

# International Study of Identity Management and IT Security in Higher Education

## Survey Questionnaire July 2007

*Identity management* refers to the business processes and infrastructure required to support the use of digital identities. It is an issue attracting much attention in the higher education information technology (IT) community. Identity management is not the same as, but is related to, *IT security*, another top concern of IT leaders in higher education. This survey is part of a study sponsored by the Council of Australian University Directors of Information Technology (CAUDIT) in Australasia, by the European University Information Systems (EUNIS) in Europe, and by the EDUCAUSE Center for Applied Research (ECAR) in North America. Data from this study will form the basis of a report designed to help institutions position themselves in these evolving areas.

The survey focuses on the key functions of establishing identity, user authentication, and authorization, as well as supporting infrastructures such as enterprise directory, reduced/single sign-on, and federated identity.

Our testing suggests that this survey will require one to two hours to complete. If you wish to print a copy of the survey before completing it online, a .pdf version is available from the survey header or at <http://www.educause.edu/ir/library/pdf/SI/esi07h.pdf>

This survey need not be completed at one time. You may save your responses and return to the survey later. If you wish to exit before submitting your final answers, set a Favorite or Bookmark for the survey, and then click the SAVE button. If cookies are enabled, when you return to the survey you will be taken to the place you left off. You may complete or revise your answers until you click the FINISH button.

**Please complete this survey by Friday, July 27, 2007.** As thanks for your time and valuable input, each participant is entitled to receive a copy of the summary report of this study. In addition, European participants will be invited to contribute to the findings and to discuss results in The Netherlands in November. In October, participants at the EDUCAUSE Annual Conference in Seattle will also have a chance to discuss early findings. A meeting in Australia will be organized for early 2008 for the discussion and interpretation of results, and CAUDIT participants will have access to two complimentary copies of ECAR studies.

We appreciate your time and participation. If you have any questions or concerns, please e-mail [ecar@educause.edu](mailto:ecar@educause.edu)

Click the Next button to begin the survey. Once again, thank you for your input.

©2007 EDUCAUSE. Reproduction by permission only.

EDUCAUSE CENTER FOR APPLIED RESEARCH

All data and information collected by the EDUCAUSE Center for Applied Research are used strictly for the purposes of research and analysis for the benefit of ECAR subscribers and EDUCAUSE members. EDUCAUSE does not make personally or institutionally identifiable information or data available to its members, sponsors, contractors, or others.

## Section 1: About You, Your Staff, and Your Institution

**1.1 What is the name of your institution? Required.** \_\_\_\_\_

**1.2 What is your name? Required.** \_\_\_\_\_

**1.3 What is your primary role at your institution?**

- Senior-most IT leader at this institution; i.e., CIO, director, or equivalent
- Senior non-IT academic official at this institution
- Senior non-IT business official at this institution
- Senior non-IT other official at this institution
- Chief/head, academic computing area
- Chief/head, administrative computing area
- Chief/head, networking area
- Chief/head, IT security
- Other IT role
- Legal affairs
- Auditor/inspector
- Other non-IT role

**1.4 Is the senior-most IT official at your institution a member of the executive/top leadership body of the institution?**

- No
- Yes
- Don't know

**1.5 What is the closest job title of the person with day-to-day responsibility for IT security at your institution?**

- CIO, director of IT, department head, or equivalent
- Chief/head, academic computing area
- Chief/head, administrative computing area
- Chief/head, networking area
- Chief/head, IT security
- Other IT role
- Chief of police, campus safety, or equivalent
- Chief/head of human resources
- Chief/head of audit
- Other non-IT role

**1.6 Has your institution formally designated an individual as its information security officer, or ISO? Required.**

- No. Go to 1.10.
- Yes. Go to 1.7.
- Don't know. Go to 1.10.

**1.7 Does the information security officer focus on IT security full time?**

- No  
 Yes  
 Don't know

**1.8 Does the information security officer have a recognized IT security certification?**

- No  
 Yes  
 Don't know

**1.9 When did your institution first designate this information security officer position?**

- |                               |                               |                                      |
|-------------------------------|-------------------------------|--------------------------------------|
| <input type="checkbox"/> 2007 | <input type="checkbox"/> 2002 | <input type="checkbox"/> 1997        |
| <input type="checkbox"/> 2006 | <input type="checkbox"/> 2001 | <input type="checkbox"/> 1996        |
| <input type="checkbox"/> 2005 | <input type="checkbox"/> 2000 | <input type="checkbox"/> 1995        |
| <input type="checkbox"/> 2004 | <input type="checkbox"/> 1999 | <input type="checkbox"/> 1994        |
| <input type="checkbox"/> 2003 | <input type="checkbox"/> 1998 | <input type="checkbox"/> Before 1994 |

**1.10 How many full time equivalent (FTE) central IT security staff members, including the person with lead responsibility, are employed by your institution?**

- |                                      |                            |                                       |
|--------------------------------------|----------------------------|---------------------------------------|
| <input type="checkbox"/> Less than 1 | <input type="checkbox"/> 5 | <input type="checkbox"/> 10           |
| <input type="checkbox"/> 1           | <input type="checkbox"/> 6 | <input type="checkbox"/> More than 10 |
| <input type="checkbox"/> 2           | <input type="checkbox"/> 7 | <input type="checkbox"/> Don't know   |
| <input type="checkbox"/> 3           | <input type="checkbox"/> 8 |                                       |
| <input type="checkbox"/> 4           | <input type="checkbox"/> 9 |                                       |

**1.11 How many of these people, including the person with lead responsibility, have some type of security certification?**

- |                            |                            |                                       |
|----------------------------|----------------------------|---------------------------------------|
| <input type="checkbox"/> 0 | <input type="checkbox"/> 5 | <input type="checkbox"/> 10           |
| <input type="checkbox"/> 1 | <input type="checkbox"/> 6 | <input type="checkbox"/> More than 10 |
| <input type="checkbox"/> 2 | <input type="checkbox"/> 7 | <input type="checkbox"/> Don't know   |
| <input type="checkbox"/> 3 | <input type="checkbox"/> 8 |                                       |
| <input type="checkbox"/> 4 | <input type="checkbox"/> 9 |                                       |

**1.12 At my institution, IT is:**

- Highly centralized  
 Centralized  
 Balanced  
 Decentralized  
 Highly decentralized

**1.13 What best describes the central IT staffing structure for central IT security?**

- One central IT security organization  
 Spread across multiple central IT organizations  
 Other  
 Don't know

**1.14 Within the next two years, central IT security staffing at my institution will:**

- Increase  
 Decrease  
 Stay the same  
 Don't know

**1.15 How would you characterize the budget climate of your central IT organization in the past three years?**

- Decreasing budgets
- Flat (stable) budgets
- Increasing budgets

**1.16 How would you characterize the budget climate of your institution in the past three years?**

- Decreasing budgets
- Flat (stable) budgets
- Increasing budgets

**1.17 What BEST characterizes your institution in terms of adopting new technologies?**

- Innovator: first 2.5%
- Early adopter: next 13.5%
- Early majority: next 34%
- Late majority: next 34%
- Laggard: last 16%

**1.18 Which of the following BEST describes your institution's goals for IT?**

- Provide reliable IT infrastructure and services at the lowest possible cost
- Provide appropriate IT infrastructure and services to different users, based on their needs
- Provide IT infrastructure and services that further the institution's strategic goals
- Provide IT infrastructure and services to create institutional competitive advantage

**1.19 Has your institution implemented, or are you currently implementing, an enterprise data warehouse or data marts?**

- No
- A single institution-wide data warehouse
- Data mart(s) for specific types of information

**1.20 Has your institution implemented, or are you planning to implement, a student portal?**

- Already implemented
- Currently implementing
- Planning to implement
- Not planning to implement
- Don't know

**1.21 Which statement best describes your institution? *Required.***

- Research and teaching are the primary missions, but research is what really drives faculty and institutional success.
- Research and teaching are both primary missions, and they are equally important for faculty and institutional success.
- Teaching is the primary mission, but faculty research is rewarded.
- Teaching is the primary mission, and faculty research does not factor heavily in faculty and institutional success.

**1.22 How many full time equivalent students are there at your institution? *Required.***

- |                                           |                                        |                                           |
|-------------------------------------------|----------------------------------------|-------------------------------------------|
| <input type="checkbox"/> Fewer than 1,000 | <input type="checkbox"/> 4,001–8,000   | <input type="checkbox"/> More than 25,000 |
| <input type="checkbox"/> 1,000–2,000      | <input type="checkbox"/> 8,001–15,000  | <input type="checkbox"/> Don't know       |
| <input type="checkbox"/> 2,001–4,000      | <input type="checkbox"/> 15,001–25,000 |                                           |



**1.23 How is your institution financed?**

- Mostly public funds
- Mostly private funds
- Don't know

**1.24 Which statement best characterizes the current overall organizational climate at your institution?**

- Stable: change is slow or rare
- Dynamic: change is continuous, orderly, planned, and navigable
- Volatile: change is episodic, discontinuous, and requires care
- Turbulent: change is often driven by events, is unpredictable, and can disrupt ongoing operations

## Section 2: Institutional Perspectives on Identity Management

*Identity management* refers to the business processes and infrastructure required to support the use of digital identities. This includes establishing identity, user authentication and authorization, enterprise directory services, reduced/single sign-on, and identity federations.

### 2.1\_2.5 What is your opinion about the following statements?

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
2.1 My institution's senior management understands the benefits of investing in identity management.						
2.2 My institution's senior management understands the costs of identity management.						
2.3 My institution's senior management is willing to address the policy issues related to identity management.						
2.4 My institution is providing the resources needed for identity management.						
2.5 It is important that our identity management solutions are consistent with emerging technologies such as service oriented architecture (SOA)/Web services.						

### 2.6 How many significant security incidents related to user identification, authentication, or authorization has your institution experienced in the past two years?

- No incidents
- One incident
- More than one incident
- Don't know

### 2.7\_2.13 What is the status of the following activities?

	Completed	In progress	Planning to do	Not planning to do	Don't know
2.7 Documented business case for any area of identity management					
2.8 Documented plan for identity management					
2.9 Released an RFI or RFP for identity management					
2.10 Risk assessment of data access security and privacy practices					
2.11 Inventory of campus identifiers, such as those used by library, e-mail, and so forth					
2.12 Documented campus data custodians/owners					
2.13 Documented data definitions, reconciling differences between different data sources					



**2.14 If you have prepared an inventory of log-in credentials, such as those used for e-mail, the library, online classes, and so forth, how many person identifiers did you find?**

- Have not completed an inventory
- Fewer than 20
- 21–50
- 51–100
- 101–250
- 251–500
- More than 500

**2.15\_2.18 Have you implemented, or are you currently implementing, any of these online self-service functions? Check all that apply.**

- 2.15 Password resets
- 2.16 Updating certain personal information
- 2.17 Mailing lists and other subscription services
- 2.18 Setting privacy preferences for release of identity information

**2.19\_2.21 Do you have documented policies for the following?**

	No documented policies	Policies are in progress or partially completed	Policies are completed	Don't know
2.19 Policies for establishing identity, such as how user IDs are issued				
2.20 Policies for user authentication, such as guidelines, responsibilities for passwords, and so forth				
2.21 Policies for user authorization, such as which groups are allowed what access				

**2.22\_2.26 Does your institution keep any of the following metrics related to identity management? Check all that apply.**

- 2.22 Number of user accounts added, changed, or deleted
- 2.23 Help desk statistics on user access problems, such as password resets
- 2.24 Average time to create a new user ID and enable authorized services
- 2.25 Average time from user termination to disablement of all of that user's IDs
- 2.26 Number of temporary affiliates with enabled accounts but expired contracts

**2.27\_2.38 What is motivating your institution to pursue identity management? Select up to three.**

- 2.27 No motivators at this time
- 2.28 Regulatory compliance
- 2.29 Security/privacy best practices
- 2.30 Enhanced user services and satisfaction
- 2.31 Cost reduction/increased efficiencies
- 2.32 Strategic value/opportunities
- 2.33 Improvements in our technical environment
- 2.34 Strategy of early adoption/experimentation
- 2.35 Keeping current with generally accepted IT directions
- 2.36 Position the institution for implementation of federated identity
- 2.37 Reduce vendor dependencies
- 2.38 Other

**2.39\_2.51 What are the challenges to your institution in pursuing identity management?**

**Select up to three.**

- 2.39 No challenges at this time
- 2.40 Lack of acceptable return on investment
- 2.41 Adequate funding not available
- 2.42 Higher IT priorities
- 2.43 Lack of IT staff expertise
- 2.44 Lack of institutional senior management's support
- 2.45 Technical solutions too immature
- 2.46 Problems with vendor software and support
- 2.47 Problems with our institution's technologies/infrastructure
- 2.48 Data integrity problems, such as consistency, accuracy, and so forth
- 2.49 Difficulty developing campus policies and procedures
- 2.50 Lack of ownership of identity management by a central group
- 2.51 Other

**2.52 Which BEST describes your institution's current thinking about identity management solutions?**

- We probably will not use vendor solutions but will build solutions using in-house-developed or open source software.
- We will address our short-term needs with best-of-breed vendor point solutions and integrate these various products in-house.
- We will first identify our long-term business and architecture strategy and then decide on a solution or set of solutions for the institution.
- We will probably buy the vendor "suite" solution that best aligns with our network, infrastructure, and hardware vendors.
- We will probably buy the vendor "suite" solution that best aligns with our administrative applications and ERP vendors.
- Other
- Don't know

### Section 3: The Benefits of Identity Management

This section presents 14 benefits related to identity management for your evaluation.

**3.1\_3.2 Capability to immediately enable all authorized services for a new user.**

	Very low	Low	Medium	High	Very high	Don't know
3.1 What is the importance to your institution?						
3.2 Please rate your institution's current capability.						

**3.3\_3.4 Capability to immediately change authorized services for a user who changes roles.**

	Very low	Low	Medium	High	Very high	Don't know
3.3 What is the importance to your institution?						
3.4 Please rate your institution's current capability.						

**3.5\_3.6 Capability to immediately disable all services and user IDs when a user is no longer affiliated with the institution.**

	Very low	Low	Medium	High	Very high	Don't know
3.5 What is the importance to your institution?						
3.6 Please rate your institution's current capability.						

**3.7\_3.8 Capability to give visitors/guests only the specific access they require and disable that access at the correct time.**

	Very low	Low	Medium	High	Very high	Don't know
3.7 What is the importance to your institution?						
3.8 Please rate your institution's current capability.						

**3.9\_3.10 Prior to issuing credentials such as a user account, ID card, and so forth, we have the appropriate level of confidence, based on the type of constituent, that a user is who he or she claims to be.**

	Very low	Low	Medium	High	Very high	Don't know
3.9 What is the importance to your institution?						
3.10 Please rate your institution's current capability.						

**3.11\_3.12 Capability to directly track illegal or unauthorized network activity back to the person responsible.**

	Very low	Low	Medium	High	Very high	Don't know
3.11 What is the importance to your institution?						
3.12 Please rate your institution's current capability.						

**3.13\_3.14 Reduced or single sign-on: one electronic identity used to access most or all institutional services.**

	Very low	Low	Medium	High	Very high	Don't know
3.13 What is the importance to your institution?						
3.14 Please rate your institution's current capability.						

**3.15\_3.16 Capability to provide self-service functions such as password reset, profile management, and so forth.**

	Very low	Low	Medium	High	Very high	Don't know
3.15 What is the importance to your institution?						
3.16 Please rate your institution's current capability.						

**3.17\_3.18 Capability to decentralize user account management and authorization of services to deans of schools, managers of business units, and so forth.**

	Very low	Low	Medium	High	Very high	Don't know
3.17 What is the importance to your institution?						
3.18 Please rate your institution's current capability.						

**3.19\_3.20 Capability of strong authentication, such as strong passwords, two-factor authentication, and so forth.**

	Very low	Low	Medium	High	Very high	Don't know
3.19 What is the importance to your institution?						
3.20 Please rate your institution's current capability.						

**3.21\_3.22 Have—as an institutional asset—a single authoritative source of information for all persons affiliated with the institution.**

	Very low	Low	Medium	High	Very high	Don't know
3.21 What is the importance to your institution?						
3.22 Please rate your institution's current capability.						

**3.23\_3.24 User authentication and authorization processes that are scalable; for example, as enrollment grows.**

	Very low	Low	Medium	High	Very high	Don't know
3.23 What is the importance to your institution?						
3.24 Please rate your institution's current capability.						

**3.25\_3.26 Capability to allow our institutional users to access off-campus resources that require their own authentication and authorization; for example, licensed library content.**

	Very low	Low	Medium	High	Very high	Don't know
3.25 What is the importance to your institution?						
3.26 Please rate your institution's current capability.						



**3.27\_3.28 Capability to allow non-institutional users access to our institutional resources for which we require authentication and authorization, such as sharing our course materials with other institutions.**

	Very low	Low	Medium	High	Very high	Don't know
3.27 What is the importance to your institution?						
3.28 Please rate your institution's current capability.						

## Section 4: Campus Identity Management Projects

**4.1 Is your institution engaged in any efforts or projects related to identity management, such as enterprise directory, reduced/single sign-on, strong authentication, automated role- or privilege-based authorization, federated identity? *Required.***

- No. Go to Section 5.  
 Yes. Go to 4.2.  
 Don't know. Go to Section 5.

**4.2\_4.9 What is your institution's implementation strategy for identity management projects? *Check all that apply.***

- 4.2 Not yet determined  
 4.3 Part of infrastructure build-out  
 4.4 Stand-alone project  
 4.5 Bundled with an ERP implementation  
 4.6 Bundled with IT security implementation  
 4.7 Bundled with campus portal implementation  
 4.8 Bundled with another project implementation  
 4.9 Other

**4.10\_4.14 Who sponsors your campus identity management projects? *Check all that apply.***

- 4.10 The institution's IT organization  
 4.11 The institution's academic organization  
 4.12 The institution's business/administrative organization  
 4.13 The institution's police/public-safety organization  
 4.13 Other institutional organization  
 4.14 An outside organization

**4.15\_4.21 Is there an oversight committee for identity management projects, and what is its role? *Check all that apply.***

- 4.15 No oversight committee  
 4.16 Advisory  
 4.17 Sets policy  
 4.18 Sets priorities  
 4.19 Adjudicates conflicts  
 4.20 Authorizes funding  
 4.21 Other

**4.22 Are your current identity management projects organized into a formal initiative?**

- No  
 Yes  
 We are considering

**4.23 What is the primary currency in use where your institution operates?**

- |                                              |                                                 |                                               |
|----------------------------------------------|-------------------------------------------------|-----------------------------------------------|
| <input type="checkbox"/> Dollar: Australia   | <input type="checkbox"/> Koruna: Czech Republic | <input type="checkbox"/> Krone: Norway        |
| <input type="checkbox"/> Dollar: New Zealand | <input type="checkbox"/> Koruna: Slovakia       | <input type="checkbox"/> Pound: Great Britain |
| <input type="checkbox"/> Euro                | <input type="checkbox"/> Krona: Sweden          | <input type="checkbox"/> Zlotys: Poland       |
| <input type="checkbox"/> Francs: Swiss       | <input type="checkbox"/> Krone: Denmark         | <input type="checkbox"/> Other                |
|                                              |                                                 | <input type="checkbox"/> Don't know           |

**4.24 If "Other" was selected in question 4.23, please describe.**\_\_\_\_\_

**4.25 Approximately how much do you think central IT will spend on implementation of identity management projects over the next three years? Please report using the currency in use where your institution operates, e.g. euros, pounds, AUD, NZD, SFr, and so forth.**

- 50,000 or less
- 50,001 to 100,000
- 100,001 to 500,000
- 500,001 to 1 million
- Between 1 million and 2 million
- Between 2 million and 5 million
- More than 5 million
- Don't know

**4.26\_4.32 How do you pay for your identity management projects? Check all that apply.**

- 4.26 Not yet determined
- 4.27 Annual central IT budget
- 4.28 Contributions from other central units
- 4.29 One time campus budget allocation
- 4.30 Bundled in other campus projects, such as ERP
- 4.31 Partnerships or grants
- 4.32 Other

**4.33 Approximately how many central IT full-time equivalent staff members are currently assigned to your identity management projects?**

- |                            |                             |                                       |
|----------------------------|-----------------------------|---------------------------------------|
| <input type="checkbox"/> 0 | <input type="checkbox"/> 10 | <input type="checkbox"/> 20           |
| <input type="checkbox"/> 1 | <input type="checkbox"/> 11 | <input type="checkbox"/> 21           |
| <input type="checkbox"/> 2 | <input type="checkbox"/> 12 | <input type="checkbox"/> 22           |
| <input type="checkbox"/> 3 | <input type="checkbox"/> 13 | <input type="checkbox"/> 23           |
| <input type="checkbox"/> 4 | <input type="checkbox"/> 14 | <input type="checkbox"/> 24           |
| <input type="checkbox"/> 5 | <input type="checkbox"/> 15 | <input type="checkbox"/> 25           |
| <input type="checkbox"/> 6 | <input type="checkbox"/> 16 | <input type="checkbox"/> More than 25 |
| <input type="checkbox"/> 7 | <input type="checkbox"/> 17 | <input type="checkbox"/> Don't know   |
| <input type="checkbox"/> 8 | <input type="checkbox"/> 18 |                                       |
| <input type="checkbox"/> 9 | <input type="checkbox"/> 19 |                                       |

**4.34 Have you used, or are you currently using, consultants or external services to help with developing a business case?**

- No
- Yes
- Don't know

**4.35 Have you used, or are you currently using, consultants or external services to help with change management?**

- No
- Yes
- Don't know

**4.36 Have you used, or are you currently using, consultants or external services to help with organization and/or process design?**

- No
- Yes
- Don't know

**4.37 Have you used, or are you currently using, consultants or external services to help with IT architecture/design?**

- No
- Yes
- Don't know

**4.38 Have you used, or are you currently using, consultants or external services to help with software development/implementation?**

- No
- Yes
- Don't know

**4.39 Have you used, or are you currently using, consultants or external services to help with policy development?**

- No
- Yes
- Don't know

**4.40 Have you used, or are you currently using, consultants or external services to help with education/training?**

- No
- Yes
- Don't know

**4.41 What is your opinion about the following statement: My institution is getting the value we expected from the money spent on identity management projects?**

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Don't know
- Not applicable

**4.42 What best describes your expectations about cost savings from your identity management projects?**

- We have not achieved identifiable cost savings and do not expect to.
- We have not achieved identifiable cost savings but expect to in the future.
- We have achieved identifiable cost savings but do not expect to achieve more.
- We have achieved identifiable cost savings and expect to achieve more in the future.
- Don't know.

**Section 5: Establishing Identity and User Authentication**

**5.1 For faculty and staff in sensitive roles, do you require stronger identity proofing than for those not in sensitive roles; for example, ensuring a person is who he or she claims to be prior to issuing a user account?**

- Yes
- Planning to do
- Not planning to do
- Don't know

**5.2 For different groups of on-campus visitors and guests, do you use different methods of identity proofing; for example, ensuring a person is who he or she claims to be prior to issuing a user account?**

- Yes
- Planning to do
- Not planning to do
- Don't know

**5.3\_5.9 What user-authentication methods does your institution use when providing access to network services?**

	Using	Planning to use	Not planning to use	Don't know
5.3 Conventional password/PIN				
5.4 Strong password				
5.5 Kerberos				
5.6 PKI				
5.7 Secure ID-style onetime password				
5.8 Other multifactor authentication methods				
5.9 Biometric identification				

**5.10\_5.12 To what extent have you implemented the following related to identity management?**

	Not at all	In some cases	In all cases	Don't know
5.10 Primary electronic identifiers assigned to individuals are "unique for all time"; that is, they are never reassigned.				
5.11 Significant events related to identity management, such as issuance or revocation of user IDs, are logged and retained securely for six months.				
5.12 We prohibit, by policy or technology, network transmission of unencrypted passwords for the primary electronic identifier.				

## Section 6: Reduced or Single Sign-On

**6.1 To what extent is your institution considering or implementing reduced or single sign-on — a single electronic identity that can be entered once for all or most of your applications? *Required.***

- Not considering. *Go to 6.10\_6.24.*
- Currently evaluating. *Go to 6.2.*
- Planned, but won't start within the next 12 months. *Go to 6.2.*
- Will start within the next 12 months. *Go to 6.2.*
- Implementation is in progress. *Go to 6.2.*
- Partially operational. *Go to 6.2.*
- Fully operational. *Go to 6.2.*

**6.2 Are you implementing, or planning to implement, your reduced/single sign-on in conjunction with a campus portal?**

- No
- In place or implementing
- Planned for the future
- Don't know

**6.3\_ 6.7 What is, or will be, your approach to implementing reduced/single sign-on? *Check all that apply.***

- 6.3 Not yet determined
- 6.4 Use open source software, such as Kerberos, CAS, PubCookie
- 6.5 Use homegrown software developed at your, or another, institution
- 6.6 Use commercial vendor software, such as RSA, Aladdin
- 6.7 Other

**6.8 If applicable, please briefly describe the technologies you use, or are planning to use, for reduced/single sign-on technology.**\_\_\_\_\_

**6.9 Do you plan to use more commercial vendor software for reduced/single sign-on in the future?**

- No
- Yes
- Don't know

**6.10\_ 6.24 What are the primary reasons your institution is not considering reduced/single sign-on? *Select up to three.***

- 6.10 Capabilities of reduced/single sign-on not required at this time
- 6.11 Consider reduced/single sign-on a security risk
- 6.12 Lack of acceptable ROI
- 6.13 Adequate funding is not available
- 6.14 Higher IT priorities
- 6.15 Lack of IT staff expertise
- 6.16 Lack of institutional senior management's support
- 6.17 Technical solutions are too immature
- 6.18 Problems with vendor software and support
- 6.19 Problems with our institution's technologies/infrastructure
- 6.20 Data-integrity problems, such as consistency, accuracy, and so forth
- 6.21 Difficulty developing campus policies and procedures
- 6.22 Lack of ownership of identity management by a central group
- 6.23 Other



**6.24 Please describe “Other.”** \_\_\_\_\_

**6.25 Do you think you will consider reduced/single sign-on at some point in the future?**

- No
- In the next 12 months
- Between one and two years from now
- Between two and three years from now
- More than three years from now
- Don't know

## Section 7: The Enterprise Directory

**7.1 To what extent is your institution considering or implementing an enterprise directory? By enterprise directory, we mean an institutional directory service that has the capability to include all persons affiliated with the institution and to be used by multiple applications. Required.**

- Not considering. *Go to 7.38.*
- Currently evaluating. *Go to 7.2.*
- Planned, but won't start within the next 12 months. *Go to 7.2.*
- Plan to start within the next 12 months. *Go to 7.2.*
- Implementation is in progress. *Go to 7.2.*
- Partially operational. *Go to 7.2.*
- Fully operational. *Go to 7.2.*

**7.2\_7.10 What is, or will be, your approach to your enterprise directory? Check all that apply.**

- 7.2 Not yet determined
- 7.3 Implemented as a stand-alone system using open source software, such as OpenLDAP
- 7.4 Implemented as a stand-alone system using homegrown software developed at your, or another, institution
- 7.5 Implemented as a stand-alone system using commercial vendor software, such as MS Active Directory, Sun JES, Novell e-directory
- 7.6 Implemented as part of vendor-supplied application software, such as an ERP
- 7.7 Implemented as part of an institutional legacy application
- 7.8 Implemented as part of a network operating system
- 7.9 Integrates multiple directories to act as a single directory
- 7.10 Other

**7.11 If applicable, please briefly describe the technologies you use, or are planning to use, for enterprise directory.**\_\_\_\_\_

**7.12\_7.16 Do you plan to change your approach to enterprise directory in any of the following ways in the future? Check all that apply.**

- 7.12 Migrate from an enterprise directory implemented as part of another application to a stand-alone enterprise directory system
- 7.13 Use more commercial vendor software
- 7.14 Use more standards-based software
- 7.15 Use more open source software
- 7.16 Replace/reduce multiple subdirectories with a single directory

**7.17\_7.24 Which of these technologies are you using, or planning to use, for your enterprise directory? Check all that apply.**

- 7.17 LDAP
- 7.18 Microsoft Active Directory
- 7.19 Novell Directory Services, or NDS
- 7.20 X.500
- 7.21 SQL
- 7.22 DSML
- 7.23 XML
- 7.24 Other

**7.25\_7.32 Are you using your enterprise directory to facilitate any of the following functions?**

	Using	Planning to use	Not planning to use	Don't know
7.25 User authentication				
7.26 User authorization				
7.27 Store affiliation and group information				
7.28 Store privileges and permissions for access to systems and resources				
7.29 Track, log, and report on user activities				
7.30 Produce campus reports, such as whitepages				
7.31 Workflow: updating user data based on defined business triggers				
7.32 Enable functionality of ID cards, such as physical access based on job function				

**7.33 Has your enterprise directory development been influenced by the eduPerson (or country-specific derivatives such as UKeduPerson or auEduPerson) object classes?**

- No  
 Yes  
 Don't know

**7.34\_7.36 Which of the following campus applications use the enterprise directory? Check all that apply.**

- 7.34 Centrally controlled academic systems, such as library, course management  
 7.36 Centrally controlled administrative systems, such as finance, human resources  
 7.36 Locally controlled or devolved information systems

**7.37 Our goal is to have all or most of our central IT applications use the enterprise directory.**

- Strongly disagree  
 Disagree  
 Neutral  
 Agree  
 Strongly agree  
 Don't know

**7.38 Do you think you will consider implementing an enterprise directory at some point in the future?**

- No  
 In the next 12 months  
 Between one and two years from now  
 Between two and three years from now  
 More than three years from now  
 Don't know

**Section 8: Automated Role- and Privilege-Based Authorization**

**8.1 To what extent is your institution considering or implementing automated role- and privilege-based authorization; that is, giving access to electronic resources using privileges or permissions derived automatically from affiliations and groups? *Required.***

- Not considering. *Go to 8.13.*
- Currently evaluating. *Go to 8.2.*
- Planned, but won't start within the next 12 months. *Go to 8.2.*
- Plan to start within the next 12 months. *Go to 8.2.*
- Implementation is in progress. *Go to 8.2.*
- Partially operational. *Go to 8.2.*
- Fully operational. *Go to 8.2.*

**8.2\_8.8 What is, or will be, your approach to automated role- and privilege-based authorization? *Check all that apply.***

- 8.2 Not yet determined
- 8.3 Stand-alone system using open source software, such as Signet, Grouper
- 8.4 Stand-alone system using homegrown software developed at your, or another, institution
- 8.5 Stand-alone solution using commercial vendor software
- 8.6 Implemented as part of vendor-supplied application software, such as an ERP
- 8.7 Implemented as part of one or more institutional legacy applications
- 8.8 Other

**8.9 If applicable, please briefly describe the technologies you use or are planning to use for automated role- and privilege-based authorization.**\_\_\_\_\_

**8.10 Do you plan to use more commercial vendor software for automated role- and privilege- based authorization in the future?**

- No
- Yes
- Don't know

**8.11\_8.12 What is your opinion about each of the following statements?**

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
8.11 Our institution is committed to revising current business policies before they are entered into an automated role- or privilege-based authorization system.						
8.12 Our goal is to have all or most of our central IT applications use the automated role- and privilege-based authorization system.						

**8.13 Do you think you will consider implementing role- or privilege-based authorization at some point in the future?**

- No
- In the next 12 months
- Between one and two years from now
- Between two and three years from now
- More than three years from now
- Don't know



## Section 9: Federated Identity

**9.1 When do you think your institution will need to participate in a federated identity solution requiring automated management of identity information between your campus and other institutions and organizations to facilitate collaborative or business initiatives?**

- We do not envision a need
- We have a need now
- In the next 12 months
- Between one and two years from now
- Between two and three years from now
- More than three years from now
- Don't know

**9.2 Are you a member of an identity federation?**

- No
- Yes
- Planned for the future
- Don't know

**9.3 What are your plans for implementing Shibboleth or another federating technology? *Required.***

- Not considering. *Go to 9.5.*
- Currently evaluating. *Go to 9.4.*
- Planned, but won't start within the next 12 months. *Go to 9.4.*
- Plan to start within the next 12 months. *Go to 9.4.*
- Implementation is in progress. *Go to 9.4.*
- Partially operational. *Go to 9.4.*
- Fully operational. *Go to 9.4.*

**9.4 What applications motivated you or are motivating you to implement federating technologies?** \_\_\_\_\_

---

**9.5 Do you think you will consider implementing Shibboleth or another federating technology at some point in the future?**

- No
- In the next 12 months
- Between one and two years from now
- Between two and three years from now
- More than three years from now
- Don't know

**Section 10: IT Security Policy**

**10.1\_10.15 My institution has implemented IT security policies or procedures that cover the following policy areas:**

	No	Yes	Don't Know
10.1 Individual employee responsibilities for information security practices			
10.2 Acceptable use of computers, e-mail, Internet, and intranet			
10.3 Protection of organizational assets			
10.4 Managing privacy issues, including breaches of personal information			
10.5 Data classification, retention, and destruction			
10.6 Sharing, storing, and transmitting of institutional data (e.g., ISPs, external networks, contractors' systems)			
10.7 Vulnerability management, such as patch management, antivirus software			
10.8 Incident reporting and response			
10.9 Security compliance monitoring and enforcement			
10.10 Physical security			
10.11 Personnel clearances or background checks			
10.12 Notification of security events to affected parties, such as individuals, law enforcement, campus organizations			
10.13 Investigation and correction of the causes of security failures			
10.14 Data backups and secure off-site storage			
10.15 Secure disposal of data, media, or printed material that contains sensitive information			

**10.16\_10.17 At my institution:**

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
10.16 IT security policies are consistently enforced.						
10.17 IT security policies are regularly updated.						

**Section 11: Current IT Security Environment**

**11.1 Is IT security an integral part of either your institutional or IT strategic plan?**

- We do not have either an institutional or an IT strategic plan.
- IT security is not a part of our institutional or IT strategic plan.
- IT security is a part of our institutional or IT strategic plan.
- Don't know

**11.2 At what stage is your institution's IT security plan?**

- Comprehensive plan in place
- Partial plan in place, or some units have plan
- Neither a comprehensive nor partial plan in place
- Don't know

**11.3\_11.16 Describe your institution's current IT security approaches.**

	Already Implemented	Implementation in Progress	Will implement within 12 months	Not planning to implement within 12 months	Don't know
11.3 Network firewalls—perimeter					
11.4 Network firewalls—interior					
11.5 Application layer firewalls, such as Web server firewall					
11.6 Electronic signature					
11.7 Encryption—transmission					
11.8 Encryption—data storage					
11.9 Centralized data backup system					
11.10 Virtual private network, or VPN, for remote access					
11.11 Security standards for application or system development					
11.12 Intrusion detection					
11.13 Intrusion prevention					
11.14 Active filtering					
11.15 Security event management, such as centralization of logging, collection, and monitoring of various IT events					
11.16 Digital certificates					

**11.17\_11.28 What wireless security protections has your institution implemented?**

	Already Implemented	Implementation in progress	Will implement within 12 months	Not planning to implement within 12 months	Not planning to implement	Don't know
11.17 40-bit Wired Equivalent Privacy (WEP)						
11.18 128-bit Wired Equivalent Privacy (WEP)						
11.19 Extensible Authentication Protocol (EAP)						
11.20 Internet Protocol Virtual Private Network (IP VPN)						
11.21 Firewall						
11.22 Kerberos						
11.23 Remote authentication dial-in user service (RADIUS)						
11.24 Advanced Encryption Standard (AES)						
11.25 Wireless-vendor-supplied proprietary solution						
11.26 Registration of MAC						
11.27 EDUROAM						
11.28 Other						

**Section 12: IT Security Awareness and Training**

**12.1\_12.4 Please give us your opinion about the following statements:**

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Don't know
12.1 IT security is one of the top-three IT issues confronting my institution today.						
12.2 IT security practices are woven into the fabric of my institution's business operations.						
12.3 IT security is now a part of our institutional employee culture.						
12.4 My institution communicates IT security awareness issues to its teaching staff, students, and staff regularly.						

**12.5\_12.7 What type of formal IT security awareness programs does your institution have?**

	Mandatory	Voluntary	No awareness program
12.5 For students			
12.6 For teaching staff			
12.7 For staff			

**12.8\_12.10 My institution's IT security awareness programs have been effective for our:**

	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Don't know
12.8 Students						
12.9 Teaching staff						
12.10 Staff						

**12.11 How often does the central IT organization make a report to senior management of the institution on IT security issues?**

- Never
- Seldom
- Occasionally
- Often
- Very often
- Don't know

**Section 13: Enterprise Processes**

**13.1 Do you require that all new enterprise systems and applications be tested for IT security?**

- No
- Yes
- Don't know

**13.2 How often does your institution scan for vulnerabilities?**

- Continuously
- Daily
- Weekly
- Monthly
- Quarterly
- Annually
- Other regular schedule
- Not regularly
- Don't scan

**13.3\_13.9 To reduce IT security vulnerability at your institution, what is the implementation status of each of the following?**

	Already implemented	Implementation in progress	Will implement within 12 months	Not planning to implement within 12 months	Not planning to implement	Don't Know
13.3 Limiting the types of protocols allowed through the firewall/router						
13.4 Limiting the URLs allowed through the firewall						
13.5 Restricting and eliminating access to servers and applications						
13.6 Timing-out access to specific applications after an idle period						
13.7 Installing a software inventory system to watch for malicious software or program changes						
13.8 Installing closed desktop systems that don't allow user configuration changes						
13.9 Isolating or quarantining computers that do not meet minimum security requirements						

**13.10 How often are passwords for key enterprise systems, such as HR, student, and financial, required to be changed?**

- Single use
- Every 30 days
- Every 60 days
- 60–180 days
- More than 180 days
- It varies
- No requirement
- Don't know



## Section 14: Incident Handling

An incident is any action/event involving information technology resources that has the potential to destabilize, violate, or damage the resources, services, policies, or data of the community or of individual members of the community.

### 14.1 Do you have a formal IT security incident-handling process? *Required.*

No. Go to 14.10\_14.20.

Yes. Go to 14.2\_14.9.

Don't know. Go to 14.10\_14.20.

### 14.2\_14.9 Does the incident-handling process include the following offices?

	No	Yes	Don't Know
14.2 Chief executive officer, such as the rector, vice chancellor, president			
14.2 Student affairs office			
14.3 Information technology office			
14.4 Business office			
14.5 Office of police/public safety			
14.6 Human resources office			
14.7 Legal counsel			
14.8 Communications/public relations			
14.9 Student judicial affairs/dean of students			

### 14.10\_14.21 What are the top-three computer security concerns for your institution? *Select up to three.*

14.10 Computer virus, worm, or Trojan horse

14.11 Denial of service

14.12 Electronic vandalism or sabotage

14.13 Embezzlement

14.14 Fraud

14.15 Theft of intellectual property, including copyrights, patents, trade secrets, trademarks

14.16 Unlicensed use, copying, or piracy of digital products such as software, music, motion pictures, and so forth

14.17 Theft of personal financial information

14.18 Other computer security incidents, such as hacking, spoofing, sniffing, pinging, scanning, spyware, and so forth

14.19 Misuse of computers, Internet, e-mail, or equivalents by employees

14.20 Breaches resulting from information obtained from stolen laptops

14.21 Other

### 14.22 In the past 12 months, was the overall number of security incidents more, less, or about the same as for the previous 12 months, regardless of whether damage or losses were sustained as a result?

More in the past 12 months

Less in the past 12 months

About the same

Don't know

**14.23\_14.31 Has your institution experienced a security incident or incidents in the past 12 months that had any of the following consequences?**

	No	Yes	Don't Know
14.23 Network unavailable			
14.24 Business application, including e-mail, unavailable			
14.25 Financial losses			
14.26 Information confidentiality compromised			
14.27 Damage to hardware			
14.28 Damage to software			
14.29 Damage to data			
14.30 Identity theft			
14.31 Negative publicity			

**Section 15: Risk Assessment**

**15.1 Has your institution undertaken a formal risk assessment in the past two years to determine the value of your IT assets and risk to those assets?**

- No risk assessments done
- For some institutional data and asset types
- For all institutional data and asset types
- Don't know

**15.2 Does your institution perform formal IT security audits? *Required.***

- Not performed
- On an irregular basis
- On a regular basis
- Don't know

**15.3 - 15.8 Which of the following have conducted IT security audits?**

	No	Yes	Don't know
15.3 IT staff			
15.4 IT security officer			
15.5 Internal auditor			
15.6 External auditor			
15.7 Vendor			
15.8 External consultant			

**15.9 Does the institution provide departments/units with a framework for performing IT security risk assessments?**

- No
- Yes
- Don't know

**Section 16: Funding for IT Security**

**16.1 What percent of the central IT budget is dedicated to IT security?**

- Less than 1%
- 1–5%
- 6–10%
- 11–15%
- 16–20%
- Over 20%
- Don't know

**16.2\_16.5 How do you expect the following categories of central IT security expenditures to change over the next 12 months?**

	Decrease more than 15%	Decrease 15%	Decrease 10%	Decrease 5%	0 %	Increase 5%	Increase 10%	Increase 15%	Increase more than 15%
16.2 Security staffing									
16.3 Security products									
16.4 Security services									
16.5 Security education/training									

**16.6 My institution has provided the needed resources to address the institution's IT security issues.**

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Don't know

**16.7 What is the primary method your institution uses to justify central IT security expenditures?**

- In reaction to major incident
- By risk assessment
- As a strategic investment in security
- As incident prevention
- To meet government mandates
- None
- Don't know

**Section 17: Outcome and Future Directions**

**17.1\_17.6 Please give your opinion about the following statements.**

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Not applicable	Don't know
17.1 The IT security program at my institution is successful.							
17.2 My institution today has gone beyond the government's recommendations for IT security.							
17.3 The centrally controlled data, networks, and applications are secure.							
17.4 The locally controlled or devolved data, networks, and applications are secure.							
17.5 We have developed metrics to determine the effectiveness of our IT security activities.							
17.6 I feel my institution is more secure today than it was two years ago							

**17.7\_17.17 What are the major barriers to IT security at your institution? Select up to 3.**

- 17.7 Technology issues
- 17.8 Lack of resources
- 17.9 Lack of awareness
- 17.10 Absence of policies
- 17.11 Lack of enforcement of policies
- 17.12 Lack of senior management support
- 17.13 Academic culture that values openness and autonomy
- 17.14 Culture of decentralization at my institution
- 17.15 Privacy of the individual
- 17.16 Increased sophistication of threats
- 17.17 Other

**17.18\_17.23 Please give us your opinion about the following statements about your institution:**

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
17.18 Business requirements take precedence over IT security when there is a conflict.						
17.19 My institution's IT security architecture and implementation sacrifice some level of protection to ensure ease of use.						
17.20 IT security inhibits academic freedom.						
17.21 IT security compromises personal privacy.						
17.22 IT security unnecessarily limits user access to information.						
17.23 Individual behaviors have become more sensitive to security and privacy in the past two years.						

## Section 18: Conclusion

**18.1 May we contact you by phone or e-mail to obtain further insights or clarifications on your responses?**

- No  
 Yes

**18.2 If yes, what is your e-mail address?** \_\_\_\_\_

**18.3 Do you wish to receive a copy of the key findings from this study?**

- No  
 Yes

**18.4 If you have any other comments or insights about identity management or IT security, please share them with us.** \_\_\_\_\_

**18.5 If your institution has a Web page with information on identity management or IT security that you think would be of value for us to look at, please provide the URL(s).** \_\_\_\_\_

**18.6 We are committed to continually improving our surveys. All comments are welcome and will be considered.** \_\_\_\_\_

You have reached the end of the survey. Thank you! ***Please consider saving and printing your responses by clicking the “Review” button now.*** Once you have done so, ***click the “Finish” button to submit your survey.***

Full ECAR studies are available either through subscription or purchase at <http://www.educause.edu/ecar/>

If you have any questions or concerns, please e-mail [ecar@educause.edu](mailto:ecar@educause.edu)

– END SURVEY –