importance of the benefits it delivers. More than six out of 10 are either implementing major IdM technolo-
gies or planning to. But reported rates of fully operational IdM technologies are generally low, use of federated identity is restricted to a narrow slice of mostly doctoral institutions, and network authentication technology remains a conservative domain for most institutions. “Don’t know” rates, a substantial factor in our findings about plans and approaches, suggest that many institutions are taking a wait-and-see attitude toward IdM issues.

An advance guard of mostly doctoral and large institutions is engaged in large-scale and sophisticated IdM projects, and this will greatly help the rest of the higher education community bring IdM and associated best practices into the mainstream. But the constraints that most institutions face in funding, staffing, and crowded IT agendas are a reality that is unlikely to go away. We believe that institutions confronted with these challenges will have to approach their IdM plans with an eye on flexibility and agility, putting limited resources where they will do the most good and covering the widest spread of new demands that future developments may bring.

This will mean

◆ seeking out data stewards and working with them to create cleaner, more portable, and better-defined data structures that can be leveraged throughout the identity infrastructure;

◆ making the most of incremental improvements with small victories that build confidence and demonstrate the value of further IdM investment;

◆ embracing standards and flexible architectures supporting IdM;

◆ building the policy foundation of which the identity infrastructure is essentially a technical implementation; and

◆ making senior management aware of the business and academic benefits of the identity infrastructure, and enlisting their assistance with political and financial challenges.

As a foundational element of almost all online transactions and a key enabler of new services that institutions will want to roll out in coming years, IdM will almost certainly justify investments beyond the modest amounts most of our respondents report making. Institutions, however, will have to prepare the ground by showing IdM’s concrete benefits and ultimately by transforming virtual identity from a parochial IT concern into an institutional priority.
Introduction

Hear me! For I am such and such a person.
Above all, do not mistake me for someone else!
—Friedrich Nietzsche

Tools for identifying people, authenticating their claims, and authorizing their transactions are at least as old as civilization itself. The earliest known written records, the clay cuneiform tablets of Sumer, are often found imprinted with the seals of scribes and other parties. Later, essentially the same technology, transferred to new media, embellished Egyptian papyri, medieval charters, and modern notarized documents. Signatures spread along with literacy and began to be accepted for the authentication of legal documents in the late Roman Empire (Fillingham, 1997). Passwords, too, have an ancient pedigree. The Roman emperor Caligula is said to have enjoyed humiliating the commander of his Praetorian Guard by giving him obscene watchwords to distribute among the Guard’s sentries. In perhaps the first recorded instance of user resistance to a password policy, the resentful tribune not only joined a conspiracy to assassinate the emperor but also personally delivered the first blow (Suetonius, 1914).

However implemented, identity technologies and the rules they embody have always been concerned with the same basic things. Those relying on them want to know: Who are you? How do I know that you are who you say you are? Once I know who you are, what should I allow you to do?

This study considers how participating higher education institutions are approaching these questions in their IT infrastructures and policies. To understand why this is an especially important topic today, we need to look at long-term trends now reaching a climax and at more recent developments that add new urgency to identity issues.

The Rising Significance of Digital Identity

The special challenge of adding identity mechanisms to IT systems is that IT is one of the fastest-changing and fastest-spreading technologies in human history. In about six decades, access to computing power has expanded from a tiny elite of technologists to circles of specialists who tended central batch processes or client-server systems, to a popular base engaged in “personal computing,” and finally to the enormous multitude using the Internet today. The last of these growth stages has been truly breathtaking. According to eTForecasts, a market research firm, the number of world Internet users rose in the decade between 1995 and 2005 from 45.1 million to over 1 billion. Even this mass user base is poised to grow dramatically as cheaper, more mobile devices free Internet users from the PC and the tethered data port.
eTForecasts (2005) predicts the number of users will reach 2 billion by 2011.

Just as important as the growth in numbers of users has been the growing sensitivity and intensity of the transactions carried out over the Web (see Figure 2-1). From the consumer’s point of view, the Web has evolved from a largely static information-gathering tool to a dynamic transactional system commonly used to manage finances, buy and sell goods, find a mate, get an education, and seek health care. Visa International (2004) estimates that online retail sales exceeded $150 billion globally in 2004, a 56 percent increase over the previous year. According to the Pew Internet & American Life Project, in the United States one in six online adults—25 million people—had sold something on the Internet by late 2005 (Lenhart & Shermak, 2005).

Virtually all higher education institutions now accept applications, permit course registration, and deliver instruction over the Web, to name only a few of their more strategic online services. Rolling out such capabilities to the masses has meant a vast increase in the number of online identity events, and in the process enterprises have acquired correspondingly vast treasure troves of sensitive personal data.

Designed with an unfortunate combination of immense scalability and assumed user trustworthiness, the Internet provides poor native mechanisms for verifying identities of the people carrying out all these transactions. As more and more services move online, the rewards of stealing or counterfeiting digital identity have grown accordingly, and both trends have put great pressure on the efforts to overlay or back-engineer secure authentication and authorization mechanisms.

Complicating this task is the fact that earlier generations of computer identity technology often treated user authorization as an aspect of business logic and embedded

---

**Figure 2-1. Internet Users and Milestones, 1990–2008**

![Figure 2-1](image-url)
it deeply in applications, making it difficult to abstract and open up to other systems. Many enterprises, including higher education institutions, now have at least two distinct identity infrastructure domains—one located in back-end systems, and one for the Web environment—built on different philosophical and architectural principles. Each domain, in turn, comprises multiple technologies, systems, protocols, and standards, few if any designed for the extent of interoperability that modern IT environments require. 

In short, geometric growth in both users and transactions has put a premium on the ability to express and consume trustworthy digital identities, while stretching existing identity solutions to the breaking point. The real-world effects of this problem are becoming increasingly evident.

**Digital Identity in the Spotlight**

In recent years, digital identity issues have evolved from the obscure concern of a small subset of IT specialists into front-page news. At the same time, public policy and technology developments have highlighted new demands that the identity infrastructure will soon have to bear, along with new possibilities it can enable. We highlight here several key influences now accelerating interest in digital identity issues.

**Identity Theft**

No topic has attracted more attention to identity issues than the rapidly growing threat of identity theft. Many transactions have become virtual, and much of the information that systems rely on to identify participants is in wide circulation. These trends have allowed criminals to “hijack” credit cards and bank accounts, obtain false credentials, and otherwise commit fraud in the apparent name of innocent parties. Phishing (using phony e-mails to collect identity or financial information) and pharming (a similar practice that uses counterfeit Web sites) have become familiar new security threats.

Reports commissioned by the Federal Trade Commission and other organizations have set the annual cost of identity theft at approximately $50 billion in the United States alone (Synovate, 2003; Javelin Strategy and Research, 2005). Although some evidence shows that most identity theft occurs offline through low-tech methods (Javelin Strategy and Research, 2005), the issue has focused attention on identity practices and led to tightened identity and privacy regulations. Furthermore, a 2004 report of the Federal Deposit Insurance Corporation specifically noted that “fraudsters are taking advantage of the reliance on single-factor authentication for remote access to online banking” and called for stronger technical measures to combat financial account hijacking (Federal Deposit Insurance Corporation, 2004).

**Breaches of Digital Private Information**

Security breaches that compromise digital personal information—especially the sort that could become the raw material of identity theft, such as Social Security numbers, credit card numbers, and financial account information—have become an unsettlingly common event, often involving many thousands or even millions of individuals. Unfortunately, this phenomenon also disproportionately involves higher education institutions. Of 123 U.S. security breaches between February 2005 and January 2006 compiled by the Privacy Rights Clearinghouse (2006), 51 were associated with higher education—far more than any other industry. This may reflect reporting practices more than security standards, but there can be little question that the open and decentralized nature of colleges and universities presents real security challenges. While security breaches have many causes, identity
mechanisms play a role by making some forms of hacking easier and by shaping the incentives to steal identifiers in the first place.

A New Regulatory Environment

U.S. higher education institutions, like organizations of all types, have been bombarded by new regulatory controls over the privacy of personal information. Familiar laws protecting student information include the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). More recently, institutions have also found themselves subject to disclosure rules for financial information and identifiers (Gramm-Leach-Bliley Act) and a wave of state laws, spearheaded by California’s SB 1386, defining protocols for the notification of anyone whose identifying information may have been compromised in a security breach. The European Union’s more comprehensive approach to data privacy, embodied in the European Data Protection Directive (EDPD), establishes protections on personal data, including limits on its transfer, and adds regulatory concerns that will affect many U.S. institutions with overseas campuses or students and personnel who are protected under the EDPD.

As we report in Chapter 10, we have every reason to believe that such regulation will continue to intensify. Under the emerging regulatory regime, institutions will have to improve identity systems both to tighten controls (for example, by ensuring that terminated employees lose account privileges in a timely fashion) and to make compromised identity information harder to abuse.

A New Public Identity Infrastructure

Driven in large measure by homeland security concerns, the U.S. federal government has taken broad and unprecedented steps to strengthen the public identification infrastructure and require adherence to federal standards when interacting with federal government systems. Homeland Security Presidential Directive (HSPD) 12 mandates a new identity system for federal employees and contractors, including the use of biometrics-based identity smart cards (Bush, 2004). The federal E-Authentication Initiative defines levels of assurance requiring specific identity practices for federal systems and the systems integrating with them. Both measures could extend beyond the federal government by influencing state, local, and corporate practices. As we note in Chapter 10, aligning institutional systems with the emerging infrastructure will be a necessity for many colleges and universities in coming years.

Federation of Information Assets

Even as identity systems endure ever-greater stresses, new models in research, teaching, and business increasingly emphasize collaboration and cross-domain access. Federated identity—the ability to allow users who are authenticated in one domain to gain authorized access to resources elsewhere through the loosely coupled, standards-based exchange of attribute information—is a response to this emerging demand. Federated identity has many potential uses, such as providing an overarching identity infrastructure for computing grids; allowing users access to extra-institutional resources such as library services, commercial databases, or content download services; exchanging customer and account information between business partners; or facilitating single sign-on between intra-institutional domains.

A closely related concept is the identity federation, an association of participants agreeing to exchange attributes and share resources according to the terms of common
trust frameworks. In higher education, the Shibboleth project has spearheaded the development of a federated identity infrastructure, while InCommon provides a Shibboleth-based federation organization. In the commercial world, the Liberty Alliance, an umbrella group of more than 150 corporate and public sector organizations, is working on federated identity standards. Microsoft, IBM, and other partners have developed a separate and proprietary specification, WS-Federation, based on a Web services model.

**A New Landscape for Identity Solutions**

Recognizing the growing strategic importance of identity and its deep roots in systems architectures, both commercial vendors and open source initiatives have made identity solutions one of the most talked-about areas of product development in recent years. Major technology “stack” vendors such as Microsoft, IBM, Sun Microsystems, and Oracle have been introducing new identity products and, in many cases, acquiring smaller vendors with best-of-breed products to fill out identity solution suites.

At the same time, open source projects such as Shibboleth, the Grouper group management initiative, and the Signet privilege management system have been prominent in higher education circles. Although identity solutions remain immature and higher education institutions have not (as this study’s findings show) settled strongly on particular solutions or approaches, intense marketing and discussion have fueled much interest in identity matters.

**Seeking a Comprehensive Approach**

Both the secular trend of rapidly growing demand for identity capability and the more recent developments mentioned above have led IT administrators to abandon older and often fragmented application- or platform-centered approaches to identity. Increasingly, administrators and vendors alike speak of identity management—a comprehensive, systemic approach to identity issues. (It is also referred to as identity and access management.) But what exactly is identity management?

**What Do We Mean by Identity Management?**

In this study, we use a definition of identity management (IdM) developed by Burton Group, a research firm specializing in enterprise IT infrastructure (and also an ECAR partner). Burton Group defines IdM as “the set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities.” Core IdM functions include establishing identity (identity proofing or vetting) and user authentication and authorization. Supporting infrastructures for these core functions include enterprise directory services, reduced or single sign-on, automation of role- and privilege-based authorization, and creation of identity federations. Definitions for each of these follow.

**Establishing Identity**

Often also termed identity proofing or vetting, establishing identity associates a physical person with verified identity information prior to issuing digital identifiers and creating a user account. Establishing identity is, then, the originating event upon which many further identity transactions will be based.

**Authentication (AuthN)**

Authentication is the process of establishing confidence that the person using a digital identity is the person qualified to use it. It is also a security measure designed to establish the validity of a transmission, message, or originator and to verify an individual’s au-
Authorization to receive specific categories of information. Identity can be proven by
- something you know, like a password;
- something you have, such as smart cards, USB tokens, or public key certificates; or
- something you are, represented by positive photo identification, fingerprints, biometrics, or other techniques.

Authorization (AuthZ)
This process determines a specific person’s eligibility to gain access to an application or function, or to use a resource. We might also describe it as a right or permission granted to access a system resource. Role-based authorization or privilege management refers to automated granting of privileges on the basis of known user attributes (such as job title or enrollment status).

Enterprise Directory
The operational linchpin of almost all middleware services, a directory is a specialized database containing information about an institution’s constituents, groups, roles, devices, systems, services, locations, and other resources. The enterprise directory is the central institutional lookup repository that holds data regarding the institution’s people and services, informing authentication and authorization processes. The information held in an enterprise directory may be consolidated from many other data sources.

Reduced or Single Sign-on
Single sign-on authentication lets a user log into a network and, for a period of time, have his or her credentials passed to multiple requested applications, resources, or domains, enabling their use without requiring separate authentication for each one. Because technical and business issues often make it difficult to deliver a literal “single” sign-on to all resources, reduced sign-on may be an acceptable practical goal.

Identity Federations
An identity federation facilitates management of identity information among its member organizations, which exchange information as appropriate about users and resources in order to enable collaborations and transactions.

IdM in Higher Education
We noted above that identity issues have been driven by global concerns common to all industries and user communities. Still, like most technologies, IdM underscores specific concerns and constraints in higher education institutions.

Diversity of Constituents and Infrastructures
The extremely wide range of activities that higher education institutions engage in, matched by a wide range of constituents who come and go continually, means that colleges and universities have diverse technology infrastructures and often multiple identity systems. Furthermore, since the institution doesn’t own many of the machines connecting to the network, political limits restrict an IT unit’s ability to impose standards and rules. IdM systems and protocols must be able to meet these demands and constraints flexibly.

Specialized Applications
Like all industries, higher education has its critical vertical-specific applications that must be incorporated into the identity infrastructure. Student administration, e-learning, grants management, library management, and fundraising systems are only some of the specialized applications that may require integration efforts not built into off-the-shelf IdM solutions.

A Research Environment
Institutions with a research mission have additional network and identity issues. Much
research requires involvement with experimental, bleeding-edge technology; specialized software and hardware; extremely high performance requirements; and compliance with regulations covering grants, contracts, and research protocols. Like many other elements of this environment, its identity infrastructure often demands capabilities beyond those built into commercial solutions and mature technology standards.

**Decentralization**

Many colleges and universities, especially larger or research-oriented institutions, have a decentralized culture. In such an environment, central IT often controls only a common core of services, while schools, departments, research institutes, hospitals, and other entities control their own networks and applications. Identity functions have historically been decentralized along with the rest of the infrastructure, often providing a good fit for local needs but adding redundancy, ambiguity, and inconsistency to the overall enterprise identity capability.

**Establishing a Baseline for Higher Education IdM**

Higher education institutions clearly share the growing interest that led the term “identity management” to generate more than 20,000,000 responses in a recent Google search. The 2006 EDUCAUSE Current Issues Survey ranked “security and identity management” as the most important issue to resolve for strategic success. This fulfills the prophecy of the 2005 Current Issues Survey which, besides ranking security and IdM as the number-two strategic concern, found that this issue had the greatest potential to become much more significant in the future (Maltz, DeBlois, & EDUCAUSE Current Issues Committee, 2005; see also the forthcoming report in *EDUCAUSE Quarterly*, Vol. 29, No. 2). This interest, combined with corresponding interest and activity in the vendor community, led us to pursue this empirical study of higher education’s IdM activity.

Though higher education IT has long managed identity issues, identity management is a new phenomenon as both a business process and a technology. When we began our study, knowledge of institutional IdM practices was anecdotal at best, and plans to adopt the technology, though often discussed, were vague. We therefore designed this study to establish a baseline of technology adoption, business practice, and resource allocation. We hope this baseline will provide a basis for future study of how IdM is growing and what best practices we can extract from institutional experience.

This study investigates several key areas of IdM:

- **Importance and capability**—Do respondent institutions really see IdM as beneficial, and how much so? How do they rate their ability to deliver its benefits?
- **Motivations and challenges**—What leads institutions to invest in IdM, and what obstacles do they see in their path as they pursue their plans? Do IT units believe they have senior management support and understanding?
- **Readiness for IdM technology adoption**—Are respondent institutions taking the measures recommended by IdM experts to lay a sound foundation for improved IdM? What plans, policies, and metrics are they working on?
- **Current and planned adoption of IdM technologies**—What are institutions doing with authentication, enterprise directories, reduced/single sign-on, role-based authorization, and federated identity technologies? What do they plan to do in the future?
- **Project management**—How are institutions organizing IdM projects, and what
funding and staff resources do they have
to achieve their IdM ambitions? What solu-
tions do they expect to implement?
◆ IdM outcomes—What factors seem to be
related to good outcomes in IdM invest-
ment and capability?
In addition to presenting the empirical
results of our survey, we conclude with a
review of how IdM’s academic and business
drivers will change in coming years. We also
look at some new concepts with the potential
to reshape our thinking about who “owns”
the identity process.

Though our coverage of IdM was wide
ranging, to keep the scope manageable and
to leverage other research studies, we did
place some bounds on what we examined.
This study does not, for example, consider
account provisioning, an area sometimes
considered an aspect of IdM. We strongly
encourage readers to review two comple-
mentary ECAR studies that deal with allied
topics: Information Technology Networking
in Higher Education: Campus Commodity and
Competitive Differentiator (Pirani & Salaway,
2005), and Information Technology Security:
Governance, Strategy, and Practice in Higher
Education (Kvavik & Voloudakis, 2003), as
well as another security study that will be
published in 2006.
Methodology and Respondent Demographics

I shall try to correct errors when shown to be errors, and I shall adopt new views so fast as they shall appear to be true views.
—Abraham Lincoln

This ECAR study used a multipart methodology to gather quantitative and qualitative data about our respondent institutions’ approach to identity management (IdM). Because this is the first such study of IdM among North American higher education institutions, we designed our survey and interview techniques to establish a broad baseline of adoption and practice rather than to examine specific IdM techniques or best practices.

Research Approach

Our research proceeded along three major pathways: a literature review, a quantitative Web-based survey of IT leaders at higher education institutions among the EDUCAUSE member base, and qualitative interviews with IT executives and other staff from selected institutions.

The Research Process

The literature review helped identify and clarify issues, suggest hypotheses for testing, and provide supportive secondary evidence. Though we reviewed a large range of studies and publications, we benefited in particular from the work of three research and advisory groups influential in the IdM field, all ECAR partners. The NSF Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium works to promote improved middleware architectures and applications within academic research and higher education generally, and its influential roadmaps and advisory documents were very helpful to this study. We also made wide use of studies by Burton Group, an advisory firm specializing in enterprise IT infrastructure, and Gartner Inc., whose broad IT advisory interests include identity and access management. Additional documents and studies from government agencies, academic researchers, standards bodies, vendors, and journalistic sources rounded out our literature review.

ECAR Fellow Gail Salaway led the effort to design the quantitative Web-based survey, which we distributed to EDUCAUSE member institutions in June 2005. Senior college and university administrators from 403 institutions, mostly CIOs and other IT leaders, responded to the survey. The survey instrument is available on the ECAR Web site, and Appendix A lists respondent institutions.

To help us understand and interpret our findings, and to uncover additional insights, we also conducted qualitative interviews with 38 IT executives and practitioners at 26 institutions (see Appendix B for their names). Early in our survey design process,
we selected several interviewees because of their experience with IdM. Twenty-four of the institutions were chosen for interviews because their survey responses fit one of the following two profiles:

- **Active planners** were planning to adopt at least one major IdM technology, were near the median (plus or minus 10 percent) of overall IdM technology adoption, and had completed or were planning an IdM business case, plan, or both.

- **Aggressive adopters** were in the top 10 percent of overall IdM technology adoption and agreed or strongly agreed that they had received value from their IdM investments.

In addition, to obtain adequate depth and breadth of practice, we chose interview institutions that varied in size and mission, including both public and private institutions.

Unlike many previous ECAR studies, this one did not include case studies to parallel the quantitative survey and qualitative interviews. However, the NMI-EDIT Consortium’s collection of IdM-related case studies, available at <http://www.nmi-edit.org/started/index.cfm>, contributed to our literature review and is recommended to readers of this study.

In the interest of manageable scope and because they are large enough to warrant separate study, we did not include the following topics in this study:

- account provisioning;
- security infrastructure beyond the identity function (see Kvavik & Voloudakis, 2003, as well as a forthcoming ECAR study on the same subject);
- networking infrastructure beyond the identity function (see Pirani & Salaway, 2005);
- responses to specific regulatory mandates (such as FERPA, HIPAA, and California SB 1386); and
- specific vendor products or suites.

### Analysis and Reporting Conventions

We followed the following conventions in analyzing the data and reporting the results:

- Some tables and figures presented in this study have fewer than 403 respondents, as we adjusted for missing information. Note also that percentages in some tables and figures do not add up to 100 percent because of rounding.

- We analyzed the data for each online survey question for differences in response patterns among Carnegie classes (including doctoral-intensive versus doctoral-extensive institutions), Canadian and U.S. institutions, private and public institutions, and institutions of varying size. The number of full-time students determines the institution size. We note any differences found that are both meaningful and statistically significant in the text and/or the supporting figures and tables. In some cases, we combined institution size categories to produce more statistically significant or compact results.

- The Likert scales used in the online survey are footnoted in the tables and figures showing results for these survey questions.

- Appendix C includes a glossary of IdM-related terms.

### Overview of Respondents

We distributed our survey to the EDUCAUSE institutional representative at each member institution. In most cases, this was the CIO. Of the 403 respondents, 379 were from the United States and 24 from Canada.

### Carnegie Class

The study grouped the sample by a modified Carnegie Classification of Institutions of Higher Education. We collapsed the Carnegie 2000 categories as
follows to obtain larger numbers for statistical and descriptive purposes:

- **Doctoral/research institutions (DR).** The study grouped the doctoral-extensive and doctoral-intensive universities together. These institutions typically offer a wide range of baccalaureate programs and graduate education through the doctorate degree.

- **Master’s institutions (MA).** The study grouped master’s colleges and universities I and II together. These institutions typically offer a wide range of baccalaureate programs and graduate education through the master’s degree.

- **Baccalaureate institutions (BA).** The study combined the three baccalaureate college groups (baccalaureate colleges—liberal arts, baccalaureate colleges—general, and baccalaureate/associate’s colleges) into a single group. Baccalaureate colleges are primarily undergraduate colleges with major emphasis on baccalaureate programs.

- **Associate’s institutions (AA).** These institutions offer associate’s degrees and certificate programs but, with few exceptions, award no baccalaureate degrees.

In addition, where appropriate we break out an “Other Carnegie” category that includes specialized institutions and U.S. higher education systems offices. Specialized institutions offer degrees ranging from the baccalaureate to the doctorate and typically award most degrees in a single field, such as engineering, law, medicine, or theology. The data presented for these schools and systems offices must be interpreted in light of the enormous diversity of institutions within this category.

Our respondent base had more public (60.0 percent) than private (38.3 percent) institutions. We note significant differences between public and private institutions, though on the whole we found little difference along this dimension. Finally, we also provide data, where appropriate, for the 24 Canadian institutions in our study, recognizing that they vary by size and mission. In general, we report the Canadian information separately only where it is a particularly significant and contrasting finding.

Figure 3-1 compares the responding institutions’ distribution by their 2000 Carnegie class, EDUCAUSE membership, and the...
universe of higher education institutions in the United States. The responding schools mirror much more closely the EDUCAUSE membership than the national population of institutions by Carnegie class. Proportionally, we have the strongest participation from doctoral-extensive institutions (53.7 percent).

Note also that because the study relied on volunteers and because participating institutions are drawn from the EDUCAUSE membership rather than from a random sample of all higher education institutions, results are not generalizable to all higher education institutions. Nevertheless, the overall 27.5 percent response rate from EDUCAUSE member institutions gives us confidence that the study’s respondents portray a reasonable image of the EDUCAUSE membership, especially for doctoral institutions.

**Institution Size**

The size of an institution’s full-time-equivalent (FTE) student enrollment often influences its technology decisions and characteristics as much as its Carnegie classification. Throughout our study, we often found significant differences based on institution size.

The median student enrollment at our study institutions was 4,919, while the mean, reflecting the weight of the largest responding institutions, was 8,765. Overall, however, smaller institutions made up the bulk of our respondent base. For analysis purposes, we divided the respondent institutions into six groups, as shown in Figure 3-2. About 60 percent of respondents were from institutions with 8,000 or fewer students, and only 8 percent were from those of 25,000 or more.

**Respondent Position**

Our survey was completed far more often by respondents holding the position of chief information officer (CIO) than by those holding any other position, and the remaining respondents overwhelmingly held IT-related positions (see Figure 3-3). Respondents were about evenly divided between institutions where the CIO was a member of the president’s cabinet (52.1 percent) and those where he or she was not (47.9 percent). With only 5.4 percent of respondents representing non-IT viewpoints, we emphasize that the study largely reflects a CIO and IT management view of IdM.
Study Organization

The remainder of this report presents our study findings and investigates what future developments might affect higher education IdM planning.

In Chapter 4, we examine the institutional context that shapes IdM concerns, including perceptions about how important IdM’s benefits are, how capable institutions are at delivering them, what motivators and challenges respondents face, and what planning and policy development work they’re doing. In Chapter 5, we turn to identity proofing and authentication technologies, while Chapter 6 examines adoption, approaches, and planning for three key IdM technologies: enterprise directories, reduced or single sign-on, and role-based authorization. We look at federated identity plans and identity federations in Chapter 7. Chapter 8 reports on project management practices and available funding and staffing resources, as well as the use of external service providers and overall characterizations of the IdM solutions institutions expect to pursue. Chapter 9 looks at what influences good outcomes in IdM investment and capability. Finally, Chapter 10 recaps what we learned about respondents’ future expectations; considers emerging academic, business, and technology drivers that may affect those plans; and concludes with advice on how to reconcile planned activity with limited resources.
The Institutional Context for
Identity Management

Key Findings

- Respondents highly rate the importance of identity management (IdM) benefits, but rate their institutions’ capability to deliver those benefits lower.
- Security and privacy best practices, enhancing user services, and regulatory compliance are the most commonly named top motivators for pursuing IdM.
- Higher IT priorities, constrained funding, and difficulty developing policies and procedures are the top-ranked challenges to pursuing IdM. Technical immaturity of solutions is a midrange challenge, while vendor support and ROI issues rank low.
- While more than half of respondents agree or strongly agree that senior management at their institution is willing to address policy issues related to IdM, and about a third agree or strongly agree that senior management understands IdM benefits, fewer than one in five agree or strongly agree that senior management understands IdM costs.
- Perceptions about getting sufficient resources for IdM vary widely, with about a third agreeing or strongly agreeing that their institution provides enough resources, a third disagreeing or strongly disagreeing, and the rest neutral.
- Only about half of institutions have completed documenting policies for authentication and establishing identity, while rates for completed data definitions, campus identifier inventories, and risk assessments are considerably lower. Most institutions that have not completed such activities, however, have them in progress or plan to undertake them.
- Overall “readiness” for IdM is low when measured by completed preparatory work. Widespread successful adoption of IdM technologies will depend heavily on whether institutions carry out planned and in-progress preparatory work, and how well they do it.
To deliver robust IdM capability, campus IT administrators and other leaders must choose among many options, prioritize them, and fit them into the political realities and operational demands of a complex institution. In this chapter, we look at this context and consider its implications for higher education IdM ambitions. Beginning with respondents’ assessments of how important IdM benefits are to their institutions and how well they say they’re delivering them, we move on to consider IdM motivations and challenges, levels of executive support, resource sufficiency, and assorted measures that contribute to institutional readiness to adopt IdM.

### Importance of IdM Benefits and Capability

To get a general picture of IdM’s status in higher education, we assembled a list of 14 practical benefits commonly attributed to IdM and asked our respondents to rate each benefit’s importance to their institution and their current capability to deliver it. Table 4-1 and Figure 4-1 summarize the results.

Respondents clearly regarded IdM benefits as important overall. Six items garnered mean ratings at or above the level of high importance, while only two were at or below medium importance. Security-related items—tracking unauthorized activity to the persons responsible, deprovisioning accounts when users leave, and improved identity proofing—dominated the top slots, followed by core-community service improvement benefits such as fast new-user account enablement and reduced or single sign-on. More advanced changes to network practices such as strong authentication and opening access to off-campus resources (for example, through federated identity) fell into the midrange, while service to peripheral users and decentralizing account management ranked low. Mean ratings were close enough together, however, that the main takeaway point is the high overall importance respondents tended to assign, rather than the slight differences between each item and those immediately above or below it.

### The IdM Capability Gap

Perhaps more striking than respondents’ ordering of IdM benefits’ importance was the relationship they described between importance and the institution’s capability in that area. In every case, capability rated lower, usually by roughly one level of the 5-point scale. Reduced or single sign-on, the benefit with the largest gap, had an importance mean slightly above high yet a capability mean well below medium. The narrowest absolute differences between importance and capability appeared in the two items ranked lowest in importance.

In part because self-assessed performance measures tend to be rosy rather than critical, we believe the capability gap reflects a widespread sense among respondents that they are not delivering IdM services at a level commensurate with their importance. What this means, however, is harder to assess. Of course, it may indicate that institutions see pressing unmet needs that they plan to fulfill. However, as we reported in the ECAR study *Good Enough: IT Investment and Business Process Performance in Higher Education*, institutions frequently tolerate suboptimal business process performance because economic or political constraints put the price of optimizing out of reach (Kvavik & Goldstein, 2005). Ambitious plans to upgrade IdM infrastructure, as reported in Chapters 6 and 8, lend some weight to the notion that institutions seriously want to close the capability gap. Nonetheless, we caution that some institutions will be content with “satisficing” at a workable performance level even if it leaves some needs unmet.
### Table 4-1. IdM Benefit Importance and Capability to Deliver

<table>
<thead>
<tr>
<th>Identity Management Benefit</th>
<th>Descriptor</th>
<th>Importance</th>
<th>Std. Deviation</th>
<th>Capability</th>
<th>Std. Deviation</th>
<th>Importance-Capability Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directly track illegal or unauthorized network activity back to the person responsible</td>
<td>Track unauthorized activity</td>
<td>4.32</td>
<td>0.757</td>
<td>3.24</td>
<td>0.946</td>
<td>1.08</td>
</tr>
<tr>
<td>Immediately disable all services and user IDs when a user is no longer affiliated with the institution</td>
<td>Immediate deprovisioning on user departure</td>
<td>4.32</td>
<td>0.711</td>
<td>3.12</td>
<td>1.077</td>
<td>1.20</td>
</tr>
<tr>
<td>Prior to issuing credentials (e.g., user account, ID card, etc.), have the appropriate level of confidence (based on type of constituent) that a user is who he or she claims to be</td>
<td>Appropriate ID proofing confidence</td>
<td>4.18</td>
<td>0.750</td>
<td>3.47</td>
<td>0.924</td>
<td>0.71</td>
</tr>
<tr>
<td>Reduced or single sign-on (one electronic identity used to access most or all institutional services)</td>
<td>RSSO</td>
<td>4.10</td>
<td>0.836</td>
<td>2.72</td>
<td>1.035</td>
<td>1.38</td>
</tr>
<tr>
<td>Have a single authoritative source of information for all persons affiliated with the institution (as an institutional asset)</td>
<td>Single affiliations source</td>
<td>4.05</td>
<td>0.890</td>
<td>2.91</td>
<td>1.043</td>
<td>1.14</td>
</tr>
<tr>
<td>Provide self-service functions (e.g., password reset, profile management)</td>
<td>Self service</td>
<td>4.05</td>
<td>0.810</td>
<td>2.94</td>
<td>1.043</td>
<td>1.11</td>
</tr>
<tr>
<td>Immediately enable all authorized services for a new user</td>
<td>Immediate new-user enablement</td>
<td>3.93</td>
<td>0.803</td>
<td>2.87</td>
<td>0.931</td>
<td>1.06</td>
</tr>
<tr>
<td>Immediately change authorized services for a user who changes roles</td>
<td>Immediate role change</td>
<td>3.89</td>
<td>0.810</td>
<td>2.74</td>
<td>0.959</td>
<td>1.15</td>
</tr>
<tr>
<td>User authentication and authorization processes that are scalable (e.g., as enrollment grows)</td>
<td>Scalable authN and authZ</td>
<td>3.89</td>
<td>0.955</td>
<td>3.24</td>
<td>0.944</td>
<td>0.65</td>
</tr>
<tr>
<td>Allow institutional users to access off-campus resources that require their own authentication and authorization (e.g., licensed library content)</td>
<td>User access to off-campus resources</td>
<td>3.85</td>
<td>0.922</td>
<td>3.10</td>
<td>1.045</td>
<td>0.75</td>
</tr>
<tr>
<td>Strong authentication (e.g., strong passwords, two-factor authentications)</td>
<td>Strong authentication</td>
<td>3.83</td>
<td>0.950</td>
<td>2.77</td>
<td>1.115</td>
<td>1.06</td>
</tr>
<tr>
<td>Give visitors/guests only the specific access they require and disable that access at the correct time</td>
<td>Appropriate guest access</td>
<td>3.62</td>
<td>0.969</td>
<td>2.61</td>
<td>1.017</td>
<td>1.01</td>
</tr>
<tr>
<td>Allow non-institutional users access to institutional resources for which we require authentication and authorization (e.g., sharing course materials with other institutions)</td>
<td>Non-institutional user access to our resources</td>
<td>3.02</td>
<td>1.038</td>
<td>2.39</td>
<td>0.932</td>
<td>0.63</td>
</tr>
<tr>
<td>Decentralize user account management and authorization of services (e.g., to deans of schools, managers of business units)</td>
<td>Decentralize account management</td>
<td>2.70</td>
<td>1.232</td>
<td>2.17</td>
<td>1.050</td>
<td>0.53</td>
</tr>
</tbody>
</table>

(1 = very low, 2 = low, 3 = medium, 4 = high, 5 = very high)
Fig. 4-1. IdM Benefit Mean Importance and Capability Ratings

(1 = very low, 2 = low, 3 = medium, 4 = high, 5 = very high)

See Chapter 9 for more analysis on the relationships between mean reported IdM capability and assorted other factors, including resource sufficiency, perceived senior management attitudes about IdM, and technology adoption strategies.

Motivations to Pursue IdM

Besides our questions about specific benefits that IdM might deliver, we asked about broader issues that might drive IdM adoption. We asked respondents to rank up to three factors motivating their institutions to pursue IdM, choosing from a list of 11 motivators (plus a “no motivators at this time” option).

As with the benefit importance questions, security took the top slot. Nearly half of all respondents chose security and privacy best practices as their institution’s number-one motivator, and 80.9 percent ranked it in their top three. Enhanced user services and regulatory compliance followed, each separated from the motivator above it by about 20 percentage points (see Table 4-2). Only 4.7 percent of respondents said they had no motivators at this time.

It’s not surprising that security and privacy stand at the top of motivators in an IdM study. As we noted in Chapter 2, recent EDUCAUSE Current Issues Surveys have put security and IdM at or near the top of higher education CIO concerns (Maltz, DeBlois, & EDUCAUSE Current Issues Committee, 2005; see also the forthcoming report in EDUCAUSE Quarterly, Vol. 29, No. 2). “Security is a very big issue these days and is the primary driver for our IdM work,” says Gary Pratt, associate provost for IT and CIO at Northern Kentucky University. As Jeff von Munkwitz-Smith and Ann West have argued, the growth of identity theft has raised awareness of IdM issues, and a variety of IdM services—such as consolidating separate application-based access services, standardizing identifiers, simplifying sign-ons, and reducing the likelihood of password theft—all speak to
pressing security weaknesses (von Munkwitz-Smith & West, 2004; see also Bruhn, Gettes, & West, 2003). Enhanced user services and satisfaction, the second highest ranked motivator, is another area where institutions seem to see strong potential for process improvement through the identity infrastructure. “The primary driver for identity management at Blinn College is to enhance services and provide proper security and access to employees,” says Michael Welch, dean of academic technology services at Blinn. “It’s critical that we get employees everything they need to do their job with one set of credentials.” Interviewees note, however, that IdM enhancements are not equally visible to all users. At Dalhousie University in Halifax, Nova Scotia, investments in an enterprise directory and consolidation on a single user ID made user account provisioning “so much easier,” says John Sherwood, executive director of University Computing and Information Systems. Noting that Dalhousie can now provision newly accepted students months before they show up on campus, Sherwood also acknowledges that most casual users are “probably not aware” of the IdM improvements. But business units are considerably more aware, “especially at the manager and director level. The more senior you get, the more they appreciate what it does.”

Though certain public policy issues relating to identity are global in nature, the situation has been particularly volatile in the United States since 2001, due to the intersection of homeland security, privacy, and corporate accountability issues. Recent legislation such as the USA PATRIOT Act, the Sarbanes-Oxley Act, and state identity theft codes have been layered on top of older structures like the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). Our data sug-

### Table 4-2. What Is Motivating Your Institution to Pursue IdM?

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Percentage Choosing</th>
<th>Rank Order</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security/privacy best practices</td>
<td>46.4%</td>
<td>24.1%</td>
<td>10.4%</td>
</tr>
<tr>
<td>Enhanced user services and satisfaction</td>
<td>19.1%</td>
<td>25.6%</td>
<td>16.1%</td>
</tr>
<tr>
<td>Regulatory compliance (such as HIPAA, GLB Act, FERPA)</td>
<td>16.4%</td>
<td>17.4%</td>
<td>8.9%</td>
</tr>
<tr>
<td>Strategic value/opportunities</td>
<td>3.0%</td>
<td>6.5%</td>
<td>13.4%</td>
</tr>
<tr>
<td>Improvements in technical environment</td>
<td>2.2%</td>
<td>7.2%</td>
<td>10.9%</td>
</tr>
<tr>
<td>Keeping current with generally accepted IT directions</td>
<td>1.7%</td>
<td>6.5%</td>
<td>10.7%</td>
</tr>
<tr>
<td>Cost reduction/increased efficiencies</td>
<td>3.2%</td>
<td>6.2%</td>
<td>9.2%</td>
</tr>
<tr>
<td>Position the institution for implementation of federated identity</td>
<td>2.2%</td>
<td>2.7%</td>
<td>9.7%</td>
</tr>
<tr>
<td>Strategy of early adoption/experimentation</td>
<td>0.0%</td>
<td>0.2%</td>
<td>1.0%</td>
</tr>
<tr>
<td>Reduce vendor dependencies</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.5%</td>
</tr>
<tr>
<td>Other</td>
<td>0.5%</td>
<td>0.0%</td>
<td>0.5%</td>
</tr>
</tbody>
</table>

*(Three responses allowed, ranked 1 to 3)*
gest just how powerful this combination has been. While 44.9 percent of U.S. institutions ranked regulatory compliance among their top motivators, only 8.3 percent of Canadian respondents did so—leaving it, in fact, the lowest-ranked motivator except for those which no Canadian institutions reported. Dalhousie’s Sherwood notes that “privacy laws are being tightened up constantly in Canada and we’re trying to stay ahead of it,” but says that he faces “nothing like” the regulatory environment in the United States. This striking difference in motivator rankings is a reminder that IT priorities are often as much a product of political as technological demands.

The three leading items were ranked almost identically across Carnegie classes (see Table 4-3). Not so the midrange motivators, where more differentiation appeared. Master’s and associate’s institutions tended to place technical improvements and cost efficiencies in their midrange motivations, while doctoral institutions stressed the strategic value of IdM and positioning for federated identity. Perhaps reflecting their less distracting regulatory environment, Canadian institutions ranked strategic value third, with 37.5 percent including it among their top motivators, compared with 21.9 percent among U.S. institutions.

Taken together, the motivation results paint a picture of IdM driven by practical (if high-priority) concerns about top-of-mind IT issues: security, service, and compliance. While some are motivated by the strategic or technological value they find in IdM, most seem to see it as a means, not an end.

**IdM Challenges**

Knowing what motivates institutions to pursue IdM is not very meaningful if you don’t

---

**Table 4-3. IdM Motivation Rankings, by Carnegie Class**

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Rank, by Carnegie Class</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All</td>
</tr>
<tr>
<td>Security/privacy best practices</td>
<td>1</td>
</tr>
<tr>
<td>Enhanced user services and satisfaction</td>
<td>2</td>
</tr>
<tr>
<td>Regulatory compliance (such as HIPAA, GLB Act, FERPA)</td>
<td>3</td>
</tr>
<tr>
<td>Strategic value/opportunities</td>
<td>4</td>
</tr>
<tr>
<td>Improvements in technical environment</td>
<td>5</td>
</tr>
<tr>
<td>Keeping current with generally accepted IT directions</td>
<td>6</td>
</tr>
<tr>
<td>Cost reduction/increased efficiencies</td>
<td>7</td>
</tr>
<tr>
<td>Position the institution for implementation of federated identity</td>
<td>8</td>
</tr>
<tr>
<td>Strategy of early adoption/experimentation</td>
<td>9</td>
</tr>
<tr>
<td>Reduce vendor dependencies</td>
<td>10</td>
</tr>
</tbody>
</table>

*(Based on percentage of respondents ranking motivation as 1, 2, or 3; blank where no respondents selected motivation)*
also know what stands in their way. To fill in this part of the story, we asked respondents to identify up to three IdM challenges, ranking them in order, from a list of 12 challenges. The results sort roughly into three clusters of related challenges that account for most of the difficulties respondents say they face: resource allocation, organizational issues, and the technical maturity of IdM.

**Resource Challenges**

The message respondents most frequently communicated in the challenges data was that they have too much to do and not enough to do it with. In total and across all Carnegie classes, respondents placed higher IT priorities and the unavailability of adequate funding at the top of their challenge rankings. (See Tables 4-4 and 4-5.)

If respondents say that IdM’s benefits are important and identify pressing motivations for pursuing them, why do so many find it challenging to make IdM a priority and fund it? The funding constraint is not too surprising. Funding was named as the top strategic issue in the EDUCAUSE Current Issues Survey in every year from 2003 to 2005, and in the 2006 data it fell to second place—behind security and IdM (Maltz, DeBlois, & EDUCAUSE Current Issues Committee, 2005; see also the forthcoming report in *EDUCAUSE Quarterly*, Vol. 29, No. 2). As the ECAR study *Information Technology Funding in Higher Education* reported in 2004, a tight budget climate settled on U.S. higher education in 2001 following the dot-com collapse and persisted across several years (Goldstein, 2004). The effects were still visible among our survey respondents. Twenty-five percent reported decreasing central IT budgets in the last three years, while 22.9 percent reported increases; the rest had flat budgets. Of those with decreasing budgets, 47.5 percent named inadequate funding as a top-three challenge,

**Table 4-4. What Are the Challenges to Your Institution in Pursuing IdM?**

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Percentage Choosing Rank Order</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Higher IT priorities</td>
<td>28.5% 14.4% 10.7%</td>
<td>53.6%</td>
</tr>
<tr>
<td>Adequate funding is not available</td>
<td>19.1% 9.9% 9.4%</td>
<td>38.5%</td>
</tr>
<tr>
<td>Difficulty developing campus policies and procedures</td>
<td>6.7% 9.4% 13.6%</td>
<td>29.8%</td>
</tr>
<tr>
<td>Lack of IT staff expertise</td>
<td>7.4% 13.4% 7.4%</td>
<td>28.3%</td>
</tr>
<tr>
<td>Lack of ownership of IdM by a central group</td>
<td>5.5% 7.9% 7.9%</td>
<td>21.3%</td>
</tr>
<tr>
<td>Technical solutions are too immature</td>
<td>5.5% 6.9% 5.2%</td>
<td>17.6%</td>
</tr>
<tr>
<td>Data integrity problems (consistency, accuracy, etc.)</td>
<td>5.7% 5.5% 5.7%</td>
<td>16.9%</td>
</tr>
<tr>
<td>Lack of institutional senior management’s support</td>
<td>4.5% 5.7% 5.7%</td>
<td>15.9%</td>
</tr>
<tr>
<td>Problems with institution’s technologies/infrastructure</td>
<td>2.5% 5.5% 6.5%</td>
<td>14.4%</td>
</tr>
<tr>
<td>Problems with vendor software and support</td>
<td>2.7% 5.5% 2.7%</td>
<td>10.9%</td>
</tr>
<tr>
<td>Lack of acceptable ROI</td>
<td>3.0% 2.2% 4.2%</td>
<td>9.4%</td>
</tr>
<tr>
<td>Other</td>
<td>0.5% 0.5% 1.5%</td>
<td>2.5%</td>
</tr>
</tbody>
</table>

(Three responses allowed, ranked 1 to 3)
while only 22.8 percent of those with rising budgets did so.

We did not ask respondents to identify specific “higher IT priorities” that challenge IdM on their campuses, but we did ask those who were not participating in IdM projects to explain why not in an open-response format. Some answers echoed empirical findings from our 2004 IT funding study, in which respondents named administrative systems and network services as the two largest anticipated areas of IT investment over the period 2004–2007. “Other priorities; resources; just beginning an ERP implementation,” one respondent answered. “[O]ther priorities with higher importance, i.e., infrastructure upgrades,” wrote another.

It is likely, however, that some of these higher priority projects are actually getting IdM work done. As we report in greater detail in Chapter 8, only slightly more than one in four respondents told us they had stand-alone IdM projects. Many more reported bundling IdM projects with items that our 2004 funding study highlighted, including ERP and infrastructure buildouts. At Anne Arundel Community College, enhancements to the student portal’s sign-on capabilities were “not specifically identified as identity management,” says J. David Becker, Anne Arundel’s chief technology officer. But, he adds, “we hope to achieve the outcome, as it’s affiliated with other projects. [There’s] a cluster of activities that have IdM outcomes.”

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Rank, by Carnegie Class</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All</td>
</tr>
<tr>
<td>Higher IT priorities</td>
<td>1</td>
</tr>
<tr>
<td>Adequate funding is not available</td>
<td>2</td>
</tr>
<tr>
<td>Difficulty developing campus policies and procedures</td>
<td>3</td>
</tr>
<tr>
<td>Lack of IT staff expertise</td>
<td>4</td>
</tr>
<tr>
<td>Lack of ownership of IdM by a central group</td>
<td>5</td>
</tr>
<tr>
<td>Technical solutions are too immature</td>
<td>6</td>
</tr>
<tr>
<td>Data integrity problems (consistency, accuracy, etc.)</td>
<td>7</td>
</tr>
<tr>
<td>Lack of institutional senior management support</td>
<td>8</td>
</tr>
<tr>
<td>Problems with institution’s technologies/infrastructure</td>
<td>9</td>
</tr>
<tr>
<td>Problems with vendor software and support</td>
<td>10</td>
</tr>
<tr>
<td>Lack of acceptable ROI</td>
<td>11</td>
</tr>
</tbody>
</table>

*Table 4-5. IdM Challenge Rankings, by Carnegie Class (Based on percentage of respondents ranking challenge as 1, 2, or 3; blank where no respondents selected motivator)*
probable, then, that without explicitly naming IdM as a high-priority item, some institutions are still acting on their IdM motivators—even as they recognize the “challenge” of doing so when other projects soak up resources.

Organizational Challenges

The challenge of IdM priority relates closely to the second major cluster of high-ranked challenges, organizational issues. Almost 30 percent of respondents named the difficulty of developing campus policies and procedures among their top challenges, making it the third-highest-ranked item overall, while 21.3 percent cited lack of IdM ownership by a central group.

Our qualitative interviews suggest that the primary obstacle in policy development is cross-departmental communication and consensus-building. Because identity issues touch on so many business and academic processes, addressing them involves breaking through organizational boundaries and bringing together departments accustomed to “owning” and using data solely for their own purposes. Administrators pursuing IdM commonly discover a lack of campus-wide agreement on even the most basic definitions—for example, who is a student or faculty member. “All sorts of people think they know what a student is,” Dalhousie’s Sherwood says. “We want a document that all the various areas agree on.”

To resolve such issues, the University of Oregon created an IdM policy committee with executive-appointed representation from each major functional area. Susan Hilton, who is director of administrative services at Oregon and chairs the committee, says it has “worked better than we ever expected” but notes that the process has also been slower than expected. “I was really surprised when we began to discover the complexity of the problem,” she says. “There was always one more meeting necessary. It was like turning over rocks and finding more and more bugs.”

Without effective cross-institutional communication, IdM runs the risk of being viewed as an IT problem; thus its advocates cannot muster the political base necessary to give it higher priority. “No one cares about it but [the IT unit],” one respondent complained in an open response. “We may need a local crisis,” wrote another, “to drive leadership toward this important undertaking.”

Technical Maturity Challenges

While IdM’s immaturity was a factor in the challenge results, it was largely a midrange issue. Only 17.6 percent of respondents named IdM solutions’ technical immaturity as a top-three challenge, and fewer still (10.9 percent) named problems with vendor software and support.

Nevertheless, interviewees mentioned issues relating to the overall maturity of commercial and open source solutions and the difficulty of bridging the deeply embedded, often homegrown, identity mechanisms of older systems and the more loosely coupled approach of modern solutions. At St. Mary’s University of Minnesota, Chad Kjorlien, director of instructional technology, says that he thinks the field is maturing fast but still sees value in a wait-and-see approach. “Ultimately as standards shape up and vendors incorporate them, that will determine which way we go,” he says. “Our strategy is basically to hold off on the full IdM solution and work on the pieces—localized enhancements that can be developed while we wait for IdM solutions to truly come online.”

One of the more highly ranked factors, lack of staff expertise, might also manifest resource constraints at some institutions, but we found no significant association between this item and decreasing budgets or the perception that the institution is not providing adequate resources for IdM. Instead, the staffing challenge may be an aspect of IdM’s early state as an operational technol-
ogy, which in turn leaves the market supply of skills limited. Noreen Hogan, principal technologist at the University of Oregon, observes that “the middleware area is somewhat different than many of the classic IT jobs…it is a bit harder to find [the needed] breadth of knowledge.”

**Challenges across Carnegie Class and in Canada**

A look at how rankings differed across Carnegie classes reveals much the same pattern as in the motivations data: general similarity at the top of the list, with more differentiation below (see Table 4-5). Master’s and baccalaureate institutions ranked lack of IT staff expertise somewhat higher than did the other Carnegie classes. Baccalaureate and associate’s institutions displayed greater concern about ROI issues and somewhat less about technical maturity and data integrity.

Overall, the differentiation in rankings among Carnegie classes was not dramatic. In some cases, however, the rankings alone do not convey the full difference between institution types. Although higher IT priorities, for example, was the top challenge identified by both doctoral and associate’s institutions, only 43 percent of doctorals cited it, while 64.6 percent of AA institutions did so.

Once again, Canada showed a different pattern. Though, like their U.S. counterparts, Canadian respondents ranked higher IT priorities as their top challenge, they also ranked policy and procedures development high. They were considerably more concerned than U.S. respondents about technical issues such as immature solutions and problems with institutional infrastructure, while being less concerned about funding. They were also more optimistic about IT staff expertise. In general, the Canadian data suggest a more hands-on approach to IdM.

**Security and Regulatory Compliance**

As noted above (see Table 4-2), our respondents named security as their top IdM motivator and regulatory compliance as their third highest. They also rated security-related IdM benefits as highly important to their institutions (see Figure 4-1). These survey findings fit comfortably alongside proclamations in all sorts of IT forums that higher education faces security and regulatory crises. Yet given the chance to express their level of agreement with statements about their institutions’ security and compliance postures, our respondents conveyed a remarkable degree of satisfaction (see Table 4-6).

**Table 4-6. Security and Regulatory Compliance Self-Ratings**

<table>
<thead>
<tr>
<th>Security/Compliance Statement</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The central data, networks, and applications at our institution are secure.</td>
<td>3.99</td>
<td>0.767</td>
</tr>
<tr>
<td>My institution is compliant with regulatory requirements affecting student information (such as FERPA, SEVIS).</td>
<td>4.41</td>
<td>0.663</td>
</tr>
<tr>
<td>My institution is compliant with regulatory requirements affecting health information (such as HIPAA).</td>
<td>4.23</td>
<td>0.757</td>
</tr>
<tr>
<td>My institution is compliant with regulatory requirements affecting financial records (such as GLB Act).</td>
<td>4.14</td>
<td>0.776</td>
</tr>
</tbody>
</table>

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)
Every measure we asked about averaged either a borderline “agree” (4 on a scale of 5) or higher response. Among those respondents providing a level of agreement or disagreement (that is, factoring out “don’t knows”), 79.1 percent agreed or strongly agreed that their institutions’ central data, networks, and applications were secure. The mean 3.99 response to this statement was considerably higher than the mean response to a similar question in our 2003 security study (Kvavik & Voloudakis), which was 3.32 when translated to our IdM study scale.1

Respondents’ agreement or strong agreement was even higher for regulatory compliance, totaling 93.1 percent for student information, 86.8 percent for health information, and 84.7 percent for financial records. Most of the remainder were neutral. Combined disagree/strongly disagree figures were 3.8 percent for the statement about security of data, networks, and applications, and even lower for all the compliance statements.

Respondents also reported low levels of IdM-related security incidents (see Figure 4-2). Asked how many significant security incidents related to user identification, authentication, or authorization their institutions had experienced in the last two years, slightly more than half of respondents reported none, and fewer than one in five reported more than one.

We should view these results with some caution. Self-reported performance measures are often optimistic and may be especially so in such sensitive areas. Also, agreement that central IT systems are secure does not equate to confidence in the many distributed systems where vulnerabilities may be highest. Finally, given the dynamic and unpredictable nature of these issues, an expression of current agreement should not be understood as an absence of concern about future weaknesses.

Still, our results do not seem to express a sense of emergency about central IT security and regulatory compliance among most of our respondents. This doesn’t necessarily contradict the finding that these areas are high motivators; after all, many institutions may feel confident precisely because they’ve invested in them and made them a priority. But it does suggest that respondents consider their immediate IT security and compliance challenges to be manageable. To the extent that these issues drive IdM investment, we expect that such attitudes would lead institutions to approach it in an evolutionary and

![Figure 4-2. Significant Security Incidents Related to IdM Processes in Past Two Years](image-url)
measured way rather than as a radical remedy to desperate operational problems.

**Perceptions of Senior Management Understanding and Support**

Somewhat surprisingly, given IdM’s immaturity, lack of senior management support did not rank high in the IdM challenges results (see Table 4-4). Responses to our more detailed questions about senior management attitudes corroborated this. However, the picture was mixed, with much optimism about senior management’s understanding of IdM benefits yet skepticism about their appreciation of its costs (see Table 4-7).

Asked how much they agreed with the statement that senior management at their institution “is willing to address the policy issues related to identity management,” 55.1 percent agreed or strongly agreed, and only 13.5 percent disagreed or strongly disagreed. (The rest were neutral.) Forty-one percent also agreed or strongly agreed that “senior management understands the benefits of investing in identity management,” but responses were more polarized for this statement: more than a third (35.4 percent) disagreed or strongly disagreed. We found little significant difference by Carnegie class or between public and private institutions, though we did find that institutions with 25,000 or more students tended to rate these senior management attitudes higher than smaller institutions.

The greatest pessimism emerged when we asked about senior management’s understanding of IdM costs: 56.4 percent answered on the disagree/strongly disagree side of the ledger and only 16.9 percent on the agree/strongly agree side.

Any situation in which a potential sponsor understands benefits better than costs is a red flag to an experienced CIO. We speculate that this mismatch may be leading some IT leaders to bide their time until they feel they can better educate their institution’s leadership, or until the budget climate improves—or, for that matter, until they themselves feel more confident about IdM’s costs and benefits. Such caution would be consistent with some of our study’s other findings, including the bundling of IdM with other projects, low adoption levels of advanced IdM technologies, and a generally IT-centered approach to identity projects (see Chapters 6, 7, and 8).

The surprising reserve of positive perceptions about understanding of benefits and willingness to address policy issues probably owes much to growing executive awareness of security issues in recent years. At Northern Kentucky University, where the IdM initiative is firmly rooted in security concerns, Gary Pratt reports that “senior management is actively

<table>
<thead>
<tr>
<th>Statement</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>My institution’s senior management is willing to address the policy issues related to IdM.</td>
<td>3.48</td>
<td>0.892</td>
</tr>
<tr>
<td>My institution’s senior management understands the benefits of investing in IdM.</td>
<td>3.11</td>
<td>1.079</td>
</tr>
<tr>
<td>My institution’s senior management understands the costs of IdM.</td>
<td>2.54</td>
<td>0.947</td>
</tr>
</tbody>
</table>

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)
engaged in IT security and privacy policies. They want to be sure we have the foundation in place to secure our personal data.”

How well campus IT units kindle the flame of executive attention they now enjoy could have important implications for IdM. The value of senior leadership support is a frequent theme in IT effectiveness studies. In recent years, ECAR studies on business process performance, networking, IT alignment, and IT security have all found that executive support is a factor in success (Kvavik & Goldstein, 2005; Pirani & Salaway, 2005; Albrecht et al., 2004; Kvavik & Voloudakis, 2003). As we report in Chapter 9 and below (see Table 4-10), we also found that IdM resource sufficiency, capability, and cost savings were all significantly associated with respondent perceptions of the senior management attitudes reported above.

**IdM Resources**

Asked whether they thought their institution provides the resources needed for IdM, respondents presented us with another mixed bag: slightly more than one-third (36.0 percent) disagreed to some extent, slightly fewer (31.9 percent) agreed, and the rest were neutral (see Figure 4-3). Their mean level of agreement on the 1-to-5 scale, at 2.96 (standard deviation = 1.023), was more positive than their assessment of senior management’s understanding of cost but less so than the management policy and understanding of benefits items.

We found no significant associations between perception of resource sufficiency and Carnegie class, institution size, private/public control, or budget climate. However, perceived resource sufficiency was associated with the institution’s technology posture. Institutions that aggressively adopt technology tend to have higher resource sufficiency responses, as do those where the IT unit aims for competitive differentiation rather than utility services (see Tables 4-8 and 4-9).

We also found a relationship between resource sufficiency and senior management attitudes. Respondents reporting greater

![Figure 4-3. Institution Provides Needed IdM Resources (N = 394)](image)
agreement with statements about senior management willingness and understanding also tend to report higher levels of resource sufficiency (see Table 4-10). While it is not surprising that IT administrators who feel they’re getting enough resources also agree that executives “understand” the situation, this finding does suggest that it is difficult to fund IdM purely from “budget dust” or other funding streams that don’t depend much on senior management awareness and support.

Our results suggest that IdM has not yet become a funding “no brainer.” As IdM technology matures, within a few years it will find resources in more mainstream, less cutting-edge IT environments. Still, with only about a third of institutions now reporting that they have what they need for IdM, it appears that both IT and executive leadership will have much to say about whether IdM blooms into a strategic, enterprise-wide infrastructure or remains a collection of IT-centered solutions pursued in the background and as a side effect of other, better-funded projects.

**Table 4-8. IdM Resource Sufficiency, by Institutional IT Goals (N = 391)**

<table>
<thead>
<tr>
<th>Which of the following best describes your institution’s goals for IT?</th>
<th>Institution Provides Needed Resources</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide IT infrastructure and services to create institutional competitive advantage</td>
<td>3.67</td>
<td>1.137</td>
</tr>
<tr>
<td>Provide IT infrastructure and services that further the institution’s strategic goals</td>
<td>3.00</td>
<td>0.986</td>
</tr>
<tr>
<td>Provide appropriate IT infrastructure and services to different users, based on their needs</td>
<td>2.92</td>
<td>0.893</td>
</tr>
<tr>
<td>Provide reliable IT infrastructure and services at the lowest cost</td>
<td>2.37</td>
<td>0.999</td>
</tr>
</tbody>
</table>

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)

**Table 4-9. IdM Resource Sufficiency, by Technology Adoption Strategy**

<table>
<thead>
<tr>
<th>What best characterizes your institution in terms of adopting new technologies?</th>
<th>Institution Provides Needed Resources</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Innovator (first 2.5%)</td>
<td>3.67</td>
<td>0.888</td>
</tr>
<tr>
<td>Early adopter (next 13.5%)</td>
<td>3.29</td>
<td>1.168</td>
</tr>
<tr>
<td>Early majority (next 34%)</td>
<td>3.00</td>
<td>0.941</td>
</tr>
<tr>
<td>Late majority (next 34%)</td>
<td>2.62</td>
<td>0.971</td>
</tr>
<tr>
<td>Laggards (last 16%)</td>
<td>2.17</td>
<td>0.753</td>
</tr>
</tbody>
</table>

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)
Typically, their advice includes assessing existing identity assets, formally analyzing risks, collecting key metrics and, above all, developing a clear business rationale for IdM investments.

The NSF Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium’s checksheet for IdM project readiness, for example, asks institutions to evaluate their ability to develop a business case by rating the extent to which (among other items) leadership and technical staff understand IdM issues, business drivers are known, campus data stewards have been identified, and identity policies are well documented. Burton Group encourages building a business case that, in part, takes into account the costs and security risks associated with a weak identity infrastructure. These risks range from the burden of identity-related help desk calls to the dangers of not terminating account privileges promptly when employees leave. Organizations like Gartner and The Open Group likewise recommend structured, empirically informed approaches to enterprise IdM.

We hypothesized early in our study that we would find relatively few institutions with deep IdM experience but many that were considering it or in the process of adoption. (Our results largely confirmed this hypothesis.) As a result, we asked respondents how they learned about IdM, what metrics they kept, whether they documented assets and policies, and what sort of planning they had carried out—in short, how well prepared they are to

<table>
<thead>
<tr>
<th>Senior Management Attitude</th>
<th>Attitude Rating</th>
<th>Institution Provides Needed Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Mean</td>
</tr>
<tr>
<td>Willing to address the policy issues related to IdM</td>
<td>Strongly agree</td>
<td>4.09</td>
</tr>
<tr>
<td></td>
<td>Agree</td>
<td>3.21</td>
</tr>
<tr>
<td></td>
<td>Neutral</td>
<td>2.72</td>
</tr>
<tr>
<td></td>
<td>Disagree</td>
<td>2.02</td>
</tr>
<tr>
<td></td>
<td>Strongly disagree</td>
<td>1.89</td>
</tr>
<tr>
<td>Understands the benefits of investing in IdM</td>
<td>Strongly agree</td>
<td>4.14</td>
</tr>
<tr>
<td></td>
<td>Agree</td>
<td>3.28</td>
</tr>
<tr>
<td></td>
<td>Neutral</td>
<td>2.94</td>
</tr>
<tr>
<td></td>
<td>Disagree</td>
<td>2.48</td>
</tr>
<tr>
<td></td>
<td>Strongly disagree</td>
<td>1.69</td>
</tr>
<tr>
<td>Understands the costs of IdM</td>
<td>Strongly agree</td>
<td>4.27</td>
</tr>
<tr>
<td></td>
<td>Agree</td>
<td>3.76</td>
</tr>
<tr>
<td></td>
<td>Neutral</td>
<td>3.32</td>
</tr>
<tr>
<td></td>
<td>Disagree</td>
<td>2.61</td>
</tr>
<tr>
<td></td>
<td>Strongly disagree</td>
<td>2.08</td>
</tr>
</tbody>
</table>

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)
act on their plans in light of the best practices that advisory groups suggest.

The items we asked about do not constitute a comprehensive checklist but are common to many different approaches to IdM and contribute some key inputs to institutional decision making in a wide variety of scenarios.

**Monitoring IdM**

Our respondent institutions are paying a lot of attention to IdM. Asked to identify which of six sources of IdM information they monitored, 93.1 percent named at least one, and the median (half above, half below) number monitored was four. Doctoral institutions were the most active monitors in every area, usually by a wide margin, though associate’s institutions were close behind them in the areas related to intra-higher-education monitoring (see Figure 4-4). We also found an association between size and monitoring activity: in general, larger institutions reported higher rates of monitoring.

Overall, respondents seemed to emphasize monitoring other higher education institutions for IdM information. Three-fourths (75.2 percent) reported monitoring the directions of peers, and two-thirds (66.3 percent) the directions of leading institutions. Close behind were technical standards and technology vendors. The advisory groups whose work helped inspire some of our questions were cited by 40 percent or more of respondents and a healthy majority of doctorals, but they were still the least monitored sources of IdM information.

**IdM Metrics**

Our questions about metrics covered cost, user service, and security exposure issues frequently mentioned in treatments of the IdM business case. Because many help desk calls involve password resets and other identity-related matters, this can be a key area for justifying an improved environment. We also asked whether institutions tracked the overall number of account management transactions they carry out, and, because slow extension of privileges is a drag on productivity and user satisfaction, whether they tracked the aver-
average time for creating new IDs and enabling authorized services. On the other end of the employment life cycle, where the failure to disable privileges for terminated employees (both permanent and temporary) is a security risk, we asked if institutions measured how long it took to close out user IDs and if they kept track of enabled accounts of temporary affiliates with expired contracts.

We found that, on the whole, responding institutions were far less active in keeping IdM metrics than in monitoring IdM information sources (see Figure 4-5). The median number of metrics kept was two; 19.9 percent of respondents kept none of the metrics we listed, and another 25.8 percent kept only one. The help desk, where performance measurement has long been part of the IT culture, was the most actively monitored area, with 71.5 percent of respondents saying they kept track of user access problems. But only half (52.4 percent) of institutions tracked the volume of account creations, changes, and deletions, and only one in five or fewer maintained the other metrics we asked about. We found little significant difference by Carnegie class or institution size, though we did find that large institutions and aggressive technology adopters tracked help desk statistics at higher rates.

It is possible that institutions are maintaining other IdM metrics that we didn’t ask about. If our findings are representative of the overall state of IdM measurement, however, most institutions will have a hard time assembling the empirical evidence necessary to evaluate their IdM performance and decide whether further investment is warranted.

### Documenting IdM Data Sources, Risks, and Needs

As our IdM challenges and senior management findings highlighted, a key obstacle to improving IdM environments is the proliferation of uncoordinated data definitions and identity practices across different campus units. We found that institutions seem to be addressing the problem through the documentation activities shown in Table 4-11, though most of the work remains planned or incomplete.

About one-third (32.5 percent) report that they’ve completed documenting campus data owners, and another third (33.5 percent) are in the process of doing so. Institutions have made considerably less progress with the data definitions themselves, with only 15 percent reporting completion. Somewhat surprisingly, only 26.2 percent of respondent institutions had completed an inventory of campus identifiers—an indicator of just how decentralized identity creation is. Despite years of rising security awareness, barely one in eight institutions (12.8 percent) has completed a security and privacy risk assessment. Low as this is, when combined with those in progress, the

![Figure 4-5. IdM Metrics Kept](image-url)
total of 47.2 percent actively doing risk assessments shows a substantial rise from a 2003 ECAR security study (Kvavik & Voloudakis), which found that 30 percent of institutions had undertaken them.

Finally, though a majority of respondents said they use vendors as a source of information about IdM, very few (5.5 percent) have formalized contacts in the form of an RFI or RFP, and most say they don’t plan to. One interviewee who had done so noted that the RFP process was more arduous than usual. “We had problems with noncompliant and out-of-budget bids,” says William Pritchard, vice chancellor for information technology at Foothill-DeAnza Community College District, where procurement rules require a bid process. “The complexity of identity management led to interesting challenges, and we needed to work with our purchasing department more closely. We found we had to loosen up the mandatory requirements to get a workable final procurement.”

Table 4-11. Documentation of IdM Data Sources, Risks, and Needs (N = 401)

<table>
<thead>
<tr>
<th>Documentation Activity</th>
<th>Completed</th>
<th>In Progress</th>
<th>Planning to Do</th>
<th>Not Planning to Do</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documented campus data custodians/owners</td>
<td>32.5%</td>
<td>33.5%</td>
<td>23.8%</td>
<td>6.5%</td>
<td>3.8%</td>
</tr>
<tr>
<td>Inventory of campus identifiers (such as used by library, e-mail, etc.)</td>
<td>26.2%</td>
<td>33.4%</td>
<td>24.7%</td>
<td>10.0%</td>
<td>5.7%</td>
</tr>
<tr>
<td>Documented data definitions, reconciling differences between different data sources</td>
<td>15.0%</td>
<td>38.3%</td>
<td>28.8%</td>
<td>10.8%</td>
<td>7.3%</td>
</tr>
<tr>
<td>Risk assessment of data access security and privacy practices</td>
<td>12.8%</td>
<td>34.4%</td>
<td>36.2%</td>
<td>11.8%</td>
<td>4.8%</td>
</tr>
<tr>
<td>Released an RFI or RFP for IdM</td>
<td>5.5%</td>
<td>4.5%</td>
<td>16.1%</td>
<td>62.0%</td>
<td>11.8%</td>
</tr>
</tbody>
</table>

Some 30.8 percent of respondents at institutions this size reported completing risk assessments, versus 4.3 percent of those from campuses with 2,000 or fewer FTE students. (The other categories ranged from 12.2 to 19.2 percent.) The contrast was almost as stark for documenting data custodianship: 72.4 percent of the 25,000-plus institutions had completed it—more than double the percentage of those in the next smaller size range (34.0 percent among institutions of 15,001–25,000 students) and more than three times the rate (21.1 percent) among institutions of 2,000 or fewer students.

As we report in Chapter 6, we found that completion rates of some documentation activities tend to rise with advancing stages of IdM technology adoption. These higher rates, however, are most evident in the later rather than the preparatory phases of adoption, and even among fully operational institutions, many have not completed documentation activities. Overall, the most striking thing about the documentation results was the pattern of relatively low completion, with high rates of in-progress and planned activity. We found the same combination of modest completion with ambitious intentions when we looked at IdM planning activity.
Documenting IdM Policies

Perhaps because of the role that policies play in day-to-day operations, institutions were generally more likely to have completed documenting IdM policies than IdM data sources and risks (see Figure 4-6; see also Table 4-11). Half or more had completed policies for establishing identity (50.5 percent) and for user authentication (57.6 percent). User authorization, generally a less developed area in other IdM aspects, was reported at 40.8 percent. Most other institutions reported policy development in progress or partially completed.

Although identity establishment and authentication policy documentation were both significantly associated with Carnegie class, tending to be more prevalent in the research and MA institutions, these areas did not produce the wide discrepancies found in other IdM documentation areas. Fifty-eight percent of doctoral institutions had completed identity establishment policies, versus 38.3 percent of associate’s institutions. The other Carnegie classes fell in between. For authentication, the figures were 71.7 percent for doctorals and 52.1 percent for BA institutions, with the others in between. At 16.7 percent in each category, Canadian institutions reported much lower rates of completed identity establishment and authentication policies.

Planning for IdM: Making the Case and Making a Plan

Because we hypothesized that different kinds of planning might be going on at respondent institutions, we asked about two different kinds of planning documents. In asking about the status of documented business cases in any IdM area, we were looking for evidence of planning explicitly linked to business justifications, even if only in select aspects of identity activity. We also asked more generally about IdM plans, which might be oriented more toward technical considerations and implementation.

The results show an interesting relationship between the two planning types (see Figure 4-7). As with many IdM areas that we studied, incomplete and planned activity far outstrips the amount completed, with only 11.8 percent of respondents having a completed IdM plan and 16.5 percent a completed business case. Although completion results were slightly higher for the business case, institutions were more likely to be currently carrying out or anticipating an IdM plan. More than one in four institutions (28.0 percent) had no plans for a
We found a strong relationship between the two types of planning. Some 57.6 percent of those respondents who have completed a business case have also completed an IdM plan, and all of the rest reported that they have a plan in progress or are planning to complete one. Nevertheless, half (50.9 percent) of those who said they had no plans for a business case still either had an IdM plan or planned to create one. In short, while most institutions that engage in IdM planning include a business case component, a significant number do not.

IdM planning was associated with both Carnegie class and institution size, with size showing the stronger relationship. Respondent institutions with more than 25,000 students were more than twice as likely to have completed a business case as those with 15,001–25,000 students (see Figure 4-8) and more than 9 times as likely as those with 2,000 or fewer students. The disproportion was even greater for completed IdM plans (see Figure 4-9), though a larger proportion of respondents overall expected eventually to complete such a plan.

Doctoral institutions, as might be expected, dominated the Carnegie figures in both areas. Their completion rate for a business case, at 32.3 percent, was five times higher than that of the lowest group, bachelor’s (6.3 percent). (Because the great majority of our BA respondents were from institutions with fewer than 4,000 students, this is more likely to be an effect of size than of institutional mission.) The gap was proportionately higher for IdM plan completions: 27.4 percent for doctorals versus 2.2 percent for associate’s institutions, which had the lowest IdM plan completion rate.

The pattern of domination by doctorals and other large institutions makes sense, given how new IdM is. These are the places where cutting-edge technologies are most often first adopted, where IT resources are greatest, and where the common denominator of all identity challenges—people—is most abundant.

As we report in Chapter 6, IdM plan completion rates tend to increase with more advanced stages of IdM technology adoption (see Table 6-6). The greatest jumps in completion rates, however, tend to appear in the later rather than the earlier stages of adoption, and, even so, most fully operational respondents are without an IdM plan.

If what our respondents told us about their plans actually happens, however, the pattern of
limited business case and plan completion will be only a passing phase. Assembling all those who have a business case or IdM plan and those who are in progress or “planning to plan” reveals that the great majority of our respondent institutions expect to complete such activities at some time in the future. Will this anticipated wave of IdM planning leave institutions well prepared to pursue ambitious IdM projects?

Our follow-up interviews with survey respondents revealed a wide variety of formality, scope, format, and completeness to IdM planning documents. The IdM plans interviewees described ranged from simple lists of bulleted items spanning a few pages to lengthy formal reports written with the help of outside consultants. Some respondents candidly confessed that they were working from plans that had become obsolete. Those who had no formal plan, or worked from relatively simple ones, often described environments in which IdM work was an operational evolution or bundled in with other projects. At Marist College, Harry Williams, director of technology and systems, hasn’t found it necessary to work from a plan because IdM “was never a formal project but has always been part of other projects…we’re moving forward at a slow and steady pace and are happy with our progress.”

Where formal plans are in place, they may serve as implementation planning documents with an orientation toward the IT environment’s technical and policy direction. Faced with a major enterprise re-
source planning implementation and other technical challenges, the University of Notre Dame has pursued an IdM planning regime linked to the project management process. Gordon Wishon, who holds the positions of CIO, associate vice president, and associate provost at Notre Dame, retained Burton Group to produce a report identifying policy issues and outlining a preliminary IdM architecture. Wishon’s team now includes a full-time IdM project manager who is further developing the initial plan. Taking this formal approach, Wishon says, “allows us to apply a rigorous program management methodology, as well as to raise the level of visibility of IdM, especially to the campus leadership.”

That fewer institutions expect to do business cases than IdM plans may stem from the tendency of identity initiatives to start in, and often stay within, the IT unit. Where the technical requirements seem imperative, projects are IT funded, and planned progress is evolutionary, IT units may see no need for a formal business case—at least until IdM activity reaches a critical mass that requires “outside” campus funding. “We don’t have a business case” for an in-progress single sign-on project, says Thomas Board, director of information system architecture at Northwestern University. “We have a technical case with business advantages.” At Notre Dame, CIO Wishon readily lists the business reasons that gave rise to the institution’s high-profile IdM project:

◆ protection of sensitive resources,
◆ a changing regulatory landscape,
◆ data integrity,
◆ collaboration enablement,
◆ improved provisioning/deprovisioning response, and
◆ the ability to delegate access approval responsibilities.

Even so, the university budget process has required only an informal case. “I have not had to argue for more resources…we do have [enough] to, in part, get the project off the ground,” Wishon says. “A formal business case has not been necessary to date, though it may be in the future.”

The variety in scope and formality that we discovered in IdM planning leads us to caution against assuming from the raw numbers that 85 percent of institutions will soon possess formal, comprehensive IdM plans. Yet neither do most “plans to plan” seem to be merely wishful thinking. Rather, they may express unease with the informality or fragmentation that has so far characterized IdM processes, and they may recognize that identity issues are becoming more complex and are moving beyond purely IT concerns.

At the same time, it is important to remember that the actual levels of business case and IdM plan completion are low. Furthermore, institutions must attend to the quality, not just the quantity, of IdM planning. Several interviewees with IdM project experience told us that the need for careful and formal planning was one of the lessons they had learned. Speaking of his campus’s enterprise directory project, Peter Murray, vice president for information technology and CIO at the University of Maryland, Baltimore, is unequivocal: “You need a plan and it needs to be communicated. It can’t be a low-visibility back-end project and be successful.” Linda Hilton, CIO of the Vermont State Colleges, says that their multicampus consolidated user logon project eventually overflowed well beyond the statement of work they started out with. “Looking back, we were too casual,” she says. “A little more awareness that it was something enormous would have saved us much time and effort.”
**Summing Up IdM Readiness**

By the standards that IdM advisory groups recommend, most institutions are not currently well positioned to take on the ambitious plans to evaluate and incorporate IdM technologies that we describe in Chapters 5 through 8. There are some bright spots, however: respondent institutions are actively informing themselves about IdM, and documentation of policies is also fairly strong. Slightly more than half of institutions report completed policies in the key areas of identity establishment and authentication, and most of the rest are working on them. As we report in Chapter 6, respondents also tend to report more complete documentation and planning activity in some areas as they move to more advanced phases of adoption. But in critical areas such as documenting data custodianship, inventorying identifiers, and creating business cases or IdM plans, planned or in-progress work far outstrips completed work. Also, IdM measurement, documentation, and planning achievements so far have generally been disproportionately concentrated among doctoral and large institutions, and are hardly universal even there.

IdM metrics is an especially worrisome area, because the low rates of measurement that we found suggest that few institutions can assemble reliable performance and cost information to inform the business case and IdM planning efforts—not to mention the implementations—many say they intend to carry out. Given the emphasis on security and privacy that we found in the motivations data, risk assessment is another area of weakness that could compromise the robustness of IdM projects. Both areas are also important for helping IT units gain credibility with senior leaders and other line-of-business managers.

All this could change radically, of course, if institutions complete the readiness initiatives that they have in progress or plan to carry out. These expectations, however, should be considered in light of the IdM challenges data that stress the competition of other priorities and tight funding. No doubt some institutions will be tempted to shortcut past foundation-building practices and muddle through with an ad hoc approach to IdM. Those that want to make IdM a strategic tool, however, may find metrics, documentation, and planning to be the most productive areas for near-term investment.

**Endnotes**

1. Because the Likert scale used in our 2003 security study (1 = strongly agree, 5 = strongly disagree) was the reverse of our IdM study scale, the data presented in that study must be translated to be comparable. The overall security rating mean of 2.68 in the security study equals 3.32 by the IdM study scale (1 = strongly disagree, 5 = strongly agree). See Kvavik and Voloudakis, 2003, Table 8-1, p. 105.

5

Establishing Identity and User Authentication

Who then to frail mortality shall trust
But limns on water, or but writes in dust.
—Francis Bacon

Key Findings

◆ Among respondent institutions that have completed a count of the person identifiers they issue, eight of 10 report 20 or fewer identifiers.

◆ Responding institutions’ ability to meet potential guidelines for stricter identifier policies is patchy. About one-third of institutions practice differentiation of identity proofing requirements for different constituencies. Slightly fewer than four in 10 report that all identifiers they issue are “unique for all time,” though another 30 percent carry out this practice in some cases.

◆ Only a little more than one-third of U.S. institutions report using Social Security numbers for identifiers, and all but a handful (3 percent) expect to discontinue their use in some time frame.

◆ User self-service for basic IdM functions such as password resets is widespread, but functions for personalizing identity profiles, such as setting privacy preferences, are available only at a minority of institutions.

◆ Respondent institutions rely overwhelmingly on passwords, both conventional and strong, for authenticating user network access. About a quarter of institutions use Kerberos, with doctoral institutions about twice as likely as other Carnegie classes to have it in use. Multifactor network authentication methods mentioned in the survey, including hard tokens, PKI (public key infrastructure), and biometrics, are in use at fewer than three in 10 institutions. About 60 percent of those reporting no such use also have no definite plans to adopt them.

◆ Biometrics use for network authentication is very low among respondent institutions (3 percent), but planned use is about four times as high.
The most fundamental aspect of IdM is ensuring that people are who they say they are. Issuing online identities to qualified parties, maintaining those identities properly, and accurately and securely evaluating the credentials attached to them are the basic processes that allow constituents to make themselves known to the IT infrastructure and gain access to its resources.

This chapter opens at the point where the user/IT infrastructure relationship begins: establishing identity and maintaining identities. We then look in depth at our respondents’ adoption of authentication technologies and the policies and metrics that accompany them.

Creating and Maintaining Identifiers

Every higher education institution knows its student, faculty, and staff headcounts in fine detail. But how do they ensure that they know who those people are before they issue them identifiers, and do institutions know how many virtual identifiers might be issued to constituents once they join the community?

Identity Proofing

Identity proofing is the process of uniquely verifying an individual’s identity before issuing him or her new credentials such as an online identifier or identity card. In a higher education setting, it may occur in such departments as admissions, the registrar’s office, or human resources, where it becomes the basis for the individual’s entry into systems of record. Because identity proofing establishes the initial trust relationship that leads to the issuance of identifiers and granting of privileges, its use and degree of strictness help determine the whole system’s trustworthiness.

This is not merely an internal institutional concern; the growth of online interactions with outside entities, especially in the context of federated identity systems, increasingly makes it necessary for entities of all kinds to demonstrate that their identity systems meet appropriate criteria. U.S. federal E-Authentication level of assurance (LoA) 2, for example, requires the presentation of identifying credentials for proofing (Burr, Dodson, & Polk, 2004). As the InCommon Federation notes, “A resource provider may be more willing to accept your assertions to the extent that [the process of issuing electronic credentials] can be seen as authoritative” (InCommon Federation, n.d.).

Higher education institutions face complex identity proofing challenges because of the diversity of their constituencies, turnover in the user community, and the open access to resources that academic work demands. Barry Ribbeck, director of systems architecture and infrastructure at Rice University, notes that different campus groups come with different identity proofing credentials that are not always appropriate for the resource access they unlock. “Students have transcripts; foreign visitors and faculty have to be highly vetted,” Ribbeck says. “Staff, though, will present a Social Security number and a driver’s license and that’s it.” Still worse are the large numbers of guest accounts many institutions maintain for people who have no clear relationship with the institution. “If that’s not a wake-up call, what is?” Ribbeck asks.

To see how institutions are responding to such issues, we asked several questions about whether they have documented policies regarding identity proofing and whether they differentiate identity proofing for different roles and constituents.

As we reported in Chapter 4, documentation of policies for establishing identity is widespread but far from universal. Half (50.5 percent) of all respondents had completed documented policies (see Figure 4-6). A closer look (see Figure 5-1) shows that among Carnegie classes, doctoral institutions are the most likely to have completed policies (58.8 percent) and associate’s institutions are the least likely (38.3 percent). But across the
board, large majorities of institutions have completed, partially completed, or in-progress policies.

Most policies do not appear to call for differentiation of identity proofing standards among different constituent groups. Only about one-third (32.3 percent) of respondent institutions report using stronger identity proofing for faculty and staff in sensitive roles than for those who are not (see Figure 5-2). About the same proportion (32.2 percent) use such methods for visitors and guests, but only about one-fourth use them for affiliates such as parents and alumni, perhaps because a lower level of access is typically granted to such groups. Higher than usual “don’t know” responses suggest that these issues either aren’t visible or are unsettled among some campus IT units.

We found no significant association between proofing differentiation and institution size. Among Carnegie classes, rates of use for faculty and staff didn’t vary widely, though among those not currently using it, doctorals were more likely than nondoctorals to say they planned to do so (see Table 5-1; note that “don’t know” responses were factored out of these results). The spread was much wider for proofing of campus affiliates and visitors, perhaps reflecting the greater variety of such constituents that institutions gain as they offer higher-level degrees.

For different groups of on-campus visitors and guests, do you use different methods of identity proofing?

For different groups of off-campus affiliates (e.g., parents, alumni), do you use different methods of identity proofing?

For faculty and staff in sensitive roles, do you require stronger identity proofing than for those not in sensitive roles?
Overall, our respondent institutions reported low to modest levels of differentiated identity proofing. This could prove a problem should more formal proofing standards become necessary because of regulatory change or the need to interact with entities, such as the U.S. federal government, that may demand them.

Biometric methods such as fingerprints and iris scanning are still not widely used for identity proofing among our respondent institutions. Only 5.6 percent of institutions reported such techniques in use. The potential for substantial growth, however, is suggested by the additional 12.5 percent who said they were planning to adopt them.

### Counting Identifiers
The proliferation of online identifiers unique to stovepiped or incompatible systems often complicates such IdM goals as consolidating identifiers, building enterprise directories, and achieving reduced/single sign-on. At the same time, the scope of the problem can be hard to measure because ferreting out identifiers requires a sweep of systems and business processes across many different departments. As we reported in Chapter 4 (Table 4-11), only about one in four institutions (26.2 percent) has completed an inventory of identifiers, though a total of 84.3 percent have either finished one, are in progress, or plan to do one. We also wanted to see how many identifiers institutions that had conducted inventories had discovered.

Among those respondents who could give us a count of campus person identifiers, most have not discovered an overwhelming abundance of them (see Figure 5-3). Altogether, 79.4 percent of them had 20 or fewer identifiers.

---

### Table 5-1. Differentiated Identity Proofing of Constituencies

<table>
<thead>
<tr>
<th>Type of Differentiation</th>
<th>Status</th>
<th>DR</th>
<th>MA</th>
<th>BA</th>
<th>AA</th>
<th>Other Carnegie</th>
<th>Canada</th>
</tr>
</thead>
<tbody>
<tr>
<td>For faculty and staff in sensitive roles, do you require stronger identity proofing than for those not in sensitive roles?</td>
<td>Yes</td>
<td>38.0%</td>
<td>34.0%</td>
<td>32.4%</td>
<td>40.9%</td>
<td>41.7%</td>
<td>19.0%</td>
</tr>
<tr>
<td>Planning to do</td>
<td>31.5%</td>
<td>14.0%</td>
<td>9.9%</td>
<td>11.4%</td>
<td>16.7%</td>
<td>28.6%</td>
<td></td>
</tr>
<tr>
<td>Not planning to do</td>
<td>30.4%</td>
<td>52.0%</td>
<td>57.7%</td>
<td>47.7%</td>
<td>41.7%</td>
<td>52.4%</td>
<td></td>
</tr>
<tr>
<td>For different groups of off-campus affiliates (such as parents, alumni), do you use different methods of identity proofing?</td>
<td>Yes</td>
<td>45.7%</td>
<td>20.4%</td>
<td>43.1%</td>
<td>15.0%</td>
<td>33.3%</td>
<td>33.3%</td>
</tr>
<tr>
<td>Planning to do</td>
<td>27.2%</td>
<td>24.7%</td>
<td>13.8%</td>
<td>12.5%</td>
<td>30.0%</td>
<td>11.1%</td>
<td></td>
</tr>
<tr>
<td>Not planning to do</td>
<td>27.2%</td>
<td>54.8%</td>
<td>43.1%</td>
<td>72.5%</td>
<td>36.7%</td>
<td>55.6%</td>
<td></td>
</tr>
<tr>
<td>For different groups of on-campus visitors and guests, do you use different methods of identity proofing?</td>
<td>Yes</td>
<td>50.6%</td>
<td>32.3%</td>
<td>39.7%</td>
<td>17.1%</td>
<td>43.8%</td>
<td>31.6%</td>
</tr>
<tr>
<td>Planning to do</td>
<td>22.4%</td>
<td>23.7%</td>
<td>16.2%</td>
<td>19.5%</td>
<td>21.9%</td>
<td>10.5%</td>
<td></td>
</tr>
<tr>
<td>Not planning to do</td>
<td>27.1%</td>
<td>44.1%</td>
<td>44.1%</td>
<td>63.4%</td>
<td>34.4%</td>
<td>57.9%</td>
<td></td>
</tr>
</tbody>
</table>
fiers, and 92.4 percent had fewer than 100. Still, an outlying group of institutions reported counts exceeding 500 identifiers.

Respondents were much more likely to respond with a count of physical ID cards than virtual identifiers, but again they reported surprisingly low numbers (see Figure 5-4). Eighty-six percent of institutions issue two or fewer ID cards, and only 2.7 percent issue five or more. The skewing of results toward the low end made breakout by Carnegie class and institution size infeasible, but many large institutions were among those reporting a single ID card.

Only 14.3 percent of respondents reported that they are integrating IdM for system and network access with physical access controls like multifunction cards. Another 27.5 percent reported plans to do so, suggesting that these largely separate realms of identity credentials may converge.

**Identifier Policies and Practices**

Guidelines for adherence to U.S. e-Authentication levels of assurance include recommendations intended to make identifiers more robust, secure, and auditable (Burr, Dodson, & Polk, 2004; Louden et al., 2005). Besides their relevance to interfacing with govern-
ment systems and processes, such evolving guidelines are likely to be incorporated more broadly in the public and private sectors, and into audit protocols.

We asked about three items mentioned in such guidelines: the perpetual (never-reassigned) uniqueness of primary identifiers assigned to individuals, the secure and long-term logging of significant identity events such as identifier issuance or revocation, and the encryption of identifier passwords for network transmission.

Our respondent institutions’ current ability to meet these guidelines should it prove necessary is patchy (see Figure 5-5). The practice most commonly followed in all cases, assigning identifiers “unique for all time,” was reported by 37.2 percent of institutions, while 26.3 percent employ event logging in all cases and 23.3 percent prohibit unencrypted passwords. When we add the figures for practice “in some cases,” a healthy majority approximating two-thirds uses each practice, though this raises the question of whether the partial users could scale or extend their usage appropriately if necessary. Between one-fifth (21.4 percent) and one-fourth (26.3 percent) of institutions in each case aren’t following these practices at all, and relatively high “don’t know” responses suggest that, as with some of our identity proofing results, these are not high-visibility questions at some institutions.

In another area of identifier vulnerability, the use of Social Security numbers (SSNs) for identity purposes, our U.S. respondent institutions seem to be making more uniform progress. Tightened control of personal identifiers like SSNs through such legislation as the federal Gramm-Leach-Bliley Act and assorted state privacy acts, along with a generally growing awareness of SSN-fueled identity theft crimes, appears to be leading institutions to abandon the once-common practice of using SSNs for student and employee identifiers. We found that among our U.S. respondents, the vast majority (97.0 percent) either did not use SSNs as an identifier or planned to discontinue their use within three years (see Figure 5-6).

Identity Management User Self-Service

Giving users the ability to review and update their own identity information online has many potential benefits. It can offload much routine work from help desks, where password resets often dominate call logs. Us-

![Figure 5-5. Identifier Policies and Practices](image-url)
ers can typically provide the most timely and accurate information about themselves, and personalizing their online environment may help them improve their own productivity. Finally, in an IT environment where Web-based commercial and campus administrative services are ubiquitous, adding identity self-service addresses user expectations and satisfaction. At the same time, rolling out IdM self-service is not trivial, because identity functions require special attention to security and privacy (Neuenschwander, 2004a).

Our results show that the self-service revolution that transformed administrative services in the last decade has also spread widely, if not quite universally, to at least the basic functions of user IdM (see Figure 5-7). Overall, 73.7 percent of respondent institutions report that they have implemented or are implementing self-service for password resets, and 72.0 percent report using it for updating certain personal information.

These categories didn’t vary widely by Carnegie class. MAs (78.6 percent) and doctorals (78.0 percent) reported higher self-service levels than other groups for password resets, but these results were not dramatically higher than those for the group with the lowest reported rate, associate’s institutions (64.6 percent). The range was wider for updating

---

**Figure 5-6.** Use of Social Security Number as an Identifier (U.S. Respondents Only, N = 367)

**Figure 5-7.** Implemented or Currently Implementing IdM Self-Service Function, by Carnegie Class
personal information, though this was largely due to the predominance of doctorals, where 89.0 percent reported completed or ongoing self-service implementations in this area. Institutional size did not dramatically affect the rate at which password reset self-service was reported, but it was associated with updating personal information, with 57.1 percent of the smallest institutions (under 2,000 students) offering it versus 98.1 percent of the largest (above 25,000 students). Percentages for categories in between rose with institution size.

Self-service is considerably less available, and more unevenly distributed, for less basic services that help constituents personalize relationships with the institution. Just under half (48.9 percent) of all respondents said that their institutions had implemented or were implementing self-service for mailing lists and other subscription services, and 38.0 percent reported completed or ongoing self-service implementations for setting privacy preferences for the release of identity information. Doctoral institutions stood well above the other Carnegie classes in these areas, with 71.0 percent offering or implementing mailing list self-service and 61.0 percent offering or implementing self-service for privacy preferences. By contrast, the rates for associate’s institutions were 16.7 percent for mailing lists and 22.9 percent for privacy preferences. Canadian institutions, at 62.5 percent, were more active in mailing list self-service than the overall respondent group, but they were much less so in setting privacy preferences, with only 8.3 percent offering or implementing self-service.

**User Authentication**

Authentication is the process of validating credentials that a user presents when requesting access to a system, to verify that the person is who he or she claims to be. Though historically authentication has often been combined with authorization—validating that a user is permitted to use specific resources—IdM best practice treats it as a distinct process that forms one basis for authorization.

Authentication is often described as relying on one or more of three factors: something you know, something you have, or something you are. Conventional IT environments rely heavily on “something you know”—typically, user passwords, which are inexpensive and easy for users to understand.

Many IdM experts insist, however, that at least some users should be authenticated on the basis of more than one factor so that the strengths of each factor can protect against the others' vulnerabilities (Henry, 2003; Allan, 2003; Carmody & West, 2005; Hirst, Wagner, & Wheatman, 2004). Multifactor authentication might combine a password with “something you have,” such as a digital certificate on a computer or a hardware token that the user inserts into a reader, and/or “something you are,” such as a biometrically captured fingerprint. For example, the U.S. federal government is moving toward multifactor authentication for employees, combining passwords with presentation of an identification smart card loaded with encrypted biometric data (National Institute of Standards and Technology, 2005). Multifactor authentication is also a required element in LoAs 3 and 4 of the U.S. federal E-Authentication levels of assurance (Burr, Dodson, & Polk, 2004), and it is increasingly under discussion for some consumer services, such as online banking (Federal Financial Institutions Examination Council, 2005).

Higher education institutions’ ability to adopt appropriate authentication processes for different users and systems, and especially their ability to offer multifactor authentication, depends on the diversity and sophistication of the authentication mechanisms they support. To find out what institutions are doing, we asked our respondents about the authentica-
tion methods they use when providing access to network services. Our list of authentication technologies included conventional and “strong” passwords, the Kerberos authentication protocol, various forms of public key infrastructure (PKI) technology, one-time passwords, biometrics, and other methods.

Table 5-2 shows the results. Password-based methods were in dramatically higher use than all others. High levels of “don’t know” responses in many categories suggest uncertain plans or lack of knowledge in some cases. Most notably, in eight of 10 categories, near-majorities or majorities (46.1 percent to 68.9 percent) had no plans to use the named category. Only 27.8 percent of respondents reported using one or more of the multifactor authentication methods we specified (that is, any method listed in Table 5-2 other than conventional and strong passwords and Kerberos), and only 0.9 percent were using more than two. Of those using no such methods, 62.5 percent either didn’t plan to use them in the future or didn’t know their plans.

Except for Kerberos, we either found limited variability among Carnegie classes or received too few responses in each category to make comparisons reliable. Detailed examination of the results follows.

**Passwords, Conventional and Strong**

The results show that our respondent institutions rely overwhelmingly on passwords rather than on the other methods specified in the survey (see Table 5-2). Ninety-one percent reported using conventional passwords or personal identification numbers (PINs). More than half (55.0 percent) are using strong passwords, and another 23.8 percent plan to use them. This was the highest absolute “planning to use” rate of all the authentication methods we named.

Strong passwords use formulation rules, forced reset dates, and other techniques to make passwords harder to guess, crack computationally, or use if obtained improperly. But they also have the potential to tempt users into writing their passwords down, and some users may see them as an annoyance. Several of our interviewees told us that they introduced stronger passwords in the context

**Table 5-2. Authentication Methods for Network Access (Multiple Responses Allowed)**

<table>
<thead>
<tr>
<th>Method</th>
<th>Using</th>
<th>Planning to Use</th>
<th>Not Planning to Use</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conventional password/PIN</td>
<td>91.1%</td>
<td>2.1%</td>
<td>6.5%</td>
<td>0.3%</td>
</tr>
<tr>
<td>Strong password</td>
<td>55.0%</td>
<td>23.8%</td>
<td>16.5%</td>
<td>4.7%</td>
</tr>
<tr>
<td>Kerberos</td>
<td>26.2%</td>
<td>11.5%</td>
<td>46.1%</td>
<td>16.1%</td>
</tr>
<tr>
<td>PKI certificate (software) without PIN</td>
<td>7.1%</td>
<td>7.4%</td>
<td>58.9%</td>
<td>26.5%</td>
</tr>
<tr>
<td>PKI certificate (software) with PIN</td>
<td>4.8%</td>
<td>10.6%</td>
<td>55.9%</td>
<td>28.7%</td>
</tr>
<tr>
<td>PKI hardware token without PIN</td>
<td>0.6%</td>
<td>2.8%</td>
<td>68.9%</td>
<td>27.7%</td>
</tr>
<tr>
<td>PKI hardware token with PIN</td>
<td>1.8%</td>
<td>7.6%</td>
<td>62.2%</td>
<td>28.4%</td>
</tr>
<tr>
<td>SecurID-style one-time password</td>
<td>12.7%</td>
<td>11.8%</td>
<td>54.6%</td>
<td>20.9%</td>
</tr>
<tr>
<td>Other multifactor authentication methods</td>
<td>6.5%</td>
<td>17.9%</td>
<td>48.7%</td>
<td>27.0%</td>
</tr>
<tr>
<td>Biometric identification</td>
<td>3.3%</td>
<td>12.6%</td>
<td>66.1%</td>
<td>18.0%</td>
</tr>
</tbody>
</table>
of a reduced/single sign-on environment, partly for security reasons but also to balance greater strictness with greater convenience. “Is a single master key better than a whole key ring with 20 keys?” asks Patrick Gossman, director of academic technologies and customer services at Wayne State University. “It is if you make it difficult to find that key. It does require us to train people to ensure they have a hardened password.” At Embry-Riddle Aeronautical University, Becky Vasquez, IT services director, acknowledges that the most common complaint she receives about ERAU’s nearly complete IdM initiative is that “the password’s too strong.” But she feels that users also welcome the simultaneous reduction of passwords that rollout of single sign-on will bring and that most users support the change. Most important, she says, “People aren’t going to be using their pet’s name for a password anymore, or anything else that is easy for others to guess.”

Kerberos

The Kerberos network authentication protocol, based on a client-server model, was created at the Massachusetts Institute of Technology and is distributed by MIT as well as commercial vendors. In Kerberos, a user authenticates to a central server by requesting credentials. The authentication server knows the user’s password and returns the credentials encrypted in that password. These credentials, which contain a time-limited “ticket-granting ticket,” can be decrypted only if the user has the correct password for his or her account. The ticket-granting ticket, in turn, lets the user get tickets permitting access to specific other systems without further authentication. Many operating systems, applications, and middleware elements, including Microsoft Active Directory, support Kerberos, though others do not.

Kerberos was reported in use by 26.2 percent of our respondents, and 11.5 percent planned to use it (see Table 5-2). This represents a considerable increase over the 19.3 percent use rate found in our 2003 security study (Kvavik & Voloudakis, p. 51), though it falls short of the number suggested by those reporting its planned adoption in 2003—a useful reminder that planned adoption doesn’t always happen. Doctoral institutions reported a current usage rate (48.3 percent) more than double that of the other Carnegie classes (see Figure 5-8). Only a single Canadian institution (4.8 percent) reported using Kerberos, while 81.0 percent said they had no plans to.

Kerberos’s home, MIT, uses it extensively for single sign-on and authentication. “Between Kerberos and X.509 certificates, we can accomplish almost everything, with the exception of public kiosks,” says Jeffrey Schiller, network manager at MIT. “We hardly spend anything.”

---

**Figure 5-8.**

*Use of Kerberos to Authenticate Network Access (N = 347)*
PKI-Based Authentication

Public key infrastructure (PKI) is a comprehensive security technology that uses paired public and private keys for encryption and decryption. Data encrypted with one key can only be decrypted with the other. Public keys are known and used in common by a community of users, while private keys are kept secret and are particular to users or devices such as servers. Identifying information bound to key pairs is issued to users and devices via digital certificates based on the X.509 standard. Certificates originate from trusted certificate authorities (CAs). These could be commercial entities; the institution itself, if it has the infrastructure to act as a CA; or partners acting as CAs. Certificates can be distributed to different kinds of devices, including smart cards and pocket-sized hard tokens.

Public key technology can address a wide range of security issues from authentication to data encryption and digital signatures, and it can radically reduce the need to transport and centrally store passwords. But cost, PKI product interoperability, application support, and other issues have tended to keep the technology restricted to niche functions, such as Secure Sockets Layer (SSL) Web data transport encryption and secure e-mail, and it is less often seen in enterprise-wide rollouts (Blum & Gebel, 2003; Wheatman & Wagner, 2003). Gartner’s security analysts recommend PKI only where enterprises can identify multiple high-value uses for it and have a central IT services culture (Wheatman, Kreizman, Pescatore, Young, & Wagner, 2004).

Relatively few of our respondents reported using PKI to provide access to network services (see Table 5-2). Most that do use it rely on software certificates, sometimes in conjunction with a PIN (4.8 percent) but more often without one (7.1 percent). Only a handful reported using PKI-based hardware tokens (1.8 percent with PIN and 0.6 percent without.) Altogether, 39 of our 403 respondents (9.7 percent) reported using one or more forms of PKI for network authentication. An additional 14.6 percent said they were planning to add one or more of the specified forms of PKI authentication. Note that as we mentioned above, public key technology has multiple uses, and an institution reporting that they are not using it for one of the user authentication methods specified in our survey questions might still be using it in other ways. This may explain the higher figures for PKI technology use in the EDUCAUSE Core Data Service summary report for 2004, which reported that 15.8 percent of respondents had deployed PKI technology, another 10.1 percent were in progress or piloting it, and another 34.0 percent were considering it (Hawkins, Rudy, & Nicolich, 2005).

High “don’t know” responses exceeding one-fourth of our respondents (26.5 to 28.7 percent) suggest the possibility that some undecided institutions will still choose to adopt PKI for network access. Yet the most striking results lay in the percentage saying they did not plan to adopt PKI for this purpose. In a survey that generally found few respondents willing to say definitely that they would not adopt some IdM technology, “not planning to adopt” rates for our specified forms of PKI hovered around 60 percent of respondents (55.9 percent to 68.9 percent). Mark Talaga, Internet specialist working on Embry-Riddle’s IdM project, notes that they are monitoring PKI as a user authentication technology but have no concrete plans to implement it. “SSL, single sign-on with a stronger password, and encrypted passwords achieve most of our objectives,” he says. Joe Progar, systems security administrator at Embry-Riddle, adds, “Identity management, encryption, and a strict but usable password policy is a good first step. PKI may or may not be the next one.”

“There has to be a need for [PKI] or it’s just not worth it,” says Rice’s Ribbeck. Ribbeck for-
merely worked at the University of Texas Health Science Center (UTHSC) at Houston, a pioneer in PKI usage, where “we did everything with it. I loved it.” At Rice, PKI is used on a more limited basis for sensitive positions. “We have a private PKI environment for system admins who can use a token to identify themselves,” Ribbeck reports.

**Token-Based Authentication Methods**

As noted above, few respondents said they used PKI-based hard tokens for authentication. The planning-to-use figures for these devices, however, were the highest multiples of current use among all the methods we asked about, exceeding current-use figures by more than a factor of four in each case. For PKI hard tokens without PINs, 2.8 percent planned to use versus 0.6 percent actually using, and for PKI hard tokens with PINs, 7.6 percent planned to use versus 1.8 percent already using. What’s more, when other technologies are taken into account, hard token use and planned use are considerably greater.

One-time password (OTP) tokens of the type made popular by RSA Inc.’s SecurID product generate a character string, synchronized with the authentication system, that changes over a short time span (perhaps every 60 seconds) or according to some other dynamic mechanism. To authenticate, users typically enter the displayed string along with a secret PIN, thus providing two authentication factors. Some devices take the form of a USB token or smart card that can be inserted into a port or reader. In addition, OTPs can be delivered from software clients that reside on a PC or on portable devices such as cell phones or PDAs. SecurID-style OTPs were reported in use for network authentication by 12.7 percent of respondents, with an additional 11.8 percent reporting plans to use them (see Table 5-2). As with PKI, we saw a high level of “don’t know” response (20.9 percent) and a majority (54.6 percent) response saying they did not plan to adopt OTPs.

One obstacle to hard tokens’ use that interviewees mentioned was keeping track of keys physically and getting users accustomed to the behavioral changes they require. “Key management is a bit of an issue” complicating wider rollout of two-factor authentication at Dalhousie University, says John Sherwood, executive director of University Computing and Information Systems. Rice’s Ribbeck acknowledges the problem but says that the large-scale rollouts like the one at UTHSC Houston were manageable. “The tokens are fairly robust—they’ll survive a laundering and so on,” says Ribbeck. “The key management issues were less onerous than the password management issues they resolved. If there is high value associated with an authentication credential, a user will take care with its use.”

**Biometrics**

Biometrics uses the digital capture of a person’s biological characteristics, such as a fingerprint, iris scan, or voiceprint, to create an authenticator. Biometric credentials have the advantages of being highly personal, always available to the user, and difficult to loan or steal. They also have several disadvantages. Natural variations and changes in bodily characteristics require that biometric capture devices be tuned within bands of variability, which may lead to false acceptance or rejection. Capturing and storing physical information about people can be politically sensitive, and some methods of biometric authentication may be subject to spoofing. As Burton Group Analyst Trent Henry dryly notes, “A detached finger may well have a totally convincing fingerprint, even if the actual user no longer possesses it” (Henry, 2003).

Biometrics was among the least-reported network access authentication technologies
we asked about, with only 3.3 percent of respondents telling us they used it (see Table 5-2). This was a large increase, however, over the 0.9 percent reported in our 2003 security study (Kvavik & Voloudakis, 2003, p. 51). Planned use in the current study, at 12.6 percent, was much higher than current use. Gordon Wishon, who is CIO, associate vice president, and associate provost at Notre Dame, notes both the promise he sees in biometrics and the cautions appropriate to it. “We are carefully watching biometrics,” he says. “We already have one-time passwords. Biometrics can provide another set of tools that could be used to authenticate users before granting access to sensitive data. We have not yet made a decision to invest and would only use it in limited cases where we need to ensure very tight controls.”

Encrypted and Digitally Signed E-Mail

Although users may be stringently authenticated before gaining access to e-mail systems, once mail is sent, it is usually no longer bound closely to the sender’s identity. Casual readers may assume that any e-mail they receive is actually from its purported sender, but in fact e-mail sender addresses can be spoofed. Plain-text e-mails are available for inspection by intermediaries and can be counterfeited for e-mail–based phishing attacks. Encrypting and/or digitally signing e-mail using PKI or other technologies can help protect sensitive information and enhance confidence that e-mail is actually from the person named as the sender.

We asked our respondents if they were using, or planning to use, encrypted e-mail or signed e-mail in any part of the institution. Encrypted e-mail was the more widely used, with 37.9 percent of respondents using it and 32.5 percent saying they had no plans to do so. Doctoral institutions (40.7 percent) and master’s institutions (41.2 percent) had the highest reported usage rates, though master’s institutions were more likely to say they had no plans for it (see Figure 5-9).

Only one in five institutions (20.2 percent) reported that they used signed e-mail, and twice that figure (41.7 percent) said they have no plans to adopt it. Doctorals were clearly the dominant users of signed e-mail (see Figure 5-10). Still, only about one in three (31.8 percent) are using it, while only 4.9 percent of associate’s institutions use it.

Summing Up Establishing Identity and User Authentication

The emerging requirement for college and university identity systems is not bulletproof high-security processes at all levels but rather a flexible, diverse spectrum of available resources that permits matching the right degrees of security and convenience to ap-

![Figure 5-9. Use of Encrypted E-Mail, by Carnegie Class (N = 300)](image-url)
appropriate situations. As Burton Group Analyst Dan Blum writes, “Enterprise authentication architectures should support multiple levels of authentication and provide risk management guidelines for assigning functions to the required authentication level” (Blum, 2004, p. 18). Finding the right match, furthermore, is not a static event. As security threats and awareness evolve along with identity technologies, institutions must be prepared to adjust the parameters of identity proofing and authentication accordingly.

For these reasons, it is noteworthy that many of our respondent institutions seem to have a limited set of arrows in their identity proofing and user authentication quivers. Though most respondent institutions have either completed or are working on documentation of identity proofing, only half or fewer currently practice or plan to practice differentiated identity proofing in the areas we asked about.

Authentication processes, moreover, continue to rely overwhelmingly on passwords. Despite some growth in the use of alternative, stronger authentication methods, nearly three-fourths of our respondents report no current use of multifactor or biometric methods, and most of those report no definite plans to adopt such methods. This makes it hard to argue the case that our respondent base is aggressively creating a more diverse ecosystem of authentication tools. Limits in current strong authentication technologies and a user culture wedded to familiar, single-factor methods are undoubtedly powerful forces retarding change. But a more strategic view must take into account the emerging need for more, and more-powerful, tools—a need for which many institutions don’t seem to be preparing themselves.

Endnotes

1. Comparisons between this study and the 2003 study Information Technology Security: Governance, Strategy, and Practice in Higher Education (Kvavik & Voloudakis, 2003) are interesting but must be made with caution. Typically, ECAR studies follow standard practice by eliminating “don’t know” responses from results when they are few in number. This is the practice followed in the authentication table of the 2003 security study, which reported a 22.0 percent rate of Kerberos adoption. Where “don’t know” rates are unusually high, however, as in this study’s authentication findings, we do report them. Because the authentication findings percentages in the studies refer to differently composed totals, they are not directly comparable. When “don’t knows” are included, the results of the 2003 security study found that 19.3 percent of respondents were using Kerberos, versus 26.2 percent in the current study.

2. The comparable figure from our 2003 security study was 8.5 percent. Note that the 2003 study asked only about the single category of PKI, while this study’s total figure of 9.7 percent counts all respondents using at least one of the four named PKI methods. See note 1 above.

3. Though the 2003 security study reported 1.1 percent biometric technologies adoption, to be commensurate with this study’s authentication technologies figures it must be recalibrated to include “don’t know” responses, which yields the 0.9 percent figure. See note 1 above.
Enterprise Directories, Sign-On, and Authorization

If you have too many roles, you have no roles at all.
—Elazar Harel, University of California at San Diego

Key Findings

◆ Interest and activity surrounding enterprise directories, reduced or single sign-on (RSSO), and automated role- and privilege-based authorization, or more simply role-based authorization (RBA), are high, though fully operational sites are few. Slightly more than half of respondent institutions report partially or fully operational enterprise directories, compared with slightly more than a third for RSSO and about three in 10 for RBA.
◆ Planning activity in IdM technologies is high. Those considering, planning, or implementing enterprise directories made up 40 percent of respondent institutions, while majorities reported the same activities for RSSO and RBA.
◆ Very few respondent institutions—fewer than 2 percent for RBA and fewer than 1 percent for the other technologies—definitely rule out at least considering each IdM technology in some time frame.
◆ The mean stage of enterprise directory and RSSO adoption tends to be higher for larger and doctoral institutions.
◆ Classic central infrastructure services and enterprise applications dominate applications’ enterprise directory use. Fewer than three in 10 respondent institutions report departmentally controlled applications using the enterprise directory.
◆ Though enterprise directory policy documentation rates increase with advancing stages of adoption, one-third of respondent institutions with fully operational enterprise directories report no documented enterprise directory policies.
◆ Large majorities aim to have most or all central IT applications use the enterprise directory and RBA system.
◆ IdM technology sourcing approaches vary widely, with enterprise directories having the highest rate of commercial solutions used and RSSO the lowest. A third of respondents have not determined an RSSO approach, and 40 percent have not determined an RBA approach.
Once a campus has issued users identifiers and assembled the means to authenticate them, how can IdM help the IT unit deliver better service? Our study looked at three areas where institutions are using IdM in the hope of creating a better user experience, improving operations, and making new resources available.

First, enterprise directories can collect the often-distributed and inconsistently recorded attributes that identify users, thereby creating a central infrastructure for authentication and authorization. Next, reduced or single sign-on (RSSO) can be implemented to cut down on the number of accounts users have to keep track of, and to provide a more seamless experience as users move from system to system. Automated role- and privilege-based authorization, or more simply role-based authorization (RBA), can translate the user’s known relationships and affiliations within the institution—that is, the roles he or she occupies—into privileges that allow appropriate resource use.

This chapter begins with a comparative assessment of how our respondents report using these technologies. We then examine each individually, looking at the approaches institutions are taking to them, why non-adopters aren’t planning to use them and, for enterprise directories, the scope and manner of their use.

**Enterprise Directories, RSSO, and RBA: A Comparative Overview**

We asked respondents to describe the extent to which their institution was implementing or considering enterprise directories, RSSO, and RBA using a 7-point scale that ranged from “not considering” (1) to “fully operational” (7). Our questions used the following definitions:

- **Enterprise directory**: an institutional directory service that has the capability to include all persons affiliated with the institution and to be used by multiple applications.
- **Reduced or single sign-on**: a single electronic identity that can be entered once for most or all of your applications.
- **Automated role- and privilege-based authorization**: a system giving access to electronic resources using privileges or permissions derived automatically from affiliations and groups.

We found a high degree of engagement with the three technologies (see Figure 6-1). The use patterns intersect at one point: among all three, roughly one in four respondents reported a partially operational implementation. Beyond this point, however, implementation rates and plans diverge considerably.

Respondents most commonly reported enterprise directories as being fully operational (27.9 percent of respondents). The additional 25.6 percent who said they had a partially operational enterprise directory made this the only technology in the group with a majority of respondents (53.5 percent) operational at some level. This was below the 63.1 percent of institutions reporting enterprise directory technology deployment in the fiscal year 2004 EDUCAUSE Core Data Service program (Hawkins, Rudy, & Nicolich, 2005). The difference may be due to this study’s more restrictive definition of enterprise directories. RSSO was reported fully operational at 10.2 percent of institutions and partially so at 24.9 percent. RBA was fully operational at only 5.7 percent and partially at 23.9 percent.

Respondents reported a great deal of ongoing or planned activity that will keep many institutions involved in some way with IdM adoption issues. A total of 41.5 percent of respondents told us they either had an RSSO implementation in progress or planned one. The totals for in-progress or planned implementations were 26.1 percent for enterprise directories and 27.6 percent for RBA. Altogether, 63.7 percent of respondents said
they were either implementing one of these technologies now or planned to do so in some time frame. When we add those currently evaluating these technologies to the ongoing and planned implementations, the percentage of institutions that are somehow “in the game” but not yet operational rises to 61.2 percent for RSSO, 39.8 percent for enterprise directories, and 56.7 percent for RBA. We speculate, furthermore, that both partially and fully active sites will see upgrade and enhancement activity.

Almost universally, respondents seemed reluctant to completely rule out the possible adoption of any of these technologies, even if they expected to defer consideration of them for some time. RSSO had the lowest reported current “not considering” rate (3.7 percent), RBA had the highest (13.7 percent), and enterprise directories were in between (6.7 percent). But even many who said they weren’t considering the technology now thought they would do so later (see Table 6-1). Only a single respondent out of 15 (6.7 percent) who said they were not currently considering RSSO reported thinking that their institution would not consider it some time in the future. For enterprise directories, that figure was 11.1

---

**Figure 6-1. Extent to Which Institution Is Considering or Implementing IdM Technologies (N = 402)**

**Table 6-1. Will Institution Consider Implementing IdM Technology in the Future?**

<table>
<thead>
<tr>
<th>Technology</th>
<th>No</th>
<th>Within Two Years</th>
<th>Between Two and Three Years from Now</th>
<th>More Than Three Years from Now</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduced or single sign-on</td>
<td>6.7%</td>
<td>20.0%</td>
<td>26.6%</td>
<td>26.7%</td>
<td>20.0%</td>
</tr>
<tr>
<td>Enterprise directory</td>
<td>11.1%</td>
<td>11.1%</td>
<td>29.6%</td>
<td>7.4%</td>
<td>40.8%</td>
</tr>
<tr>
<td>Automated role-based authorization</td>
<td>10.9%</td>
<td>27.3%</td>
<td>14.5%</td>
<td>3.6%</td>
<td>43.7%</td>
</tr>
</tbody>
</table>
percent, and for RBA it was 10.9 percent. Most of the future consideration, however, was anticipated to take place in time frames beyond two years.

When expressed as a percentage of all survey respondents, those answering with definite “not now and not later” responses were 0.2 percent for RSSO, 0.7 percent for enterprise directories, and 1.5 percent for RBA. High “don’t know” responses here suggest much uncertainty, and of course those evaluating the technologies may eventually decide against them. Whatever they ultimately decide, however, we found no evidence that a sizable portion of our respondent community has yet concluded that they have no place for these technologies.

Using the 7-point scale described above (see Figure 6-1), we calculated the mean extent to which various respondent categories have adopted each technology. We found significant associations between mean extent of adoption and both Carnegie class and institution size for two technologies: enterprise directories and RSSO (see Tables 6-2 and 6-3). Within Carnegie class, mean extent of adoption was highest for doctorals (5.07 for RSSO and 5.86 for enterprise directories) and lowest for associate’s institutions (3.58 for RSSO and 4.33 for enterprise directories).

Table 6-2. Mean Extent of IdM Technology Adoption, by Carnegie Class and Canada

<table>
<thead>
<tr>
<th>Technology</th>
<th>DR</th>
<th>MA</th>
<th>BA</th>
<th>AA</th>
<th>Other Carnegie</th>
<th>Canada</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduced or single sign-on</td>
<td>Mean</td>
<td>5.07</td>
<td>4.26</td>
<td>4.22</td>
<td>3.58</td>
<td>3.93</td>
<td>4.25</td>
</tr>
<tr>
<td></td>
<td>Std. deviation</td>
<td>1.618</td>
<td>1.681</td>
<td>1.936</td>
<td>1.748</td>
<td>1.895</td>
<td>1.648</td>
</tr>
<tr>
<td>Enterprise directory</td>
<td>Mean</td>
<td>5.86</td>
<td>4.79</td>
<td>5.00</td>
<td>4.33</td>
<td>4.19</td>
<td>4.92</td>
</tr>
<tr>
<td></td>
<td>Std. deviation</td>
<td>1.648</td>
<td>2.086</td>
<td>1.811</td>
<td>2.077</td>
<td>2.050</td>
<td>1.863</td>
</tr>
<tr>
<td>Automated role-based authorization</td>
<td>Mean</td>
<td>4.01</td>
<td>3.35</td>
<td>3.80</td>
<td>3.21</td>
<td>3.40</td>
<td>3.92</td>
</tr>
<tr>
<td></td>
<td>Std. deviation</td>
<td>2.028</td>
<td>1.971</td>
<td>2.136</td>
<td>1.774</td>
<td>1.904</td>
<td>1.586</td>
</tr>
</tbody>
</table>

(1 = not considering, 2 = currently evaluating, 3 = planned, won’t start within next 12 months, 4 = will start within next 12 months, 5 = implementation in progress, 6 = partially operational, 7 = fully operational)

Table 6-3. Mean Extent of IdM Technology Adoption, by Institution Size

<table>
<thead>
<tr>
<th>Technology</th>
<th>1–2,000</th>
<th>2,001–4,000</th>
<th>4,001–8,000</th>
<th>8,001–15,000</th>
<th>15,001–25,000</th>
<th>More than 25,000</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduced or single sign-on</td>
<td>Mean</td>
<td>3.99</td>
<td>4.09</td>
<td>4.10</td>
<td>4.51</td>
<td>4.87</td>
<td>5.34</td>
</tr>
<tr>
<td></td>
<td>Std. deviation</td>
<td>1.888</td>
<td>1.895</td>
<td>1.657</td>
<td>1.706</td>
<td>1.493</td>
<td>1.818</td>
</tr>
<tr>
<td>Enterprise directory</td>
<td>Mean</td>
<td>4.32</td>
<td>4.74</td>
<td>4.90</td>
<td>5.34</td>
<td>5.76</td>
<td>5.59</td>
</tr>
<tr>
<td></td>
<td>Std. deviation</td>
<td>2.055</td>
<td>1.911</td>
<td>2.043</td>
<td>1.866</td>
<td>1.737</td>
<td>2.009</td>
</tr>
<tr>
<td>Automated role-based authorization</td>
<td>Mean</td>
<td>3.73</td>
<td>3.30</td>
<td>3.38</td>
<td>3.74</td>
<td>3.65</td>
<td>4.55</td>
</tr>
<tr>
<td></td>
<td>Std. deviation</td>
<td>2.174</td>
<td>1.983</td>
<td>1.862</td>
<td>1.842</td>
<td>1.934</td>
<td>2.010</td>
</tr>
</tbody>
</table>

(1 = not considering, 2 = currently evaluating, 3 = planned, won’t start within next 12 months, 4 = will start within next 12 months, 5 = implementation in progress, 6 = partially operational, 7 = fully operational)
The other categories fell in between, with baccalaureate institutions accumulating a slightly lower mean than master’s institutions for RSSO and slightly higher for enterprise directories.

Larger institutions tended to have a greater mean extent of adoption for RSSO and enterprise directories. High standard deviations reveal considerable variation of reported technology adoption within groups. RBA was not significantly associated with either Carnegie class or institution size.

We also found some affinities between the reported use of other technologies and IdM technologies. Institutions that had implemented or were currently implementing a single institution-wide data warehouse had higher IdM technology adoption extent means than those implementing data marts for specific purposes, which in turn had higher means than those without implementations of data warehouses or data marts (see Table 6-4). Likewise, IdM technology adoption extent means were higher for those with a more advanced stage of student portal implementation than for those at less advanced stages or those with no plans for a portal (see Table 6-5). We found a similar association with faculty and staff portals.

These relationships between IdM technologies and data warehouse and portal projects may stem from the data integrity, integration, and user service issues that such projects all touch upon (DeSimone, 2002). In particular, many of our interviewees stressed the relationship between portal projects and IdM. “The portal is a sister project” to enterprise directories and RSSO projects at the University of New Hampshire, says Bill Baber, associate director of academic technology and portal coordinator at UNH. “From the portal you want to communicate to a select population and get the right people, right mechanisms, and so on. It’s hard to do that without a good infrastructure.” At Trinity University, a student portal implementation led to the decision to stop implementing systems not compliant with Lightweight Directory Access Protocol (LDAP), which became a first step toward a single sign-on project. “There’s a point at which you’re going to make the first move,” says Charles White, vice president for information resources and administrative affairs at Trinity. “The portal is what kicked it off for us.” For Chris Holsman, director of enterprise Internet solutions at the University of Wisconsin–Madison, the ability to enhance

<table>
<thead>
<tr>
<th>Data Warehouse Status (Implemented or Currently Implementing)</th>
<th>Reduced or Single Sign-On</th>
<th>Enterprise Directory</th>
<th>Automated Role-Based Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>A single institution-wide data warehouse</td>
<td>Mean: 4.81</td>
<td>5.46</td>
<td>4.03</td>
</tr>
<tr>
<td></td>
<td>Std. Deviation: 1.596</td>
<td>1.824</td>
<td>1.943</td>
</tr>
<tr>
<td>Data mart(s) for specific types of information</td>
<td>Mean: 4.36</td>
<td>5.38</td>
<td>3.76</td>
</tr>
<tr>
<td></td>
<td>Std. Deviation: 1.803</td>
<td>1.741</td>
<td>1.897</td>
</tr>
<tr>
<td>No data warehouse or data marts</td>
<td>Mean: 3.99</td>
<td>4.34</td>
<td>3.23</td>
</tr>
<tr>
<td></td>
<td>Std. Deviation: 1.860</td>
<td>2.094</td>
<td>2.006</td>
</tr>
</tbody>
</table>

(1 = not considering, 2 = currently evaluating, 3 = planned, won’t start within next 12 months, 4 = will start within next 12 months, 5 = implementation in progress, 6 = partially operational, 7 = fully operational)
portal capabilities was a key IdM selling point. “You need the killer app,” Holsman says. “The portal with its various services needs this infrastructure.”

Surprisingly, although some of our interviewees told us their IdM initiatives began with or were enabled by an enterprise resource planning implementation, we found no association between ERP status and IdM technology adoption means. We speculate that other kinds of administrative systems environments generate their own, comparable pressures or opportunities for IdM activity, though perhaps of a qualitatively different nature.

In Chapter 4, we reported generally low levels of completion for documentation, policy, and planning work that is often recommended as preparation for IdM initiatives. We found some evidence that completion rates for certain items increase with advancing stages of IdM technology adoption. As Table 6-6 shows, completion rates for documented IdM plans rise from the very low rates found among those evaluating technologies (4.0 to 10.8 percent) to considerably higher rates among those who have fully operational implementations (21.3 to 45.5 percent). The completion rates, however, tend to rise most dramatically in the implementation and fully operational phases rather than among those planning to adopt.

Having a documented IdM plan was the only IdM readiness activity we found that was associated with advancing adoption for all three technologies. We found a few similar patterns, however, with specific technologies and activities. Having a documented business case for some area of IdM tended to increase with advancing stages of RSSO and RBA adoption. Degree of completion of an inventory of campus identifiers was likewise significantly associated with stage of adoption for enterprise directories (12.2 percent completion rate for those evaluating, rising to 48.1 percent for those fully operational) and RBA (20.5 percent for those evaluating, 40.9 percent for those fully operational). Such increases in completion, of course, still leave a large body of fully operational respondents without completed “readiness” activities.

The technology-specific sections that follow offer detailed information about adoption and approaches.

### Table 6-5. Mean Extent of IdM Technology Adoption, by Student Portal Status

<table>
<thead>
<tr>
<th>Student Portal Status</th>
<th>Reduced or Single Sign-On</th>
<th>Enterprise Directory</th>
<th>Automated Role-Based Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Already implemented</td>
<td>Mean: 5.14</td>
<td>5.35</td>
<td>4.11</td>
</tr>
<tr>
<td></td>
<td>Std. Deviation: 1.674</td>
<td>1.886</td>
<td>2.021</td>
</tr>
<tr>
<td>Currently implementing</td>
<td>Mean: 4.32</td>
<td>5.26</td>
<td>3.64</td>
</tr>
<tr>
<td></td>
<td>Std. Deviation: 1.658</td>
<td>1.677</td>
<td>1.902</td>
</tr>
<tr>
<td>Planning to implement</td>
<td>Mean: 3.72</td>
<td>4.61</td>
<td>3.19</td>
</tr>
<tr>
<td></td>
<td>Std. Deviation: 1.523</td>
<td>2.002</td>
<td>1.854</td>
</tr>
<tr>
<td>Not planning to implement</td>
<td>Mean: 3.31</td>
<td>4.33</td>
<td>3.19</td>
</tr>
<tr>
<td></td>
<td>Std. Deviation: 1.957</td>
<td>2.436</td>
<td>1.966</td>
</tr>
</tbody>
</table>

(1 = not considering, 2 = currently evaluating, 3 = planned, won’t start within next 12 months, 4 = will start within next 12 months, 5 = implementation in progress, 6 = partially operational, 7 = fully operational)
Identity Management

Enterprise Directories

In many IT environments, institutional data about system users is anything but easily accessible from an enterprise standpoint. Applications with their own idiosyncratic identity mechanisms, incompatible directories that don’t know about each other’s existence, ambiguous and conflicting data in systems of record, and many other challenges make it difficult to collect, join, and centrally access identity information. Enterprise directories address such problems by acting as the operational hub for IdM, enabling users and applications to find information about people and things.

Typical enterprise directory components include
- a registry of personal identity data and other necessary information;
- a metadirectory infrastructure that controls and reconciles information flowing from systems of record, distributed physical directories, and other components; and
- an interface that may connect directly to consuming applications or to an LDAP directory.

The enterprise directory assembles information from feeding systems, joins and reconciles it for storage in the person registry, and loads it into physical directories for serving out to applications. The enterprise directory may also maintain organization or group registries containing affiliation information (West, 2005; Bellina, 2002).

Interviewees experienced with enterprise directories stress their versatility and ability to eliminate data conflicts that have bedeviled identity tasks for years. Thanks to an enterprise directory project, “We now have one campus repository of people’s identities and attributes,” says Peter Murray, vice president of information technology and CIO at the University of Maryland, Baltimore. “It’s a hub from which we can leverage the portal, improve security, and give access to current and future systems. We’re resolving the question, ‘Who is affiliated with the institution?’” At Northwestern University, says Thomas Board, director of information systems architecture, “We want to have an environment with a single identity. We’re doing a lot of initiatives in the ERP arena, and this is the time to pull it together [in an enterprise directory] and make sense of it.”

Another theme was the enterprise directory’s capacity to prepare for multiple “downstream” initiatives. The enterprise directory “has positioned us for the future,” says Joel Cooper, director of information technology services at Carleton College. “It’s demonstrating the importance of integrating this data to

Table 6-6. IdM Plan Completed, by Stage of IdM Technology Adoption (N=377)

<table>
<thead>
<tr>
<th>Technology</th>
<th>Currently Evaluating</th>
<th>Planned, but Won’t Start within the Next 12 Months</th>
<th>Will Start within the Next 12 Months</th>
<th>Implementation Is in Progress</th>
<th>Partially Operational</th>
<th>Fully Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Directory</td>
<td>4.0%</td>
<td>5.0%</td>
<td>0.0%</td>
<td>19.7%</td>
<td>9.5%</td>
<td>21.3%</td>
</tr>
<tr>
<td>RSSO</td>
<td>5.5%</td>
<td>6.0%</td>
<td>9.5%</td>
<td>16.2%</td>
<td>12.9%</td>
<td>31.6%</td>
</tr>
<tr>
<td>RBA</td>
<td>10.8%</td>
<td>11.4%</td>
<td>13.3%</td>
<td>22.6%</td>
<td>7.7%</td>
<td>45.5%</td>
</tr>
</tbody>
</table>
both the IT staff and the business users. It’s the most beneficial of our identity management initiatives."

As we reported above, among the IdM technologies we asked about, enterprise directories were most often reported to be operational (see Figures 6-1 and 6-2). At 49.5 percent, doctorals had the highest reported rate of full operation, while at 14.6 percent associate’s institutions had the lowest. High levels of partial operation, implementation, and planned adoption mean that more than 70 percent in every Carnegie class expressed some form of commitment to enterprise directories.

We asked those who were not considering an enterprise directory to choose their primary reasons from a list, but the results were notable mainly for how few of our 403 total respondents fell into this category. Among the 27 respondents who gave at least one reason, the reasons most commonly selected were higher IT priorities (15 respondents), not requiring an enterprise directory at this time (13), and lack of adequate funding (5). Only four respondents said that lack of institutional senior management support was a primary reason for not considering one.

Note that except where indicated otherwise, the results presented in the following enterprise directory sections represent respondents who were at least considering enterprise directory technologies (that is, those “not considering” enterprise directories were excluded).

Enterprise Directory Functionality

The enterprise directory is by nature a multifunction system configurable to support a wide range of activities. We asked all respondents who were at least considering enterprise directories (that is, considering, planning, implementing, or at some level of operational) to tell us what IdM functions they were using enterprise directories to facilitate, which they planned to use them for, and which they had no plans for. User authentication (reported in use by 73.4 percent and planned by 21.9 percent) and user authorization (used by 62.7 percent and planned by 29.2 percent) were, not surprisingly, the leading functions reported (see Figure 6-3). Storing affiliation and group information and storing privileges and permissions for systems access—both of which lay the basis for supporting automated role-based authorization—were also common functions.

Respondents reported these transaction-oriented capabilities more often than those
that leverage enterprise directory information for reporting. About one-third of respondents said they use enterprise directories for activities such as producing reports (32.4 percent) or tracking, logging, and reporting on user activities (29.3 percent).

Overall, our respondents reported an ambitious pattern of use and planned use for enterprise directories. Combined use and planned use added up to a majority of respondents in every function named and exceeded 80 percent for all the top four functions. Among the bottom four functions named, all had planned use exceeding current use, and in the case of workflow methods that automatically update user records on the basis of defined business triggers, planned use (41.4 percent) was more than four times higher than current use (9.7 percent). We found no significant associations between reported functionality levels and Carnegie class or other institutional characteristics.

Plans to add functionality were not limited to those in a preoperational state: large majorities of operational respondents expect to increase their enterprise directories’ functional scope. Nearly three-fourths (73.8 percent) of partially operational respondents reported planning to add at least one function to their enterprise directory, as did two-thirds (66.1 percent) of those fully operational.

Application Use of Enterprise Directories

One key purpose of an enterprise directory is to offload authentication and authorization functions from distributed systems so that these tasks can be conducted more consistently, securely, and efficiently. At the same time, because these functions have historically often been built into applications, or because local units have maintained their own identity infrastructure, centralizing has been a challenge.

To find out how much of this functionality the enterprise directory has assumed, we asked respondents to choose from a list of 12 common system types the ones that use their enterprise directories. Figure 6-4 presents the results for those respondents who were “operational,” that is, reported having a partially or fully operational enterprise directory. Among operational respondents, the mean number of applications reported to be using the enterprise directory was 6.40 (std. deviation = 3.021), and the median was 6.0. Somewhat surprisingly, we did not find that
the mean varied significantly by Carnegie or other institutional characteristics.

Classic central infrastructure services and enterprise applications dominate the high end of the use results. The highest use rates were reported for directory-friendly network systems such as e-mail directories (93.5 percent) and network operating systems (75.8 percent). Among core campus applications, course management systems had the highest reported rate (73.0 percent), perhaps reflecting the relative newness of these systems. Majorities reported enterprise directory use by student information (59.1 percent) and human resource systems (53.5 percent), but surprisingly, business services systems rated low relative to the others (36.3 percent). We found little significant variation by Carnegie class or other institutional characteristics. Alumni systems were an exception: their enterprise directory use was reported at 42.4 percent of privately controlled institutions, versus 23.0 percent of publicly controlled ones.

Among operational respondents from institutions where the enterprise directory’s scope includes the medical center (N = 40), 32.5 percent report that medical center applications use the enterprise directory.

The general tendency for enterprise directories to support central rather than departmental infrastructure and applications was clear from the low usage reported by departmentally controlled systems. Only 27.4 percent of operational respondents reported that any such systems used the enterprise directory. The rate was much higher among doctorals (47.3 percent) than among the other Carnegie classes, which ranged from 15.8 percent (associate’s and master’s institutions) to 17.1 percent (baccalaureate). Institutions with more than 15,000 students also had a higher rate of reported departmental system use (46.6 percent) than those having between 4,001 and 15,000 (25.0 percent) and those with 4,000 or fewer students (14.3 percent). We speculate that these patterns are influenced by the relatively greater size and sophistication of departmental applications and support staff in doctoral and larger institutions.

At Northern Kentucky University, the IT unit confronted the issue of departmental systems by doing the groundwork of establishing infrastructure policies and standards—and by beefing up the IT unit’s authority. “The network is our network,” says Gary Pratt, associate provost for IT and CIO at Northern Kentucky University.
“We have the ultimate authority, and having policies gives us the ability to say ‘this is what you need to do.’” Pratt presses for departmental adherence to enterprise directory standards wherever possible. “If a department wishes to install local software, we request that it be able to interface with the enterprise directory, and if it can, we require them to purchase that component. This is now a standard for all software we bring in.” The University of Wisconsin–Madison also encourages departmental system enterprise directory use. “One well-managed central authentication is better than lots of separate systems,” says Mairéad Martin, manager of middleware systems technology at UW–Madison, where more than one hundred applications use the central WebISO facility. “The end users ultimately benefit. They don’t have to build their own authentication. There’s a security piece also, and there is more accurate information.”

Whatever the challenges of reaching departmental systems, our respondents overwhelmingly endorse the goal of enterprise directory use by central IT resources. Asked to state their level of agreement with the statement “Our goal is to have all or most of our central IT applications use the enterprise directory,” 85.5 percent agreed or strongly agreed (see Figure 6-5).

**Enterprise Directory Policies**

As the sections above indicate, enterprise directories touch on many facets of institutional life. They inform decisions about access and resource availability; they reconcile conflicting or ambiguous information from many sources; and they may become a standard in the institutional infrastructure that other systems reference and rely on.

All of these tasks imply that enterprise directories need policy decisions to function, but are those policies simply embodied in enterprise directories de facto or are they documented? David Renaker, lead systems analyst at Northern Kentucky University, thinks they need to be documented. “We look at our security and privacy policies not as something you use or think about once in a while,” says Renaker, “but as part of our daily campus life. That establishes a good working baseline, so that when people come to the table to talk about issues such as IdM, they have a common

![Figure 6-5. Goal Is to Have All or Most Central IT Applications Use the Enterprise Directory (N = 360)](image)
reference point and are already engaged.” UW–Madison’s Martin adds that getting data owners involved is critical. “If you’re going to build a person registry, get your requirements and business case up front and build to scale initially,” she says. “Start with stakeholder involvement. Because you’re using others’ data, you need to involve them.”

We asked our respondents who were at least considering an enterprise directory to tell us whether they had documented policies for their enterprise directories in specific areas, or no documented policies at all. Figure 6-6 shows the results.

We found that overall documentation runs behind the pattern of enterprise directory use and planned use shown in Figure 6-1. The reported 46.9 percent “no policies documented” rate suggests that a small majority of those respondent institutions at least considering an enterprise directory (53.1 percent) do have some policy documentation. However, this should be compared with the overall 69.4 percent that reported currently implementing an enterprise directory or having one at least partly operational; the additional 10.2 percent that have planned one; and the 13.7 percent currently considering one. What’s more, specific policy documentation areas are reported at much lower rates. The most common area of policy reported was user access control (who gets access to what), at 29.3 percent of those institutions at least considering an enterprise directory, while 24.8 percent have documented their enterprise directory’s role and authority.

We found a few associations between institution size, Carnegie class, and some of the policy areas shown in Figure 6-6. Midsize institutions, those with between 4,001 and 15,000 students, had a higher “no policies documented” rate (54.5 percent) than those with 4,000 or fewer students (48.6 percent) or more than 15,000 (28.8 percent). We speculate that this may be a result of having more-complex policy decisions to make than smaller institutions, thereby requiring more effort to document them, while having fewer resources than bigger institutions. Several key specific policy areas showed a pattern of dominance by doctorals and lower figures, with little variation, among the other Carnegie classes. Documented policies for data ownership and definitions, for example, were reported by 39.2 percent of doctorals, while the other Carnegie classes ranged between 16.7 percent (BA institutions) and 19.0 percent (AA institutions). Policies for enterprise directory data privacy were reported by 43.3 percent of doctorals, 20.8 percent of master’s and associate’s institutions, and 21.4 percent of baccalaureate institutions.

![Figure 6-6. Documented Policies for Enterprise Directory (N = 375)](image-url)
This pattern may be due to the greater resources available at doctoral institutions. Even strong advocates for documented policies acknowledge that creating them is a big job. “The first step is to categorize data and develop policies for each category—who has access and under what conditions,” says Gordon Wishon, CIO, associate vice president, and associate provost at Notre Dame. “There are also policies regarding a variety of data integrity standards. We have been working on these policy issues over the past three years. We established a data oversight committee to develop such policies, including a governance structure and framework for applying policies.”

The good news about enterprise directory policy documentation is that reported “no policies documented” rates tended to drop with advancing stages of enterprise directory adoption. As Figure 6-7 shows, these rates were highest among those respondent institutions still planning to implement an enterprise directory and lowest among those that were fully operational. Interestingly, those currently considering an enterprise directory had lower “no policies documented” rates than planners. The bad news, however, is that even among those with fully operational enterprise directories, 33.0 percent had no documented policies, and among those planning to implement within 12 months, 75.0 percent had none. Figure 6-8 breaks out the reported documentation rates for specific policies among those institutions with partially and fully operational enterprise directories. Documentation rates of specified policies (not counting “other”) range from 25.2 percent to 35.9 percent for partially operational institutions and from 32.1 percent to 43.8 percent for fully operational ones. In short, no single policy category that we specified is reported to be documented by a majority of operational institutions.

**Enterprise Directory Approaches**

To find out how institutions are approaching the often complex task of implementing an enterprise directory, we provided a list of common approaches and asked respondents who were at least considering enterprise directories to tell us which ones they had taken or would take. (Note that the results mix both current and planned approaches.) As Figure 6-9 shows, commercial approaches dominated. The most common reported approach is via multifunction network operating systems (NOSs) such as Microsoft Active Directory and Novell Directory Services (NDS)/eDirectory. While 44.0 percent of users report an
NOS approach, more than one in four (28.0 percent) report implementing or planning to implement an enterprise directory as a stand-alone system using commercial software, and another 21.1 percent report approaching it as part of vendor-supplied application software such as an ERP solution.

Open source software such as OpenLDAP was not as large a factor in enterprise directories as in RSSO (see Figure 6-13), though nearly one in four respondents (22.9 percent) did name it. Legacy applications were a negligible source for enterprise directory approaches (2.1 percent), but stand-alone homegrown enterprise directory solutions (10.1 percent) were more common.

To John Grosen, director of infrastructure services at North Dakota State University, both open source and homegrown solutions are part of the campus’s IT culture. “This is in part a philosophical issue for us,” Grosen says. “We have traditionally been a part of the UNIX community, and historically, this is a community that shares software. When we went to a distributed...
environment, there were not any real proven IdM vendor options, so we decided to remain consistent with our UNIX heritage and develop our own solutions. We are committed to open standards and will not choose proprietary software for IdM.” But to Michael Welch, dean of academic technology services at Blinn College, the development demands of open source rule it out as an alternative to the college’s blend of Sun Directory Services and LDAP server with Microsoft Active Directory. “We do not have the resources to implement open source software, and it doesn’t appear to fit well with our community college environment. Perhaps if we had a development staff, it might be an option.”

Only 16.8 percent of respondents say they have an enterprise directory that integrates multiple directories to act as a single directory. As we will see shortly, many institutions have the ambition to do just this, but some of our interviewees said they recognized that a single directory wasn’t feasible. “We’re taking the approach that there’s not a single directory that will serve as the complete authoritative source,” says Wishon of Notre Dame, “but a set of directories, or a directory ‘cloud,’ that will be fed information from different data sources. There are lots of moving parts in this process, and no single magic bullet will provide all the services we need.”

We found little significant variation among Carnegie classes or other institutional categories concerning enterprise directory approaches. One exception was the use of stand-alone commercial enterprise directory software: 42.3 percent of doctorals reported that they used it or would use it, while all the other Carnegie classes ranged from 18.1 percent (baccalaureate) to 23.8 percent (associate’s institutions).

Surprisingly, given the complexity of implementing an enterprise directory, individual responding institutions did not report using numerous approaches. Among those respondents naming any approaches, more than half (57.5 percent) named only one, while the mean number was 1.71 (std. deviation = 1.007).

When we asked how they planned to change their approach in the future, the most frequently named plan (24.3 percent) was to replace or reduce multiple directories with a single directory (see Figure 6-10). Plans to use more standards-based software and open source solutions followed close behind, however, and 17.1 percent of respondents reported plans to use more commercial software. Few respondents (8.0 percent) plan to migrate from an enterprise directory that is now part of another application to a stand-alone enterprise directory system.

**Enterprise Directory Technologies**

 Asked to select from a list of seven technologies (plus “other”) those they were using or planned to use for their enterprise

![Figure 6-10. Plans to Change Enterprise Directory Approach (Multiple Responses Allowed, N = 375)](image-url)
directories, our respondents reported a mix of commercial and open solutions similar to what we saw in the approaches results above (see Figure 6-11; compare with Figure 6-10).

LDAP, supported by many commercial and open source products, was easily the most commonly reported technology. Interviewees repeatedly described LDAP as the key tool they were using to bridge between applications and the identity infrastructure they were building. Embry-Riddle Aeronautical University, for example, began moving toward its Oracle-based enterprise directory by requiring that all new applications coming to campus support LDAP. Wayne State University did the same. “We led the charge toward enterprise directory early on with LDAP,” says John Camp, CIO at Wayne State.

Though widely used, LDAP is not universal, and its reported use or planned use varied with institutional size and Carnegie class. Among institutions of 4,000 or fewer students, 71.9 percent of respondents reported using it, while the rate was 95.0 percent among institutions of more than 15,000 students, and 82.6 percent for those in between. Reported LDAP use also tended to rise along with Carnegie degree levels, ranging from 70.8 percent among baccalaureate institutions to 90.7 percent at doctorals.

Despite its popularity, LDAP has limitations that have led institutions to blend it with other approaches. “LDAP is good for managing people assets, but not so good for objects,” says Notre Dame’s Wishon. “[Microsoft] Active Directory is far better than LDAP for objects such as servers, so our enterprise directory uses a combination of solutions including LDAP, Active Directory, and others.”

Consistent with these observations, network operating systems were prominent in our results. Running second in popularity to LDAP, Microsoft Active Directory, at 66.7 percent, was the most common technology of this type, while Novell Directory Services (NDS) was reported by 18.1 percent. The pattern of reported or planned Active Directory use among Carnegie classes was the opposite of that for LDAP, ranging from 51.5 percent among doctorals to 85.7 percent among associate’s institutions. We found no significant variation in NDS use by institution size or Carnegie class.

Structured Query Language (SQL), the database access standard that can be used to introduce relational features into historically hierarchical directory environments, achieved modest penetration at 24.5 percent of respondents, but some more recent and exotic technologies remain marginal. Extensible markup language (XML), the versatile W3C tool for structuring and exchanging data, found a foothold among our respondents (16.8 percent use or planned use), but only a few (2.1 percent) use or plan to use the XML-based Directory Services Markup Language (DSML) standard, approved in 2002. The older
X.500 directory services standard, from which LDAP was derived, was also a minor presence, with 3.7 percent reported or planned use.

Besides the technologies listed in Figure 6-11, we asked respondents whether their enterprise directory development has been influenced by the eduPerson object classes, which are LDAP-based directory schema overseen by an EDUCAUSE/Internet2 task force (MACE-Dir, 2003). It has been an influence, according to 35.3 percent of respondents, while another 25.3 percent said they didn’t know. “We adhered to eduPerson and emerging standards to the extent possible,” says Wayne State’s Camp of their enterprise directory project, “so we’d have a high likelihood of being able to collaborate.”

**Reduced or Single Sign-On**

Also known simply as single sign-on, RSSO has often taken on an extra modifier in recent years because many IT units have discovered that providing a user with a single authentication event that will work across systems seamlessly, invisibly entering new authenticated sessions as he or she moves from application to application, can be fiendishly difficult. When an RSSO project was approved at Embry-Riddle Aeronautical University, says IT Services Director Becky Vasquez, “We on the IT staff said, ‘yeah, right.’ It’s not an easy thing to do. There’s so much disparity between applications, it’s almost overwhelming.”

The Vermont State Colleges system office “started out using the term ‘single sign-on,’” reports Linda Hilton, CIO at VSC, “but this term creates the unrealistic expectation that you log in once for the day and, bingo, everything is delivered to you. In practicality, we can’t do that for five campuses and a system office, so we began to use other terms such as ‘consolidated user logon.’”

Just the same, RSSO is a popular IdM technology application because, as interviewees told us repeatedly, it has obvious appeal as an improvement in user service. The University of California at San Diego’s large-scale IdM efforts grew out of a staff survey on how to improve the university’s business processes. “We were surprised to find that single sign-on came out on top,” says UCSD’s CIO, Elazar Harel. “Our customers said it was too complicated to have so many accounts and passwords.”

Embry-Riddle’s Vasquez found RSSO to be the most convincing argument in favor of IdM when they present to business departments. “Whenever we show single sign-on, people get it,” she says.

As we noted above (see Figure 6-1), only 10.2 percent of our respondents reported a fully operational RSSO implementation, though another 24.9 percent report being partially operational. As Figure 6-12 shows, RSSO adoption varied across Carnegie classes. Doctorals reported the highest fully operational rate at 16.2 percent, but baccalaureate institutions were nearly as high (14.5 percent), while the other Carnegie classes reported considerably lower levels (master’s 6.3 percent, associate’s 2.1 percent). No Canadian institutions reported being fully operational, but 29.2 percent reported being partially operational and another 29.2 percent reported an implementation in progress.

As with enterprise directories, RSSO proved so popular among our respondents that few answered our questions about why they were not considering it. Nonetheless, we gathered some useful insights. Ten of the 14 respondents who gave us at least one primary reason for not considering RSSO named higher IT priorities. Six said RSSO capabilities were not required at this time, and five said they considered it a security risk. Interestingly, no respondents cited either data integrity problems or the difficulty of developing campus policies and procedures as a primary reason not to pursue RSSO.

Our questions about what approaches respondent institutions at least considering RSSO (that is, considering, planning, implementing,
or operational at some level) are or will be taking to the technology revealed a mixed pattern with no dominant approach (see Figure 6-13). Reflecting RSSO’s unsettled status at many institutions, in fact, the number of respondents who had not determined an approach (33.6 percent) was in a near-tie with the two top approaches named. About one-third each said they were using or planned to use commercial vendor software (32.8 percent) such as products from RSA or Aladdin, or open source software (31.5 percent) such as MIT’s Kerberos, Yale’s Central Authentication Service (CAS), or the University of Washington’s PubCookie. Homegrown software, though named by only 24.3 percent of respondents, was more popular for RSSO than for enterprise directories or RBA (compare with Figures 6-9 and 6-15).

Open source solutions were associated with Carnegie class: 51.0 percent of doctorals reported using them, compared with 20.9 percent of associate’s institutions; MA and BA institutions were close together in between, at 28.7 percent and 25.7 percent respectively. Likewise, 50.6 percent of institutions with more than 15,000 students reported open source as an RSSO approach, compared with 19.7 percent of those with 4,000 or fewer students and 33.6 percent of those in between. By contrast, we found no significant variation by Carnegie class or institution size in commercial RSSO solutions use.

A follow-up question to the RSSO approaches items mentioned above succeeded mainly in reemphasizing the extent to which our respondents’ plans remain unsettled. Asked if they expected to use more commercial RSSO software in the future, about one-third (33.9 percent) said they did, and another one-fifth (21.5 percent) said they didn’t. But the largest group, 44.6 percent, responded “don’t know.”

![Figure 6-12. RSSO Adoption Status (N = 403)](image)

![Figure 6-13. Current and Planned RSSO Approaches (Multiple Responses Allowed, N = 387)](image)
Role-Based Authorization

The ability to give users automatic authorized access to IT resources on the basis of the roles they occupy within the institution and their affiliations with other entities and users is a goal shared by a large majority of our respondent institutions. As we noted above, only 13.7 percent of respondents told us they were not considering RBA (see Figure 6-1). Still, this was a higher “not considering” response than we got for either enterprise directories or RSSO, and correspondingly, RBA also had the lowest fully operational rate—5.7 percent. We found no statistically significant associations of RBA adoption with Carnegie class or other institutional characteristics.

It isn’t hard to understand both the desire for RBA and the challenge of implementing it. Deciding what people can do (authorization) is inherently more complex than determining who they are (authentication). While authentication relies on a relatively limited set of data elements and credentials that trace back to a particular individual’s verified existence, authorization depends on a large and constantly changing set of characteristics associated with the individual, as well as on business rules that are themselves subject to frequent permutation. An extra complication is that the business rules governing authorization are often developed in isolation, leaving users with multiple roles ensnared in a tangle of ambiguous, overlapping, or mutually contradictory privileges (Gebel, 2004b). At the same time, taking a strongly centralized approach to defining roles in the decentralized management environments that typify most universities can create backlash and enmesh the project in time-consuming negotiations (Kampman, 2003). Though a standard for role-based access control (ANSI INCITS 359-2004), developed by the National Institute of Standards and Technology, was approved by the American National Standards Institute in 2004, its influence so far has not been widespread.

It’s not surprising, then, that authorization is often imbedded deep within the logic of applications, where it is inaccessible to other systems or handled through manual interventions in which IT staff write scripts treating discrete situations. “We don’t want to authorize access so much by exception, as in the past, but rather by role,” says Northern Kentucky’s Pratt of their RBA initiative. RBA systems can supply a structure for matching individuals, roles, and rules automatically, while potentially also allowing privilege management to be delegated to appropriate persons outside the IT unit (Barton, 2002).

RBA was the one technology we asked about that a sizeable number of respondents (49) told us why they were not considering it at this time. The responses suggest that many respondents see RBA as a “downstream” element of the IdM infrastructure that requires preparation they haven’t yet completed (see Figure 6-14). By a large margin, the reason with the highest number of responses (34) was that “we are not that far along in our identity management project,” while higher IT priorities (24) was second. As one respondent put it in an open response, “Authorization is still done by our individual ‘best of breed’ administrative systems, although we are lurching and stumbling towards a partial enterprise directory and are part of the way there.”

By contrast, only 13 of the 49 respondents not considering RBA said that their institution didn’t need RBA capabilities at this time. Technical and policy reasons were mentioned even less often. Four respondents said that the immaturity of technical solutions was a primary reason, and two or fewer mentioned such issues as the difficulty of developing campus policies, lack of senior management support, or data integrity problems. It should be kept in mind, however, that this response pattern may reflect the early state of some respondents’ IdM projects or engagement with RBA, rather than the perceived ultimate difficulty such issues pose.
Responses to our questions about current and planned RBA approaches among institutions at least considering the technology (that is, considering, planning, implementing, or operating at some level) also suggested an unsettled and contingent state of preparation (see Figure 6-15). The most common response was “not yet determined,” which at 42.1 percent was higher than the comparable rates for both enterprise directories and RSSO. Among those reporting specific approaches, commercial ones dominated. RBA implemented as part of vendor-supplied application software (such as ERP systems) was the most commonly reported specific approach, at 33.4 percent; another 18.2 percent reported the use or planned use of stand-alone commercial RBA software.

Asked whether they planned to use more commercial RBA software in the future, more respondents said they did (32.2 percent) than didn’t (16.5 percent), but the largest group (51.3 percent) replied “don’t know.”

Somewhat surprisingly, given the intimate relationship between RBA and local business practices, homegrown software had a smaller presence within RBA (21.3 percent) than within RSSO, though a larger presence than within enterprise directories.

Responses to an open question asking respondents to describe the technologies they were using for RBA generally mirrored the approach results shown in Figure 6-15, as did comments from some of our interviewees. In particular, several confirmed that RBA depended on “upstream” developments, especially an enterprise directory. “Most role/privilege-based/group authorization will be implemented in the enterprise directory,” one respondent wrote. “The ED is automatically managed via data from various authoritative sources that are vendor-supplied and legacy applications.” The University of New Hampshire’s Baber told us they had “invested a lot in three years in bringing the core infrastructure into place. The next thing is exploring how to do authorization better.”

Many open responses mentioned commercial directory products such as Microsoft Active Directory, Novell eDirectory, and the Sun and Oracle IdM suites, as well as vendor portal products, as current or planned RBA-enabling technologies. However, enough open responses and interviewees mentioned interest in open source solutions to suggest that the low 8.9 percent rate gathered by our approaches question understates interest in open source. The Signet privilege manage-
ment and Grouper group management initiatives being overseen by the NSF Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium drew particular mention; both are available in pre-1.0 evaluation versions. “One of the most significant challenges [in IdM] will be to develop and deploy a single, delegated access approval service,” says Notre Dame’s Wishon. “The Signet Project is doing interesting work in this area, and we’re watching this carefully.”

Because of the tangle that can develop in authorization processes over time, advisory groups recommend that RBA projects include policy documentation and business practice rationalization phases (Nikols, 2005; Gebel, 2004b; Bellina, 2002). We asked respondents who were at least considering RBA their opinion about whether their institution was committed to revising current business practices before entering them into an RBA system (see Figure 6-16). While the results produced a mixed picture, respondents overall were more optimistic than pessimistic. A total of 42.7 percent agreed or strongly agreed that the institution was committed, while only 13.9 percent disagreed or strongly disagreed. About one-third (32.5 percent) were neutral, while a 10.9 percent “don’t know” response indicated the degree of uncertainty that attends RBA planning.

At the University of California at San Diego, the IT unit’s IdM project committee, led by Charlotte Klock, data center director, is working with individual business departments to define a manageable role structure. “We’re trying to sensitize the campus to have a small number of manageable roles,” says CIO Harel. “If you have too many roles, you have no roles at all.” UCSD’s data security manager, Gabriel Lawrence, wrote programs to look for commonalities in how the institution’s authorizations were set up. “It turns out a large number of people with similar job types had similar access,” says Lawrence. “But they’d gotten authorization the hard way, by calling up and getting it. We want the role system to say, ‘This is someone who works, say, with employment information.’ We don’t want to tweak each person’s access rights down to the individual level.” Where roles are more broadly defined, Lawrence notes, they can be more easily and flexibly reassigned. “If you’re a financial manager for federal grants and another person does state grants, what if that person gets hit by a bus? Departments need to be able to have people work interchangeably.”

As they did with enterprise directories, respondents who were at least considering RBA described ambitious goals for their RBA systems. Asked their opinion about the statement “Our goal is to have all or most of our
central IT applications use the automated role- and privilege-based authorization system,” more than two-thirds (67.6 percent) agreed or strongly agreed (see Figure 6-17). Only 5.3 percent disagreed or strongly disagreed, though another 9.3 percent responded “don’t know.” As with other RBA results, we found no significant association between levels of agreement and Carnegie class or institution size.

**Sourcing Approaches to Enterprise Directories, RSSO, and RBA**

The results above make it clear that IdM’s prominence in IT circles during recent years is not just the product of hype. Slightly more than half of respondents had operational enterprise directories at some level, and roughly one in three reported fully or partially operational RSSO and/or RBA (see Figure 6-1). Very few institutions, furthermore, were willing to rule out these technologies, and reported future plans suggest high growth rates for operational implementations.

At the same time, the variation in adoption rates at different stages makes it clear that these technologies’ maturity—and respondent institutions’ experience with them—diverges considerably. Enterprise directories are by far the most likely to be reported as fully operational; overall, they seem to be acting as the technological vanguard for IdM infrastructure. Table 6-7, which summarizes the sourcing approaches for each technology, shows that respondent institutions reported their current or planned enterprise directory approach “not yet determined” at less than half the rate than for the other two technologies. (Note that respondents were able to select more than one approach in each case, so the columns in Table 6-7 do not total 100 percent.) Enterprise directories were also the area where respondents were the most likely to use or plan to use one or more commercial software approaches (including stand-alone systems using commercial vendor software, systems implemented as part of vendor application software such as ERP or, in the case of enterprise directories, network operating systems).

On the surface, at least, it appears that commercial software approaches to both RSSO and RBA are likely to grow. About one-third of respondents who were at least considering the technologies told us in each case that they planned to use more commercial software in the future for RSSO (33.9 percent)
and RBA (32.2 percent), close to double the rate of those saying the same about enterprise directories (17.1 percent). However, high “don’t know” rates suggest that for much of our respondent base, the jury is still out on more adoption of commercial solutions. More than half of RBA respondent institutions (51.3 percent) said they didn’t know whether they planned to use more commercial software, and nearly as many (44.6 percent) said the same for RSSO—in each case, more than said they did or did not plan to.

None of this is surprising, given the large proportion of institutions in a preoperational state in all IdM technologies, especially RSSO and RBA. But the combination of a great deal of planned activity and a large dose of uncertainty underscores the amount of work that our respondent institutions have to do. As we reported in Chapter 4 and further describe in our section on enterprise directories above, accomplished levels of IdM preparation in areas such as metrics, documentation, and risk assessment are relatively low, even as planned work is in many cases much higher. Our respondents’ ability to successfully realize their IdM technology adoption plans may depend on how well they realize these other plans.

Table 6-7. Current and Planned Sourcing Approaches for IdM Technologies, by Technology and Approach (Multiple Responses Allowed)

<table>
<thead>
<tr>
<th>Sourcing Approach</th>
<th>Enterprise Directory</th>
<th>Reduced or Single Sign-On</th>
<th>Automated Role-Based Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>One or more commercial software approaches</td>
<td>68.8%</td>
<td>32.8%</td>
<td>43.8%</td>
</tr>
<tr>
<td>Open source</td>
<td>22.9%</td>
<td>31.5%</td>
<td>8.9%</td>
</tr>
<tr>
<td>Homegrown, developed at home or other institution</td>
<td>10.1%</td>
<td>24.3%</td>
<td>21.3%</td>
</tr>
<tr>
<td>Part of legacy application</td>
<td>2.1%</td>
<td>N/A</td>
<td>6.9%</td>
</tr>
<tr>
<td>Not yet determined</td>
<td>15.5%</td>
<td>33.6%</td>
<td>42.1%</td>
</tr>
</tbody>
</table>

Figure 6-17. Goal Is to Have All or Most Central IT Applications Use the RBA System, (N = 311)
Federated Identity

Key Findings

- Doctoral institutions are almost three times as likely as the next nearest Carnegie class (associate's) to be among the 14 percent of institutions reporting that they see a need now for a federated identity solution.

- Roughly half of respondents said they saw a future need to take part in a federated identity solution, suggesting high relative growth of this need in the next few years. However, we found no clear "tipping point" toward ubiquitous adoption. More than one in five respondents said they didn’t know when they would need such a solution.

- Rates for actually implementing federating technologies such as Shibboleth or Liberty Alliance run lower than those for reporting a current need to take part in a federated identity solution. About four in 10 of those institutions reporting a current need also report implementing a federating technology, with implementations by doctoral institutions greatly exceeding those of other Carnegie classes. Overall, about 13 percent of total respondents said they were implementing a federating technology.

- Fewer than 4 percent of responding institutions report belonging to the InQueue or InCommon federations, but planned membership exceeds current membership in both cases.

With roots in the monastery and an old habit of self-sufficiency that causes many campuses to look like city-states, modern colleges and universities can be self-absorbed places. Even in the Internet era, much institutional strategy remains governed by a conviction that the institution with the richest internal resources—in the library, the laboratory, or the IT infrastructure—wins the prestige race. To a considerable degree, the identity processes this study has investigated so far remain focused on local administration.

Trends in research, learning, and business, however, are also stimulating higher education's other heritage—the outreach to scholarship and communities necessary to maintain a vital academic life. Network technologies have, of course, created an impressive technical capability to share, yet thorny problems remain that put practical limits on resource exchange. Many of these relate to identity. Even as privacy regulations increasingly limit the degree to which institutions can expose identities, enormous realms of academic content have migrated to digital environments restricted to duly authorized users. Many business processes have made a similar migration. And research grids linking resources and investigators from many institu-

Let olde angrie fathers lurke in an Hermitage: Come, weele associate this jolly Pilgrimage!
—Thomas Campion
tions face special challenges passing authorization attributes from diverse environments.

“Owning” all such resources internally is neither feasible nor desirable. Securely opening them up to large collaborative communities is one of the key challenges facing higher education IT. Indeed, it is conceivable that in a densely networked future, the greatest competitive advantage will accrue not to those with the most internal resources but to those with the most fluent and flexible pathways to the world’s riches.

In recent years, a new model of networked resource sharing has emerged to confront this challenge. Federated identity lets entities in different IT domains share user attribute information, making resources from the entire group available to users who are known and authorized in only one domain. In contrast to unwieldy older methods of cross-domain authentication and authorization that tightly coupled technical infrastructures, federated identity seeks a standards-based, loosely coupled approach to interoperability (Carmody, 2001; Blum, 2005). Nor are its concerns purely extra-institutional. Federated identity can also be used to cross intra-institutional domains—for example, by enabling reduced or single sign-on, authentication, or authorization.

Federated identity is still in its technological infancy, and the critical policy and community-building components that make it work are, if anything, even less developed. But enough progress has been made to merit studying how higher education is now using it and planning for it. This chapter addresses our respondents’ perceived need for federated identity solutions, their plans for implementing its technologies, and their participation in identity federations.

**Institutional Need for a Federated Identity Solution**

To gauge interest in federated identity among our respondents, we asked them when they thought their institutions would need to participate in a federated identity solution—that is, one requiring automated management of identity information between their campus and other institutions and organizations—to facilitate collaborative or business initiatives. The responses spread widely, suggesting rapid growth over the next few years but with no obvious “tipping point” toward ubiquitous adoption. Altogether, 62.3 percent reported a need for federated identity in some time frame (see Figure 7-1). About one in seven respondents (14.3 percent) said they had a need...
now, and a similar number (15.1 percent) said they did not envision a need. Roughly half of respondents reported a future need, divided about evenly between those who envisioned it in the next two years (23.6 percent) and those who thought it would be two or more years (24.4 percent). “Don’t knows” were a sizable factor at 22.6 percent.

Doctoral and large institutions reported a perceived need more often than others. Of institutions with more than 15,000 students, 26.5 percent reported a current need, while only 7.5 percent of those with 4,000 or fewer students did so. As Figure 7-2 shows, doctorals reported a current need for federated identity at nearly three times the rate (30.3 percent) of associate’s institutions (10.6 percent), and they reported not envisioning a need at roughly one-third the rate (6.1 percent versus 17.0 percent). A corresponding and equally striking difference between doctorals and other institutions was their lower “don’t know” rate. Respondents at master’s and bachelor’s institutions were about two and a half times more likely than those at doctorals to report not knowing when their institution would need to take part in a federated identity solution, and respondents at associate’s institutions were nearly five times as likely.

Among the needs that federated identity must address is appropriate user privacy protection. While federated resources might exchange user-identifying information—say, account data about a mutual customer shared between an airline and a rental car company—they can also authorize use on the basis of trusted assertions that reveal only nonidentifying status or privilege information. Thus, a student at one university might gain anonymous access to digital library resources at another university solely on the strength of the second institution’s acceptance of assertions from the first that it has authenticated and authorized the student as a legitimate user. Thanks in part to federal protections on student information and the principle of keeping library patronage confidential, an emphasis on user privacy has been a strong shaping force on Internet2’s Shibboleth federated identity project for higher education (Morgan et al., 2004; Simmons, 2004).

Our survey results strongly suggest that our respondents will wish to maintain anonymity in some situations that federated identity may enable. Asked to rate their level of agreement with the statement that “it is important to provide anonymous access to certain network services, such as library content, whistle-blowing, etc.,” two-thirds (68.4 percent) agreed or strongly agreed, while only 11.4 percent disagreed or strongly disagreed (see Figure 7-3).
Federated Identity Implementation and Approaches

No single framework governs federated identity. The main focus of higher education activity has been Internet2’s Shibboleth project, which is built on the Security Assertion Markup Language (SAML) standard but adds functionality, in particular user anonymity, of special interest to higher education. Outside higher education, the most prominent organization promoting federated identity is the Liberty Alliance, an umbrella group of more than 150 corporate and public sector organizations that has worked on SAML-based open standards. While Shibboleth is both a set of specifications and an open source implementation of them, the Liberty Alliance focuses on specifications for use by external technology providers, as well as policy guidelines and interoperability tests. An additional initiative driven mainly by IBM and Microsoft, WS-Federation, takes a Web services approach to federation and may be of interest to institutions because of its incorporation into products from Microsoft and other providers. Unfortunately, conflicts between the different standards initiatives have compromised their interoperability, though a degree of convergence is evident as well (Blum, 2005; Liberty Alliance Project, 2003; IBM Corp. & Microsoft Corp., 2003). One recent sign of progress was Shibboleth Version 1.3’s extension of support for Microsoft’s Active Directory Federated Services, which will open up Shibboleth-based federations to institutions using ADFS.

We found that implementation rates of such technologies were roughly in line with, but somewhat lower than, the responses of those reporting a perceived need for a federated identity solution. Asked if they were implementing Shibboleth, Liberty Alliance, or another federating technology, or planned to in the future, half of respondents (50.5 percent) said no (see Figure 7-4). Given that only 15.1 percent had said they saw no need for federated identity in any time frame (see Figure 7-1), this higher “no” rate makes it clear that many respondents who see a need are at institutions that have no corresponding plans to fulfill it with current technologies. Among those who say they have a need now to adopt a federated identity solution, only 42.3 percent reported implementing a federating technology, while another 28.8...
percent planned to. Among those saying they saw a need in some future time frame, 15.9 percent reported implementing a technology and 38.2 percent reported planning to do so.

Altogether, 13.4 percent of respondents said that they were implementing federating technologies, and another 22.7 percent said their institution planned to do so in the future. Doctoral dominance was even greater for implementation than in the need-to-participate results (see Figure 7-5). While 34.3 percent of doctorals reported an ongoing implementation of federating technology, no associate’s institutions did so, and the second-highest reported rate (among master’s institutions) was 6.3 percent. Majorities of all the nondoctoral Carnegie classes reported no implementation in progress or planned.

Though our implementation question didn’t distinguish among federating technologies, virtually all interviewees’ comments referred to Shibboleth. Collaborative use of extra-institutional resources was one prominent theme. The Houston Academy of Medicine’s Texas Medical Center Library, which serves more than 40 institutional consortium partners, Shibbolized its Web access system in a pilot project, funded by an NSF Middleware Initiative (NMI) grant, that it is now moving to production status. “They loved it,” says Barry Ribbeck, Rice University’s director of systems architecture and infrastructure, who led that part of the project. “It will reduce their IdM

![Figure 7-4. Implementing Shibboleth, Liberty Alliance, or Another Federating Technology (N = 396)](image)

![Figure 7-5. Implementing Shibboleth, Liberty Alliance, or Another Federating Technology, by Carnegie Class (N = 331)](image)
requirement to a few hundred accounts, as opposed to the 17,000 they were looking at.” Organizations deploying Shibboleth for collaborative or extra-institutional resources include

◆ Pennsylvania State University, which has used it for student authorizations to the Napster music download service and in its LionShare peer-to-peer academic content exchange;

◆ Duke University, which is partnering with the library management systems vendor Ex Libris to Shibbolize Ex Libris products; and

◆ the London School of Economics and Columbia University, which have used Shibboleth to enable the mutual exchange of anthropology teaching and library materials.

The early state of higher education identity federations, however, has so far limited extra-institutional Shibboleth uses. Perhaps reflecting this, several interviewees emphasized their interest in Shibboleth for internal processes. The University of California at San Diego is using it to tie together authentication among its diverse systems. “We do 15,000 successful authentications a day, with peaks of 30–35,000 at times,” says UCSD’s data security manager, Gabriel Lawrence. “We’ve customized parts of it. The Shib piece covers attribute resolution and exchange, not the actual authentication event.” At North Dakota State University, IT Infrastructure Director John Grosen notes that “we think there is a good marriage between Shibboleth and what we’ve done with Hurderos,” the university’s open-source IdM initiative. “We are considering integrating Shibboleth with Hurderos for use as our single sign-on and authorization for Web applications.”

Interviewees not currently implementing Shibboleth frequently expressed an interest in it but were holding back to wait for the technology, constituent demand, or their own infrastructures to mature. “We don’t have many users who want it yet,” says Patrick Gossman, director of academic technologies and customer services at Wayne State University. “When we get a driving need, we’ll do it.” Even some strong Shibboleth advocates, like Rice’s Ribbeck, cautioned that it relies on a strong supporting identity infrastructure. “Not many institutions have the infrastructure to stand it up,” Ribbeck says. “You need an authoritative authentication system and a well maintained directory service to control authorization.”

To understand how institutions view Shibboleth in the context of other technologies and their overall federated identity strategies, we asked respondents which of various statements best described their institution’s approach to it (see Figure 7-6). As with other federated identity results, we found a high degree of uncertainty, but among those who are using or planning to use Shibboleth and have decided on an approach, most view it as a long-term part of their IT infrastructure. Only a handful of respondents (1.8 percent) described it as a short-term solution that they planned to replace with a commercial vendor solution in the future. Among the rest, those who described it as a long-term “niche” solution to be used with select applications (15.0 percent) outnumbered those who saw it as a long-term strategic solution to be used with most applications (12.1 percent). By far the largest number of respondents, however, weren’t planning to use Shibboleth (36.6 percent) or said their institution’s approach to it was not yet determined (34.5 percent).

Identity Federations

Technology solutions alone aren’t enough to achieve federated identity’s greatest potential. Trust communities or federations must also define the standards and operational practices required for membership, decide what kinds of resources to support and under
what conditions, determine liability and rectification procedures in the event that some member compromises or abuses data supplied by another, and otherwise build up the community “fabric” that puts federated identity technology to a particular use.

Within higher education, the InCommon Federation, overseen by Internet2, serves this function for educational and research collaborations enabled by Shibboleth. Another Internet2 initiative, the InQueue Federation, supports institutions that want to investigate Shibboleth but are not yet ready to establish production-level federated identity services. Shibboleth-based higher education federations similar to InCommon and InQueue are also being developed in other countries, including the UK (Shibboleth Development and Support Services, or SDSS), Finland (Haka), and Switzerland (SWITCHaai).

Our study asked respondents if their institutions belonged to InQueue or InCommon, or planned to join them in the future. Not surprisingly, given both federations’ newness, we did not find membership widespread (see Figure 7-7). Fifteen respondents (3.8 percent) said they belong to InQueue, while 13 (3.3 percent) told us their institution belongs to InCommon. Because of overlaps between the two, however, these 28 memberships represented only 20 individual institutions. Planned membership, though still modest, suggests room for considerable growth: 4.1 percent told us they had plans to join InQueue, and 6.9 percent plan to join InCommon. Though response sizes were too small to determine significant associations between membership and Carnegie class or institution size, doctorals were the large majority of those reporting memberships.

Because one task of a federation is to ensure a common level of operational integrity, joining a federation adds policy and legal requirements beyond the purely technical demands of operating Shibboleth or another federating technology. The bar is likely to rise as federation moves out of the experimental stage. At the University of Wisconsin–Madison, Mairéad Martin, manager of middleware systems technology, reports that the institution is strongly considering Shibboleth and is “exploring an initiative to make sure we meet the requirements of joining InCommon. Our authentication would have to be strong enough for their identity proofing requirements. We’ve been preparing. Building an identity management system is first.”
Summing Up the State of Federated Identity

Our survey results for federated identity present a somewhat exaggerated version of the same pattern of “great expectations” that we found in other areas we studied. Like IdM generally, federated identity seems to have won converts well beyond the ranks of those who have hands-on experience with the technology. Anticipated future activity considerably exceeds current activity both in perceived need to take part in a federated identity solution and in the actual implementation of federating technologies. With more than 60 percent of respondents reporting that they either currently need federated identity solutions or will in coming years, the occasionally voiced complaint that federated identity is a “solution in search of a problem” appears not to keep most from believing that, at the least, an appropriate problem will be found.

At the same time, both the quantitative results and our qualitative interviews suggest that the search is a real one. Many nonadopting institutions see potential in federated identity but do not yet have a campus constituency specifically demanding it. This may be one reason why some of our respondents are focusing on internal processes, like reduced or single sign-on, which have fairly immediate and comprehensible benefits for users and don’t require a high degree of coordination with outside parties. But to turn the high levels of planned activity into reality and convert the numerous “don’t knows” into committed implementers, federated identity will have to deliver concrete benefits of interest to institutions outside the realms of the large, deep-pocketed research universities. As we note in Chapter 10, digital content delivery and procurement are potential areas where federated identity could deliver a critical mass of benefits sufficient to encourage wider adoption.
Identity Management Projects

Amid a multitude of projects, no plan is devised.
—Publilius Syrus

Key Findings

♦ Involvement in IdM projects is nearly universal. About nine of 10 respondent institutions report being engaged in IdM efforts or projects.

♦ About one-third of institutions report that they have organized their IdM projects into a formal initiative.

♦ IdM projects are frequently bundled in with other projects such as ERP, security, and portal implementations. While six of 10 project-active institutions report some sort of bundling as an IdM project implementation strategy, fewer than three of 10 report stand-alone IdM projects.

♦ Experience with IdM projects is widely distributed, but more than 40 percent of project-active institutions had been working on their IdM projects for 18 months or less at the time of our survey.

♦ Anticipated central IT spending on IdM projects over the next three years is modest, with nearly half of project-active institutions expecting to spend $100,000 or less and only 10 percent expecting to spend $500,000 or more. Though these results do not capture all anticipated institutional IdM spending, they suggest that funding will be a challenge to IdM technology adoption plans.

♦ IdM project staffing levels are also modest. Nearly six of 10 project-active institutions report either one or two full-time-equivalent (FTE) staff assigned to IdM projects, and 14 percent have no assigned staff.

♦ The annual central IT budget was named as a project funding source by three-fourths of project-active institutions, while the next most common source, bundling with other campus projects, was named by 27 percent.

♦ When asked their current thinking about the IdM solutions approach their institutions will take, about four in 10 say they’ll use vendor solutions, though this is fragmented among different best-of-breed and suite approaches. Nearly one in four say they have not decided on a solutions approach.
The preceding three chapters dealt with what institutions are doing with IdM technologies. In this chapter, we look at how they’re going about it. Starting with an overview of IdM project activity and strategies, we go on to examine how IdM projects are funded and staffed, who sponsors and participates in them, and the challenges that respondents report facing when they implement IdM. Finally, we look at our respondents’ thinking about IdM solutions approaches and at what approaches they want their ERP vendors to take toward IdM.

Readers should note that except where otherwise indicated, the results presented here refer to those respondent institutions that are engaged in IdM-related efforts or projects, not the entire respondent population.

IdM Project Activity and Strategies

Given the importance our respondents see in IdM benefits (see Chapter 4) and their use and planned use of IdM technologies (Chapters 5 through 7), it’s not surprising to find that IdM project activity is nearly ubiquitous among them: 88.9 percent of our total respondent base reported being engaged in IdM-related efforts or projects such as enterprise directories, reduced or single sign-on, automated role- or privilege-based authorization, or federated identity. We found no significant variation among Carnegie classes. Though participation was lower among the smallest institutions, it was high across the board (see Figure 8-1). Among institutions with fewer than 4,000 students, 78.3 percent reported being active, compared with rates over 95 percent for the largest institutions.

Figure 8-1. Institutions Engaged in IdM Projects, by Institution Size (N = 379)
This activity is backed at most project-active institutions by some level of strategic recognition. Six of 10 respondents (60.6 percent) reported that IdM projects are included in their IT strategic plan or an institutional strategic plan that includes IT. At the same time, fewer respondents report organizing their IdM projects as a formal initiative. About one-third (34.3 percent) said they had done so, though another 21.6 percent reported that they were considering it. As Table 8-1 shows, doctorals were the most likely of the Carnegie groups to both report a formal initiative (39.9 percent) and to be considering one (25.3 percent). Organizing projects into a formal initiative was also associated with institution size: 50.0 percent of institutions with more than 15,000 students reported doing so, compared with 24.4 percent of those with 4,000 or fewer and 32.3 percent of those in between.

Including IdM in a strategic plan and organizing projects into a formal initiative proved to be related (see Table 8-2). Where IdM was included in strategic plans, only about one-third of respondents (33.5 percent) reported not organizing projects into a formal initiative, and the rest of the respondents either reported a formal initiative (43.7 percent) or were considering one (22.8 percent). Where IdM was not included, or where there was no strategic plan, most respondents said they had not organized their projects into a formal initiative. We speculate that the validation and enhanced visibility that inclusion in a strategic plan implies—along with, perhaps, the preparatory work necessary to secure inclusion—encourages IT units to secure the funding and political backing, and to take the risks, appropriate for a formal initiative.

Some of our interviewees saw formality as a stage in the evolution of their IdM capability. “It was good for us to be less formal until we got more experience,” says John Camp, CIO at Wayne State University. “We didn’t know enough three to five years ago.”

### IdM Project Implementation Strategies

In addition to finding that most responding institutions had not organized their IdM projects into a formal initiative, we found that most of them bundled IdM projects with other project implementations or with other IT initiatives. Table 8-1 shows the distribution of IdM projects organized as a formal initiative, by Carnegie class and Canada.

<table>
<thead>
<tr>
<th>DR</th>
<th>MA</th>
<th>BA</th>
<th>AA</th>
<th>Other Carnegie</th>
<th>Canada</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>39.9%</td>
<td>33.3%</td>
<td>21.7%</td>
<td>25.6%</td>
<td>44.5%</td>
<td>31.8%</td>
</tr>
<tr>
<td>Considering</td>
<td>25.3%</td>
<td>17.2%</td>
<td>16.7%</td>
<td>17.9%</td>
<td>33.3%</td>
<td>27.3%</td>
</tr>
<tr>
<td>No</td>
<td>30.8%</td>
<td>49.5%</td>
<td>61.6%</td>
<td>56.5%</td>
<td>22.2%</td>
<td>40.9%</td>
</tr>
</tbody>
</table>

Table 8-2 shows the relationship between IdM inclusion in a strategic plan and the proportion of respondents who organized their IdM projects as a formal initiative.

<table>
<thead>
<tr>
<th>Included in IT or Institutional Strategic Plan</th>
<th>IdM Projects Organized as a Formal Initiative</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Included</td>
<td>43.7%</td>
</tr>
<tr>
<td>Not included</td>
<td>17.0%</td>
</tr>
<tr>
<td>Neither an IT nor an institutional strategic plan</td>
<td>26.5%</td>
</tr>
</tbody>
</table>
work of some other sort, rather than pursuing them as stand-alone projects. As Figure 8-2 shows, the most commonly reported efforts with which IdM was bundled were IT security implementations (37.8 percent of IdM project-active respondents) and campus portals (34.9 percent). Accounting for overlap in responses, altogether 62.0 percent of respondents said they were bundling IdM work with a security, portal, ERP, or other implementation project, and many of these were bundling with multiple implementations. Slightly more than one in four (28.1 percent) reported a stand-alone IdM project. Doctorals, at 37.2 percent, were the most likely Carnegie group to report a stand-alone IdM project, while associate’s institutions, at 12.5 percent, were the least likely.

These project strategies suggest that many respondent institutions are taking an opportunistic approach to IdM. This isn’t necessarily a bad thing; bundling with security implementations, for example, is consistent with the high ratings respondents gave to security as a motivator for IdM (see Table 4-2), while portal bundling similarly serves another major motivator, enhanced user services.

Piggybacking on a major project may also be a way to carry local IT initiatives to a larger campus community. At Northern Kentucky University, the IT unit had already done some IdM work when a major ERP project brought a campus-wide reengineering of all critical business processes. “A campus-wide ERP implementation committee reporting to the CFO is overseeing the project,” says CIO Gary Pratt. “This is purposely not an IT project. When it comes to issues that are IdM related, they’re handled in the implementation committee forum, and from that point, IT takes the lead in getting the work done. The process is very open and collaborative.”

It’s also possible, however, that for some institutions, bundling may be a “stealthy” way to get IdM work done while grappling with some of the challenges we reported in Chapter 4, such as constrained funding and higher IT priorities (see Table 4-4). The major concerns that these tendencies toward the lack of a formal IdM initiative and bundling raise are whether they permit a sufficiently broad and architecturally independent approach to IdM, and whether such projects sufficiently educate the campus community about IdM’s strategic value across applications, business processes, and infrastructure.
When IdM Projects Started

To gauge how long projects are taking and how much experience respondent institutions have with IdM, we asked what year respondents began their IdM projects. Although we found a sizable group of institutions (28.2 percent) had been pursuing IdM projects since 2001 or earlier, the most striking result was the number of respondents whose project experience began very recently (see Figure 8-3). At the time of our survey in May and June 2005, 46.3 percent of respondents had been working on their IdM projects no more than 18 months.

As with other aspects of IdM project management, we found that the dates IdM projects began differed by Carnegie class and institution size. As Figure 8-4 shows, doctorals were the most likely respondent institutions to report starting projects in 2001 or earlier (44.6 percent), and associate’s institutions were the least likely (13.5 percent). Even so, one-third of doctorals (33.7 percent) began only in 2004 or 2005, as did nearly three-quarters of associate’s institutions (73.0 percent). Among institutions of 15,000 or more students, 48.1 percent reported project start dates of 2001 or earlier, double the rate among institutions of

Figure 8-3. When IdM Projects Began (N = 330)

![Figure 8-3](image)

Figure 8-4. When IdM Projects Began, by Carnegie Class (N = 275)

![Figure 8-4](image)
4,001 to 15,000 students (24.0 percent) and far higher than that of institutions of 4,000 or fewer students (18.4 percent).

The inexperience of many institutions and the concentration of earlier project start dates among doctorals and large institutions are noteworthy because institutions that started IdM projects earlier tend to report higher IdM capabilities. In Chapter 4, we reported the mean ratings that institutions gave themselves on a 5-point scale measuring their capability to deliver each of 14 separate IdM benefits (see Table 4-1 and Figure 4-1). From these 14 performance ratings, we created a summary IdM performance rating—termed the IdM capability score—to give us an overall measure of IdM capability for each institution. This summary measure is the mean value of all the 14 individual capability rankings each respondent reported. To evaluate the effect of IdM project start dates on overall IdM capability, we calculated the mean capability score in each project start-date category. (See Chapter 9 for further discussion and use of the IdM capability score.)

The mean IdM capability score reported by respondents was 2.67 among those whose projects began in 2005 (see Table 8-3), but it was 3.13 and 3.08 for those beginning, respectively, in 2002 and 2001 or earlier. This may be due to the resources and aggressiveness of the earlier IdM project starters, but it also gives some hope that working on IdM projects does improve capability over time. It also, however, underscores the relative lack of capability among the less experienced respondent institutions.

### Spending and Staffing

No matter how large or small, all project plans depend on funding. To learn the financial limits our project-active respondents are operating within, we asked them to select a range that matched their expectations of how much their central IT unit would spend on IdM project implementations over the next three years. Figure 8-5 summarizes the results; however, before looking at them, it is important to understand the scope and limits of the information we captured.

### Scope and Limitations of IdM Project Spending Results

We did not attempt to capture all institutional IdM spending comprehensively. In particular, by asking about central IT spend-

<table>
<thead>
<tr>
<th>Project Start Date</th>
<th>Mean Capability Score</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before 2002</td>
<td>3.08</td>
<td>0.625</td>
</tr>
<tr>
<td>2002</td>
<td>3.13</td>
<td>0.606</td>
</tr>
<tr>
<td>2003</td>
<td>2.91</td>
<td>0.660</td>
</tr>
<tr>
<td>2004</td>
<td>2.85</td>
<td>0.593</td>
</tr>
<tr>
<td>2005</td>
<td>2.67</td>
<td>0.712</td>
</tr>
<tr>
<td>Total</td>
<td>2.92</td>
<td>0.649</td>
</tr>
</tbody>
</table>

(1 = very low, 2 = low, 3 = medium, 4 = high, 5 = very high)
ing on IdM project implementation over the next three years, we framed a question that did not ask our respondents to report:
- routine maintenance or other activities not considered part of an implementation;
- any IdM spending not related to projects; or
- spending by departments or other entities, possibly including special project offices, outside the central IT organization.

The last point deserves special attention because, as we reported above, many respondent institutions use bundling as an implementation strategy for IdM projects. Such bundled initiatives may involve IdM spending that is not controlled by central IT and is therefore not reported. Also, some respondents may have thought of these as something other than “IdM projects” and so did not include IdM spending taking place within them, even if it was controlled by central IT. It is worth noting that bundling with another project does not necessarily equate to funding for IdM. While about six out of 10 institutions report some kind of bundling as an IdM project implementation strategy, when asked explicitly if they use project bundling as a way of paying for IdM projects, only about 27 percent of respondent institutions reported that they do (see Figures 8-2 and 8-8).

To verify and better interpret the spending results, we asked all of our postsurvey qualitative interviewees to confirm their answers, and we further asked them what sort of items they included in their chosen spending response. Only one of our interviewees said that, in retrospect, she would answer differently (and with a higher spending range). Interviewees varied more widely, however, in the kinds of expenditures they told us they had considered when answering. Though many said they had included staff costs as well as external expenditures, others said they included only spending for external goods and services. Many commented on the difficulty of arriving at a good spending estimate, citing the distributed nature of IdM, its incorporation in infrastructure and project spending, and the uncertainty of their plans. Notre Dame’s CIO, associate vice president, and associate provost, Gordon Wishon, says, “One reason why there is such a widely ranging view of cost estimates for IdM among universities is that there is not yet a consistent view of what all the elements of IdM are.”

Figure 8-5. Anticipated Central IT Spending on IdM Projects in Next Three Years (N = 339)
Central IT Spending on IdM Projects

The anticipated spending shown in Figure 8-5 suggests that even if not all spending is being captured, reported expenditures will be low to modest in light of the ambitious IdM technology and policy initiatives many respondents report. Even with 13.9 percent of respondents answering “don’t know,” nearly half (47.1 percent) expect their central IT units to spend $100,000 or less implementing IdM projects over the next three years. Of the 36 respondents (10.6 percent) who expect to spend over $500,000, 20 expect to spend under $1 million and 10 more anticipate spending between $1 million and $2 million. To put these figures in perspective, consider that a Burton Group/PricewaterhouseCoopers study of 11 “large to very large” corporate and government entities in 2003 found expenditures ranging from $150,000 to $6.5 million for directory-service projects alone (Gebel & PricewaterhouseCoopers, 2003).

Among respondents who gave us spending ranges, we found significant differences among Carnegie classes and institutional size ranges (see Figures 8-6 and 8-7). Not surprisingly, doctorals overwhelmingly dominated the over-$500,000 spending range, with nearly a third (31.2 percent) answering in that range, versus 6.4 percent at associate’s institutions, the next highest Carnegie group. Virtually all of these high-spending doctorals (24 of 25) were doctoral-extensive rather than doctoral-intensive institutions. Despite this powerful doctoral presence at the high end, almost one in five respondents (18.8 percent) at doctorals reported thinking that their institution would spend under $100,000. Spending in the over-$500,000 range was also strongly dominated by institutions with more than 15,000 students.

Spending levels were not significantly associated with respondents’ opinions about resource sufficiency at their institutions, but they were associated with organizing IdM projects as a formal initiative. Among institutions reporting expenditures of $50,000 or less over the next three years, 17.8 percent reported organizing projects as a formal initiative, and 62.2 percent said they were not doing so. Among those expecting to spend over $500,000, the ratio was nearly reversed: 69.4 percent reported organizing projects as a formal initiative, and 19.4 percent said they were not.

Figure 8-6. Anticipated Central IT IdM Project Spending over Next Three Years, by Carnegie Class (N = 239)
Given the limitations discussed above, we believe that the spending results reported here should be seen as a lower bound to what, when all internal and external expenditures are considered, would certainly be higher levels of spending on IdM. At the same time, our interviewees’ confirmations suggest that we did capture most or all anticipated external central IT IdM project spending for goods and services, as well as some purely internal spending. It’s also well to remember that, as we reported in Chapter 4, respondents ranked inadequate funding as the number-two challenge to IdM at their institutions and that only 31.9 percent of them agreed or strongly agreed that their institution was providing the resources needed for IdM (see Table 4-4 and Figure 4-3). Our conclusion remains that anticipated spending on IdM projects over the next three years is modest enough to challenge the aggressive adoption plans many respondents report, and that the multimillion-dollar IdM projects that some products and services firms promote will be relatively rare among our respondent base.

Project Funding Sources

The central IT budget and campus project budgets in which central IT is likely to have a hand were the most common sources we found for IdM project funding. Asked to indicate the ways they pay for their IdM projects from a list of sources, nearly three-fourths (73.6 percent) of project-active respondents selected the annual central IT budget (see Figure 8-8). Bundling with other projects such as ERP was the second most reported source of funding, at 27.3 percent. It is interesting to note that this is well below the 62.0 percent who report one or more kinds of bundling among their IdM project implementation strategies (see Figure 8-2 and associated text).

Those who identified the central IT budget as their sole source of project funding made up 51.0 percent of all those naming at least one funding source (other than “not yet determined”). Another 7.3 percent named bundling with other projects as their sole IdM project funding source.

Funding sources that suggest a higher profile for IdM and less dependence on IT operational resources were reported considerably less often: 14.8 percent of respondents said they used a one-time campus budget allocation, and only 4.8 percent reported getting contributions from other central units in the institution.

As these data suggest, we did not find
great diversity in funding sources overall. Leaving out those who reported “not yet determined,” 63.3 percent of respondents named only one source of funding and 98.3 percent named three or fewer.

We found little significant variation by Carnegie class or other institutional characteristics in these funding sources. One exception was contributions from non-IT central units, which was reported far more often by large institutions than by smaller ones. Of the 16 respondents that reported this source of funding, 11 were from institutions with 15,000 or more students.

**IdM Project Staffing**

We found that most project-active respondent institutions have assigned central IT staff to IdM projects, though the staffing levels are generally modest. Figure 8-9 shows that only about one in seven respondents (14.4 percent) reported no central IT staff currently assigned to IdM projects. Well over half (58.0 percent) have either one or two FTE staff currently assigned to IdM. Though 7.2 percent of respondents reported assigning six or more staff, and some reported numbers as high as 18, the large proportion of smaller staffing levels extended across the Carnegie classifications. Doctorals, for example, had the highest reported rate (12.5 percent) of six or more assigned staff, yet a slight majority of doctorals (52.2 percent) still reported two or fewer FTE staff assignments.

Likewise, while the number of institutions reporting larger staffing levels tended to rise with institutional size, even among institutions with 15,000 or more students, a majority (55.1 percent) had two or fewer assigned staff (see Table 8-4). Among institutions with 4,000 or fewer students, the median number of central IT staff reported assigned to IdM was one; among those larger than 4,000, it was two.

Even at these modest levels, the staffing results confirm a high rate of engagement with IdM among our respondent institutions, and they further suggest that the low levels of IdM project spending that we reported previously (see Figure 8-5) probably do not, in many cases, reflect internal spending on staff salaries.
Consultants and External Services

To see how institutions might be supplementing in-house staff and skills with external IdM expertise, we asked project-active respondents if their institutions had used or were currently using consultants or external services providers. Most said no, but a large minority (42.1 percent) reported using them. We found no significant variation by Carnegie class or institution size, but the tendency to use consultants was associated with anticipated IdM project spending levels (see Table 8-5). Among institutions expecting central IT spending on IdM projects to be $50,000 or less over the next three years, 30.0 percent reported using consultants or external services, while among those reporting $500,000 or more, 63.9 percent said they used them. Use of consultants was also higher among institutions whose IdM projects were organized as a formal initiative than among those whose projects were not.

Among those respondents whose institutions had used or were currently using IdM consultants or external services providers, the most commonly reported areas of use were “hard” technical skills (see Figure 8-10). At the top of the list, 44.7 percent of external services users reported using consultants for...
architecture and design issues, and another 38.3 percent for software development and implementation. “Soft” skills such as assistance with organization and process issues, business case and policy development, and change management were mid- to low-range areas of reported use.

Several of our interviewees reported using outside consultants to fill in gaps in staff skills or just to provide a project “reality check.” At Embry-Riddle Aeronautical University, the IdM team brought in a consultant referred by another university to help the team get up to speed with its new Oracle directory products. “We had him in for a week,” says ERAU’s IT Services Director Becky Vasquez, “mostly for brainstorming and confirming whether we were going in the right direction.” Though only a few reported using consultants for more strategic or business-oriented purposes, their comments were positive. Rice University’s Barry Ribbeck, director of systems architecture and infrastructure, described the effect that an outside opinion voiced by an external consultant in favor of IdM had on an institution Ribbeck previously worked at. “We had been preaching strong identity and access management for eight years with little traction. [The consultant’s opinion] got them on board. No prophet is accepted in his own country.” The University of Notre Dame retained Burton Group to provide recom-

<table>
<thead>
<tr>
<th>Consultants to Help with IdM</th>
<th>Anticipated IdM Project Spending over Next Three Years</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$50,000 or less</td>
<td>$50,001–$100,000</td>
</tr>
<tr>
<td>Have used or currently using</td>
<td>30.0%</td>
<td>28.6%</td>
</tr>
<tr>
<td>Have not used</td>
<td>70.0%</td>
<td>71.4%</td>
</tr>
</tbody>
</table>

Table 8-5. Use of Consultants/External Services for IdM Projects, by Anticipated IdM Spending
mendations on needed policy changes and a “very preliminary” architectural approach. “It was very worthwhile,” says Wishon. “They were well into the issues and could provide very good visibility into the currently available products in the marketplace.”

Most of those respondents who are using or have used consultants and expressed an opinion on the value of doing so seem to be satisfied with the investment. Asked for their level of agreement with the statement “My institution is getting the value we expected from the money spent on consultants/external services,” 59.8 percent agreed or strongly agreed, and only 7.2 percent disagreed or strongly disagreed (see Figure 8-11). The mean response of 3.71 (std. deviation = 0.885) was a little short of “agree” (= 4) on our 5-point scale, due in part to the 33.0 percent of respondents who gave a neutral (= 3) response.

Project Sponsorship and Participation

As we reported above (see Figure 8-8), IT-related funding sources were most often the ways respondents told us they paid for IdM projects. IT dominance was also clear in the sponsorship of IdM projects (see Figure 8-12). Asked to choose all the relevant sponsors for their campus IdM projects from a list of eight sponsor categories, 86.1 percent of project-active respondents cited the CIO (or equivalent)—far more than the next most-reported sponsor, the director or manager of IT networking. As this second-ranked choice implies, most of those who did not name the CIO cited some other IT sponsor, suggesting that these IdM projects, though “below the radar” of CIO involvement, nonetheless stood in the CIO’s reporting line. Altogether, 98.6 percent of respondents named at least one IT sponsor, and seven of 10 (71.9 percent) named only IT sponsors for their IdM projects. It seems evident, then, that not much happens in IdM projects that does not, in some way, pass through the CIO’s office.

This means, of course, that IdM project sponsorship might also be seen as a glass three-tenths full of non-IT sponsors. And in fact, though no non-IT sponsor category captured more than the 15.6 percent that “administrative functional area executive” did, a total of 28.1 percent of respondents named at least one non-IT sponsor. Exclusive non-IT sponsorship, however, was rare; 96.0 percent of those who named a non-IT sponsor named
an IT sponsor as well. It should also be kept in mind that some CIOs report through higher administrative or academic posts, such as the chief financial officer or provost, so some of these non-IT sponsorships may refer to a higher level in the IT chain of command.

We found no significant relationship between naming a non-IT sponsor and Carnegie class or institutional size, but we did find an association with project formality. Respondents who said their institution’s IdM projects were organized as a formal initiative were about twice as likely to report a non-IT sponsor as those who reported no formal initiative.

Though one respondent cited no sponsors at all, and two checked all eight of the sponsor categories our survey mentioned, generally respondents reported a small number of IdM project sponsors. The median number of sponsors was two, and 81.3 percent reported three or fewer.

**Role and Use of Project Oversight Committees**

Following a practice common in project management, NSF Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium’s Enterprise Directory Implementation Roadmap recommends that enterprise directory projects include a steering committee composed “entirely of key decision-makers, all at levels of senior manager, director or above, representing the primary constituencies of the campus … with the authority to approve process change and institute campus-wide policy” (West, 2005). At the University of Colorado at Boulder, for example, a major enterprise directory project steering team included the vice president of university systems, the registrar, the dean of libraries, and the directors of human resources, enrollment services, and housing. Evolving eventually into a directory governance board, this team’s major roles were to make directory policy decisions and establish affiliation definitions based on relationships to the university (Giltner et al., 2004).

Without specifying any particular composition, we asked respondents if an oversight committee existed for their IdM projects, and we further asked them to describe its role by choosing from a list of six functions. One-third of our project-active respondents (33.0 percent) reported the existence of an oversight committee.
We found no significant associations between the presence of an oversight committee and Carnegie class, institution size, or the technology adoption phase for reduced or single sign-on, enterprise directories, or automated role- and privilege-based authorization. But we did find that institutions reporting higher levels of anticipated IdM project spending over the next three years were more likely to have an oversight committee (see Table 8-6). Similarly, institutions reporting higher staffing levels reported oversight committees at higher rates. While only 8.3 percent of institutions reporting no central IT staff dedicated to IdM projects said they had an oversight committee, the figure rose to 27.1 percent for those with one dedicated staff member and to 54.2 percent for those reporting six or more staff members. Respondent institutions reporting that their IdM projects were organized as a formal initiative were also more likely to report having an oversight committee than those that did not.

These patterns suggest that oversight committees are being created where projects reach a certain threshold of complexity or resource commitment. It’s worth noting, however, that only at the highest spending and staffing levels does a majority of project-active respondent institutions report oversight committees, and they are not universal even there.

Where oversight committees exist, what do they do? Figure 8-13 suggests that most are not endowed with strong powers. The role that project-active institutions with oversight committees most commonly reported was an advisory one (69.8 percent); only about a third of institutions said their oversight committees assumed the role of setting policy (32.8 percent) or priorities (31.0 percent). Fewer still adjudicated conflicts (17.2 percent) or had the power to authorize funding (6.9 percent). Overall, it appears that oversight committees mainly provide a forum for communication and advice above the project implementation level, though in a significant minority of cases they have the power to play a stronger role in setting project direction.

### Participation of Functional Areas

If, as we noted above, IdM project sponsorship and funding are heavily dominated by IT (see Figures 8-8 and 8-12), this is not to say that other campus units are left out of projects altogether. When we asked respondents involved in projects to tell us which of 13 different functional areas actively participated in their campus IdM projects, we found majority participation in four major business or academic areas and double-digit rates of participation in all the others (see Figure 8-14). At the top of the list were the business units that control the major systems of record that feed much of the IdM infrastructure: human resources (68.5 percent), student affairs (62.2 percent), and financial services (57.4 percent).

---

**Table 8-6. IdM Project Oversight Committee Status, by Anticipated IdM Project Spending in Next Three Years**

<table>
<thead>
<tr>
<th>Oversight Committee Status</th>
<th>Anticipated Central IT Spending on IdM Projects in Next Three Years</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$50,000 or less</td>
</tr>
<tr>
<td>Have oversight committee</td>
<td>23.3%</td>
</tr>
<tr>
<td>Do not have oversight committee</td>
<td>76.7%</td>
</tr>
</tbody>
</table>
With the exception of the library (53.4 percent), academic units and services were not as well represented as administrative ones. Academic schools and departments were reported as participants in IdM projects by only about a quarter of respondents (24.7 percent), and research administration was cited by only 13.6 percent. In both cases, doctoral institutions were far more likely to report such participation. Perhaps owing to the greater presence of large-scale devolved IT units with identity infrastructure in areas like engineering, science, and business, doctorals reported about double the rate of academic school or department participation (41.5 percent) as BA and MA institutions, which respectively reported 20.0 and 19.2 percent. The disproportion was even greater for re-
search administration, where 33.0 percent of doctorals reported participation, versus 6.1 percent at master’s institutions, the next highest group.

The widespread practice of working with other business units on IdM projects suggests that many of our respondent institutions are working with their campus peers to address the policy, data ownership, and data definition challenges that we reported in Chapter 4 and which are further highlighted below (see Figure 8-15). Our interviewees repeatedly emphasized the importance of such outreach. “Bring in all the people together that you’re going to touch,” advises Bill Baber, associate director of academic technology and portal coordinator at the University of New Hampshire, “a huge diversity of folks who need to see it as adding value. If you can’t put together a solution that they can understand and buy in to, it won’t work.”

**IdM Project Challenges**

We reported in Chapter 4 that respondents most often named higher IT priorities and funding as their primary challenges to pursuing IdM, while data integrity and technical matters were midrange challenges (see Table 4-4). Still, when we asked our respondents about challenges relating to data integrity and technology in the context of their IdM projects, many of them reported grappling with these issues.

Not surprisingly, the data integrity challenge results reflected problems arising from IT environment complexity and lack of coordination (see Figure 8-15). Duplication of data in multiple systems and inconsistencies in data definitions were the most often reported challenges (56.5 percent and 54.5 percent of respondents, respectively). Comparatively few respondents (23.9 percent) reported that needed data were not being collected. We found little significant variation between Carnegie classes or institution size, though institutions with more than 15,000 students more often reported being challenged by poor accuracy or timeliness of data (56.3 percent) than those with 4,000 or fewer students (34.1 percent) or those in between (43.9 percent).

Among technology challenges (see Figure 8-16), accommodating existing homegrown or legacy applications or systems was the front-runner (51.1 percent), though this was reported most often by doctoral institutions (70.2 percent) and master’s institutions (49.5 percent). By contrast, the second-ranked challenge, adopting new and complex technolo-
IdM Solutions

As respondent institutions keep busy with IdM projects, what product approaches and IdM solutions are they considering? Choices have been evolving rapidly in recent years because of dramatic change in the product solutions marketplace (Neuenschwander, 2005b).

Major technology stack vendors such as Sun Microsystems, Oracle, IBM, HP, and others have discovered a new level of strategic significance in IdM and have competed to build up IdM product suites through development or acquisition. At the same time, boutique vendor products remain numerous, and new start-ups continue to emerge, while higher education-specific vendors such as SunGard SCT have explored IdM’s infrastructure and services implications. Open source options such as OpenLDAP, Red Hat’s Fedora Directory Server, and the Shibboleth federated identity system have also been growing. While this situation develops and solutions mature, institutions face a complex array of overall solution approaches, mixing legacy identity tools with point solution products, elements of IdM that are “baked into” applications, and comprehensive IdM suites.

In Chapter 6 we found that respondents were for the most part taking a mixed sourcing approach to specific IdM technologies, with a considerable degree of uncertainty in their sourcing plans (see in particular Table 6-6). To cap off our look at IdM projects, we also wanted to find out how respondents view the overall IdM solutions picture. We asked them to choose from a list of possible

<table>
<thead>
<tr>
<th>Technology Challenges to Implementing IdM (Multiple Responses Allowed, N = 352)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodating existing homegrown or legacy applications or systems</td>
</tr>
<tr>
<td>Adopting new and complex technologies</td>
</tr>
<tr>
<td>Lack of vendor software interoperability</td>
</tr>
<tr>
<td>High cost of vendor solutions</td>
</tr>
<tr>
<td>Proprietary vendor solutions</td>
</tr>
<tr>
<td>Lack of mature vendor products</td>
</tr>
<tr>
<td>Poor vendor support for their products</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Project-Active Institutions</td>
</tr>
</tbody>
</table>

Figure 8-16
approaches the one that best described their institution’s IdM solutions approach as they currently think about it (see Table 8-7). (Note that the questions in this section were asked of all respondents, not just those actively pursuing IdM projects.)

As with our individual technologies sourcing data, we found that a significant proportion of respondents had not yet decided on a solution or set of solutions, either because they were still identifying long-term business and architecture strategies (24.6 percent) or because they simply didn’t know how best to describe their solutions approach (6.8 percent). Those considering vendor solutions made up the largest part of the remainder, though this group was divided among those thinking they would pursue a best-of-breed/in-house integration strategy (17.4 percent), those who expected to purchase a suite solution aligned with their network and hardware infrastructure (10.8 percent), and those who thought they would buy the suite best aligned with their administrative/ERP applications (12.3 percent). Nearly one in four (24.6 percent) thought they would use in-house or open source IdM solutions.

Vendor solutions, in short, appear to be the most common path that responding institutions will pursue, but current expectation of adopting them still accounts for fewer than half of respondents. Moreover, these respondents are sufficiently fragmented among different point and suite approaches that no strongly dominant approach is evident. We discovered no significant variation of solutions approaches by Carnegie class, institution size, or other basic institutional characteristics. However, we did find that among those institutions that had decided on a solution or set of solutions, the likelihood of choosing some

<table>
<thead>
<tr>
<th>Approach Category</th>
<th>Approach</th>
<th>Approach Percentage</th>
<th>Category Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not yet decided</td>
<td>We will first identify our long-term business and architecture strategy and then decide on a solution or set of solutions for the institution.</td>
<td>24.6%</td>
<td>24.6%</td>
</tr>
<tr>
<td>In-house or open source</td>
<td>We probably will not use vendor solutions but will build solutions using in-house developed or open source software.</td>
<td>24.6%</td>
<td>24.6%</td>
</tr>
<tr>
<td>Vendor solutions</td>
<td>We will address our short-term needs with best-of-breed vendor point solutions and integrate these various products in-house.</td>
<td>17.4%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>We will probably buy the vendor “suite” solution that best aligns with our network, infrastructure, and hardware vendors.</td>
<td>10.8%</td>
<td>40.5%</td>
</tr>
<tr>
<td></td>
<td>We will probably buy the vendor “suite” solution that best aligns with our administrative applications and ERP vendors.</td>
<td>12.3%</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td>Other</td>
<td>3.5%</td>
<td>3.5%</td>
</tr>
<tr>
<td>N/A</td>
<td>Don’t know</td>
<td>6.8%</td>
<td>6.8%</td>
</tr>
</tbody>
</table>
form of vendor solution was higher among those who used or were implementing a complete vendor-supported ERP suite (68.6 percent) than among those with some (51.6 percent) or no (41.7 percent) vendor-supported ERP applications (see Table 8-8).

Finally, because the ERP environment is such a large and strategically important investment for most institutions, we asked respondents to choose from a list the one item best describing the approach they wished their ERP vendor to take toward IdM (see Table 8-9). We found little evidence that respondents look for a major convergence of ERP and IdM solutions at the vendor level. There was a distinct lack of enthusiasm for comprehensive IdM solutions from ERP vendors, with only 10.0 of respondents asking for such an approach, though an additional 14.3 percent looked for specific point solutions that contribute to the overall IdM solution. Relatively few (11.7 percent) even looked for formal partnerships between their ERP vendors and key IdM providers. Overwhelmingly, the most common approach named (61.4 percent) was for ERP vendors to ensure that their software is compliant with IdM-relevant standards and industry regulations.

Table 8-8. Anticipated IdM Solution Approach, by ERP Status

<table>
<thead>
<tr>
<th>Anticipated Approach</th>
<th>ERP Status (Using or Implementing)</th>
<th>Complete vendor-supported ERP, including HR, financials, and student applications</th>
<th>Some vendor-supported ERP applications</th>
<th>No vendor-supported ERP applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-house or open source</td>
<td>31.4%</td>
<td>48.4%</td>
<td>58.3%</td>
<td></td>
</tr>
<tr>
<td>Vendor solution</td>
<td>68.6%</td>
<td>51.6%</td>
<td>41.7%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>100.0%</td>
<td>100.0%</td>
<td>100.0%</td>
<td></td>
</tr>
</tbody>
</table>

Table 8-9. Desired IdM Approach from ERP Vendor (N = 350)

<table>
<thead>
<tr>
<th>ERP Vendor Approach</th>
<th>Percentage of Institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure their ERP software is compliant with industry standards and regulations relevant to IdM</td>
<td>61.4%</td>
</tr>
<tr>
<td>Provide specific, focused “point solutions” that contribute to our overall identity management solution</td>
<td>14.3%</td>
</tr>
<tr>
<td>Create formal partnerships with key identity management providers to offer attractive IdM solutions</td>
<td>11.7%</td>
</tr>
<tr>
<td>Provide comprehensive IdM solutions for our institution</td>
<td>10.0%</td>
</tr>
<tr>
<td>Other</td>
<td>2.6%</td>
</tr>
</tbody>
</table>
Summing Up IdM Projects

The level of our respondents’ project activity fully confirms some of this study’s earlier findings—for example, that institutions see IdM as important, are motivated to pursue it, and are adopting its technologies. With nearly nine out of 10 respondent institutions engaged in IdM efforts, it’s hard to deny that identity issues are on the institutional radar screen.

Though this activity is nearly universal, it isn’t unbounded. Two different kinds of constraints are apparent. First, modest resource levels, in both dollars and staff, suggest that for most institutions, IdM will likely progress in the near future in a measured way at best, except perhaps where it can hitch its wagon to a high-profile, complementary project such as an ERP implementation. Second, and again with a partial exception where the right kind of bundling is available, IdM is heavily IT-centric. Its funding sources and sponsorship are dominated by central IT; oversight is both uncommon and, where it exists, mostly advisory in nature. The frequent participation in IdM projects by other functional units appears to complement, but not diversify, this hegemony. In short, most of the activity we found suggests that IdM is being treated tactically rather than strategically.
Acting on what proved to be an accurate assumption that our respondent base did not include a large proportion of institutions with deep experience in IdM, we designed our study to capture baseline information about the state of practice, rather than to highlight specific best practices in IdM use. Nonetheless, our survey did collect substantial information about the outcomes of IdM initiatives. In addition, our qualitative interviewees shared lessons they had learned and helped us interpret and contextualize our quantitative findings.

In this chapter, we look at our respondents’ views on the value they got from their IdM projects, their experience with and expectations about cost savings, and the factors associated with overall IdM capability and cost savings. We also draw on results presented previously in this study to synthesize and highlight findings in light of these outcomes.

**Value and Cost Savings**

We asked our respondents who had engaged in IdM efforts or projects whether their institution was getting the value they expected from the money they had spent on IdM initiatives. Figure 9-1 shows that most of them

---

**Key Findings**

- A large majority of respondents report that they agree or strongly agree that their institution received the value expected from money spent on IdM projects; most of the rest are neutral.
- Only about one in 10 respondents who have taken part in IdM projects report achieving cost savings from them, though another one in four expect to in the future. Respondents who named cost reduction or greater efficiencies as a top IdM motivator were more likely to report cost savings or expectations of them.
- Respondents who report higher agreement that their institution is providing necessary resources for IdM also tend to report higher IdM capability scores. Likewise, those who have achieved cost savings tend to report higher agreement about resource sufficiency than those who have not.
- Higher agreement that senior management understands IdM costs and is willing to address IdM policy issues correlates with higher IdM capability scores and higher rates of cost savings from IdM projects.
- Completion of authorization and authentication policies is associated with higher IdM capability scores. Likewise, those who have completed certain IdM readiness activities are more likely to report cost savings from IdM projects.
- Institutions reporting more aggressive technology adoption strategies also tend to have higher IdM capability scores and are more likely to report cost savings from IdM projects.
(62.2 percent) agreed or strongly agreed that they had, and that most of the rest were neutral (26 percent) or didn’t know (9.6 percent). So few disagreed—only six out of 281 project-active respondents—that we were unable to find any significant differences between categories on the basis of Carnegie class, institution size, or other institutional measures.

We found a more mixed and nuanced response when we asked about project-active respondents’ expectations about cost savings from IdM projects. Only 10.1 percent told us they had achieved cost savings as a result of their IdM initiatives, and only about another quarter (26.8 percent) told us they expect to (see Figure 9-2). The largest group (44.1 percent) told us they had neither achieved savings nor expected to, and a substantial remnant (19.0 percent) said they didn’t know.

If so few respondents have realized cost savings from IdM and not a lot more expect to, why are respondents mostly convinced that IdM investments have met their value expectations? The answer seems to be that...
many see the value of IdM in other areas, especially in protecting the institution from risk and providing a better user experience. As we reported in Chapter 4, the most often cited motivations for IdM were to support security and privacy best practices, improve user support, and comply with regulations; only 18.6 percent named cost reduction or greater efficiencies as a top-three motivator (see Table 4-2).

As the foundational component establishing trust for a multitude of online business processes, IdM strikes some of our interviewees as a strategic imperative. “I think it’s part of our strategic direction,” says Mairéad Martin, manager of middleware systems technology at the University of Wisconsin–Madison. “IT is not happening in isolation.” At the University of California, San Diego, CIO Elazar Harel says he’s confident that by pursuing an IdM initiative that grew out of an effort to improve the work experience at the university, his unit is realizing difficult-to-quantify but real gains. “The goal is first to make the system secure, and then save people’s time,” Harel explains. “I don’t know how you put a dollar amount on that, but I’m sure it’s valuable.”

But what about those who did name cost savings as a top motivator? We found that they were more likely than our other respondents to say they had achieved cost savings (18.3 percent versus 8.0 percent) and, if they hadn’t, to say that they expected to (40.8 percent versus 23.2 percent). It appears that recognizing cost savings as a motivator may help realize that goal.

As it happens, however, the gulf between pursuing cost savings and pursuing other goals may not be so wide. As we report in the next section, the attributes characterizing those who report cost savings through IdM are in many ways similar to the attributes associated with those who report more-general outcomes, such as having sufficient resources and overall IdM capability.

**IdM Capability and Cost Savings: What Matters**

In Chapter 4, we reported finding an IdM “capability gap” among our respondents. Given a list of 14 potential benefits that IdM might deliver, our respondents gave generally high ratings to those benefits’ importance but ranked their capability to deliver the same benefits lower (see Table 4-1 and Figure 4-1).

To help us measure overall IdM capability, we created an IdM capability score by calculating the mean of the 14 separate benefit capability self-ratings each respondent reported. (Ratings were measured on a scale ranging from 1 = very low to 5 = very high.) We then looked for attributes and practices associated with higher capability scores. We also made the same search for characteristics associated with those who, as discussed above, reported achieving cost savings from their IdM projects. We present our findings about what matters in producing good outcomes below.

It’s important to note that the capability ratings we captured were subjective, self-reported measures. In principle, two different respondents with identical situations might have given different responses. But subjectivity also means respondents were free to take into account all the factors bearing on their IdM efforts and to gauge their answers according to their sense of what their institutions needed. This ability to rate according to their own situation may explain why, though we found significant patterns in the capability score results, we did not find much association with Carnegie class, institution size, or reported IdM spending levels.

**Resources Matter**

Not surprisingly, we found the IdM capability score to be related to respondents’ perceptions of resource sufficiency. As Table 9-1 shows, institutions where respondents strongly agreed that their institution provided the needed resources for IdM had mean ca-
pability scores 0.83 higher than those where respondents strongly disagreed. Perhaps less intuitively, respondents who reported achieving cost savings tended to rate their level of resource sufficiency higher than those from institutions where savings were anticipated but not yet achieved, and still higher than those who reported no cost savings or expectation of them (see Table 9-2).

The lesson may be that it takes resources to save resources. “A single identity for each person across the institution is a very important end point to reach,” says Thomas Board, Northwestern University’s director of information systems architecture. “It’s the only way universities can keep their costs in line and regulatory requirements in control.”

**Senior Management Understanding Matters**

No finding has made its way into more ECAR studies over the years than the conclusion that “senior management matters.” Yet our study results make it clear that IdM must be added to the company of other topics, including security (Kvavik & Voloudakis, 2003), networking (Pirani & Salaway, 2005), business process performance (Kvavik & Goldstein, 2005), and IT alignment (Albrecht et al., 2004), where executive support has been named a factor in success.

There are, however, some interesting wrinkles to our results. As we reported in Chapter 4, our respondents were relatively optimistic about their senior management’s understanding of IdM benefits, though much less so about their understanding of costs, and most optimistic of all about their willingness to address the policy issues relating to IdM (see Table 4-7). We also reported there that respondents who gave higher agreement ratings about these senior management attitudes tended also to rate IdM resource sufficiency higher at their institutions (see Table 4-10).

---

**Table 9-1. Mean IdM Capability Score, by Resource Sufficiency (N = 393)**

<table>
<thead>
<tr>
<th>Institution Is Providing Needed Resources</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>3.34</td>
<td>0.838</td>
</tr>
<tr>
<td>Agree</td>
<td>2.96</td>
<td>0.611</td>
</tr>
<tr>
<td>Neutral</td>
<td>2.89</td>
<td>0.571</td>
</tr>
<tr>
<td>Disagree</td>
<td>2.75</td>
<td>0.650</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>2.51</td>
<td>0.449</td>
</tr>
</tbody>
</table>

(1 = very low, 2 = low, 3 = medium, 4 = high, 5 = very high)

**Table 9-2. Resource Sufficiency, by Cost Savings Status**

<table>
<thead>
<tr>
<th>Cost Savings Status</th>
<th>Institution Is Providing Needed Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean</td>
</tr>
<tr>
<td>Have achieved</td>
<td>3.53</td>
</tr>
<tr>
<td>Have not but expect to</td>
<td>3.23</td>
</tr>
<tr>
<td>Have not, don’t expect to</td>
<td>2.95</td>
</tr>
</tbody>
</table>

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)
In examining the relationships between these senior management questions and IdM capability and cost savings, we discovered several additional significant associations. Institutions expressing stronger agreement that senior management understood IdM costs tended to have higher mean capability scores (see Table 9-3), as did those expressing stronger agreement that their senior management was willing to address IdM-related policy issues. Likewise, those reporting that they had achieved cost savings tended to express stronger agreement with the same two statements about senior management than those that hadn’t achieved cost savings (see Table 9-4).

If there is a special challenge to gaining senior management attention and support for IdM initiatives, it is probably the technology’s arcane nature and its relative lack of a business track record. “Without a doubt, our number-one problem with IdM is the difficulty in communicating about it,” reports John Grosen, director of infrastructure services at North Dakota State University. “When you sit with a VP for business, for example, it’s almost impossible to get them to understand the issues.”

Still, senior management support does not necessarily imply direct involvement in IdM initiatives but rather a willingness to create the context for it and break political or policy logjams. Jeffrey Schiller, network manager at MIT, says that senior management there is “only vaguely aware of the benefits [of IdM]. They are, however, involved in policies that affect authentication—in the broader question of who is a member of the MIT community. Defining who is a part of the community is a senior leadership responsibility.” At Wayne State University, CIO John Camp says that their maturing IdM projects have reached a point where greater senior management participation is needed. “We’re going to formalize the IdM initiative, and it will require a lot of policies, so management personnel will need to be more involved.”

We speculated in Chapter 4 that some CIOs, confronted with a mismatch between

<table>
<thead>
<tr>
<th>Attitude</th>
<th>Agreement Rating</th>
<th>IdM Capability Score</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Mean</td>
</tr>
<tr>
<td>Understands costs of IdM</td>
<td>Strongly agree</td>
<td>3.05</td>
</tr>
<tr>
<td></td>
<td>Agree</td>
<td>3.06</td>
</tr>
<tr>
<td></td>
<td>Neutral</td>
<td>2.97</td>
</tr>
<tr>
<td></td>
<td>Disagree</td>
<td>2.80</td>
</tr>
<tr>
<td></td>
<td>Strongly disagree</td>
<td>2.68</td>
</tr>
<tr>
<td>Willing to address policy issues</td>
<td>Strongly agree</td>
<td>3.21</td>
</tr>
<tr>
<td></td>
<td>Agree</td>
<td>2.93</td>
</tr>
<tr>
<td></td>
<td>Neutral</td>
<td>2.87</td>
</tr>
<tr>
<td></td>
<td>Disagree</td>
<td>2.56</td>
</tr>
<tr>
<td></td>
<td>Strongly disagree</td>
<td>2.44</td>
</tr>
</tbody>
</table>

(1 = very low, 2 = low, 3 = medium, 4 = high, 5 = very high)
senior management comprehension of benefits and costs, might be keeping IdM to a low management profile while waiting for more balanced understanding to develop. Our results suggest that CIOs should be proactive in moving that understanding along and, where it has matured, using it to build support for IdM initiatives.

Policies and Readiness Matter
We noted in Chapter 4, and again in Chapter 6, that IdM advisors commonly recommend that institutions set the stage for IdM initiatives by collecting metrics, building business cases, cleaning up data, establishing clear identity policies, and otherwise preparing both the IT unit and the institution at large for a revitalized identity infrastructure. We also reported that while many institutions are taking such steps, readiness measures seem not to be commensurate with ambitious plans for IdM activity. We suggested that successfully realizing those plans may depend more on completing these tasks than on mastering IdM technology.

But does all this complicated, politically charged, resource-draining work really matter? Our findings suggest that at least some of it does. As Table 9-5 shows, institutions that have completed policies for user authentication and authorization have a higher mean IdM capability score than those with policies in progress, which in turn have a higher mean capability score than those with no documented policies.

We found a similar pattern, though involving different readiness activities, with cost savings from IdM projects. Institutions that had a business case, a documented IdM plan, or documented data definitions were in each case more than twice as likely to have achieved cost savings as those not planning to do the activity (see Table 9-6). Carrying out planning and documentation projects, however, was no guarantee of realizing cost savings. Given the low rate of reported cost savings overall, it’s not surprising that those who didn’t realize savings or expect to outnumbered those who did, even among respondent institutions with completed documentation projects.

Our interviewees confirmed that sorting out—and, in fact, simply discovering—the complexities of a campus that has generated a maze of uncoordinated systems, data definitions, and business rules over the years is a big job, but it’s critical to giving an IdM initiative a good start and keeping it on track. Doing so also quickly uncovers the benefits of senior management involvement. When the University of Oregon first began to work on identity issues, “We began to solve some general access issues and knew that we needed to have buy-in from higher up,”

### Table 9-4. Agreement Rating of Management Attitudes, by Cost Savings Status

<table>
<thead>
<tr>
<th>Cost Savings Status</th>
<th>Senior Management Understands IdM Costs</th>
<th>Senior Management Is Willing to Address Policy Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean (Std. deviation)</td>
<td>Mean (Std. deviation)</td>
</tr>
<tr>
<td>Have achieved</td>
<td>2.97 (0.985)</td>
<td>4.03 (0.785)</td>
</tr>
<tr>
<td>Have not but expect to</td>
<td>2.71 (0.978)</td>
<td>3.48 (0.893)</td>
</tr>
<tr>
<td>Have not, don’t expect to</td>
<td>2.41 (0.923)</td>
<td>3.47 (0.891)</td>
</tr>
</tbody>
</table>

(1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree)
says Susan Hilton, director of administrative services at Oregon. After senior executives appointed representatives of the major functional areas to an IdM policy group, the new team “began looking at current access policies, and we were beyond surprised, say totally amazed, at how many IT resources we had without adequate access control.” After uncovering vulnerabilities and developing strategies for addressing them, the group passed its recommendations on to a larger oversight committee in charge of IT strategy. The inclusive group, Hilton says, “has worked better than we ever expected. The non-IT

Table 9-5. Mean IdM Capability Score, by Policy Status

<table>
<thead>
<tr>
<th>Policy</th>
<th>Policy Status</th>
<th>IdM Capability Score</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Mean</td>
<td>Std. Deviation</td>
<td></td>
</tr>
<tr>
<td>User authentication</td>
<td>Policies are completed</td>
<td>3.05</td>
<td>0.602</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policies are in progress or partially completed</td>
<td>2.68</td>
<td>0.558</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No documented policies</td>
<td>2.36</td>
<td>0.809</td>
<td></td>
</tr>
<tr>
<td>User authorization</td>
<td>Policies are completed</td>
<td>3.13</td>
<td>0.598</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policies are in progress or partially completed</td>
<td>2.77</td>
<td>0.593</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No documented policies</td>
<td>2.49</td>
<td>0.628</td>
<td></td>
</tr>
</tbody>
</table>

(1 = very low, 2 = low, 3 = medium, 4 = high, 5 = very high)

Table 9-6. Cost Savings, by IdM Readiness Activity

<table>
<thead>
<tr>
<th>Activity</th>
<th>Activity Status</th>
<th>Have Achieved</th>
<th>Have Not But Expect To</th>
<th>Have Not, Don’t Expect To</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documented business case for any area of IdM</td>
<td>Completed</td>
<td>22.0%</td>
<td>39.0%</td>
<td>39.0%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>In progress</td>
<td>10.6%</td>
<td>45.5%</td>
<td>43.9%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>Planning to do</td>
<td>7.2%</td>
<td>37.7%</td>
<td>55.1%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>Not planning to do</td>
<td>12.5%</td>
<td>15.3%</td>
<td>72.2%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Documented plan for IdM</td>
<td>Completed</td>
<td>25.0%</td>
<td>31.8%</td>
<td>43.2%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>In progress</td>
<td>15.5%</td>
<td>37.9%</td>
<td>46.6%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>Planning to do</td>
<td>2.3%</td>
<td>38.6%</td>
<td>59.1%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>Not planning to do</td>
<td>12.1%</td>
<td>12.1%</td>
<td>75.8%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Documented data definitions</td>
<td>Completed</td>
<td>23.4%</td>
<td>29.8%</td>
<td>46.8%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>In progress</td>
<td>10.8%</td>
<td>41.4%</td>
<td>47.8%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>Planning to do</td>
<td>10.8%</td>
<td>33.7%</td>
<td>55.5%</td>
<td>100.0%</td>
</tr>
<tr>
<td></td>
<td>Not planning to do</td>
<td>6.5%</td>
<td>9.7%</td>
<td>83.8%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>
members go away from policy meetings with most of the action items. And the IT staff take away almost all the action items from our technical meetings.” Hilton cautions, though, that the work is “a continual project. People need to understand that it is ongoing, always changing, and will always require resources.”

Notre Dame’s Gordon Wishon, CIO, associate vice president, and associate provost, urges a similar approach. “A framework for handling policy issues is extremely important,” he says. “There needs to be a governance process and an oversight committee that is empowered to make decisions on policy. This allows policy issues to be developed right up front in an identity management project.”

Technology Leadership Matters

It’s probably a measure of IdM’s newness that, along two different spectra of institutional technology strategy, mean IdM capability scores rise neatly along with the aggressiveness of the IdM effort (see Tables 9-7 and 9-8). The highest mean capability scores appear among self-described technology adoption “innovators” and among those who describe their IT goal as creating competitive advantage. Somewhat surprisingly, we also found that institutions reporting that they had achieved cost savings with IdM projects tended also to report more aggressive technology adoption strategies than those who have not realized savings (see Table 9-9).

In Chapter 8, we reported several indicators of a generally IT-centric approach to IdM, including the heavy dominance of the central IT budget as a funding source and the fact that sponsorship usually originates in, and almost always involves, the IT unit. As some of the outcomes mentioned earlier in this chapter suggest, IT-centrism has its risks, since senior management support and the broad campus participation implied in policy preparation both demand a broader base for IdM initiatives.

This is not to say, however, that IT leadership in the identity realm is either unwise or unwelcome. As a new technology, IdM needs experimenters and champions who can develop a competence in it ahead of the mainstream demand curve. Higher education, like other industries, has historically relied on innovators (and aggressive competitors) to shepherd now-ubiquitous technologies like Ethernet, TCP/IP, and wireless networking from the experimental stage to the mainstream. “We benefit from watching the R1’s and taking what we can from their successes, and avoiding what doesn’t work for them,” says Chad Kjorlien, director of instructional

Table 9-7. Mean IdM Capability Score, by Technology Adoption Strategy

<table>
<thead>
<tr>
<th>Strategy for Adopting New Technologies</th>
<th>IdM Capability Score</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean</td>
</tr>
<tr>
<td>Innovator</td>
<td>3.13</td>
</tr>
<tr>
<td>Early adopter</td>
<td>3.11</td>
</tr>
<tr>
<td>Early majority</td>
<td>2.95</td>
</tr>
<tr>
<td>Late majority</td>
<td>2.61</td>
</tr>
<tr>
<td>Laggard</td>
<td>2.29</td>
</tr>
</tbody>
</table>

(1 = very low, 2 = low, 3 = medium, 4 = high, 5 = very high)
technology at St. Mary’s University of Minnesota. “We like to keep a close ear to the rail and then leverage the positive results to our competitive advantage.”

None of our interviewees, however, and very few survey respondents reported any desire to pursue IdM purely for the sake of experiment. Among the IdM motivators we asked about, only four of 403 respondents named “strategy of early adoption/experimentation” as a top-three motivator.

**Summing Up What Matters**

Our study did not uncover an exhaustive list of best practices or a magic bullet for perfect IdM implementation. But our findings do confirm that the great majority of respondent institutions that have undertaken IdM projects believed they were getting the value they expected from their IdM project investments. In addition, we found that institutions reporting a higher mean capability to deliver benefits also tend to report higher agreement that they’re getting the resources they need, that senior management at their institution understands IdM costs and is willing to address related policy issues, and that their institutions have made progress on policy work. Aggressive IT adoption and institutional IT goals also correlate with higher IdM capability scores. While cost savings from IdM projects remain elusive for most of our respondents, those that have achieved them also tend to report similarly higher levels of resource sufficiency, senior management understanding, preparatory work, and aggressiveness in technology adoption.

### Table 9-8. Mean IdM Capability Score, by Institutional Goals for IT

<table>
<thead>
<tr>
<th>Institution’s Goals for IT</th>
<th>IdM Capability Score</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean</td>
</tr>
<tr>
<td>Provide IT infrastructure and services to create competitive advantage</td>
<td>3.20</td>
</tr>
<tr>
<td>Provide IT infrastructure and services that further the institution’s strategic goals</td>
<td>2.91</td>
</tr>
<tr>
<td>Provide appropriate IT infrastructure and services to different users based on their needs</td>
<td>2.81</td>
</tr>
<tr>
<td>Provide reliable IT infrastructure and services at the lowest possible cost</td>
<td>2.61</td>
</tr>
</tbody>
</table>

(1 = very low, 2 = low, 3 = medium, 4 = high, 5 = very high)

### Table 9-9. Technology Adoption Strategy, by Cost Savings Status

<table>
<thead>
<tr>
<th>Cost Savings Status</th>
<th>Technology Adoption Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean</td>
</tr>
<tr>
<td>Have achieved</td>
<td>2.51</td>
</tr>
<tr>
<td>Have not but expect to</td>
<td>3.11</td>
</tr>
<tr>
<td>Have not, don’t expect to</td>
<td>3.06</td>
</tr>
</tbody>
</table>

(1 = innovator, 2 = early adopter, 3 = early majority, 4 = late majority, 5 = laggards)
In the process of finding out what our respondent institutions were doing with IdM, we also gathered a lot of information about what they plan to do. None of these plans, however, can be achieved simply by drawing a straight line forward from present circumstances because identity demands are evolving rapidly. In this concluding chapter we look at the business and academic drivers that will affect institutional IdM over the next three to five years, considering them in the context of existing plans and the resources that are expected to be available. Finally, we look at actions institutions can take to move their IdM agendas forward.

**Higher Education IdM Ambitions: What’s on the Table?**

Our survey respondents have already, to a certain degree, defined the future they expect, and it’s crowded with activity. To recap, almost nine of 10 institutions are active with IdM projects, and only tiny numbers of respondents ruled out at least considering such technologies as enterprise directories, reduced or single sign-on, and role-based authorization. Almost two-thirds of respondent institutions (63.7 percent) were either currently implementing or planned to implement one or more of these technologies. Among the 53.5 percent of those with at least partially operational enterprise directories, a large majority planned to add functionality to them.

Alongside this project and implementation work, we found high rates of planned attention to the “soft infrastructure” of policy, metrics, and documentation but often low completion rates. About a quarter of institutions (26.2 percent) reported completing an inventory of identifiers, for example, compared with 58.1 percent that were in progress or planning to do so. Only 12.8 percent reported completing a risk assessment of data access security and privacy practices, but 70.6 percent said they were in progress or planning one.

What resources are available? Almost half of institutions (47.1 percent) pursuing IdM projects say they will have $100,000 or less of central IT funding to spend on such projects over the next three years, and three-fourths (75.5 percent) will have $500,000 or less. (Another 13.9 percent gave “don’t know” responses.) Even keeping in mind that our study did not capture all forms of IdM spending, these are modest levels. Nearly three out
of four respondent institutions (72.4 percent) said they currently had two or fewer full-time-equivalent central IT staff dedicated to IdM projects, and 14.4 percent had none. Not surprisingly, by healthy margins respondents named higher IT priorities and lack of funding as their top IdM challenges. And though collaboration with other business units is common, sponsorship from outside IT is not. Seven of 10 respondents named only IT sponsors for their institution’s IdM projects.

To be sure, exceptions exist. As with past technology innovations, some research universities are engaged in large-scale and innovative enterprise projects that will greatly help the rest of the higher education community bring IdM and associated best practices into the mainstream. But bridging the chasm between the innovators and the mainstream will take more than exemplary projects and the accumulation of best practices. As they confront not only the work that’s on the table now but also the emerging IdM drivers described below, most institutions will have to find ways to get the most out of limited resources and to make the case for better support for the identity infrastructure.

**Government and Regulatory Drivers**

In recent years, governments around the world have introduced a new regime of privacy regulation and tightened personal identification criteria. Spurred by concerns ranging from globalized Internet-based commerce to identity theft and terrorism, governments at all levels have taken a hard look at identity and privacy issues, creating a complex and rapidly changing web of regulations and infrastructures. Nowhere has this been more apparent than in the United States, where homeland security initiatives have set the stage for a fundamentally reshaped public identity infrastructure.

Passage of the Real ID Act in May 2005 is perhaps the most dramatic example (United States Congress, 2005). This law sets stricter and more uniform standards for the issuance of driver’s licenses within the states, effectively bringing the driver’s license under greater federal control. Besides specifying tighter identity proofing standards for state issuing agencies and creating a framework for interstate exchange of identity information, the law requires that driver’s licenses possess an as-yet-unnamed “common machine-readable technology” and antitampering features. The Department of Homeland Security also gained the power to require additional features, potentially including a biometric capability. Though states are not formally required to comply with Real ID, the law specifies that by 2008 only compliant licenses will be accepted for federally overseen identification purposes, which might include boarding an aircraft or taking advantage of government services.

Mounting opposition from state governments and civil liberties groups suggests that Real ID’s requirements may yet be modified, but the law’s passage highlights the federal government’s determination to formalize and strengthen identity credentials through the use of technology. Other examples include incorporating radio frequency identification (RFID) chips in a new generation of passports, the Transportation Security Agency’s proposed Registered Travelers program (in which travelers with special biometrics-based identity credentials might be allowed expedited security clearance in airports), and Homeland Security Presidential Directive (HSPD) 12, which mandates a new secure identification card for all federal employees and contractors. The resulting ID card standard, FIPS 201, describes a smart card format with embedded biometric information (Bush, 2004; National Institute of Standards and Technology, 2005).
How will these developments affect higher education? In a practical sense, FIPS 201 will probably have the most direct impact, at least on those universities that do government contract work and interact heavily with federal agencies. But the larger implication is the emergence of a more rigorous, technology-enabled approach to identity throughout American society. The new criteria may well become de facto standards for identity providers of many varieties, ranging from state and local governments to corporations and universities themselves. (FIPS 201 has already spawned a minor industry of consultants and solutions vendors eager to see the standard spread beyond the federal domain.) Widespread adoption of the federal initiatives could help diminish the cultural opposition to biometrics and other forms of strong identifiers and encourage the spread of smart card readers, while also beefing up identity proofing by providing stronger and more easily verified credentials. But the same initiatives will bring new integration demands to some institutions, and the civil liberties issues surrounding Real ID seem tailor-made to raise policy controversies regarding how campuses capture, use, and exchange information contained in the new cards.

Though less visible to the public at large, the federal government’s E-Authentication initiative represents another element in the growth of a new public identity infrastructure. Taking its mandate from an Office of Management and Budget directive defining levels of assurance (LoAs) for the identity processes associated with federal government systems, the E-Authentication initiative has produced a guiding Credential Assessment Framework that will present some challenges to higher education (Bolton, 2003; Louden et al., 2005a).

Depending on the levels of assurance needed, institutions may find it necessary to strengthen identity proofing; issue more robust, nonreassignable identifiers; employ multifactor authentication; and track identity transactions with greater care. As one of our respondents remarked in an open response comment, “We are working with the U.S. federal E-Authentication program. Their assurance requirements are causing us to make changes in our operations and documentation.” More broadly, E-Authentication signals that stricter and more standards-based identity capabilities are becoming a business requirement for interaction with the federal government—a trend that could eventually be extended to research funding, student financial aid, regulatory reporting, and other processes that higher education depends on.

E-Authentication will also likely encourage federated identity models; it is already converging to some degree with higher education’s federation initiatives. With both Shibboleth and E-Authentication moving toward support of Security Assertion Markup Language (SAML) 2.0, the technical basis for convergence will be much improved. Furthermore, as part of its stated intention of working through identity federations, E-Authentication is collaborating with InCommon in trial projects that would align federation membership (perhaps through a multilevel membership framework) with the E-Authentication LoA credentialing process (Klingenstein, 2005). Another significant development is the proposed USPerson attribute schema, modeled on the eduPerson schema that defines basic attribute exchange within InCommon. As additional schema frameworks and the flavors of identity attributes they spawn spread, they will put a premium on flexible identity infrastructures that can incorporate and leverage them.

A final consideration of government identity policy is the growing trend toward privacy regulation. California’s landmark SB 1386 privacy law, which requires enterprises to notify any California resident whose personal
information may have been compromised in a computer security breach, has become something of a de facto standard in lieu of federal legislation, and it has been widely imitated. In 2005 alone, 35 states introduced security breach legislation, and 22 adopted some form of it (National Conference of State Legislatures, 2006). A federal statute, however, may not be far behind; at the time of this writing (January 2006), a dozen separate privacy-related bills were before Congress (Zeller, 2005). An increasing emphasis on security and privacy due diligence, notification, and rectification will likely be part of the identity and privacy discussion in the United States for some time, though there is no sign of moving toward the sort of comprehensive, consumer-oriented policy represented in the European Data Protection Directive.

In combination with such laws as the Sarbanes-Oxley Act and the Gramm-Leach-Bliley Act, the new privacy and identity regulatory regime has sometimes been presented as a dangerous crisis for institutions, one that threatens campus business processes and even the personal liberty of campus officers. At a conference sponsored by the NSF Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium in June 2005, representatives of IdM solutions vendors ominously warned in one presentation after another of a harsh new climate; some even warned of jail sentences for recalcitrant CIOs.

In fact, the wave of new federal legislation has not resulted in a draconian era of exposure and prosecution, at least within higher education. Though mindful of a new burden, institutions seem to have found it possible to comply without extraordinary hardship. Some new practices, such as the Gramm-Leach-Bliley protection of Social Security numbers, would certainly have been necessary because of public or internal constituent pressure anyway.

Looking forward to what is likely to be a still more regulated and formalized identity sphere, higher education CIOs should consider how a new regime could present opportunities as well as challenges. Stricter regulation may give the force of mandate to identity practices that, as our results show, respondents believe are important and beneficial but which they are struggling to give appropriate priority. The message that “it’s not just a good idea, it’s the law” can cut through a lot of institutional obstacles. Federal privacy and identity measures, combined with the emerging infrastructure that federal initiatives are defining, may also help put an end to the patchwork regulations and integrations, and the chaotic atmosphere of unknown liability and inadequate auditability that now characterize many IdM environments.

**Academic and Business Drivers**

In contrast to the clear sense of direction toward stricter controls and official specifications evident in U.S. federal government identity policy, academic and business IdM drivers are more fragmented and tentative. Nevertheless, we can discern several trends that will likely drive IdM investment in coming years.

Some of the strongest indicators involve federated identity, especially as it relates to research and digital content issues. The absence of a scalable and effective mechanism for authorizing access to electronic content has bedeviled online research and e-learning environments since the explosion of Web access in the 1990s. Not surprisingly, academic publishers have been among the most conspicuous commercial supporters of the Shibboleth initiative and the Shibbolizing of such products as Elsevier’s ScienceDirect bibliographic database, the ARTstor digital image and JSTOR scholarly journal archives, OCLC’s FirstSearch multidatabase search service, and
databases from EBSCO and Thomson Gale, among others. This support underscores the potential that publishers see in federated identity as an alternative to current IP- or proxy-based access approaches. Likewise, support for Shibboleth credentials is available or in development for both commercial learning management systems such as those marketed by Blackboard Inc. (including its WebCT lines) and open source learning products like Moodle and ILIAS. Federated identity also shows promise in grid computing, which demands distributed identity functions. The NMI-funded GridShib project is working to add Shibboleth interoperability to the Globus open source toolkit for building grids and grid applications (Barton et al., 2006).

Purely academic solutions are not the only ones being supported. Shibboleth is being used for access to the Napster online music service at a number of campuses, an application that highlights the potential of federated identity’s loose-coupling approach as a means of extending student services. At many campuses today, the portal is the primary mechanism for delivering online services in the context of authenticated and authorized access, but the portal as a hub for diverse services presents limiting integration challenges. A robust federated identity system operating in the context of widespread federated trust frameworks could help augment portal capabilities while easing the portal “channelization” burden.

Similarly, federated identity could help revive the “market maker” concept, which promised to revolutionize procurement and supply-chain management by dynamically bringing together buyers and suppliers in third-party Web portals that enforced rule frameworks. In a federated model, trust frameworks might achieve the flexible interactions that portal and market-maker advocates originally sought, without a complex intermediate infrastructure or an unmanageable number of point-to-point integrations.

Will federated identity be adopted widely enough to make federation a requirement for doing business beyond the confines of higher education’s specific needs? The jury is still out, but there are signs that the same pattern of keen interest, experimental early adoption, and watchful waiting that prevails in higher education holds in corporate IT environments as well.

A 2003 Burton Group study of 15 early adopters from the financial services, manufacturing, telecommunications, and insurance industries, as well as higher education institutions, found that 90 percent reported using federated identity to support internal applications, 60 percent for business-to-business supplier relations, 47 percent for business-to-employee benefits applications, and 40 percent for business-to-business customer relations (Blum, 2003). Some of the most significant technical weaknesses in the SAML protocol noted in that report, such as weak session management and logout capabilities, have since been addressed in the SAML 2.0 standard, released by OASIS in early 2005 (Gebel, 2005). Major IdM technology vendors now offer federated identity systems within their product suites, and the Liberty Alliance offers conformance testing and certification for products that use its standards. Though interoperability still needs to improve, federated identity is a natural fit within industries that must manage complex interfaces and supply chains, including telecommunications, financial services, and retail. There is a good chance, then, that federated identity will emerge as a routine part of business-to-business and perhaps business-to-consumer interaction.

The fundamental question regarding federated identity’s value as a business enabler is whether the adoption of standards-based, loosely coupled identity attribute exchange will actually eliminate enough complexity to create value or simply expose the intractability of the underlying issues of trust and
demand, the Liberty Alliance has also initiated work to improve the interoperability of strong authentication in federated environments.

Corporations investing to extend stronger authentication to one slice of their customer base will probably also soon look for ways to gain efficiencies of scale and exploit new business opportunities. If such initiatives succeed, they could lower the barriers to stronger authentication within higher education environments by improving the technology and by helping acquaint masses of Internet-active consumers with stronger identity practices.

**Toward a New Paradigm: User-Centric IdM**

This study has looked at identity issues from the standpoint of higher education institutions as providers, administrators, and consumers of identity. But a gathering collection of technologists and social theorists is promoting a new vision of identity as a personal and social, rather than an enterprise or administrative, concern. Variously known as user-centric identity, personal digital identity, or decentralized identity, the new thinking seeks to distribute and standardize the process of identity exchange, allow users more granular control over the information they reveal, and give them more say over how that information is used. As Burton Group Analyst Mike Neuenschwander writes, “User-centric identity products will put new demands on the enterprise identity management infrastructure and have the potential to revolutionize the way individuals and enterprises relate to Internet communities” (Neuenschwander, 2005c, p. 19; see also Searls, 2005; and Grice & Goodman, 2005).

Certain user-centric identity (UCI) goals are practical: UCI addresses the Internet’s lack of a standard mechanism for conveying personal information to a Web site, still a major obstacle to e-commerce, and it provides a means for single sign-on and profile portability across
Web sites. But UCI also expresses larger cultural and social concerns. Developed more to fit the libertarian culture of the cybersphere than the hierarchical needs of enterprise IT, UCI reminds us that the Internet has always been a place where users have wanted to construct their own identities.

While a product marketplace for UCI doesn’t really exist yet, several initiatives suggest the direction the technology could take. Undoubtedly the most important of these is Microsoft’s InfoCard technology, which is slated for inclusion in Vista, the Windows XP successor product, and will be accessible to non-Microsoft applications. Conceived of as an implementation of a more abstract “identity metasystem” and developed to replace Microsoft’s ill-fated Passport technology, InfoCard takes a distributed approach to identity that allows the user to decide what information he or she wants to expose (Cameron, 2005). Using a wallet metaphor, InfoCard users can create their own identity “cards” or request them from external identity providers. Cards may have different characteristics, depending on the identity provider’s nature and the user’s preferences. A user requesting access to a resource triggers a request from the resource to InfoCard, which presents the user with a choice of appropriate responding cards. When the user selects a card, InfoCard retrieves the user’s information from the identity provider and passes it to the resource.

UCI protocols and technologies are also being developed by start-up firms and open source initiatives. Sxip (pronounced “skip”), a Vancouver-based start-up, has developed a protocol (Simple eXtensible Identity Protocol, or SXIP) and a hosted network service to deliver its version of what it styles Identity 2.0. Through the Sxip Network, users registered at a Sxip “homesite” can associate their personal properties with multiple personas that might be used for different purposes, and they can control how that information is released to consuming “membersites” (Hardt, 2004). Technologies that employ UCI concepts to advance social networking, blogging, and other kinds of Internet peer interaction include Lightweight Identity (LID), a set of personal digital identity protocols developed by NetMesh, and OpenID, which permits a user logged in to one OpenID-enabled site to cross over to other trusted OpenID-enabled sites without reauthenticating.

Helping to enable UCI as well as more traditional IdM is the Extensible Resource Identifier (XRI) standard from OASIS, a naming standard compatible with the IETF/W3C Uniform Resource Identifiers (URI) Web addressing standard (OASIS, 2005). XRIs can be used to identify persons, companies, network resources, and any other type of object, providing an identifier that can cross systems and means of access. One implementation of XRI is i-names, developed by the Identity Commons. I-names are global, persistent personal identifiers that let individuals identify themselves and share personal profiles across enabled means of access—potentially including e-mail, telephone, and instant messaging, as well as single sign-on—to enabled Web sites. Another initiative, OpenXRI.org, is modeled on the Apache Foundation and is working on an open source infrastructure for implementing XRI.

UCI is a far-edge concept in a field characterized, even in its most traditional manifestations, by immature and emerging technologies. As Burton Group’s Neuenschwander writes, “Architecting for user-centric IdM is, at this point, premature” (Neuenschwander, 2005c, p. 4). Even so, because it involves a significant paradigm change and addresses real problems with the existing identity infrastructure, it deserves the attention of higher education IT planners.

UCI could potentially help with some thorny problems for which no good solution currently exists. For example, many institutions
and technology vendors are now promoting electronic portfolios for students, conceived of as lifelong, cross-institutional repositories of student work and performance. One of the unaddressed issues with e-portfolios is how to combine the authoritative certification of e-portfolio entries (for example, grades or instructor comments on student work) with flexible student control over who sees the e-portfolio and what users can review. UCI integration could provide just such a capability. UCI might also provide a good identity model for collaboration and peer-to-peer exchange networks. “Cards” or other kinds of UCI credentials could be a way to extend privileges to the large body of users—like prospective students, visitors, and alumni—who aren’t represented in systems of record and therefore make an awkward fit with institutional authentication and authorization mechanisms. At the same time, UCI presents another potential infrastructure (or set of them) that institutions will have to incorporate at both the technical and policy levels.

**Moving Forward**

Our study found that respondent institutions are busy with IdM. This chapter’s review of emerging IdM drivers suggests that they’re going to get busier still because new identity needs will appear at every level.

From “above,” government regulation of personal information will continue to grow more widespread and stringent, and the creation of new identity infrastructures will present integration and architectural challenges. Among peer institutions and business partners, the seamless exchange of academic content and business information will increasingly demand that identity infrastructures operate across domains. And from “below,” institutions can expect to find users possessing more-sophisticated identity credentials and demanding more control over their personal information.

How can institutions meet these challenges when their IdM agendas are already crowded and they confront other IT priorities and constrained funding? It would be idle to suggest that IT administrators simply demand a lot more money and staff. While IdM is both strategic enough and driven enough by external mandates to justify a bigger slice of institutional support, constraint is likely to remain a fact of life for most institutions, and the deep-pocketed, broad-front strategic project will be the exception. As ECAR reported in an IT funding study in 2004, “IT budgets are constrained and consumed by fixed costs.... Few expect this situation to improve through any sizable IT budget increases for the foreseeable future” (Goldstein, 2004, p. 93; see also Jones, 2006). What’s more, large-scale “big bang” projects of the type that characterized the ERP wave of the Y2K era today meet with more skepticism than they once did, and senior leadership expects IT projects to justify themselves less by vision and more by value.

It would be going too far to call this situation a blessing in disguise, but it is also possible to identify strategies that allow institutions to move forward effectively in an atmosphere of constraint. As our 2004 funding study noted, institutions can respond to the funding crunch by pursuing agility and flexibility. Specifically, they can use such techniques as emphasizing collaboration and shared services, establishing flexible architectures and standards that facilitate integration, and focusing on smaller, targeted projects that produce benefits quickly (Goldstein, 2004).

An agile and flexible approach to IdM means putting limited resources where they will do the most good, covering the widest possible spread of new demands and priorities that future developments may bring. This suggests that committing to broad technology solutions is not the most pressing task; indeed, this is one area where time is probably on institutions’ side. Many IdM vendors are still developing
their product suites and absorbing the wave of acquisitions that has recently swept the marketplace, and important open source solutions such as Shibboleth, Signet, and Grouper are still in early or prerelease stages. Therefore, in most situations, institutions can get the most value by focusing now on high-value point projects and the IdM “soft infrastructure”—the data structures, policies, plans, collaborations, and management issues that secure a sound foundation for technical progress. We offer the following specific suggestions:

Unsnarl the data tangle. No comment was voiced more often in the course of our study than the observation that basic identity-related data elements lack an enterprise-wide definition. As one of our survey respondents said in an open-format remark, IdM “is much more complex than I had imagined it would be. The biggest problem has to do with data quality and policies.” Seeking out data stewards and working with them to create cleaner, more portable, and better-defined data structures is a collaborative effort that can eliminate redundancies and improve identity systems’ leveragability. Yet as we reported in Chapter 4, only about a third of respondent institutions had completed documenting their data custodians, and only 15 percent had completed documenting and reconciling data definitions (see Table 4-11).

Make the most of incremental improvements. Small victories that build confidence and encourage further investment are a key aspect of IT agility. Where central IT needs to move forward without a lot of resources or campus buy-in, projects should be organized to demonstrate quick wins with clear business benefits that are brought to the notice of users. The danger of an IT-centric “stealth” approach is that projects will be purely reactive or will address only narrow IT interests, bypassing essential awareness-raising and policy development in the larger community. But as NMI-EDIT notes in the context of enterprise directory deployments, IT-driven projects can be used “at first to demonstrate value to campus stakeholders and provide incentives to engage them in the necessary institutional policy and business process discussions” (West, 2005, p. 5; emphasis added).

Embrace standards and flexible architectures. It’s hard to think of any technology area that can benefit more from open standards and architectures than IdM. Though IdM standards remain underdeveloped, core standards such as the Lightweight Directory Access Protocol (LDAP), SAML, and X.509 provide a foundation for a standards-based identity infrastructure. Newer standards such as XRI and its companion, the data exchange standard XDI, will soon make their influence felt, as will the Liberty Alliance and WS-* specifications. Work toward a more comprehensive IdM framework now being done through the ISO/IEC (International Organization for Standardization and the International Electrotechnical Commission) and spearheaded by the European Union’s Future of Identity in the Information Society (FIDIS) could also help resolve some of the confusion and overlap now apparent in IdM standards. Institutions that make the maximum possible use of standards and orient their architectures toward flexible incorporation of new identity systems will be in the best position to respond to emerging IdM demands.

Build the policy foundation. The identity infrastructure is in essence a technical implementation of rules about access, data control and, ultimately, the management of the institution. Where these rules are ad hoc and undocumented, identity systems are exposed to security risks and inefficiencies caused by inconsistencies, redundancies, and an accretion of “one-off” quick fixes. Auditability suffers as well. As we noted in Chapter 9, institutions that have completed authentication and authorization policies report, on average, considerably higher IdM capability
than those with partially completed or no policies (see Table 9-5). Though roughly half of respondent institutions report completing documented policies in major areas of IdM (see Figure 4-6), the high proportion of those with incomplete or partial policies is worrisome. As identity systems become ever more interconnected and visible, clear policies reflecting an explicit campus consensus will likewise become ever more valuable.

Get senior management aware and involved. Though it is something of an old chestnut in IT administration, the value of senior management awareness and support is hard to overstate. We found that institutions expressing higher levels of agreement that their senior management understands IdM and is willing to address related policy issues also tend to report higher resource sufficiency and IdM capability (see Tables 4-10 and 9-3). Making senior leaders aware of the business and academic benefits of a sound identity infrastructure is a way to enlist their assistance with the political and financial challenges that must be met to achieve ambitious IdM goals.

Conclusion

In emphasizing agility and foundational work, we do not mean to be fatalistic about the importance of securing appropriate resources for IdM. To quote our funding study once again, “We cannot secure the future through agility alone” (Goldstein, 2004, p. 97). IdM is and will continue to be the basic enabler of secure and effective online transactions, and as transactions become more numerous, distributed, sensitive, and regulated, identity systems will almost certainly need increasing resources. With or without the help of government mandate or some other exogenous factor, securing better resources will mean preparing the ground for success and demonstrating that improving identity systems brings concrete benefits. As higher education moves from the present baseline of IdM toward the mainstream adoption of better-architected, more robust, and far more comprehensive identity infrastructures, it must also transform virtual identity from a parochial IT concern to an enterprise priority.
Appendix A

Institutional Respondents to the Online Survey

Alfred University–New York State College of Ceramics
Amherst College
Anne Arundel Community College
Appalachian State University
Arizona State University
Arkansas State University
Arkansas Tech University
Auburn University at Montgomery
Austin College
Austin Community College
Azusa Pacific University
Babson College
Baker University
Bates College
Baylor University
Benedictine University
Bismarck State College
Black Hawk College
Blinn College
Board of Regents of the University System of Georgia
Boise State University
The Boston Conservatory
Boston University
Bradley University
Brandeis University
Brown University
Bucknell University
Buffalo State College
Caldwell College
California Maritime Academy
California State Polytechnic University, Pomona
California State University, Bakersfield
California State University, Chico
California State University, Dominguez Hills
California State University, East Bay
California State University, Fresno
California State University, Long Beach
California State University, Los Angeles
California State University, Monterey Bay
California State University, Northridge
California State University, Office of the Chancellor
California State University, Sacramento
California State University, San Bernardino
California State University, San Marcos
Calvin College
Camosun College
Canisius College
Carleton College
Carleton University
Case Western Reserve University
Cecil Community College
Cedarville University
Central Missouri State University
Central Washington University
Charleston Southern University
City University of New York, The Graduate Center

©2006 EDUCAUSE. Reproduction by permission only.
<table>
<thead>
<tr>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claflin University</td>
</tr>
<tr>
<td>Clark University</td>
</tr>
<tr>
<td>Clemson University</td>
</tr>
<tr>
<td>Colby-Sawyer College</td>
</tr>
<tr>
<td>Colgate University</td>
</tr>
<tr>
<td>College of Lake County</td>
</tr>
<tr>
<td>College of Mount Saint Joseph</td>
</tr>
<tr>
<td>College of New Jersey</td>
</tr>
<tr>
<td>College of Saint Rose</td>
</tr>
<tr>
<td>College of Saint Scholastica</td>
</tr>
<tr>
<td>Collin County Community College District</td>
</tr>
<tr>
<td>Colorado State University</td>
</tr>
<tr>
<td>Colorado State University–Pueblo</td>
</tr>
<tr>
<td>Columbia University</td>
</tr>
<tr>
<td>Columbia-Greene Community College</td>
</tr>
<tr>
<td>Concordia University, Portland</td>
</tr>
<tr>
<td>Concordia University, St. Paul</td>
</tr>
<tr>
<td>Coppin State University</td>
</tr>
<tr>
<td>Corinthian Colleges, Inc.</td>
</tr>
<tr>
<td>Cornell University</td>
</tr>
<tr>
<td>Dalhousie University</td>
</tr>
<tr>
<td>Davenport University</td>
</tr>
<tr>
<td>Denison University</td>
</tr>
<tr>
<td>DePauw University</td>
</tr>
<tr>
<td>Dickinson College</td>
</tr>
<tr>
<td>Drexel University</td>
</tr>
<tr>
<td>East Stroudsburg University of Pennsylvania</td>
</tr>
<tr>
<td>Eastern Arizona College</td>
</tr>
<tr>
<td>Edinboro University of Pennsylvania</td>
</tr>
<tr>
<td>Edison Community College</td>
</tr>
<tr>
<td>Elizabeth City State University</td>
</tr>
<tr>
<td>Elmhurst College</td>
</tr>
<tr>
<td>Emory University</td>
</tr>
<tr>
<td>Empire State College SUNY</td>
</tr>
<tr>
<td>Emporia State University</td>
</tr>
<tr>
<td>Fairfield University</td>
</tr>
<tr>
<td>Fashion Institute of Technology</td>
</tr>
<tr>
<td>Fielding Graduate University</td>
</tr>
<tr>
<td>Florida Memorial University</td>
</tr>
<tr>
<td>Florida Southern College</td>
</tr>
<tr>
<td>Foothill-DeAnza Community College District</td>
</tr>
<tr>
<td>Fordham University</td>
</tr>
<tr>
<td>Franklin and Marshall College</td>
</tr>
<tr>
<td>Franklin W. Olin College of Engineering</td>
</tr>
<tr>
<td>Furman University</td>
</tr>
<tr>
<td>GateWay Community College</td>
</tr>
<tr>
<td>Genesee Community College</td>
</tr>
<tr>
<td>George Fox University</td>
</tr>
<tr>
<td>George Washington University</td>
</tr>
<tr>
<td>Georgetown University</td>
</tr>
<tr>
<td>Georgia State University</td>
</tr>
<tr>
<td>Georgian Court University</td>
</tr>
<tr>
<td>Glendale Community College</td>
</tr>
<tr>
<td>Gloucester County College</td>
</tr>
<tr>
<td>Grand Valley State University</td>
</tr>
<tr>
<td>Guilford College</td>
</tr>
<tr>
<td>Hamilton College</td>
</tr>
<tr>
<td>Hampton University</td>
</tr>
<tr>
<td>Harford Community College</td>
</tr>
<tr>
<td>Harrisburg University of Science and Technology</td>
</tr>
<tr>
<td>HEC Montreal</td>
</tr>
<tr>
<td>Highline Community College</td>
</tr>
<tr>
<td>Hollins University</td>
</tr>
<tr>
<td>Howard Community College</td>
</tr>
<tr>
<td>Hudson County Community College</td>
</tr>
<tr>
<td>Humber College Institute of Technology and Advanced Learning</td>
</tr>
<tr>
<td>Humboldt State University</td>
</tr>
<tr>
<td>Hutchinson Community College &amp; Area Vocational School</td>
</tr>
<tr>
<td>Idaho State University</td>
</tr>
<tr>
<td>Illinois Wesleyan University</td>
</tr>
<tr>
<td>Indiana University</td>
</tr>
<tr>
<td>Indiana University Kokomo</td>
</tr>
<tr>
<td>Indiana University of Pennsylvania</td>
</tr>
<tr>
<td>Indiana University Southeast</td>
</tr>
<tr>
<td>Iowa State University</td>
</tr>
<tr>
<td>Ithaca College</td>
</tr>
<tr>
<td>Ivy Tech State College Central Office</td>
</tr>
<tr>
<td>Jackson Community College</td>
</tr>
<tr>
<td>John Brown University</td>
</tr>
<tr>
<td>Johnson County Community College</td>
</tr>
<tr>
<td>Juniata College</td>
</tr>
<tr>
<td>Kansas State University</td>
</tr>
<tr>
<td>Kent State University</td>
</tr>
<tr>
<td>Kwantlen University College</td>
</tr>
<tr>
<td>Lafayette College</td>
</tr>
<tr>
<td>Lakehead University</td>
</tr>
<tr>
<td>Lawrence University</td>
</tr>
<tr>
<td>Institution Name</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Lebanon Valley College</td>
</tr>
<tr>
<td>Lethbridge Community College</td>
</tr>
<tr>
<td>Lewis University</td>
</tr>
<tr>
<td>Life Pacific College</td>
</tr>
<tr>
<td>Lincoln Memorial University</td>
</tr>
<tr>
<td>Linn-Benton Community College</td>
</tr>
<tr>
<td>Lock Haven University of Pennsylvania</td>
</tr>
<tr>
<td>Longwood University</td>
</tr>
<tr>
<td>Loyola Marymount University</td>
</tr>
<tr>
<td>Lynn University</td>
</tr>
<tr>
<td>Lyon College</td>
</tr>
<tr>
<td>Maricopa Community College District</td>
</tr>
<tr>
<td>Marist College</td>
</tr>
<tr>
<td>Marquette University</td>
</tr>
<tr>
<td>Marygrove College</td>
</tr>
<tr>
<td>Massachusetts College of Art</td>
</tr>
<tr>
<td>Massachusetts Institute of Technology</td>
</tr>
<tr>
<td>McGill University</td>
</tr>
<tr>
<td>Medicine Hat College</td>
</tr>
<tr>
<td>Mercy College</td>
</tr>
<tr>
<td>Metropolitan Community College</td>
</tr>
<tr>
<td>Metropolitan State College of Denver</td>
</tr>
<tr>
<td>MGH Institute of Health Professions</td>
</tr>
<tr>
<td>Miami University</td>
</tr>
<tr>
<td>Michigan State University</td>
</tr>
<tr>
<td>Middle Tennessee State University</td>
</tr>
<tr>
<td>Middlebury College</td>
</tr>
<tr>
<td>Millersville University of Pennsylvania</td>
</tr>
<tr>
<td>Mills College</td>
</tr>
<tr>
<td>Millsaps College</td>
</tr>
<tr>
<td>Minneapolis College of Art and Design</td>
</tr>
<tr>
<td>Minnesota State Colleges and Universities</td>
</tr>
<tr>
<td>Minot State University</td>
</tr>
<tr>
<td>Mississippi University for Women</td>
</tr>
<tr>
<td>Monmouth College</td>
</tr>
<tr>
<td>Monmouth University</td>
</tr>
<tr>
<td>Monroe Community College</td>
</tr>
<tr>
<td>Montclair State University</td>
</tr>
<tr>
<td>Montgomery College</td>
</tr>
<tr>
<td>Mount Holyoke College</td>
</tr>
<tr>
<td>Mount Mary College</td>
</tr>
<tr>
<td>Mount Saint Mary's College</td>
</tr>
<tr>
<td>Mount Vernon Nazarene University</td>
</tr>
<tr>
<td>Muhlenberg College</td>
</tr>
<tr>
<td>Murray State University</td>
</tr>
<tr>
<td>Nashville State Community College</td>
</tr>
<tr>
<td>Nevada System of Higher Education</td>
</tr>
<tr>
<td>New England College</td>
</tr>
<tr>
<td>New York University</td>
</tr>
<tr>
<td>Nipissing University</td>
</tr>
<tr>
<td>Norfolk State University</td>
</tr>
<tr>
<td>North Carolina A&amp;T State University</td>
</tr>
<tr>
<td>North Dakota State University</td>
</tr>
<tr>
<td>North Harris Montgomery Community College District</td>
</tr>
<tr>
<td>North Lake College</td>
</tr>
<tr>
<td>Northeastern Illinois University</td>
</tr>
<tr>
<td>Northeastern University</td>
</tr>
<tr>
<td>Northern Illinois University</td>
</tr>
<tr>
<td>Northern Kentucky University</td>
</tr>
<tr>
<td>Northwest University</td>
</tr>
<tr>
<td>Northwestern University</td>
</tr>
<tr>
<td>Oakland University</td>
</tr>
<tr>
<td>Oberlin College</td>
</tr>
<tr>
<td>Ocean County College</td>
</tr>
<tr>
<td>Ohio Northern University</td>
</tr>
<tr>
<td>The Ohio State University Mansfield Campus</td>
</tr>
<tr>
<td>The Ohio State University Newark Campus</td>
</tr>
<tr>
<td>Ohio University</td>
</tr>
<tr>
<td>Oklahoma State University College of Osteopathic Medicine</td>
</tr>
<tr>
<td>Oregon State University</td>
</tr>
<tr>
<td>Otterbein College</td>
</tr>
<tr>
<td>Pace University</td>
</tr>
<tr>
<td>Pellsissipi State Technical Community College</td>
</tr>
<tr>
<td>Pennsylvania College of Technology</td>
</tr>
<tr>
<td>The Pennsylvania State University</td>
</tr>
<tr>
<td>Phoenix College</td>
</tr>
<tr>
<td>Plymouth State University</td>
</tr>
<tr>
<td>Pomona College</td>
</tr>
<tr>
<td>Presbyterian College</td>
</tr>
<tr>
<td>Prince George’s Community College</td>
</tr>
<tr>
<td>Princeton University</td>
</tr>
<tr>
<td>Providence College</td>
</tr>
<tr>
<td>Purdue University</td>
</tr>
<tr>
<td>Queens University of Charlotte</td>
</tr>
<tr>
<td>Radford University</td>
</tr>
<tr>
<td>Randolph-Macon College</td>
</tr>
<tr>
<td>Raritan Valley Community College</td>
</tr>
</tbody>
</table>
Red Deer College
Rensselaer Polytechnic Institute
Rhode Island School of Design
Rice University
Richard Bland College
Rochester Institute of Technology
Roosevelt University
Rutgers, The State University of New Jersey
Saint John’s University/College of Saint Benedict
Salve Regina University
Sam Houston State University
Samford University
San Diego State University
Santa Clara University
Santa Fe Community College
Saskatchewan Institute of Applied Science and Technology
School of the Art Institute of Chicago
Schreiner University
Seattle Pacific University
Seton Hall University
Shepherd University
Sinclair Community College
Solano Community College
Sonoma State University
South Dakota State Board of Regents System Office
Southern Adventist University
Southern Illinois University at Carbondale
Southern Illinois University at Edwardsville
Southern Methodist University
Southwest Baptist University
Southwest Missouri State University–West Plains
Southwestern University
St. Cloud State University
St. Lawrence University
St. Mary’s College of Maryland
St. Olaf College
St. Philip’s College
State Fair Community College
SUNY College at Cortland
SUNY College at Geneseo
SUNY College of Optometry
SUNY College of Technology at Alfred
Sweet Briar College
Syracuse University
Taylor University
Temple University
Texas Christian University
Texas State Technical College–Harlingen
Texas State University–San Marcos
Texas Wesleyan University
Thomas Jefferson University
Trinity College
Trinity University
Truckee Meadows Community College
Tufts University
Tulane University
Ulster County Community College
United States Air Force Academy
United States Coast Guard Academy
University at Buffalo
University College of the Fraser Valley
University of Alabama
University of Alaska
University of Alaska Anchorage
University of Arizona
University of British Columbia
University of Calgary
University of California Office of the President
University of California, Berkeley
University of California, Irvine
University of California, Los Angeles
University of California, Merced
University of California, San Diego
University of California, San Francisco
University of California, Santa Barbara
University of California, Santa Cruz
University of Central Florida
University of Colorado at Boulder
University of Delaware
University of Detroit Mercy
University of Florida
University of Guelph
University of Hawaii
University of Houston
University of Houston–Downtown
Identity Management

ECAR Research Study 2, 2006

University of Illinois at Chicago
University of Illinois at Springfield
University of Kansas
University of Kansas Medical Center
University of Louisville
University of Maine at Presque Isle
University of Manitoba
University of Mary Washington
University of Maryland
University of Maryland, Baltimore
University of Massachusetts at Amherst
University of Massachusetts at Worcester
University of Memphis
University of Miami
University of Michigan–Ann Arbor
University of Minnesota
University of Minnesota Duluth
University of Mississippi
University of Missouri–Columbia
University of Montana
University of Nebraska
University of Nebraska–Lincoln
University of Nebraska at Kearney
University of Nevada, Las Vegas
University of New Brunswick
University of North Carolina at Chapel Hill
University of North Carolina at Charlotte
University of North Carolina at Wilmington
University of North Texas HSC at Fort Worth
University of Northern Colorado
University of Notre Dame
University of Oklahoma Health Sciences Center
University of Oregon
University of Puget Sound
University of Rochester
University of Saskatchewan
University of South Carolina–Beaufort
University of South Dakota
University of Tennessee
University of Tennessee at Chattanooga
The University of Texas at Austin
University of Texas at San Antonio
University of Texas at Tyler

University of Texas HSC at San Antonio
University of Texas Medical Branch
University of Texas of the Permian Basin
University of Texas System
University of Utah
University of Victoria
University of Washington
University of Washington, Bothell
University of Waterloo
University of West Florida
University of Winnipeg
University of Wisconsin–Madison
University of Wisconsin–Milwaukee
University of Wisconsin–River Falls
University System of Maryland
University System of New Hampshire
Vancouver Community College
Vermont State Colleges
Villanova University
Virginia Tech
Volunteer State Community College
Walsh University
Wayland Baptist University
Wayne State University
Webber State University
Webster University
Wellesley College
West Virginia School of Osteopathic Medicine
West Virginia State University
Western Illinois University
Western Kentucky University
Western Michigan University
Western New England College
Western New Mexico University
Westminster College
Wheaton College
Whitman College
Widener University
Wilkes University
Willamette University
Williams College
Wisconsin Lutheran College
York College of Pennsylvania
Appendix B

Interviewees in Qualitative Research

Anne Arundel Community College
    John David Becker, Chief Technology Officer, Information Services

Blinn College
    Michael Welch, Dean, Academic Technology Services

Carleton College
    Joel Cooper, Director of Information Technology Services

Dalhousie University
    John Sherwood, Executive Director of University Computing and Information Systems

Embry-Riddle Aeronautical University
    Becky Vasquez, IT Services Director
    Mark Talaga, Internet Specialist
    Joe Progar, Systems Security Administrator

Foothill-DeAnza Community College District
    William Pritchard, Vice Chancellor for Information Technology

Marist College
    Harry Williams, Director of Technology and Systems

Massachusetts Institute of Technology
    Jeffrey I. Schiller, Network Manager, Information Systems and Technology

North Dakota State University
    John Grosen, Director, Infrastructure Services
    Greg Wettstein, Manager of Research Computing Group and Hurderos Architect

©2006 EDUCAUSE. Reproduction by permission only.
Identity Management

ECAR Research Study 2, 2006

Northern Kentucky University
Gary Pratt, Associate Provost for IT and Chief Information Officer
Jason Allen, Manager of Servers and Operations
Bill Cooper, Senior Information Systems Specialist
David Renaker, Lead Systems Analyst

Northwestern University
Thomas E. Board, Director, Information Systems Architecture

Princeton University
Daniel Oberst, Director of Enterprise Business Services

Rice University
Barry Ribbeck, Director of Systems Architecture and Infrastructure

St. Cloud State University
Philip Thorson, Chief Information Officer

St. Mary’s University of Minnesota
Chad L. Kjorlien, Director of Instructional Technology

Trinity University
Charles B. White, Vice President for Information Resources and Administrative Affairs

University of California, San Diego
Elazar Harel, Chief Information Officer
Charlotte Klock, Director, Data Center
Gabriel Lawrence, Data Security Manager

University of Florida
Mike Conlon, Director of Data Infrastructure

University of Maryland, Baltimore
Peter Murray, Vice President for Information Technology and Chief Information Officer

University of New Hampshire
Bill Baber, Associate Director of Academic Technology and Portal Coordinator

University of Notre Dame
Gordon Wishon, Chief Information Officer, Associate Vice President, and Associate Provost

University of Oregon
Susan Hilton, Director of Administrative Services
Noreen Hogan, Principal Technologist
University of Texas Health Science Center at Houston
William Weems, Assistant Vice President for Academic Technology

University of Wisconsin–Madison
Mairéad Martin, Manager of Middleware Systems Technology
Chris Holsman, Enterprise Internet Solutions
Jim Lowe, Manager, IT Security

Vermont State Colleges
Linda Hilton, Chief Information Officer

Wayne State University
John Camp, Chief Information Officer
Patrick Gossman, Director of Academic Technologies and Customer Services
Appendix C

Glossary

-A-

Authentication: The process of gaining confidence that a subject using a digital identity or presenting a credential is the subject that is qualified to use it. It is, further, a security measure designed to establish the validity of a transmission, message, or originator, and it is a means of verifying an individual’s authorization to receive specific categories of information.

Authentication server: A system that provides authentication services to other systems on a network.

Authorization: The process of determining a specific person’s eligibility to gain access to an application or function, or to make use of a resource. It may also be described as a right or permission that is granted to access a system resource.

-B-

Biometrics: In computer security, biometrics refers to authentication techniques that rely on physical characteristics that can be automatically checked. Examples include computer analysis of fingerprints or speech.

-C-

Certificate (digital): A data structure signed by a certification authority that binds a subject’s name identifier to a public key or other attributes of the subject.

Certification authority: A service that issues certificates to subjects and generates certificate revocation lists.

Credential (digital): A shared secret or a token (such as biometric data, a hashed password, or a signature proving possession of a private key) that imparts confidence in the claimed identity of the subject (or other claims).

©2006 EDUCAUSE. Reproduction by permission only.
Cryptography: A coding method, using an algorithm, by which data is encrypted (translated into an unreadable format) and then decrypted (translated back into a readable format) to ensure the secrecy and/or authenticity of data.

Digital identity: The representation of a subject that includes a unique number or identifier, credential(s), and attributes (a profile); it may comprise one account or a collection of accounts referring to the same subject.

Directory: A repository of information about subjects or objects that is used to provide directory services. The repository may be distributed, and the information in the repository may be accessible via the Lightweight Directory Access Protocol (LDAP) or other protocols.

Directory service: A network service that identifies resources on a network and makes them accessible to users and applications. Resources include e-mail addresses, computers, and peripheral devices such as printers. Ideally, the directory service should make the physical network topology and protocols transparent so that a user on a network can access any resource without knowing where or how it is physically connected.

Electronic signature: A method and tools used to authenticate the identity of the sender of a message or to ensure the integrity of the content of the message. Electronic signatures use public key encryption techniques to create a verifiable signature for each document. Use of electronic signatures was legalized at the federal level by the Electronic Signatures in Global and National Commerce Act of 2000.

Encryption: The conversion of text or data into unintelligible (coded) form by means of a reversible translation that is based on a translation table or algorithm.

Enterprise directory: A system for centrally organizing information about an organization’s users, passwords, and authorizations to access networked resources.

Entitlement: The capability-based reason (i.e., a user has a valid role, ticket, or token) a user should be given a permission or set of permissions.

ERP: Refers to an integrated suite of administrative information systems designed to support and automate business processes through a centralized database system. In higher education, these systems usually include student systems, financial systems, and human resources systems, as well as warehouse and planning tools.

Federated identity: A collective term describing agreements, standards, and technologies that make identity and entitlements portable across autonomous domains. See also “identity federation.”

**Grid computing:** A form of networking that, unlike conventional networks that focus on communication among devices, harnesses unused processing cycles of all computers in a network for solving problems too intensive for any stand-alone machine.

**Grouper:** An open source toolkit developed by Internet2/MACE for managing groups. It is designed to function as the core element of a common infrastructure for managing group information across integrated applications and repositories. See <http://middleware.internet2.edu/dir/groups/grouper/>.

**Gramm-Leach-Bliley Act of 1999:** This act of Congress requires higher education to notify people they deal with of their right to keep their financial information confidential and to protect their financial data. Protection involves having a plan or security policy that includes designating an employee to coordinate information security, identify and repair weaknesses in computer systems, continually monitor systems, provide security training for employees, and require service providers to comply with the law through contract language requiring compliance. More information is available at <http://www.senate.gov/~banking/conf/>.

**Hardware token:** A security device carried by a user, required to authenticate to the system. Examples could include a dongle attached to a PC’s USB or serial port or a password generator, such as RSA’s SecurID product. Such devices are often used in conjunction with a password, resulting in two-factor authentication.

**HIPAA (Health Insurance Portability and Accountability Act):** Multifaceted U.S. law passed in 1996. In an information security context, the law sets standards for information security and privacy for organizations dealing with patient-identifiable medical data, as well as penalties for noncompliance. More information is available at <http://www.hipaa.org/>.


**Identifier:** A function that maps real-world subjects into name or character strings so that distinct subjects have distinct strings. A real-world subject may be a person, an object (i.e., a printer or a file), a group, or a department. A real-world subject can have multiple identifiers, such as e-mail addresses or network IDs.

**Identity:** See “digital identity.”

**Identity federation:** A community of identity provider and service provider domains that use federated identity in support of shared applications or services.

**Identity management (IdM):** The set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities.
ISO (International Organization for Standardization): ISO is not an acronym; instead, the name derives from the Greek word iso, which means equal. Founded in 1946, ISO is an international organization composed of national standards bodies from more than 75 countries. For example, ANSI belongs to the ISO.

Internet2: A university-led effort to develop advanced network applications and the network technologies needed to support them. The 200+ U.S. universities that lead the project work closely with partners in industry and government and with advanced networks around the world.

Kerberos: A secret-key network authentication system used for encryption and authentication. Kerberos was designed to authenticate requests for network resources rather than to authenticate authorship of documents. Kerberos was developed at and continues to be enhanced by MIT. More information is available at <http://web.mit.edu/kerberos/>.

Liberty Alliance: A consortium founded by Sun Microsystems representing corporate and public-sector organizations from around the world, created in 2001 to address the technical, business, and policy challenges around federated identity and identity-based Web services. See <https://www.projectliberty.org>.

LDAP (Lightweight Directory Access Protocol): A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but it is significantly simpler. Unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Because it’s a simpler version of X.500, LDAP is sometimes called X.500-lite. Because LDAP is an open protocol, applications need not worry about the type of server hosting the directory.

Multifactor authentication: Authentication is typically based on factors such as something a user knows (e.g., a password), has (such as a hardware token), or is (e.g., biometrically-captured physical characteristics). Multifactor authentication employs two or more such factors so that a breach in the security of one factor (e.g., a password being guessed or stolen) leaves additional secure factors in place.

OASIS (Organization for Advancement of Structured Information Standards): A standards body involved in the creation of international standards for electronic business. OASIS particularly focuses on standards for Web services and security. OASIS is responsible for the SAML standard, among others. See http://www.oasis-open.org/who/.
**Open source:** A program in which the source code is available to the general public for use and/or modification from its original design free of charge—that is, open. Open source code is typically created as a collaborative effort in which programmers improve upon the code and share the changes within the community. Open source sprouted in the technological community as a response to proprietary software owned by corporations.

**Password:** A protected and private character string assigned to a specific user. Often knowledge of the password associated with the user ID is considered proof of authentication.

**Password, one-time:** A password that can only be used once. Such passwords are often generated by a hardware token that is synchronized to a server. Single-use passwords remove the danger of a password’s being compromised during transmission across the network.

**Password, strong:** A password created with formulation rules and other characteristics, such as a forced reset date, that make it harder to guess, steal, decode computationally, or use if improperly obtained.

**PKI (public key infrastructure):** A cryptographically based coding system and supporting infrastructure in which encryption and decryption are done with public and private keys, allowing users who don’t know each other to send secure or verifiable messages.

**Reduced/single sign-on (RSSO):** Single sign-on is a method of authentication that allows a user to log in to a network, and, for a period of time, have his or her credentials passed to multiple requested applications, resources, or domains, enabling their use without requiring separate authentication for each one. Because technical and business issues often make it difficult to deliver a literally “single” sign-on to all resources, reduced sign-on may be an acceptable practical goal.

**Risk assessment:** An estimate of the harm to business likely to result from a security failure and of the likelihood of such a failure occurring, given the threat environment and the measures in place to prevent a failure.

**Role:** A conceptual, semantic object that represents a collection of permissions (e.g., information technology roles) or a collection of users (e.g., user roles) and generally relates to a class of business functions.

**Role-based authorization (RBA):** The ability to automate the granting of privileges or permissions to authenticated users on the basis of known user attributes (such as job title, enrollment status, etc.). Also known as role-based access control.
SAML (Security Assertion Markup Language): An XML-based framework developed by OASIS for communicating user authentication, entitlement, and attribute information. SAML is employed in the Shibboleth and Liberty Alliance federated identity systems.

Self-service: In an identity management context, functions that permit individual users to administer specific attributes of their own profiles, typically restricted to changing passwords and other personal information.

Shibboleth: An open source middleware federated identity solution created by Internet2/MACE to allow organizations to exchange information about their users in a secure manner that ensures protection of privacy. The purpose of the exchange is typically to determine if a person using a Web browser has permission to access a target resource based on information such as being a member of an institution or a particular class. More information about Shibboleth is available at <http://shibboleth.internet2.edu/>.

Signet: An open source privileges-management solution developed by Internet2/MACE that supports distributed privileges management. Administrators and business analysts first model the privilege requirements in a set of distinct rules. Applications may need to be enabled to accept information from Signet. Once this is done, users can begin to assign and delegate their privileges through a Web interface. Roles across all applications can be aggregated and flexibly assigned to individuals, and permissions for individuals can be globally understood and revoked when needed. See <http://middleware.internet2.edu/signet/>.

Single sign-on: See “reduced/single sign-on.”

Smart card: A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual and/or other information such as digital cash. A smart card holds its own data and applications and does its own processing.

SSL (secure sockets layer): A protocol, originally developed by Netscape, that creates a secure connection between a client (typically a Web browser) and a server through the use of either 40-bit or 128-bit public key encryption. Web pages protected with SSL usually use the “https” prefix.

Two-factor authentication: See “multifactor authentication.”

User-centric identity management: An approach to identity management stressing the user’s ownership of his or her identity information. The approach seeks to distribute and standardize the process of identity exchange, to allow users more granular control over the information they reveal, and to give them more say over how that information is used.
Identity Management

-X.500: An ISO and ITU standard that defines how global directories should be structured. X.500 directories are hierarchical, with different levels for each category of information, such as country, state, and city.

XRI (eXtensible Resource Identifier): An OASIS standard that defines an IETF/W3C Uniform Resource Identifier–compatible scheme and resolution protocol for abstract identifiers used to identify and share resources across domains and applications. XRIs can be used to identify persons, companies, network resources, and any other kind of object, providing an identifier that can cross systems and means of access. See <http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xri>.

References


Appendix D

References


©2006 EDUCAUSE. Reproduction by permission only.


bookstore/catalog/k023.htm
education: Campus commodity and competitive differentiator (Research Study, Vol. 2). Boulder, CO: EDUCAUSE 
Center for Applied Research.
dir-roadmap_200510.pdf