

# IT Readiness for Business Continuity Survey Questionnaire

May 2006

Thank you for participating in the study being conducted by the EDUCAUSE Center for Applied Research (ECAR). This survey is a critical part of the study and seeks to understand your institution's plans, infrastructure, experience, and capability in the area of IT support for business continuity. Our testing suggests that it will require 30–40 minutes to complete this survey. If you wish to print a copy of the survey before completing it online, a .pdf version is available from the header on each survey page and at

[http://www.educause.edu/ir/library/pdf/ecar\\_so/ers/si/esi06c.pdf](http://www.educause.edu/ir/library/pdf/ecar_so/ers/si/esi06c.pdf)

By “business continuity” we mean the institution's ability to maintain or restore its business and academic services when some circumstance threatens or disrupts normal operations. As used in this survey, business continuity encompasses disaster recovery—the activities that restore the institution to an acceptable condition after suffering a disaster—and also includes activities such as risk and impact assessment, prioritization of business processes, and restoring operations to a “new normal” after an event.

Note that our survey asks about business continuity activities at two levels:

- *institutional business continuity*, referring comprehensively to activities relating to overall business continuity across the whole institution; and
- *central IT support for business continuity*, referring to the activities specific to central IT's contributions to institutional business continuity, such as providing IT expertise to institutional business continuity planning activities, testing IT readiness for business continuity, and restoring IT services when a disruption takes place.

As you work on the survey, we encourage you to consult with other offices, such as your office of emergency preparedness, auditors, and managers of major business units.

Our survey software allows you to:

> **Print a blank survey.** To **print a blank copy of the survey** before completing it, click “Printable version of this survey” in the header. Once you have completed the online survey, you can **print your responses** by clicking the “Review” button at the end of the survey.

> **Save partially completed surveys.** The survey need not be completed at a single sitting. To save and return to a partially completed survey, set a Favorite or Bookmark for the survey and then click the SAVE button at the bottom of the screen. If cookies are enabled, when you return to the survey you will be taken to the place you left off.

> **Review, revise, print, and save your responses.** You may review and revise your answers before clicking the “Finish” button to submit your response. On the last screen of the survey, select the “Review” button to review, revise, print, and save your responses. Always print a copy of your completed survey and retain it for your records.

**Please complete this survey by Tuesday, May 23, 2006.** As thanks for your time and valuable input, each participant is entitled to receive a summary of key findings from the study.

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!

## Section 1: About You and Your Institution

1.1 Survey ID <Required> \_\_\_\_\_ <Survey ID Lookup>

1.2 Your name <Required> \_\_\_\_\_

### 1.3 Your position.

- |  |  |
|--|--|
| <input type="checkbox"/> President/chancellor  | <input type="checkbox"/> Auditor                         |
| <input type="checkbox"/> Vice president/provost/vice provost or equivalent (non-CIO) | <input type="checkbox"/> Other IT management             |
| <input type="checkbox"/> CIO (or equivalent)   | <input type="checkbox"/> Other administrative management |
| <input type="checkbox"/> Director of administrative computing                        | <input type="checkbox"/> Other academic management       |
| <input type="checkbox"/> Director of academic computing                              | <input type="checkbox"/> Other                           |

### 1.4 I am personally very involved in central IT support for business continuity at my institution.

- Strongly disagree  
 Disagree  
 Neutral  
 Agree  
 Strongly agree

### 1.5 What best describes the budget climate of your central IT organization in the past three years?

- Decreasing budgets                       Flat budgets                       Increasing budgets

### 1.6 What best characterizes your institution in terms of adopting new technologies?

- Early adopter                       Mainstream adopter                       Late adopter

### 1.7 What 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

### 1.8 Is the senior-most IT leader (e.g., CIO) at your institution a member of the president/chancellor's cabinet?

- No                       Yes

### 1.9 Does your institution have a hospital that serves the general public?

- No                       Yes

### 1.10 What percentage of your students live in campus residences?

- |  |   |
|--|---|
| <input type="checkbox"/> Do not have campus residences | <input type="checkbox"/> 51–75 percent  |
| <input type="checkbox"/> Less than 25 percent          | <input type="checkbox"/> 76–100 percent |
| <input type="checkbox"/> 25–50 percent                 | <input type="checkbox"/> Don't know     |

### 1.11 Is your institution part of a university system or community college district organization?

- No                       Yes

## Section 2: Institutional Perspectives on Business Continuity Planning

### 2.1\_2.3 At my institution:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
2.1 Awareness of the need for business continuity planning is high.						
2.2 Awareness of the need for business continuity planning is higher today than two years ago.						
2.3 Senior management places high priority on business continuity planning.						

### 2.4\_2.14 What are the primary drivers for business continuity planning at your institution?

**Select up to three.**

- 2.4 Threats specific to our geographic location
- 2.5 Hazards arising from our institution's operations (e.g., nuclear reactor, virus lab)
- 2.6 Institutional leadership mandate
- 2.7 Demand from constituents (e.g., faculty, students, etc.)
- 2.8 Audit requirements
- 2.9 Regulatory compliance
- 2.10 Keeping current with generally accepted business directions/best practices
- 2.11 Awareness of recent global natural disasters (e.g., hurricanes, tsunami)
- 2.12 Terrorism/homeland-security concerns
- 2.13 A recent incident at our institution causing or threatening disruption to operations
- 2.14 Other

### 2.15\_2.22 What are the primary barriers to business continuity planning at your institution? Select up to three.

- 2.15 Lack of adequate funding
- 2.16 Lack of acceptable ROI
- 2.17 Technology issues
- 2.18 Lack of institutional leadership's support
- 2.19 Business/academic units have not defined business continuity needs
- 2.20 Lack of staff expertise
- 2.21 Difficulty developing campus policies and procedures
- 2.22 Other

### 2.23 Has your institution designated at least one senior executive who is responsible for institutional business continuity planning activities? <Required>

- No <Go to 2.25>
- Yes
- Don't know <Go to 2.25>

### 2.24 The senior executive responsible for institutional business continuity planning activities is:

- President/chancellor
- Executive vice president/chancellor
- Chief academic officer/Provost
- Chief business officer
- Chief of campus security/police
- CIO (or equivalent)
- Academic dean
- Other

**2.25 Has your institution designated an emergency response team to manage the overall institutional response in the event of a disruption to normal operations? <Required>**

- No <Go to 2.27>
- Yes
- Don't know <Go to 2.27>

**2.26 Is central IT represented on this emergency response team?**

- No
- Yes
- Don't know

**2.27 Does your institution have an established office for institutional business continuity planning?**

- No
- Yes
- Don't know

**2.28 Has your institution undertaken a formal overall risk assessment to evaluate the events/threats—such as natural disasters, accidents, terrorism, etc.—that can cause interruptions to the institution's operations? <Required>**

- No risk assessment anticipated <Go to 2.29\_2.37; then to 2.63\_2.65>
- Planned for the future <Go to 2.38\_2.42; then to 2.63\_2.65>
- Work is in progress <Go to 2.38\_2.42; then to 2.43>
- Work is completed <Go to 2.43>

**2.29\_2.37 What are the primary reasons why your institution has not conducted a formal overall risk assessment at this time? Select up to three.**

- 2.29 Threats do not justify effort
- 2.30 Benefits do not justify investment
- 2.31 Prefer an ad hoc approach
- 2.32 Lack of adequate funding
- 2.33 Lack of institutional leadership's support
- 2.34 Business/academic units have not defined business continuity needs
- 2.35 Lack of staff expertise
- 2.36 Difficulty developing campus policies and procedures
- 2.37 Other

**2.38\_2.42 My institution's effort to complete an overall risk assessment:**

	No	Yes	Don't know
2.38 Has been assigned a completion date			
2.39 Has been assigned staff			
2.40 Has been allocated funds			
2.41 Has executive or management sponsor			
2.42 Has participation from functional business/academic units			

**2.43 Did your institution use or is it using a formal methodology to conduct its overall risk assessment?**

- No
- Yes
- Don't know

**2.44\_2.61 Which functional areas have actively participated in developing your institution's overall risk assessment?**

	No	Yes	Don't know	Not applicable
2.44 Academic affairs/provost				
2.45 Academic schools and departments				
2.46 Admissions				
2.47 Audit				
2.48 Business/administrative services				
2.49 Campus security/police				

2.50 Central IT				
2.51 Financial services				
2.52 Housing/residential life				
2.53 Human resources				
2.54 Legal counsel				
2.55 Library				
2.56 Office of emergency planning				
2.57 Public affairs				
2.58 Registrar's office				
2.59 Research administration				
2.60 Risk management				
2.61 Student affairs				

**2.62 Our institution's overall risk assessment is kept up to date.**

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

**2.63\_2.65 Does your institution have documented plans or processes that do the following?**

	No	Yes	Don't know
2.63 Identify the probability of disruptive events/threats			
2.64 Assess the potential impact of disruptive events/threats on business and academic processes			
2.65 Prioritize risks from disruptive events/threats			

**2.66 Does your institution have a formal, documented plan for overall institutional business continuity? <Required>**

- No plan anticipated <Go to 2.68>
- Planned for the future <Go to 2.68>
- Work is in progress
- Work is completed

**2.67 Does your institution have a formal process for updating its overall business continuity plan?**

- No
- Yes
- Don't know

**2.68 Does your institution provide departments/units with a framework for developing their own business continuity plans?**

- No
- Yes
- Don't know

**2.69\_2.70 If central IT systems and services were not operational at my institution:**

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
2.69 Business units could carry out essential operations.						
2.70 Academic units could carry out essential operations.						

### Section 3: IT Perspectives on Business Continuity Planning

**3.1\_3.4 At my institution, central IT is actively involved in business continuity planning conducted by:**

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know	Not applicable
3.1 Overall institutional business continuity planners							
3.2 Business units							
3.3 Academic units							
3.4 Local IT units							

**3.5\_3.8 At my institution, central IT planning to support business continuity is aligned with the business continuity goals of:**

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know	Not applicable
3.5 Overall institutional business continuity planners							
3.6 Business units							
3.7 Academic units							
3.8 Local IT units							

**3.9 Has your central IT unit conducted an IT risk assessment to evaluate the impact that disruptive events/threats would have on IT systems and assets? <Required>**

- No IT risk assessments done <Go to 3.11>
- For some IT systems and assets <Go to 3.10>
- For all IT systems and assets <Go to 3.10>
- Don't know <Go to 3.11>

**3.10 Our IT risk assessment is kept up to date.**

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

**3.11 Does your institution have a documented inventory of central IT systems and assets? <Required>**

- No inventory <Go to 3.13>
- For some central IT systems and assets <Go to 3.12>
- For all central IT systems and assets <Go to 3.12>
- Don't know <Go to 3.13>

**3.12 Our inventory of central IT systems and assets is kept up to date.**

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

**3.13 Does your institution have a documented inventory of local IT unit systems and assets (i.e., those not controlled by central IT)? <Required>**

- No inventory <Go to 3.15>

- For some local IT systems and assets <Go to 3.14>
- For all local IT systems and assets <Go to 3.14>
- Don't know <Go to 3.15>

**3.14 Our inventory of local IT unit systems and assets is kept up to date.**

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

**3.15 The individual responsible for day-to-day management of IT planning to support business continuity is:**

- CIO (or equivalent)
- Chief information security officer
- Full-time IT manager for business continuity support
- Director of administrative computing
- Director of academic computing
- Director of networking
- Other IT management
- Director of institutional emergency response planning
- Other administrative management
- Other academic management

**3.16 Does your central IT unit have a standing committee that is responsible for business continuity planning activities?**

- No
- Yes
- Don't know

**3.17\_3.29 Has your central IT unit documented procedures for the following, either as part of a formal plan or as a separate procedure?**

	No	Yes, in plan	Yes, as separate procedure	Don't know
3.17 Declaring an IT emergency when disruption falls outside normal operating/troubleshooting bounds				
3.18 Activating/escalating IT emergency response				
3.19 Notifying appropriate parties of emergency				
3.20 Performing damage assessments				
3.21 Prioritization of systems for purposes of recovery				
3.22 Recovery of IT operations				
3.23 Moving necessary activities/equipment to alternate sites				
3.24 Transportation/logistical support for staff at alternate sites				
3.25 Notifying constituents of system status				
3.26 Returning activities/equipment to primary locations				
3.27 De-escalation of IT emergency response				
3.28 Declaring resumption of normal operations				
3.29 Evaluation of post-recovery IT environment (establishing "new normal")				

**3.30\_3.46 Which functional areas actively participate in developing your central IT procedures for business continuity?**

	No	Yes	Don't know	Not applicable
3.30 Academic affairs/provost				
3.31 Academic schools and departments				
3.32 Admissions				
3.33 Audit				
3.34 Business/administrative services				
3.35 Campus security/police				
3.36 Financial services				
3.37 Housing/residential life				
3.38 Human resources				
3.39 Legal counsel				
3.40 Library				
3.41 Office of emergency planning				
3.42 Public affairs				
3.43 Registrar's office				
3.44 Research administration				
3.45 Risk management				
3.46 Student affairs				

**3.47\_3.48 How often does your institution carry out the following types of reviews of your central IT procedures to support business continuity?**

	Never	On a regular basis	On an ad hoc basis	Don't know
3.47 Comprehensive review				
3.48 Component-level review				

**3.49 Our IT procedures for supporting business continuity are kept up to date.**

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

**3.50 Which of the following best describes the status of a formal, documented central IT plan for business continuity and/or IT disaster recovery at your institution? <Required>**

- No plan anticipated <Go to 3.51\_3.59; then to 3.65>
- Planned for the future <Go to 3.60\_3.64>
- Work is in progress <Go to 3.60\_3.64>
- Work is completed <Go to 3.65>

**3.51\_3.59 What are the primary reasons why your institution does not anticipate formulating such a plan? Select up to three.**

- 3.51 Our people and processes are sufficient to meet needs
- 3.53 Threats do not justify investment
- 3.54 Lack of adequate funding
- 3.55 Lack of institutional leadership's support
- 3.56 Business/academic units have not defined business continuity needs
- 3.57 Lack of IT staff expertise
- 3.58 Difficulty developing campus policies and procedures
- 3.59 Other

**3.60\_3.64 My institution's effort to complete a documented central IT plan for business continuity and/or IT disaster recovery:**

	No	Yes	Don't know
3.60 Has been assigned a completion date			
3.61 Has been assigned staff			
3.62 Has been allocated funds			
3.63 Has executive or management sponsor			
3.64 Has participation from functional business/academic units			

**3.65 What best describes central IT's goals for restoration of IT services in the event of a disruption to normal operations?**

- Provide minimum acceptable restoration of IT services at the lowest possible cost
- Provide quick restoration of high priority IT services, then phase in lower-priority services
- Provide quick restoration of all IT services

**Section 4: Recovery Objectives**

**Definition:** A recovery time objective, or RTO, is the period of time within which the institution plans to restore a given system after suffering a disruption.

**4.1 Does your institution have a formal process for establishing recovery time objectives for central IT systems?**

- No  Yes  Don't know

**4.2\_4.17 Does your institution have documented recovery time objectives for the following central IT systems?**

	No RTO documented	0-4 hours	5-24 hours	1-2 days	3-6 days	7-14 days	More than 14 days	Don't know	Not applicable
4.2 Institutional Web site									
4.3 E-mail									
4.4 Campus network									
4.5 Campus connection to Internet									
4.6 Voice telephony									
4.7 Purchasing									
4.8 Central finance/accounting									
4.9 Payroll									
4.10 Benefits administration									
4.11 Recruiting									
4.12 Admissions									
4.13 Student billing and payment processing									
4.14 Financial aid									
4.15 Student records/registration									
4.16 Course management system									
4.17 Library management system									
4.18 Grants management									

**Definition:** A recovery point objective, or RPO, is the maximum acceptable interval between a backup and a potential interruption, during which data will be lost. When a system is recovered, the RPO defines how old the restored data may be relative to the time of the interruption.

**4.19 Does your institution have a formal process for establishing recovery point objectives for central IT systems?**

- No  Yes  Don't know





	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
6.14 Our tests are frequent enough.						
6.15 Our tests are challenging enough.						
6.16 We are able to get the right parties to participate in our tests.						
6.17 We formally assess the results of our tests.						
6.18 Results of tests are communicated to all appropriate parties.						
6.19 Results of tests are used to improve our business continuity plans and procedures.						

## Section 7: Business Continuity Infrastructure and Technologies

**Definition:** A hot site is a space with appropriate connectivity, environmental infrastructure, and equipment in place for systems recovery in the event of a disruption that makes the primary operations site unusable.

### 7.1 Does your institution have at least one hot site capable of assuming key IT operations?

<Required>

- Not planning to do <Go to 7.2\_7.10; then to 7.14>
- Planned for the future <Go to 7.14>
- In development <Go to 7.11>
- Operational <Go to 7.11>

### 7.2\_7.10 What are the primary reasons why your institution does not have a hot site?

Select up to three.

- 7.2 Do not believe a hot site is necessary
- 7.3 Do not believe benefit justifies expense
- 7.4 Lack of adequate funding
- 7.5 We are not far enough along in our business continuity planning
- 7.6 Lack of staff resources
- 7.7 Lack of staff expertise
- 7.8 Technical issues
- 7.9 Lack of institutional leadership's support
- 7.10 Other

### 7.11 Describe the geographic location of your primary hot site in relation to your institution's central IT operations.

- Same building
- Different building, same campus
- Off campus, less than 5 miles
- Off campus, 5–25 miles distant
- Off campus, 26–100 miles distant
- Off campus, more than 100 miles distant
- Don't know

### 7.12 Which best describes the status of your primary hot site?

- Institutionally owned/leased
- Owned/leased by other higher education institution
- Ownership/lease shared with other higher education institution
- Owned/leased by higher education system, district, or consortium
- Commercial site available by contract
- Owned/leased by public sector entity

- Other
- Don't know

**7.13 Does at least one other higher education institution use this hot site?**

- Yes
- No
- Don't know

**Definition: A cold site is a space with appropriate connectivity and environmental infrastructure to which equipment can be moved for systems recovery in the event of a disruption that makes the primary operations site unusable.**

**7.14 Does your institution have at least one cold site capable of being provisioned to assume key IT operations? <Required>**

- Not planning to do <Go to 7.15\_7.23; then to 7.27\_7.31>
- Planned for the future <Go to 7.27\_7.31>
- In development <Go to 7.24>
- Operational <Go to 7.24>

**7.15\_7.23 What are the primary reasons why your institution does not have a cold site? Select up to three.**

- 7.15 Do not believe a cold site is necessary
- 7.16 Do not believe benefit justifies expense
- 7.17 Lack of adequate funding
- 7.18 We are not far enough along in our business continuity planning
- 7.19 Lack of staff resources
- 7.20 Lack of staff expertise
- 7.21 Technical issues
- 7.22 Lack of institutional leadership's support
- 7.23 Other

**7.24 Describe the geographic location of your primary cold site in relation to your institution's central IT operations.**

- Same building
- Different building, same campus
- Off campus, less than 5 miles
- Off campus, 5–25 miles distant
- Off campus, 26–100 miles distant
- Off campus, more than 100 miles distant
- Don't know

**7.25 Which best describes the status of your primary cold site?**

- Institutionally owned/leased
- Owned/leased by other higher education institution
- Ownership/lease shared with other higher education institution
- Owned/leased by higher education system, district, or consortium
- Commercial site available by contract
- Owned/leased by public sector entity
- Other
- Don't know

**7.26 Does at least one other higher education institution use this cold site?**

- Yes
- No
- Don't know

**7.27\_7.31 Describe your institution’s current approaches to central IT data storage and recovery.**

	Not used	Used for some systems	Used for many systems	Used for all systems	Don't know
7.27 Backup to media that is stored on campus					
7.28 Backup to media that is stored off campus					
7.29 Batch electronic vaulting via network					
7.30 Continuous data mirroring to direct-access device via network					
7.31 High-availability redundant transaction systems with failover capability					

**7.32\_7.36 When restoring operations following a disruption, how does your institution currently plan to replace central IT hardware that is damaged or unavailable?**

	Not for any systems	For some systems	For many systems	For all systems	Don't know
7.32 Use redundant hardware reserved solely for this purpose					
7.33 Repurpose hardware from lower-priority systems (e.g., test environments)					
7.34 Acquire/lease new hardware via expedited shipping or Quickship process					
7.35 Acquire new hardware via normal purchasing process					
7.36 Commercial hot site					

**7.37\_7.47 Which of the following has your institution implemented or formally arranged to have available when needed?**

	Not planning to do	Planned for the future	Work is in progress	Work is completed	Don't know
7.37 Special emergency Web site					
7.38 Alternate host for institutional Web site					
7.39 Alternate host for e-mail					
7.40 Alternate ISP					
7.41 Alternate voice telephony provider					
7.42 Pagers					
7.43 Walkie-talkies					
7.44 VOIP telephony					
7.45 Satellite phones					
7.46 Automated phone/e-mail notification system					
7.47 Backup power for central IT site(s)					
7.48 Institutional emergency command center					

**Section 8: Incident Management**

**8.1 Does your institution have an IT emergency response team? <Required>**

- No <Go to 8.3\_8.6>
- Yes
- Don't know <Go to 8.3\_8.6>

**8.2 Who leads this team during an emergency?**

- No assigned leader
- CIO
- Other specific IT manager
- Assignment rotates
- Other
- Don't know

**8.3\_8.6 Does your institution have documented protocols in place for the following?**

	No	Yes	Don't know
8.3 Assigning powers to designated individuals to declare an IT emergency			
8.4 Notifying the IT response team of an emergency			
8.5 Notifying senior management of an emergency			
8.6 Providing backup communications channels for notification if standard channels are unavailable			

**8.7 Does your institution have a designated spokesperson to make public statements regarding an IT emergency?**

No  Yes  Don't know

**8.8 In an emergency, is central IT formally empowered to assume control over systems, facilities, or processes that it does not normally control?**

No  Yes  Don't know

*Definition: A mutual aid agreement is a reciprocal arrangement in which participating institutions or organizations that are unaffected or not seriously affected by a disruption render assistance to other participants that have been more seriously affected.*

**8.9 Does your institution participate in formal mutual aid agreements? <Required>**

No <Go to 8.15\_8.21>  
 Yes  
 Don't know <Go to 8.15\_8.21>

**8.10\_8.13 With which of the following do you participate in formal mutual aid agreements?**

	No	Yes	Don't know
8.10 Other higher education institution(s)			
8.11 Local government agencies			
8.12 State government agencies			
8.13 Other entities			

**8.14 Does your central IT unit have documented plans or procedures in place to provide IT support to other participants in your mutual aid agreements when needed?**

No  Yes  Don't know

**8.15\_8.21 Please give us your opinion on the following statements about your institution.**

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
8.15 We keep contact information for IT emergency response personnel up to date.						
8.16 We keep contact information for non-IT emergency response personnel up to date.						
8.17 We keep contact information for faculty and staff up to date.						
8.18 We keep contact information for students up to date.						
8.19 We keep contact information for student next-of-kin up to date.						
8.20 We are prepared to handle a surge of inbound phone calls during an emergency.						

8.21 We are prepared to send a large quantity of outbound notifications to institutional constituents during an emergency.						
--	--	--	--	--	--	--

**8.22\_8.25 Rate the impact that the following contingencies would have on your central IT unit's ability to support business continuity during a disruption at your institution.**

	Very little impact	Little impact	Moderate impact	Severe impact	Very severe impact	Don't know
8.22 Inability to gain access to primary IT facilities						
8.23 Inability of IT emergency response personnel to meet in person						
8.24 Inability to communicate with senior management						
8.25 Insufficient staff depth if key IT personnel were unavailable						

**Section 9: Incident Experience and Effects**

**9.1 Has your institution experienced any disruptions to normal business and academic operations in the past five years that caused central IT to implement formal or ad hoc emergency response procedures? <Required>**

- No <Go to 10.1>
- Yes
- Don't know <Go to 10.1>

**9.2 How many such disruptions have occurred in the past five years?**

- 1                       4                       7                       10
- 2                       5                       8                       More than 10
- 3                       6                       9                       Don't know

**9.3\_9.18 Describe the impact of the following types of events that triggered an emergency response by central IT in the last five years.**

Event	None	Impact on a few facilities/business processes	Impact on many facilities/business processes	Campus-wide impact	Campus- and region-wide impact	Don't know
9.3 Seismic — earthquake, tsunami						
9.4 Hurricane						
9.5 Tornado						
9.6 Flood						
9.7 Other severe weather						
9.8 Disease outbreak/pandemic						
9.9 Fire						
9.10 Electrical failure						
9.11 Hazardous materials spill						
9.12 Hardware failure						
9.13 Cooling/IT environmental failure						
9.14 Theft						
9.15 Cable cut						
9.16 Cyber attack						



9.44 Institutional emergency command center							
9.45 Alternate IT facilities							

**9.46\_9.47 The central IT response to this specific disruption:**

	No	Yes	Don't know
9.46 Met institutional business continuity objectives			
9.47 Met central IT business continuity support objectives			

**9.48\_9.49 Following this specific disruption, central IT:**

	No	Yes	Don't know
9.48 Assessed our response to the disruption			
9.49 Updated our documented business continuity plans and procedures as a result of the disruption			

**Section 10: Funding**

**10.1\_10.3 Please give us your opinion on the following statements.**

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
10.1 We have the necessary funding to deliver IT support for business continuity.						
10.2 We have the necessary staff resources to deliver IT support for business continuity.						
10.3 Senior management understands the costs of IT support for business continuity.						

**10.4 Approximately what percentage of the central IT budget is currently dedicated to supporting business continuity, including staff costs and goods and services?**

- 0%
- 1%
- 2%
- 3%
- 4%
- 5%
- 6%
- 7%
- 8%
- 9%
- 10%
- 11%
- 12%
- 13%
- 14%
- 15%
- More than 15%
- Don't know

**10.5\_10.8 How do you anticipate the following categories of central IT spending on business continuity will change over the next 12 months?**

	Decrease more than 15%	-15%	-10%	-5%	0%	+5%	+10%	+15%	Increase more than 15%
10.5 Staffing									
10.6 Products									
10.7 Services									
10.8 Education/training									

**10.9 What is the primary source of funding for IT upgrades and improvements related to business continuity?**

- Augmentation to annual IT budget
- Reallocation within annual IT budget
- Annual contributions to a reserve fund
- Capital budget allocation
- Legislative allocation
- Bond issue
- Grants
- Other
- Don't know

## Section 11: Outcomes

**11.1\_11.5 Please give us your opinion on the following statements.**

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
11.1 IT capacity to support business continuity at my institution is aligned with senior management expectations.						
11.2 My institution is prepared to restore centrally controlled systems in the event of a disruption.						
11.3 My institution is better prepared to restore centrally controlled systems in the event of a disruption than it was two years ago.						
11.4 My institution is prepared to restore locally controlled systems in the event of a disruption.						
11.5 My institution is better prepared to restore locally controlled systems in the event of a disruption than it was two years ago.						

**11.6 What level of performance has your institution achieved in its IT readiness to support business continuity?**

- We are at risk.
- We are adequate.
- We are leaders.
- We are exemplars.
- Don't know.

## Section 12: Conclusion

**12.1 May we contact you to obtain further insights or clarifications on your responses?**

<Required>

- No            <Go to 12.3>
- Yes

**12.2 What is your e-mail address?** \_\_\_\_\_

**12.3 If you have any other comments or insights about IT readiness for business continuity, please share them with us.**

\_\_\_\_\_

**12.4 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! Choose the “Review” button to review, revise, and print your answers (always print a copy of your completed survey and retain it for your records). Once this is done, submit the survey by clicking “Finish.”

Full ECAR studies are available either through subscription or purchase at the ECAR Web site, <http://www.educause.edu/ecar/> . If you have any questions or concerns, please e-mail [ecar@educause.edu](mailto:ecar@educause.edu) .

– END SURVEY –