ECAR

IT Governance, Risk, and Compliance Survey, 2014

Thank you for participating in this ECAR survey of IT governance, risk, and compliance (GRC). EDUCAUSE has made IT GRC a strategic initiative for 2014, and your participation will enable us to understand and characterize the current state of IT GRC, explore and disseminate best practices, and ultimately develop tools for benchmarking and measuring progress in the area of IT GRC.

Only EDUCAUSE researchers will have access to individually identifiable data collected in this survey. Aggregated results may be included in reports, publications, or other products of this research, but they will not contain any information that could be used to identify an individual or a particular institution.

This survey covers various questions in the areas of IT GRC. As such, we are asking primary representatives to identify the individuals at their institution who are best qualified to respond to the questions in each section. These may be CIOs, risk officers, compliance officers, security officers, institutional researchers, legal counsel, or other administrators or professionals, depending on the existence and structure of your institution's IT GRC programs. A PDF of the survey (http://net.educause.edu/ir/library/pdf/SI/ESI1402.pdf) may be sent to these individuals to have them complete identified questions and return to you. A single individual should complete the online version of the survey after collecting the responses.

After all responses have been collected, it should take approximately 20 minutes to complete the online survey.

Please complete this survey by February 21, 2014.

Your name: Required.*

____

Your e-mail address: Required.*

____

What is the job title of the primary person completing this survey?

____

Please note: This survey contains some "slider" questions that ask you to move the slider to the position that best represents your answer to the question. If you do not click on the slider at all, it will be recorded as a non-response. If you wish to submit a neutral response, you must click on the slider button in its original position. If you have been forwarded the PDF version of this survey to record your answers, it is suggested you mark the spot on the line where you think the slider should be moved.

Section A. IT Risk Management

IT risk management is defined as programs or processes that help an institution identify the risks that it faces with regard to its present or planned IT resources and systems and affirmatively address those risks in a way that satisfies its overall goals. Enterprise risk management (ERM) programs move beyond security and technology risks presented by IT resources and systems, holistically addressing all aspects of risk that may impact the institution, including strategic, financial, legal, operational, and reputational risks.

1. To what extent does your institution have an *enterprise risk management (ERM)* program in place?
( ) We have a formal ERM program in place. <<May see question 2b>>
( ) We have a formal ERM program planned, but it is not yet in place. <<Will not see question 2b>>
( ) Risk management at our institution is ad hoc/reactive/informal. <<Will not see question 2b>>
( ) We do not have any processes or procedures in place for risk management.
<<Will not see question 2b>>

2. To what extent does your institution have an *IT risk management* program in place?
( ) We have a formal IT risk management program in place. <<Go to 2b or 2c>>
( ) We have a formal IT risk management program planned, but it is not yet in place. <<Go to 2a>>
( ) IT risk management at our institution is ad hoc/reactive/informal. <<Go to 2a>>
( ) We do not have any processes or procedures in place for IT risk management. <<Go to 2a>>

2a. Describe how your institution currently addresses IT risk management issues as they arise.

<<Go to 3>>

2b. Is your IT risk management program part of your institution's ERM program?
( ) Yes
( ) No
( ) Don't know

2c. Who leads the IT risk management program?

( ) CIO or equivalent

( ) Deputy CIO or equivalent

( ) Chief information security officer (CISO) or equivalent

( ) Chief risk officer (CRO) or equivalent

( ) IT policy director

( ) Other IT director/manager

( ) Legal counsel

( ) Internal audit officer

( ) Non-IT officer; please specify: ____

( ) We currently have no designated lead for IT risk management.

2d. To whom does the IT risk management lead report? [Check all that apply.]

[ ] CIO or equivalent

[ ] CISO or equivalent

[ ] CRO or equivalent

[ ] Chief financial officer (CFO)

[ ] Provost

[ ] President

[ ] Other IT officer/director/manager; please specify: ______________________________________

[ ] Other non-IT officer/director/manager; please specify: __________________________________

[ ] Board committee

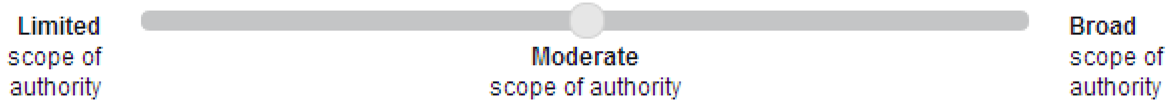
[ ] Not applicable

2e. Move the slider to the position that best represents the scope of authority of your institution's IT risk management program lead.

Limited scope of authority
The program lead may report identified risks to executive leadership but has no authority to require institutional response to risks.

Moderate scope of authority
The program lead reports identified risks to executive leadership and makes recommendations for an institutional response to risk.

Broad scope of authority
There is executive leadership representation within the program, and the program lead has authority to require institutional response to risk.



3. Which frameworks are used at your institution to assess and respond to IT risk? (Check all that apply.)

[ ] Control Objectives for Information and Related Technology (COBIT)

[ ] EDUCAUSE Higher Education Information Security Council Risk Management Framework (HEISC)

[ ] Information Technology Infrastructure Library (ITIL)

[ ] International Organization for Standardization (ISO)

[ ] Management of Risk (MoR; APMG International)

[ ] National Institute of Standards and Technology (NIST; United States)

[ ] Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

[ ] Other; please specify: ___________________________________

[ ] No framework used

4. How is IT risk managed at your institution?

( ) Primarily central IT

( ) Primarily a unit other than central IT; please specify: _________________________

( ) Shared between central IT and another unit; please specify: ________________________

( ) Distributed among several units

( ) Not applicable or not formally assigned

5. Indicate your level of agreement with the following statements about IT risk *at your institution*:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
We have a formal procedure for identifying IT risks.						
IT effectively participates in institutional risk assessment.						
We regularly update a list of IT risks.						
We regularly reprioritize a list of IT risks.						
We effectively track and report IT risks.						
We implement policies and controls in response to IT risk analysis.						
We continuously monitor IT risk policies and controls for effectiveness.						
We have a process in place for reviewing and updating our IT risk management practices.						
We have a common understanding and language around IT risk management.						
We effectively communicate about IT risks with all relevant parties.						
Institutional leadership has a good understanding of the benefits of IT risk management.						
Institutional leadership is adequately involved in IT risk management.						
We train employees to respond to IT risk.						

Cont'd

Cont'd

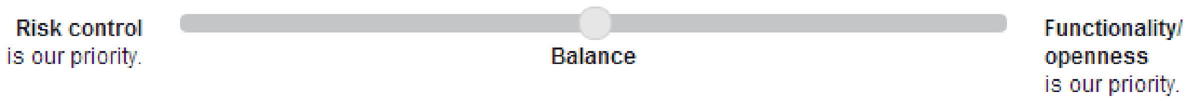
	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
We assess IT risks related to cloud-computing activities.						
We assess IT risks related to other (non-cloud-related) end-user activities such as downloading software and using USB/thumb drives.						
Our IT risk assessment is not solely "top-down"; we enable and encourage IT risks to be identified from within the organization at any level.						
Our existing technologies are too complex.						
Our existing technologies are adequate.						
Our faculty are resistant to IT risk management.						
Our administration is resistant to IT risk management.						
Our staff are resistant to IT risk management.						
We have adequate staff hours devoted to IT risk management.						
We have enough qualified staff devoted to IT risk management.						
We have an adequate budget devoted to IT risk management.						
There is adequate investment in IT services.						
We have the authority to manage or control decentralized (end-user) actions that involve release of data or security breaches.						

6. Move the slider to the position that best represents where your institution generally falls in balancing IT risk control and functionality/openness.

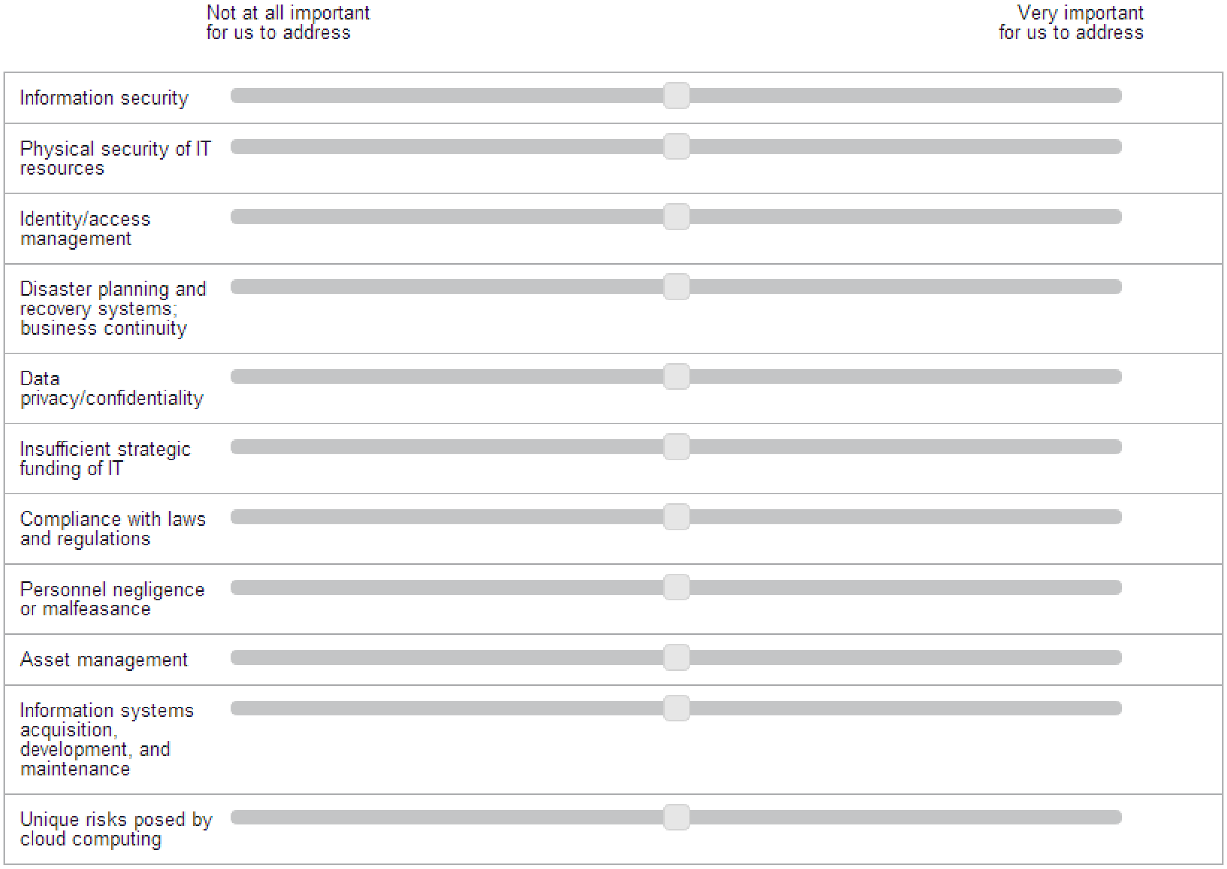
Risk control is our priority:
Risk control is our dominant priority, and we are willing to sacrifice functionality/openness to achieve it.

Balance:
Risk control and functionality/openness are equal priorities, and we strive to balance them.

Functionality/openness is our priority:
Functionality/openness is our dominant priority, and we are willing to accept risks to achieve it.



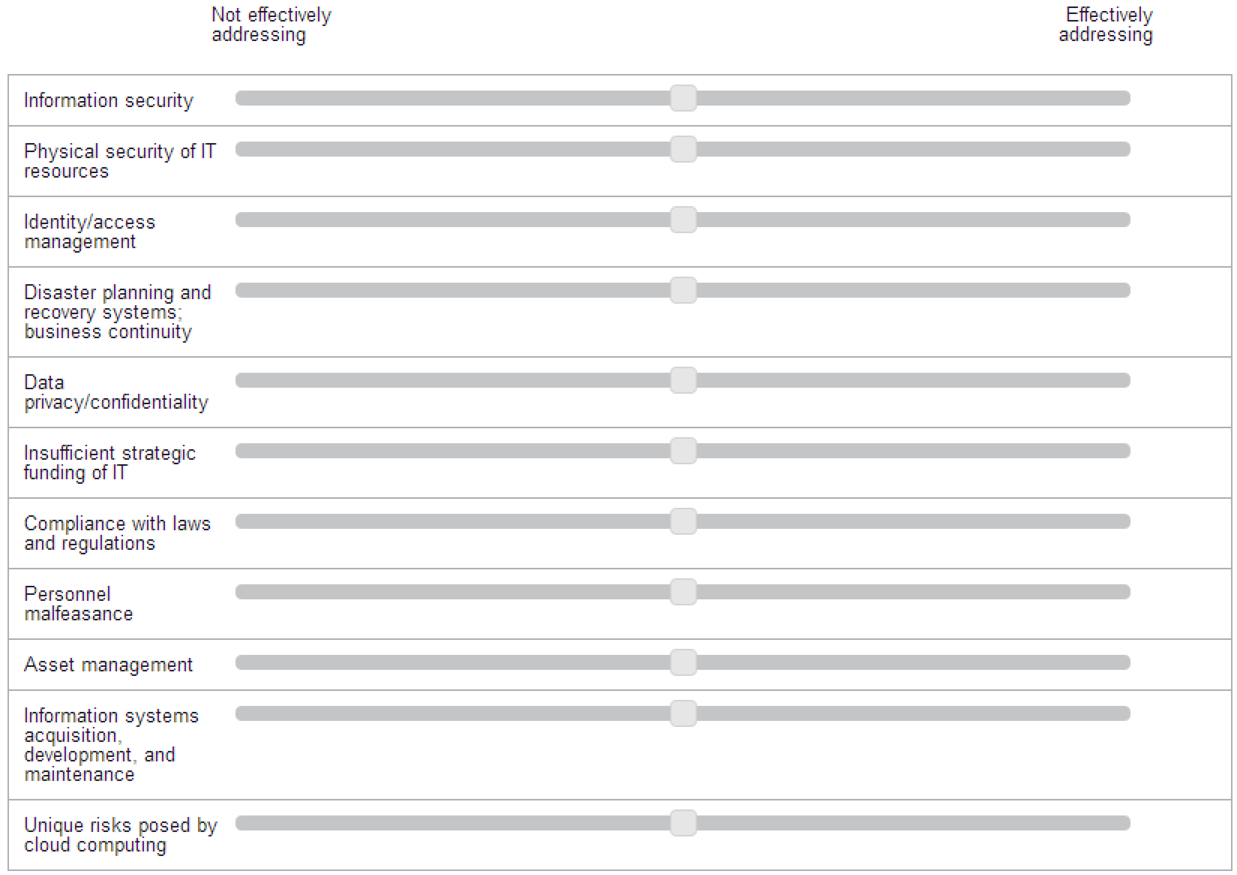
7. For each of the following, move the slider bar to rate the following IT risks in terms of their importance for being addressed *at your institution* (regardless of how effectively you are currently addressing them).



	Not at all important for us to address	Very important for us to address
Information security		
Physical security of IT resources		
Identity/access management		
Disaster planning and recovery systems; business continuity		
Data privacy/confidentiality		
Insufficient strategic funding of IT		
Compliance with laws and regulations		
Personnel negligence or malfeasance		
Asset management		
Information systems acquisition, development, and maintenance		
Unique risks posed by cloud computing		

8. Are there any other significant identified IT risks at your institution not mentioned above? If so, please specify.

9. For each of the following, move the slider bar to rate the effectiveness with which your institution is addressing these IT risks.



	Not effectively addressing	Effectively addressing
Information security		
Physical security of IT resources		
Identity/access management		
Disaster planning and recovery systems; business continuity		
Data privacy/confidentiality		
Insufficient strategic funding of IT		
Compliance with laws and regulations		
Personnel malfeasance		
Asset management		
Information systems acquisition, development, and maintenance		
Unique risks posed by cloud computing		

10. Is IT risk management explicitly listed as a goal or objective in your institution's strategic plan?

( ) Yes

( ) No

( ) Don't know

( ) Our institution does not have a strategic plan.

11. Are there any other barriers or concerns about IT risk management at your institution that are not listed above? If so, please describe them.

12. If you have other comments about your institution's IT risk management processes or if you have links that could provide us with more information about how your institution manages IT risk, please provide those here.

Section B. IT Compliance

IT compliance is defined as programs or processes that ensure the institution's IT resources and systems are operated in ways that meet the laws and regulations impacting those systems and comply with institutional policy.

1. To what extent does your institution have an *institutional* compliance program in place?

( ) We have a formal institutional compliance program in place. <<May see question 2b>>
( ) We have a formal institutional compliance program planned, but it is not yet in place. <<Will not see question 2b>>
( ) Institutional compliance at our institution is ad hoc/reactive/informal. <<Will not see question 2b>>
( ) We do not have any processes or procedures in place for institutional compliance.
<<Will not see question 2b>>

2. To what extent does your institution have an *IT* compliance program in place?

( ) We have a formal IT compliance program in place. <<Go to 2b or 2c>>
( ) We have a formal IT compliance program planned, but it is not yet in place. <<Go to 2a>>
( ) IT compliance at our institution is ad hoc/reactive/informal. <<Go to 2a>>
( ) We do not have any processes or procedures in place for IT compliance. <<Go to 2a>>

2a. Describe how your institution currently addresses IT compliance issues as they arise.

<<Go to 3>>

2b. Is your IT compliance program part of your institutional compliance program?

( ) Yes
( ) No
( ) Don't know

2c. Who leads the IT compliance program?

( ) CIO or equivalent

( ) Deputy CIO or equivalent

( ) Chief information security officer (CISO) or equivalent

( ) Chief risk officer (CRO) or equivalent

( ) IT policy director

( ) Other IT director/manager

( ) Legal counsel

( ) Internal audit officer

( ) Non-IT officer; please specify: ____

( ) We currently have no designated lead for IT compliance.

2d. To whom does the IT compliance lead report? (Check all that apply.)

[ ] CIO or equivalent

[ ] CISO or equivalent

[ ] CRO or equivalent

[ ] Chief financial officer (CFO)

[ ] Provost

[ ] President

[ ] Other IT officer/director/manager; please specify: ____

[ ] Other non-IT officer/director/manager; please specify: ____

[ ] Board committee

[ ] Not applicable

2e. Move the slider to the position that best represents the scope of authority of your institution's IT compliance program.

Limited scope of authority

The program lead may report compliance status to executive leadership but has no authority to require institutional response to compliance mandates.

Moderate scope of authority

The program lead reports compliance status to executive leadership and makes recommendations for an institutional response to compliance mandates.

Broad scope of authority

There is executive leadership representation within the program, and the program lead has authority to require institutional response to compliance mandates.

3. Indicate your level of agreement with the following statements about IT compliance *at your institution*:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don’t know
We have a process in place for reviewing and updating our IT compliance practices.						
We have adequate staff hours devoted to IT compliance.						
We have enough qualified staff devoted IT compliance.						
We have an adequate budget devoted to IT compliance.						
The regulatory environment is too complex.						

4. Rate the following IT compliance issues in terms of the difficulty your institution is having in addressing them:

	Not at all difficult 1	2	3	4	Very difficult 5	Don’t know
Your institution’s IT policies						
Family Educational Rights and Privacy Act (FERPA)						
Health Insurance Portability and Accountability Act (HIPAA) Security Rule						
HIPAA Privacy Rule						
International data protection laws (e.g., European Union Safe Harbor rules)						
U.S. state privacy and data protection laws						
PCI Data Security Standard (PCI DSS)						
Fair and Accurate Credit Transactions Act (FACTA) Red Flags Rule						
Federal Information Security Management Act (FISMA)						
Gramm-Leach-Bliley Act (GLBA)						
International Traffic in Arms Regulations (ITAR)						

5. What are your primary concerns about IT compliance *at your institution*?

6. If you have other comments about your institution’s IT compliance program or if you have links that could provide us with more information about how your institution manages IT compliance, please provide those here.

Section C. IT Governance

IT governance is defined as programs or processes that ensure that the campus IT strategy is aligned with the institution's strategic plan. Information technology thus becomes a strategic partner in the institutional mission.

1. To what extent does your institution have an *institutional* governance body in place, such as the president's cabinet, the institutional senate or equivalent, or an institutional policy council?
( ) We have a formal institutional governance body in place. <<May see question 2b>>
( ) We have a formal institutional governance body planned, but it is not yet in place. <<Will not see question 2b>>
( ) Institutional governance at our institution is ad hoc/reactive/informal. <<Will not see question 2b>>
( ) We do not have any processes or procedures in place for institutional governance.
<<Will not see question 2b>>

2. To what extent does your institution have an *IT* governance body in place?
( ) We have a formal IT governance body in place. <<Go to 2b or 2c>>
( ) We have a formal IT governance body planned, but it is not yet in place. <<Go to 2a>>
( ) IT governance at our institution is ad hoc/reactive/informal. <<Go to 2a>>
( ) We do not have any processes or procedures in place for IT governance. <<Go to 2a>>

2a. Describe how your institution currently addresses IT governance issues as they arise.

<<Go to 3>>

2b. Is your institution's IT governance body part of or represented on your enterprise governance body, such as the president's cabinet, the institutional senate or equivalent, or an institutional policy council?
( ) Yes
( ) No
( ) Don't know

2c. Who leads the IT governance body?

( ) CIO or equivalent
( ) Deputy CIO or equivalent
( ) Chief information security officer (CISO) or equivalent
( ) Chief risk officer (CRO) or equivalent
( ) IT policy director
( ) Other IT director/manager
( ) Legal counsel
( ) Internal audit officer
( ) Other non-IT officer; please specify: ____
( ) We currently have no designated lead for IT governance.

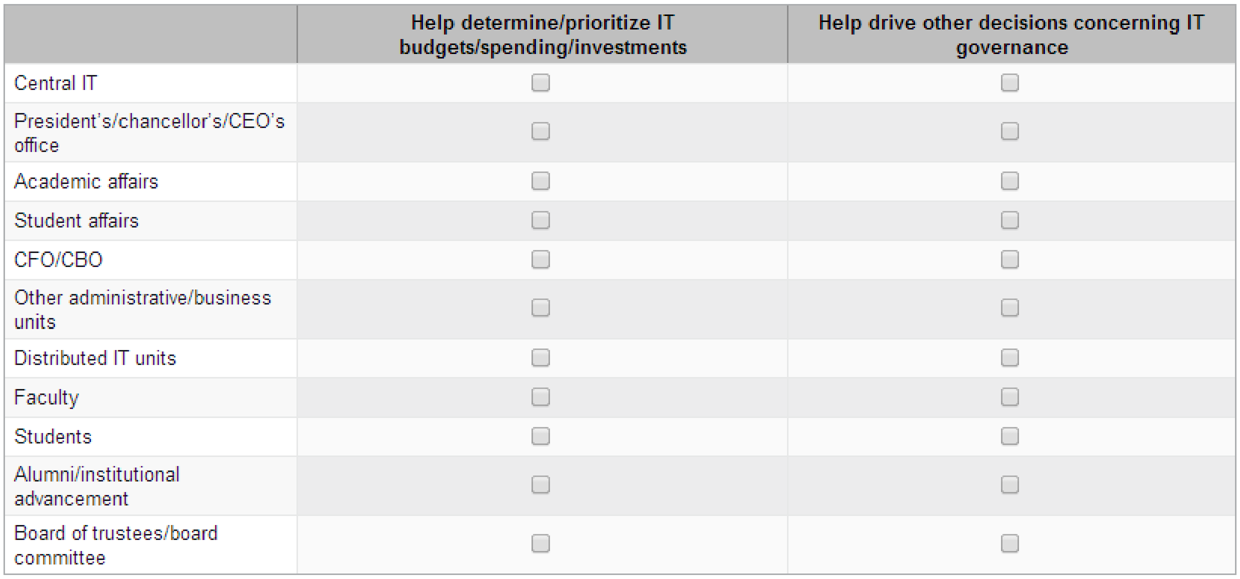
2d. To whom does the IT governance lead report? [Check all that apply.]

[ ] CIO or equivalent
[ ] CISO or equivalent
[ ] CRO or equivalent
[ ] Chief financial officer (CFO)
[ ] Provost
[ ] President
[ ] Other IT officer/director/manager; please specify: ____
[ ] Other non-IT officer/director/manager; please specify: ____
[ ] Board committee
[ ] Not applicable

2e. Indicate your level of agreement with the following statements about the IT governance body (ITGB) *at your institution*:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
ITGB formulates binding policy.						
ITGB prioritizes projects.						
ITGB controls the budget.						
ITGB aligns IT strategy with institutional strategy.						
ITGB guides IT risk management.						
ITGB advises on service levels.						
ITGB advises on service improvement priorities.						
ITGB reports to institutional leadership (president's/chancellor's/CEO's office).						
ITGB influences institutional leadership.						

3. Which units/organizations are involved with the following? (Check all that apply.)



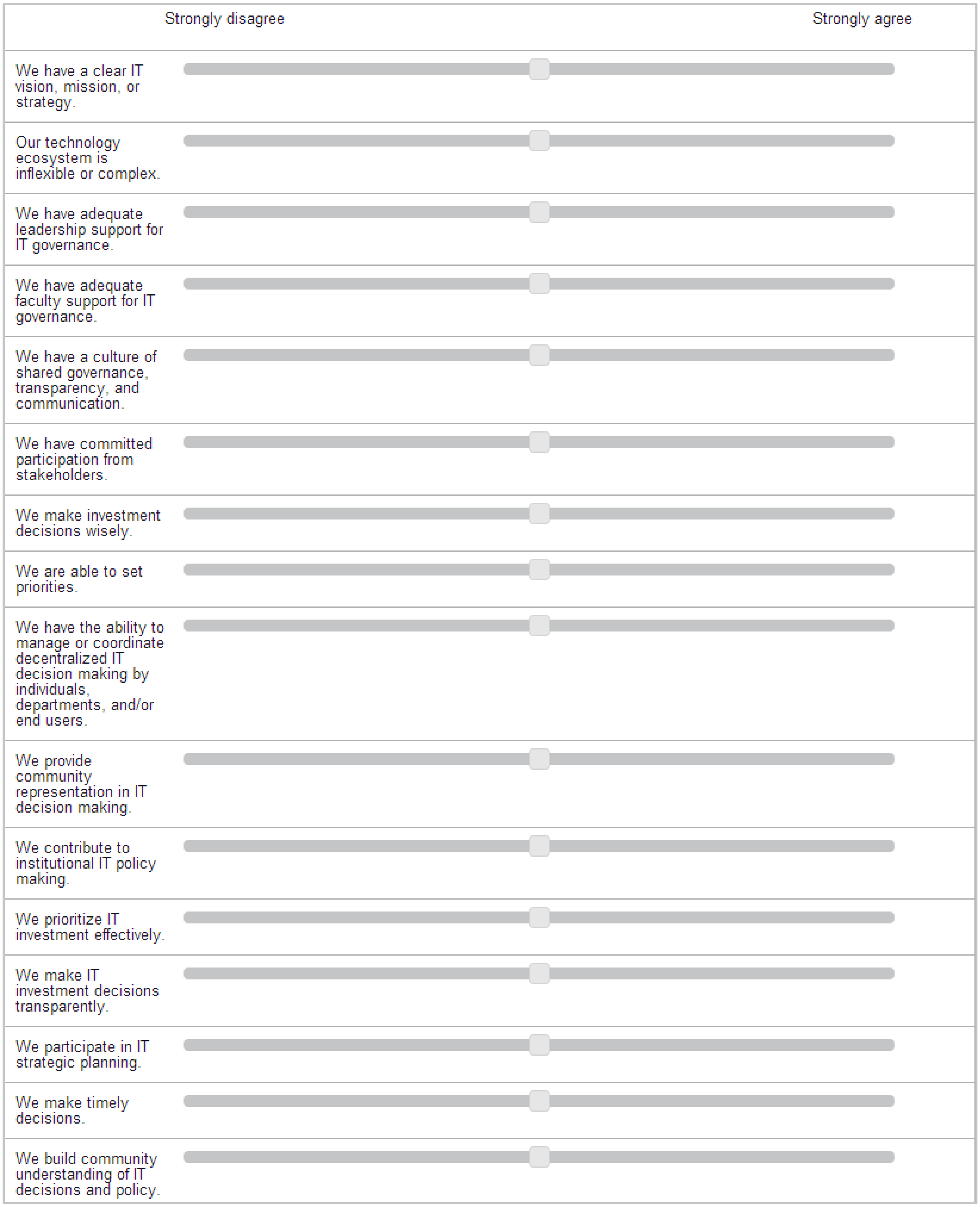
	Help determine/prioritize IT budgets/spending/investments	Help drive other decisions concerning IT governance
Central IT	□	□
President's/chancellor's/CEO's office	□	□
Academic affairs	□	□
Student affairs	□	□
CFO/CBO	□	□
Other administrative/business units	□	□
Distributed IT units	□	□
Faculty	□	□
Students	□	□
Alumni/institutional advancement	□	□
Board of trustees/board committee	□	□

3a. Are there any other units/organizations not previously identified that are involved with the IT governance activities specified above? If so, please specify:

4. Which standards are used for IT governance at your institution? (Check all that apply.)

[ ] Control Objectives for Information and Related Technology (COBIT)
[ ] Information Technology Infrastructure Library (ITIL)
[ ] International Organization for Standardization (ISO)
[ ] Other (please specify): ____
[ ] No formal standards

5. Rate the extent to which you agree with the following statements about IT governance at your institution:



	Strongly disagree	Strongly agree
We have a clear IT vision, mission, or strategy.		
Our technology ecosystem is inflexible or complex.		
We have adequate leadership support for IT governance.		
We have adequate faculty support for IT governance.		
We have a culture of shared governance, transparency, and communication.		
We have committed participation from stakeholders.		
We make investment decisions wisely.		
We are able to set priorities.		
We have the ability to manage or coordinate decentralized IT decision making by individuals, departments, and/or end users.		
We provide community representation in IT decision making.		
We contribute to institutional IT policy making.		
We prioritize IT investment effectively.		
We make IT investment decisions transparently.		
We participate in IT strategic planning.		
We make timely decisions.		
We build community understanding of IT decisions and policy.		

6. Are there any other barriers or concerns about IT governance at your institution that are not listed above? If so, please describe them.

7. If you have other comments about your institution's IT governance processes or if you have links that could provide us with more information about how your institution manages IT governance, please provide those here.

8. Has your institution purchased any of the following GRC software systems or GRC modules of ERP systems? If so, please indicate whether their use at your institution is strictly for governance, risk, or compliance or whether they have multiple uses at your institution. Subparts of 9a and 9b will only display for purchased systems.

	Have not purchased	Used strictly for **governance**	Used strictly for **risk management**	Used strictly for **compliance**	Used for **multiple areas**
Agiliance RiskVision					
ARIS Risk & Compliance Manager					
IBM OpenPages GRC					
MetricsSteam GRC Platform					
Navex Global					
Protiviti					
RSA Archer GRC					
SAP GRC Suite					
Thomson Reuters GRC Suite (Accelus)					

8a. Has your institution purchased GRC software or modules not listed above? If so, please specify:

9a. For each GRC software system in Question 8, please rate its ease of use.

(display only those checked in Q8)	**Not at all easy to use 1**	**2**	**3**	**4**	**Very easy to use 5**
Agiliance RiskVision					
ARIS Risk & Compliance Manager					
IBM OpenPages GRC					
MetricsSteam GRC Platform					
Navex Global					
Protiviti					
RSA Archer GRC					
SAP GRC Suite					
Thomson Reuters GRC Suite (Accelus)					

9b. For each GRC software system in Question 8, please rate its effectiveness at your institution.

(display only those checked in Q8)	**Not at all effective 1**	**2**	**3**	**4**	**Very effective 5**
Agiliance RiskVision					
ARIS Risk & Compliance Manager					
IBM OpenPages GRC					
MetricsSteam GRC Platform					
Navex Global					
Protiviti					
RSA Archer GRC					
SAP GRC Suite					
Thomson Reuters GRC Suite (Accelus)					

Thank you for participating in ECAR's GRC survey! Aggregated responses to this survey will be analyzed and published in a report that is planned for release in early summer 2014. Thank you for being a part of this important research.