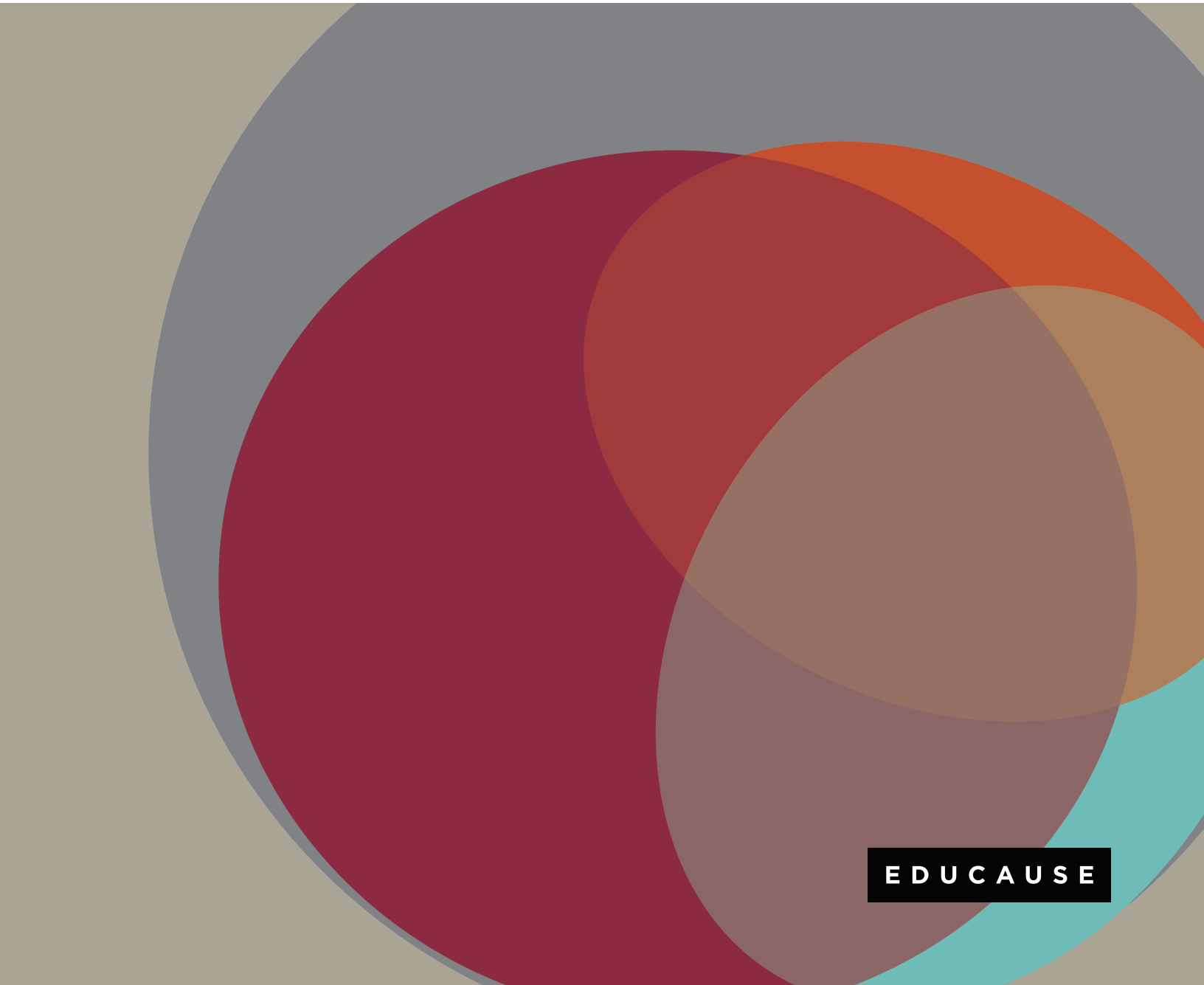
EDUCAUSE CENTER FOR ANALYSIS AND RESEARCH

Getting Your Ducks in a Row

IT Governance, Risk, and Compliance Programs in Higher Education



EDUCAUSE

Contents

Authors

Jacqueline Bichsel, Senior Research Analyst, EDUCAUSE

Patrick Feehan, Director of IT Privacy and Cybersecurity Compliance, Montgomery College

Citation

Bichsel, Jacqueline, and Patrick Feehan. *Getting Your Ducks in a Row: IT Governance, Risk, and Compliance Programs in Higher Education.* Research report. Louisville, CO: ECAR, June 2014. Available from http://www.educause.edu/ecar.

EDUCAUSE

EDUCAUSE is a nonprofit association and the foremost community of IT leaders and professionals committed to advancing higher education. EDUCAUSE programs and services are focused on analysis, advocacy, community building, professional development, and knowledge creation because IT plays a transformative role in higher education. EDUCAUSE supports those who lead, manage, and use information technology through a comprehensive range of resources and activities. For more information, visit educause.edu.

Foreword

Summon to mind what governance, risk, and compliance (GRC) means to your institution. Is GRC three interdependent activities that together form a program of IT management, or is it three specific but separate efforts? Consider the following:

- The chief privacy officer at one institution might be thinking: "We did not purchase any GRC system or tool, but my institution has a data governance or stewardship policy. That policy was developed because of continuing and substantial risk to our institutional data. Finally, we determine on a periodic basis compliance with all our policies, including this one. We have G, we have R, and we have C."
- At another institution, however, the chief risk officer (CRO) might need a GRC solution. The CRO may purchase an enterprise GRC system. There are innumerable risks beyond the information security risks most familiar to the IT organization. There are environmental risks. There are personal security risks. There are risks to foundations. There are employee risks. There are risks in an athletic program. Every department in the higher education institution has some form of risk, and we need an enterprise system to systemically assess, track, and control for these risks.
- The Office of General Counsel or the Office of Compliance might request another type of GRC solution. Their needed solution might be a legal GRC system that has control mechanisms or policy settings related to legal, regulatory, or contractual obligations.
- A different type of GRC solution is available to the chief auditing officer. This type of GRC solution is sometimes referred to as finance GRC by vendors. This use of GRC aims to manage the financial controls put into place by internal and external auditors.
- Finally, an IT department's chief information officer (CIO) might be looking for a GRC solution—an IT GRC system. The typical IT GRC system can be helpful in addressing the institution's need to mitigate the increasing uncertainty of how data are received, stored, used, shared, extracted, interpreted, or destroyed by the institution. The higher education enterprise, in meeting increasing demands for entity transparency and student success, is moving increasingly to third-party technical solutions. These solutions may require enterprise data—sometimes personally identifiable information—to be extracted outside the enterprise. These purchases or installations of third-party systems or cloud solutions may conceivably be accomplished without sufficient IT collaboration in the planning, assessment, or decision to use these tools. The use of a GRC system or processes to set measurable control objectives for the IT portion of data or technological risk in a given endeavor has gained prominence as an ever-important step in reducing institutional risk.

These examples show how GRC can mean different things to different parts of the higher education institution. GRC can—and may already—be separate activities within your organization that arose to address specific issues. GRC may also be an enterprise- or institution-wide effort. Breadth and latitude are sufficiently flexible when defining what GRC means for your IT organization to allow initial or burgeoning programs to fit into efforts already under way. Although GRC is often introduced as a software or cloud solution, its roots in long-term IT efforts identify it more fittingly as a program. GRC in its rawest form, and regardless of the tool used, ties an organization's policies, controls, and regulations together into repeatable and reportable actions.

The individual processes of a GRC program, without recognition of the inextricable link between execution and strategy, yield mainly siloed activities equaling, at most, the sum of their parts. Partnering the processes of governance and compliance against the backdrop of institutional risk will better allow an institution to converge common goals in a strategic manner.

Patrick Feehan, Director of IT Privacy and Cybersecurity Compliance, Montgomery College

Overview

Higher education IT governance, risk, and compliance (GRC) programs are in the development stage. Few institutions have all three programs in place, and many institutions are unclear where they should start when instituting or maturing their IT GRC programs. In addition, they are often uncertain as to whether GRC programs should be developed in parallel or separately.

Institutions take various approaches in deciding which programs—IT governance, risk, and/or compliance—should be instituted. Ideally, all three would be in place, but resources and culture may dictate the priority and progress of IT GRC initiatives. There is consensus in who leads IT GRC programs—most often it is the CIO or the chief information security officer (CISO)—and these leads are generally given a relatively broad scope of authority.

This 2014 ECAR study of IT GRC describes the current landscape of IT GRC programs in higher education; identifies aspects of the IT GRC environment that will aid CIOs, CISOs, and other leads to make decisions about IT GRC initiatives; and outlines steps institutions can take to become more mature in their IT GRC programs.

Key Findings

- **Formal enterprise or IT risk management and compliance programs are the exception rather than the rule.** More common are informal processes and procedures for dealing with risk management and compliance.
- **Most institutions have a formal institutional governance body in place.** About half have a formal IT governance body.
- **There are significant gaps between the perceived importance of specific risks and the effectiveness with which they are being addressed.** Information security is viewed as the most important risk to address, yet the perceived effectiveness with which it is addressed does not match its importance.
- **Maturity in IT risk management can be assessed along four dimensions:**
  - **Communication/End-User Management** (communication about IT risk throughout the organization, as well as management of end-user activities)
  - **Acceptance** (lack of resistance from faculty, staff, and administration to risk management efforts)
  - **Risk Assessment/Management** (identifying, tracking, prioritizing, and reporting risks; implementing policies and controls; and involvement of leadership)
  - **Investment** (adequate investment in risk management staff and services)

- **Maturity in risk management is associated with stronger governance and compliance efforts and processes.** In addition, those with more mature IT risk management programs have a greater influence on institutional leadership decisions.
- **Fewer than half of institutions report that they effectively communicate about IT risks to all relevant parties.** Better communication can improve the institutional culture of acceptance and awareness of IT risk.
- **Those with an IT governance body in place are more likely to involve others—particularly faculty, students, and alumni—in both IT budgeting and other IT governance decisions.** This increased involvement may facilitate or enhance communication of IT GRC issues across the institution.
- **Investment in risk management is associated with more progressive GRC efforts.** Only 1 in 10 institutions have an adequate budget devoted to IT risk management.

Introduction

A classic story provides an interesting analogy for IT GRC. In the most commonly known version, six blind men are asked to describe an elephant. The first blind man touches the elephant's tail and describes the elephant as a rope. A second blind man feels the leg of the elephant and describes the elephant as a pillar. Other blind men variously describe the elephant as a wall, a tree branch, a solid pipe, and a hand fan. A king explains to the blind men, "All of you are right. The reason every one of you is telling it differently is because each one of you touched a different part of the elephant. So, actually the elephant has all the features you mentioned."[1]

Welcome to the inclusive world of GRC. GRC can be:

- An IT-centric tool
- An enterprise risk management tool
- A legal compliance tool
- A financial controls tool
- No tool at all, but instead a program merging recognition of risk with policy and governance

The path of how some institutions come to view GRC, or the component processes, necessarily depends on which part of the proverbial elephant was touched. Where did or does your institution step into the discussions of GRC? The stepping-off point may dictate what kind of GRC tool or program—if any—is implemented.

The concept of a GRC program (or set of processes) addresses the reality of this common organizational tension. As Gartner defines it, "Governance, risk, and compliance (GRC) is a set of processes, supported by enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks."[2]

- *Governance* typically refers to how a higher education institution is organized for the purposes of decision making and resource allocation and how the varying parts are managed in a way that promotes the mission of the institution.
- *Risk management* details how an institution determines its appetite for risk, as well as how risk controls and mitigation strategies for any given endeavor are developed and enforced throughout the enterprise.
- *Compliance* represents the effort to ensure that laws, regulations, and even an institution's own policies are complied with and that efforts are coordinated institution-wide.

Examining the various ways in which institutions may investigate IT GRC processes as solutions is not as daunting as it may first appear. The tools and efforts will necessarily vary among institutions, but the underlying common assumption is that IT GRC is a set of internal processes that help bridge the gap between higher education

IT GRC is a set of internal processes that helps bridge the gap between higher education institutional strategies and IT's own plans for strategic execution.

institutional strategies and IT's own plans for strategic execution. IT departments have strategic plans, and enterprises have strategic plans. How can an IT organization match its own strategic execution to the enterprise's strategies and goals? Many institutions of higher education have integrated their own IT strategy into institutional strategy. Others have integrated risk assessment and risk management into enterprise strategy, including IT. Still other institutions have ensured that the strategic steps taken are in compliance with known laws, regulations, and policies. Any of these efforts, or a combination of them, can rightfully be recognized as GRC, or at least an institution's version of GRC.

GRC is not the elephant in the room (or in the CIO's office); GRC practices are methods recognized by every institution of higher education. An even better animal analogy was proffered by EDUCAUSE President Diana Oblinger:

> Information technology is critical to higher education. But unless aligned with the institution's goals and based upon sound policies and procedures, information technology will not be trusted, reliable, efficient, or effective. This alignment can be furthered through governance, risk, and compliance (GRC) programs. Such programs are about adding value through planning and decision making—that is, about getting your ducks in a row.[3]

This ECAR report is a review of higher education's current IT GRC practices, programs, and processes and how those efforts are characterized in terms of their depth and scope. The data provided are from a survey to which 246 institutions responded. The report provides an overview of the current landscape of IT GRC efforts in higher education. Some efforts are relatively mature; others are just beginning.

Origins of GRC in Corporate Malfeasance

The impetus for GRC as an aspiration (whether manifested as software or a system) and even as a conclusion can be expressed many ways under myriad theories, mostly depending on the department implementing the strategy. GRC's emergence into common corporate and ultimately higher education parlance, however, is clearer. The path was created, or at least accelerated, by the corporate financial reporting debacles of 2001–2004, which were governance-defying, risk-producing, and compliance-ignoring. The most well-known case is Enron.

Enron was not alone in the lurid corporate malfeasance that dominated the headlines from 2001 to 2004. WorldCom, Tyco, and Adelphia are three other examples that have "come to represent a wave of corporate scandal that plagued America in the early 2000s."* Enron was a hugely successful company in the late 1990s, rising in apparent value and growing from 7,500 employees in 1996 to more than 20,000 in 2001. Its SEC filings portrayed it as a company worth billions, but it was all a mirage. The financial information backing Enron's value was badly misstated, and Enron declared bankruptcy in 2001, yielding worthless stock to external shareholders and company shareholders alike. Its chairman of the board and CEO were eventually convicted of fraud and conspiracy charges in federal court. Enron's accounting firm was also criminally convicted.

The result was the July 30, 2002, passage of the Sarbanes-Oxley Act of 2002, commonly called SOX. Among various provisions, the act created a Public Company Accounting and Oversight Board (PCAOB). Chief among the many PCAOB conditions are ones that require greater openness between a corporation and its auditors. A key provision within PCAOB is that an auditor must understand the internal environment of the corporation being audited to better understand the "company's objectives and strategies and those related business risks that might reasonably be expected to result in risks of material misstatement."†

This requirement for an auditing firm to be aware of its client's strategy and the risks of that strategy drove the development of tools to aid the auditing firms. GRC was adopted by consultants as an expression of a program that allowed an outside firm to determine whether the risks to the strategy of the public company were properly stated or mitigated. GRC's evolution as a tool to measure strategy and risk has found a good fit in nonprofit situations, such as the institution of higher education.

* Joanna L. Grama, *Legal Issues in Information Security* (Sudbury, MA: Jones & Bartlett Learning, 2011), 181.

† Public Company Accounting Oversight Board, Auditing Standard No. 12, "Identifying and Assessing Risks of Material Misstatement," http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_12.aspx.

The Current Landscape of Higher Education GRC Programs

In this section, we characterize what GRC programs currently look like in higher education and answer the following questions:

- What percentage of institutions currently have GRC programs?
- Who leads these programs and to whom do these program leads report?
- What is the scope of authority of GRC programs?

IT Risk Management Programs

Most institutions employ some means of addressing issues in enterprise risk management (95%) and IT risk management (96%), with informal programs outnumbering formal ones (figure 1). Although formal enterprise and IT risk management programs are currently the exception rather than the rule, 1 in 10 institutions with no formal enterprise risk management programs are planning to migrate to formal programs, and about one in six with no formal IT risk management programs are planning to migrate to formal programs. These data indicate a likelihood of some future growth in formal risk management programs.

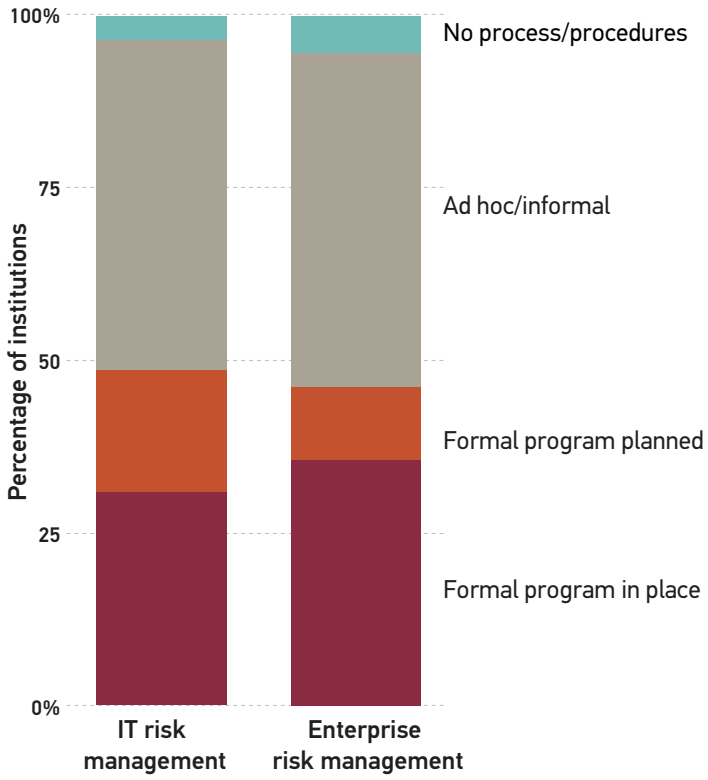


Figure 1. Prevalence of Enterprise and IT Risk Management Programs

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.

Public institutions (42%) are significantly more likely than private institutions (26%) to have a formal enterprise risk management program in place.[4] When it comes to IT risk management programs, the gap between public (38%) and private (25%) institutions is slightly narrower.[5] In addition, larger institutions (> 8,000 student FTE) are much more likely to have either a formal enterprise risk management program or a formal IT risk management program in place than are smaller institutions (< 2,000 student FTE).

Out of 51 institutions with both an enterprise risk management and an IT risk management program in place (21% of the total respondents; see figure 2), about three-fourths (76%) have them under the same umbrella. In other words, the IT risk management program is a component of the enterprise risk management program. The large gray circle in figure 2 represents all institutions, so the area not covered by a teal or crimson circle (54% of the gray circle) represents those institutions that have neither a formal enterprise risk management nor a formal IT risk management program.

Findings presented later in this report suggest that a formal risk management program can drive institutional GRC maturity. Institutions that have *either* an enterprise risk management program *or* an IT risk management program have higher scores on a number of maturity dimensions. This finding may seem intuitive, but it points to the importance of establishing a formal risk management program rather than dealing with risks on an ad hoc or informal basis.

Figure 2. Overlap of Enterprise and IT Risk Management Programs[6]

Who Leads the IT Risk Management Program?

Figure 3 outlines the leadership of formal IT risk management programs for the 31% of institutions that have those programs in place.

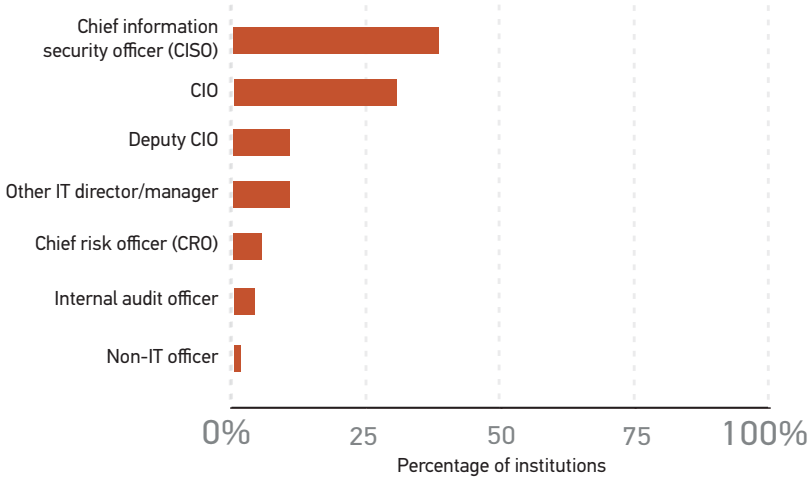


Figure 3. Position Leads for IT Risk Management Programs

More than one-third (38%) of formal IT risk management programs are led by CISOs. This suggests that these risk management programs may be based on information security programs or information security compliance requirements. Another 30% of IT risk management programs are led by CIOs. In doctoral (DR) institutions, more than half (52%) of IT risk management leads are CISOs, perhaps because these institutions have more resources to dedicate to employing the specialized position of CISO. In associate's (AA) institutions, the majority (60%) of IT risk management leads are CIOs.

To Whom Does the IT Risk Management Lead Report?

More than half of IT risk management leads report to the CIO or CIO equivalent (figure 4). Most CISOs (76%) who are IT risk management leads report to the CIO. CIOs who are IT risk management leads most frequently report to the president (26%), the provost (22%), and/or the CFO (22%).[7]

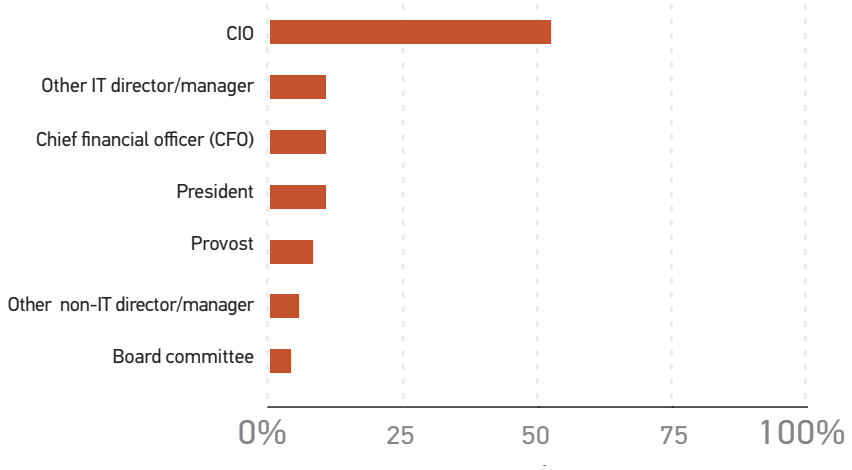


Figure 4. Positions to Which the IT Risk Management Lead Reports (More Than One Response Possible)

Scope of Authority of IT Risk Management Lead

Respondents who reported having a formal IT risk management program (31% of all respondents) were asked about the scope of authority of the IT risk management lead (on a scale from 0 to 100 where 0 = "limited scope of authority" and 100 = "broad scope of authority").

Figure 5 shows that the majority of responses fall at the middle and high end of the scale (with a mean of 64), indicating that most institutions allow their risk management lead a moderate to broad scope of authority. Scope of authority does not differ depending on whether the risk management lead is a CISO or a CIO. In addition, there are no significant differences based on Carnegie Classification, control (public versus private), or institution size.

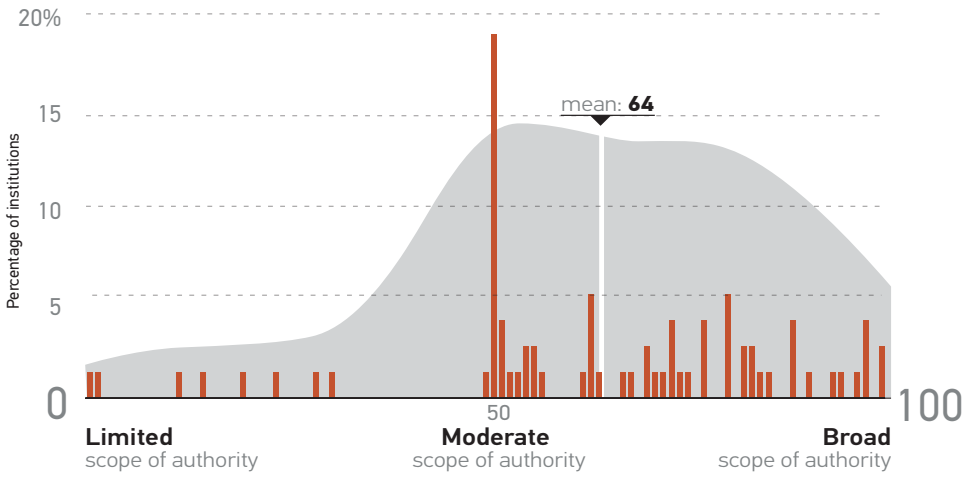


Figure 5. IT Risk Management Lead's Scope of Authority

Definitions of "scope of authority"

Limited scope of authority

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

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.

IT Compliance Programs

Similar to the findings about IT risk programs, nearly all institutions (93%) have some means of addressing compliance issues (figure 6). Informal programs are more common than formal ones. Similar to the trend we saw in the development of risk programs, one in nine institutions with no formal institutional compliance programs are planning to migrate to formal programs, and one in six with no formal IT compliance programs are planning to migrate to formal programs.

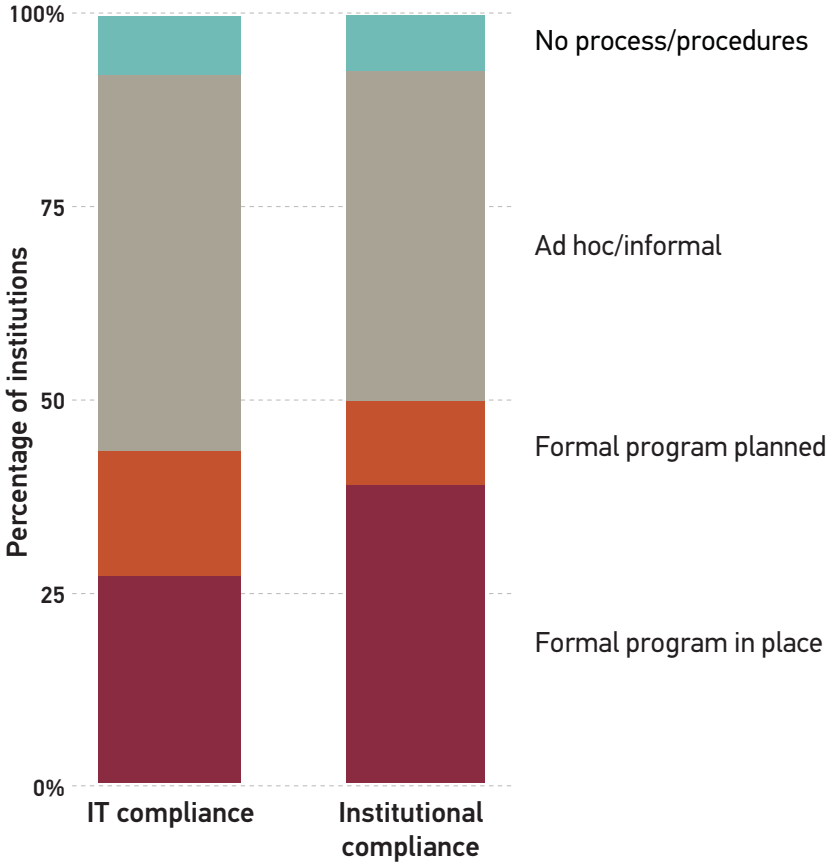


Figure 6. Prevalence of Institutional and IT Compliance Programs

Nearly two-fifths (39%) of institutions have a formal institutional compliance program in place; fewer (27%) have a formal IT compliance program in place. About one-fourth (23%) of institutions have both an institutional compliance and an IT compliance program in place (figure 7). More than three-fourths (77%) of those with both programs have them under the same umbrella. In other words, the IT compliance program tends to be part of the institutional compliance program. The large gray circle in figure 7 represents all institutions, so the area not covered by a teal or crimson circle (57% of the gray circle) represents those institutions that have neither a formal institutional compliance nor a formal IT compliance program.

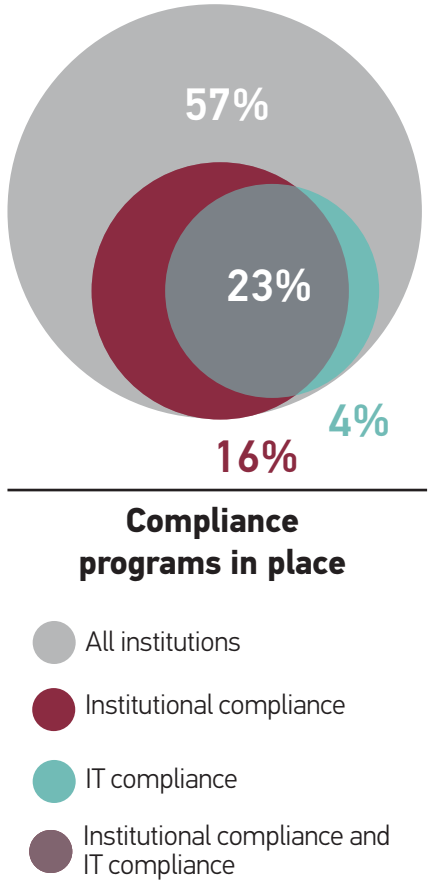


Figure 7. Overlap of Institutional and IT Compliance Programs

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. **Institutional compliance** addresses all compliance issues that affect the institution.

Who Leads the IT Compliance Program?

Figure 8 outlines the leadership of formal IT compliance programs for the 27% of institutions that have them in place. Just as with IT risk management, the CISO and the CIO are the most common leads. These data suggest that GRC processes often operate out of functional areas with many other significant responsibilities.

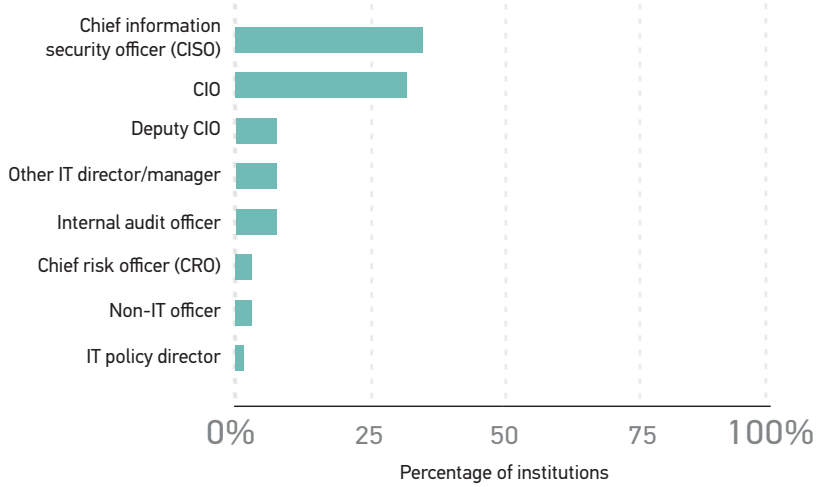


Figure 8. Position Leads for IT Compliance Programs

To Whom Does the IT Compliance Lead Report?

Just as with IT risk management, half of IT compliance leads report to the CIO or CIO equivalent (figure 9). CISOs who are IT compliance leads report most often to the CIO (87%). CIOs who are IT compliance leads most frequently report to the CFO (43%) and/or the president (29%).

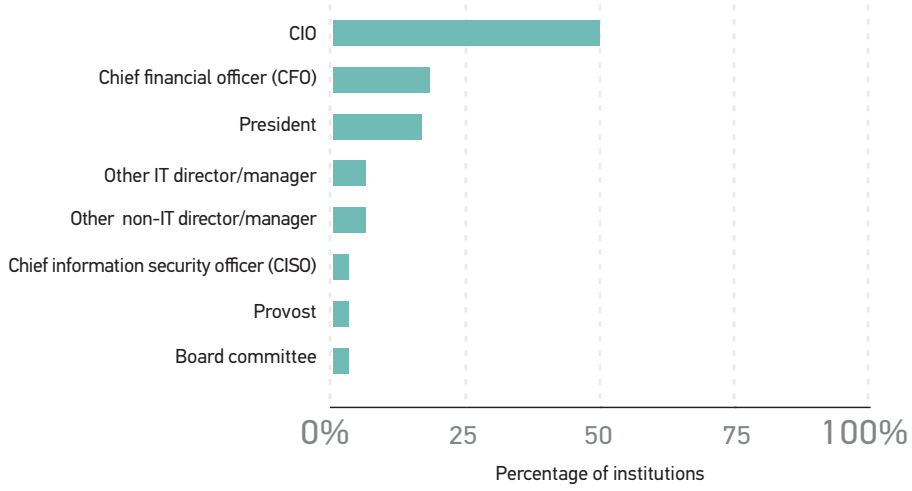


Figure 9. Positions to Which the IT Compliance Lead Reports (More Than One Response Possible)

Scope of Authority of IT Compliance Lead

Respondents who reported having a formal IT compliance program (27% of all respondents) were asked about the scope of authority of the IT compliance lead (on a scale from 0 to 100 where 0 = "limited scope of authority" and 100 = "broad scope of authority").

Respondents reported an average scope of authority of 72 (figure 10). This is significantly higher than the mean for the IT risk management lead (64, $p < .05$). Scope of authority for IT compliance is somewhat (but not significantly) higher if the compliance lead is the CIO (76) than if the compliance lead is the CISO (70).

The vast majority of responses fall toward the high end of the scale, indicating that most institutions allow their compliance lead a relatively broad scope of authority. Many ratings were at the highest possible point on the scale: 12% of respondents indicated that their compliance lead has the broadest scope of authority possible. The differences in scope of authority between IT risk management and IT compliance may be due to the fact that compliance is tied to regulatory requirements, whereas risk management permits more discretion. There may be a higher level of comfort in allowing broader authority in an area where actions are dictated by rules and laws.

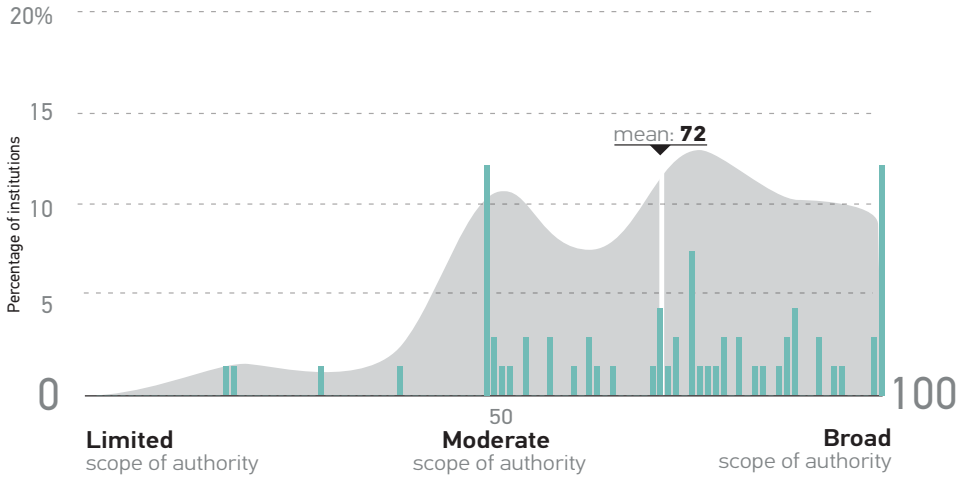


Figure 10. IT Compliance Lead's Scope of Authority

IT Governance Programs

Formal governance programs are more common than formal risk or compliance programs, with the majority (83%) of institutions having a formal institutional governance body in place and about half (55%) having a formal IT governance body in place (figure 11). About one in seven institutions with no formal IT governance processes are planning to transition to a formal IT governance body.

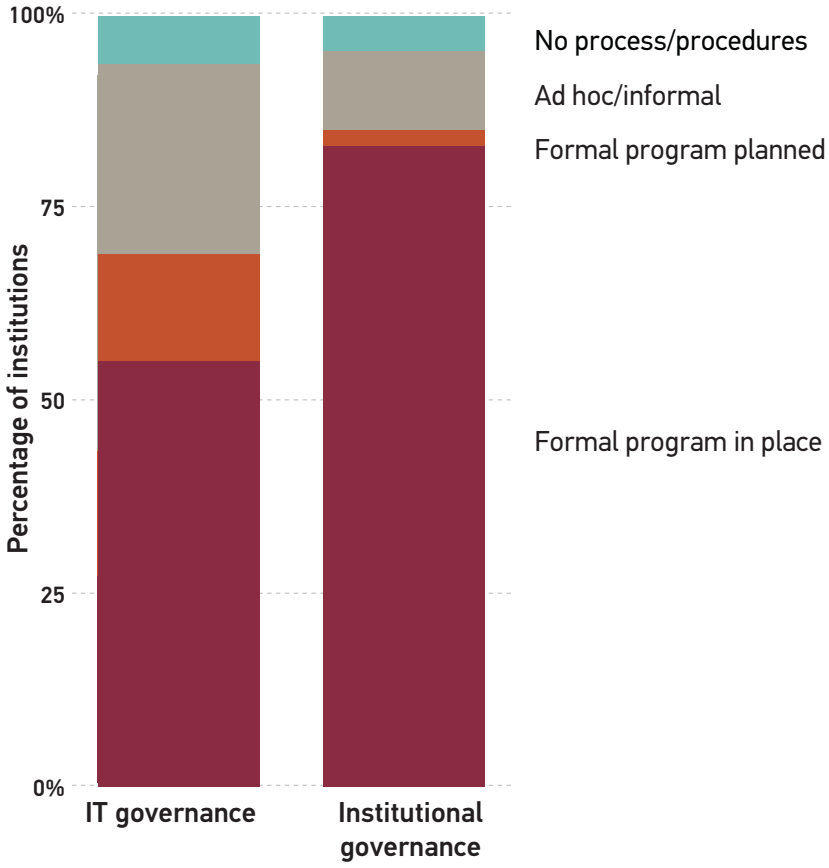


Figure 11. Prevalence of Institutional and IT Governance Programs

About half (53%) of institutions have both an institutional and an IT governance body in place. More than three-fourths of those institutions (79%) have their IT governance body as part of or represented on their institutional governance body, such as the president's cabinet, the institutional senate or equivalent, or an institutional policy council.

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

Who Leads the IT Governance Program?

Figure 12 outlines the program leadership for the 55% of institutions with a formal IT governance body in place. Nearly three-fourths (73%) of IT governance bodies are led by the CIO.

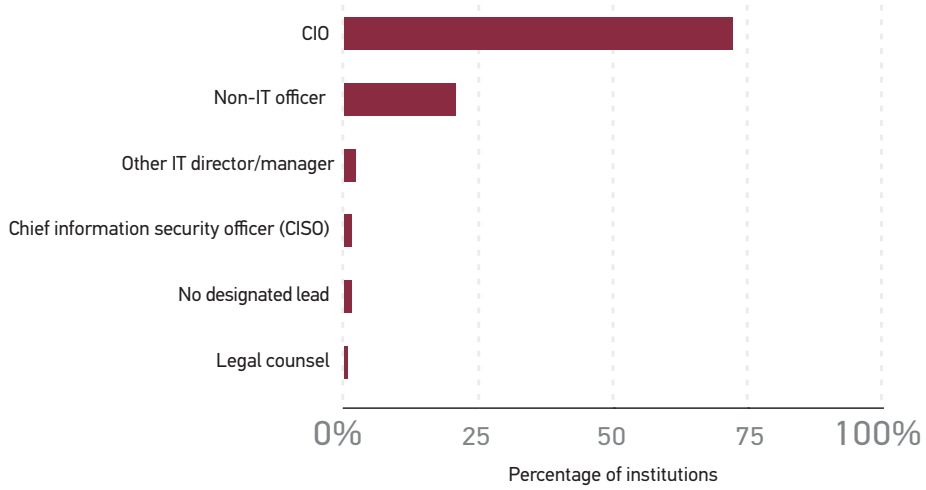


Figure 12. Position Leads for IT Governance Programs[8]

To Whom Does the IT Governance Lead Report?

The majority (62%) of IT governance leads report to the president and/or provost (figure 13).

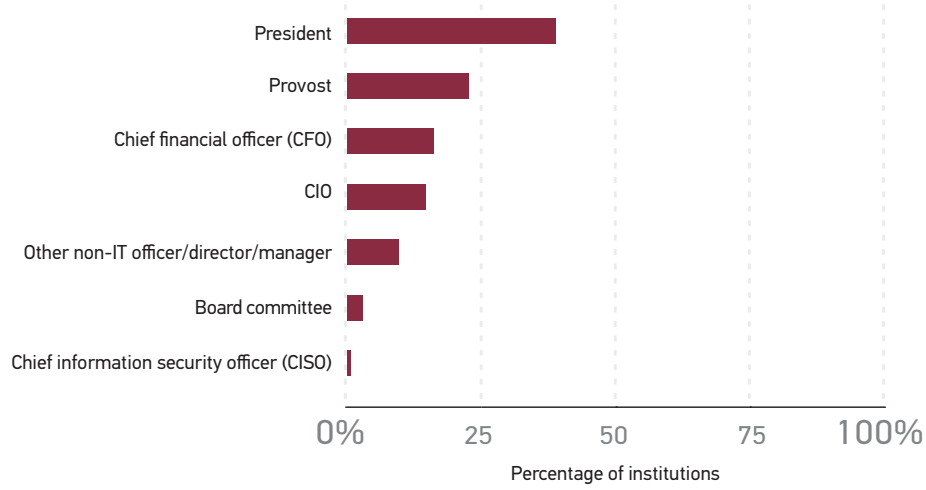


Figure 13. Positions to Which the IT Governance Lead Reports (More Than One Response Possible)

Scope of the IT Governance Body

Among those who reported having a formal IT governance body (ITGB), figure 14 displays the percentage who agreed with the corresponding statements about the scope of their ITGB. It appears that the most frequent activities engaged in by the ITGB concern advising: on strategy, on service levels, and on service improvement and project priorities. The extent to which an ITGB influences institutional leadership is understandably associated with whether the ITGB reports to institutional leadership ($r = .43$, $p < .001$).

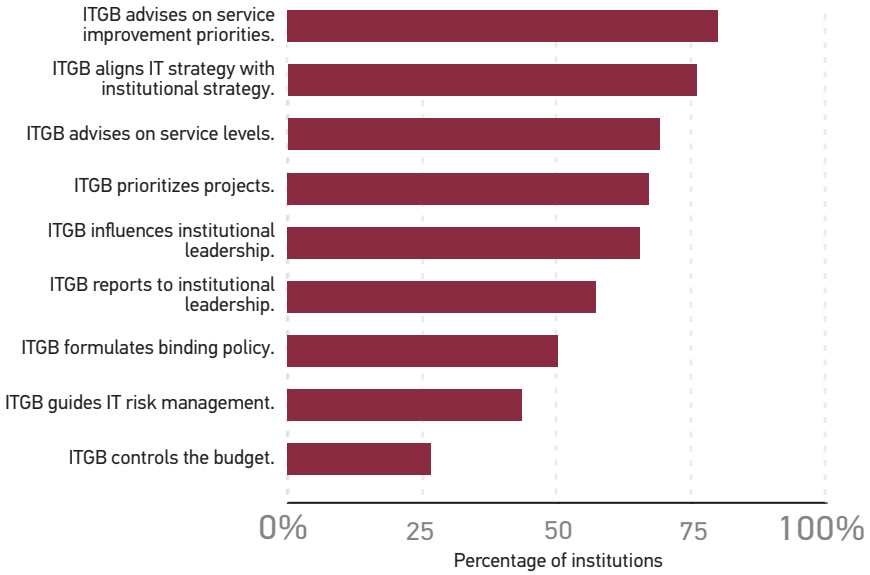


Figure 14. Percentage of Respondents Agreeing with Statements about ITGB Governance Processes

Note: ITGB = IT Governance Body

Summary of IT GRC Programs

Figure 15 summarizes the percentage of institutions with formal IT governance, risk, and compliance programs. It also indicates the degree of overlap between these programs. The gray circle represents all institutions. The red ellipse represents the institutions with a formal IT governance body, the orange ellipse represents those with a formal IT risk management program, and the turquoise ellipse represents those with a formal IT compliance program. The other shaded areas represent the degree of overlap between institutions with these programs. To find the percentage of total institutions with a formal IT risk management program, for example, one would add 12% + 4% + 4% + 9% to get 29%.[9] The percentage of institutions with both an IT governance and an IT compliance program = 12% + 8% = 20%. The percentage of institutions with all three IT GRC programs is 12%.

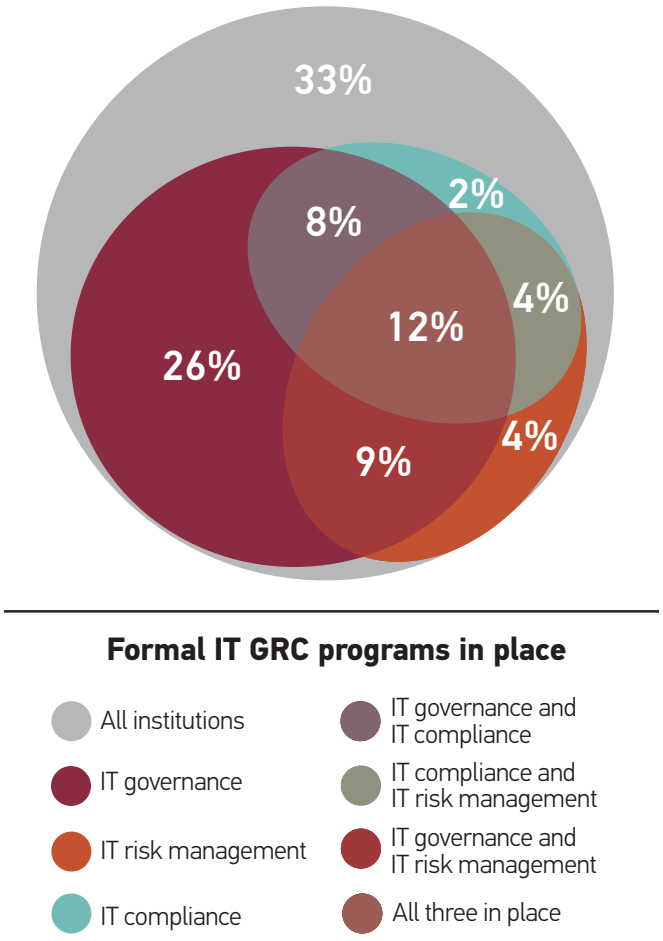


Figure 15. Prevalence and Degree of Overlap of Formal IT GRC Programs

The degree of overlap can tell us some interesting things about IT GRC programs. For example, although the percentages of institutions having a formal IT risk management program and a formal IT compliance program are about the same, these are not the same institutions (having both IT risk management and IT compliance). About 39% of institutions have a formal IT risk management or IT compliance program. Only 16% have both a formal IT risk management and a formal IT compliance program. Therefore, it is not the case that the same institutions (e.g., those with more resources) are the ones with both formal IT risk management and IT compliance programs. Many institutions are choosing to have *either* a formal IT risk management *or* a formal IT compliance program.

As another example, although CIOs are generally leading the effort in IT governance, only about half of those with formal IT governance programs have either a formal IT risk management program or a formal IT compliance program. Given the value of IT risk management and compliance programs, as revealed in this report, CIOs have the opportunity to leverage their positions as IT governance leads to convey the importance of initiating and developing these programs.

The IT GRC Environment

In this section, we explore the details of how IT GRC issues are being addressed in higher education, regardless of whether formal GRC programs are in place. We answer the following questions:

- To what extent do institutions try to balance IT risk control and functionality/openness?
- Which IT risks are most important, and how effectively are they being addressed?
- Which frameworks are used to respond to IT risk?
- Which compliance rules or laws are most difficult to address?
- To what extent does IT governance involve other departments in IT decision making?
- Does having a formal IT governance body make a difference for key IT governance functions?
- Is using an IT governance standard associated with key IT governance functions?

The IT Risk Management Environment

Evidence presented later in this report shows that the ways institutions manage IT risk are most important for IT GRC efforts. Therefore, we look separately at several facets of risk management.

Balance of IT Risk Control and Functionality/Openness

In a higher education setting, it is important to focus on the balance between IT risk control on one hand and functionality and openness on the other. Research and teaching both require certain freedoms for exploration and creativity. More open access to data frequently offers certain advantages in producing greater analytics opportunities.[10] However, unless the risk appetite of the institution has been gauged and is understood, accountability for compliance regulations and possible data breaches places CIOs and CISOs in the position of constantly negotiating between security and openness.

Respondents were asked where their institution generally falls in balancing IT risk control with functionality/openness on a slider scale from 0 (risk control is our priority) to 100 (functionality/openness is our priority). Figure 16 shows that responses were fairly normally distributed, with a mean of 56. There were no significant differences based on Carnegie Classification, control (public versus private), or institution size. In addition, for those with formal IT risk management programs, there were no differences dependent on whether the risk management lead is a CISO or a CIO.

Unless the risk appetite of the institution has been gauged and is understood, accountability for compliance regulations and possible data breaches places CIOs and CISOs in the position of constantly negotiating between security and openness.

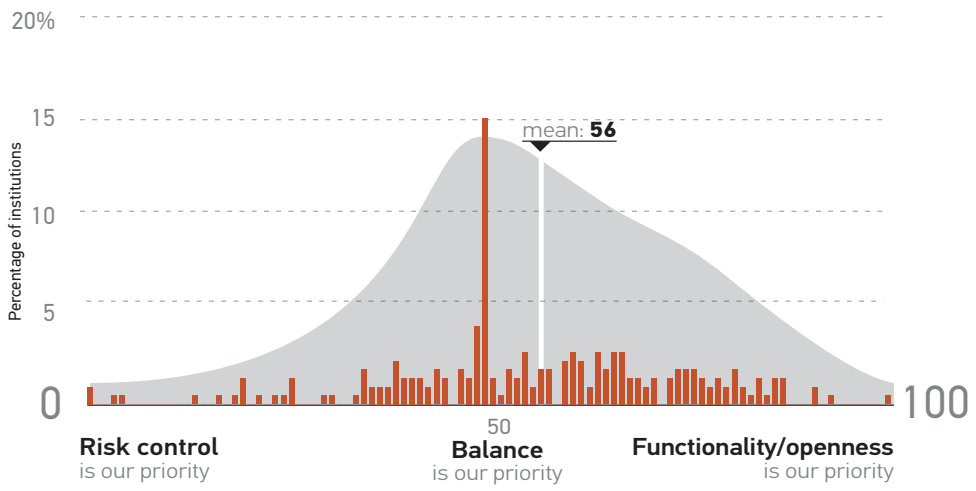


Figure 16. Spread of Respondent Ratings on Their Institution's Balance of IT Risk Control and Functionality/Openness

More responses fall toward the openness side of the scale, indicating a slight preference toward functionality/openness. Few institutions reported extremes in favor of either risk control or functionality/openness. These results may be indicative of a certain level of risk acceptance on the part of most institutions. The baseline of risk management requires accepting certain risks and implementing sufficient controls accounting for those risks.

General agreement that higher education will lean toward openness and functionality makes sense intuitively, and these results may reflect the unique mission of higher education in relation to other industries. The tendency for institutions to report more of a balance may mean that higher education institutions are doing a good job of addressing these competing priorities through compromise. Precisely where in the middle of the scale an individual institution falls may depend on its values and general tolerance for risk. CIOs and CISOs might view their need to negotiate these priorities not so much as a lose-lose situation but as a necessary soft skill in managing IT risk in higher education.[11]

Specific Risks and Institutional Involvement in IT Risk Management

Respondents were asked to indicate the importance of addressing specific IT risks at their institution using a scale from 0 (not at all important) to 100 (very important). They were also asked to assess their effectiveness in addressing these risks on a similar scale from 0 (not at all effective) to 100 (very effective). Figure 17 displays these risks in decreasing order of rated importance. On average, all risks were rated above a moderate level of importance.

Risk management definitions

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.

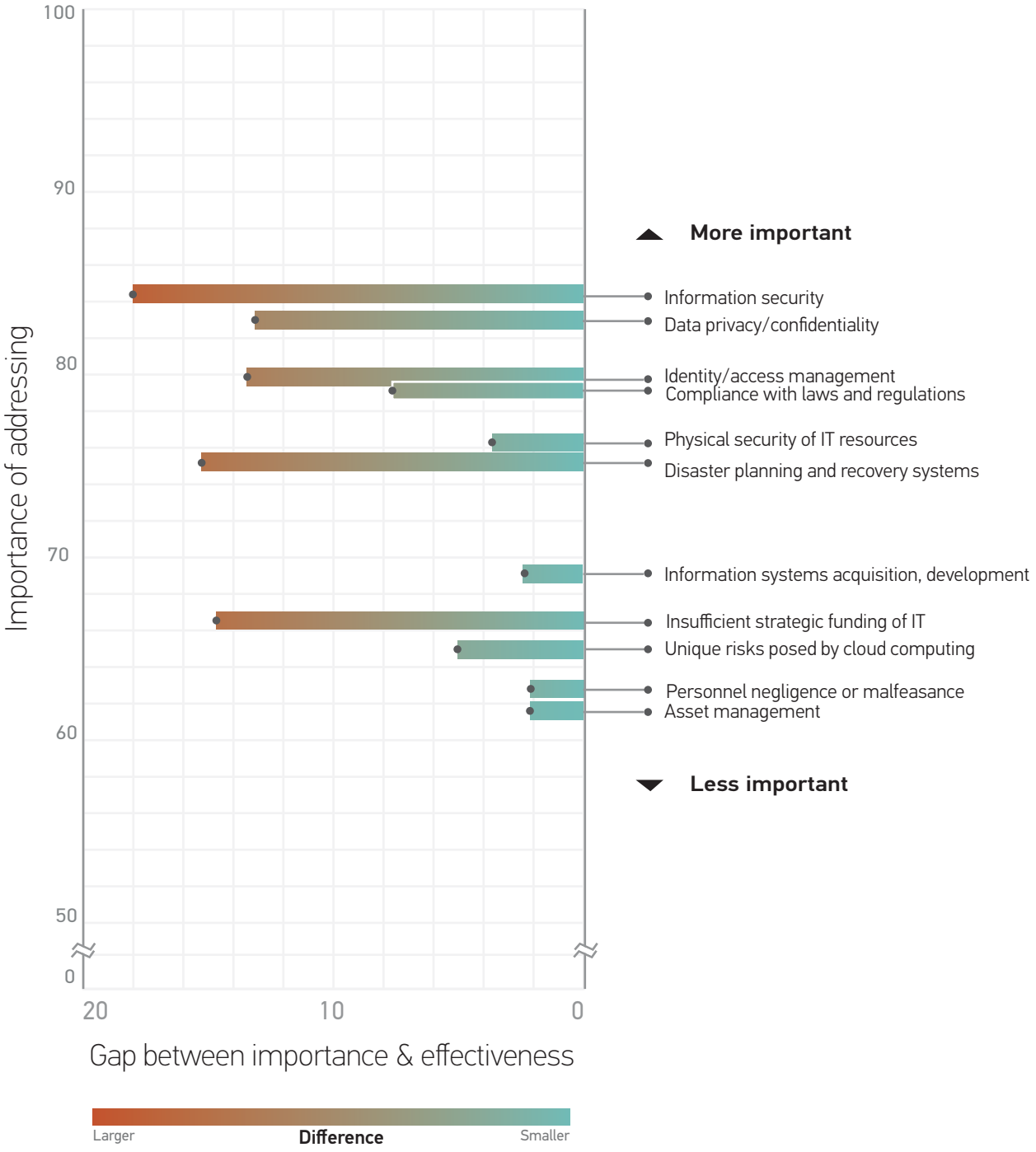


Figure 17. Importance of and Effectiveness in Addressing Specific Risks

Figure 17 also shows the gap between the rating of importance and that of effectiveness for each risk. For example, there is an 18-point gap between the average rating of the importance of information security (84) and the average rated effectiveness with which the risk of information security is addressed (66).[12]

Analyzing the gaps between importance ratings and effectiveness ratings provides insight about the most urgent areas on which to focus to develop or improve risk management programs. The biggest gaps between importance and effectiveness are in the areas of information security, disaster planning and recovery systems, insufficient strategic funding of IT, identity/access management, and data privacy/confidentiality. Several of the widest gaps are among those risks deemed most important. Information security tops the list as the most important risk to address, yet it has the widest gap between its importance and the effectiveness with which it is addressed. Data privacy/confidentiality is another risk deemed very important that is not being addressed as effectively as its importance suggests. These risks were likely deemed the most important in part because they have a high likelihood of impacting the institution's reputation. Assessing and managing these risks should therefore be part of overall institutional strategy.

Information security tops the list as the most important risk to address, yet it has the widest gap between its importance and the effectiveness with which it is addressed.

However, the vast majority of institutions (81%) do not include IT risk in their institution's strategic plan. Assuming technology may be required to complete portions of the project portfolio in the institution's strategic plan, this lack of inclusion creates a potential disconnect between institution strategy and IT execution. IT risk need not be limited to a discussion within IT but should theoretically be included in the larger risk discussion regarding the various strategies involved throughout the institution's risk management ecosystem.

81%
of institutions
do not
include IT risk
in their institution's strategic plan

For most institutions (85%), the management of IT risk is under the purview of central IT (figure 18).[13] This is true whether or not the institution has an enterprise risk management program. Viewed positively, this means that IT has control over the processes involved in IT risk management. However, this may be a reflection of the common belief or approach that IT is something "different" and that only IT professionals can understand or manage something called "IT risk." The fact that investment in IT risk is relatively low (see the later section on maturity) may be evidence of this belief. If IT risk is not integrated with institutional efforts, and if institutional leadership isn't aware of and invested in it, IT risk efforts may not receive the attention and resources needed.

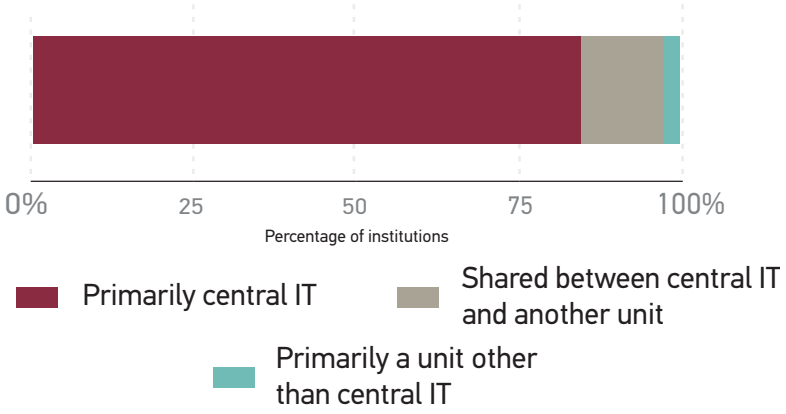


Figure 18. Units Managing IT Risk

Frameworks Used in Responding to IT Risk

Frameworks are references that serve as useful guides for implementing IT risk assessment and management. Frameworks generally include models and processes that are modifiable according to individual operations/organization. Two in three institutions use at least one framework for responding to IT risk, with ITIL topping the list of frameworks used (figure 19). Of those institutions using a framework, more than half (56%) reported using more than one, and nearly a third (30%) reported using more than two.

Institutional Differences in Addressing Specific Risks

For the most part, the perceived *importance* of the specific IT risks queried does not differ between public and private institutions, between institutions of different Carnegie Classifications, or between institutions of varying size. However, the perceived *effectiveness* with which certain IT risks are addressed does differ:

- **Public institutions** rate themselves as more effective at addressing information security, disaster planning and recovery systems, and compliance with laws and regulations.
- **Public master's (MA) and AA** institutions rate themselves as more effective at addressing the physical security of IT resources than do institutions of other Carnegie classes.
- **AA institutions** see themselves as more effective than other Carnegie classes at addressing asset management.
- The **larger the institution**, the more effective respondents rate it at addressing information security.
- **Medium-size institutions** (4,000–14,999 FTE) report being more effective at addressing the physical security of IT resources than smaller (< 4,000 FTE) or larger (> 15,000 FTE) institutions.

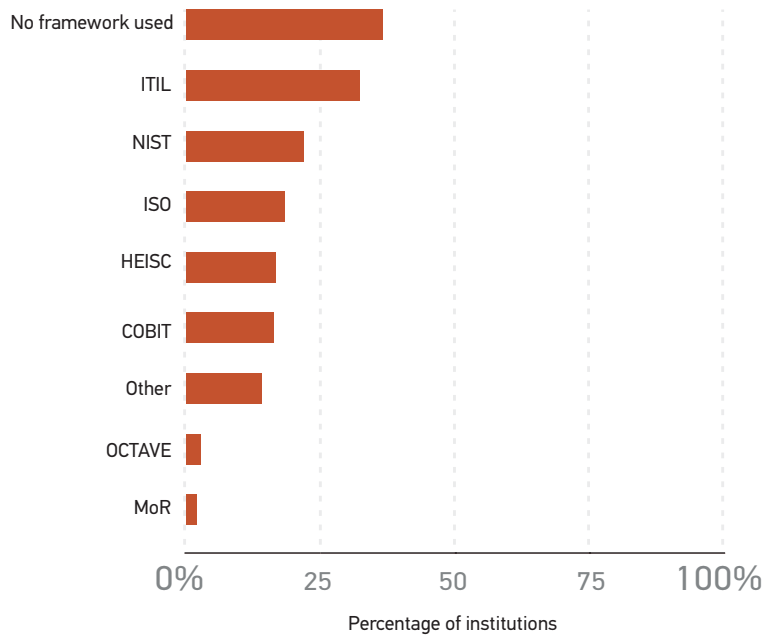


Figure 19. Frameworks Used in IT Risk Management (Multiple Responses Possible)

ITIL: Information Technology Infrastructure Library
NIST: National Institute of Standards and Technology (U.S.)
ISO: International Organization for Standardization
HEISC: EDUCAUSE Higher Education Information Security Council Risk Management Framework
COBIT: Control Objectives for Information and Related Technology
OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation
MoR: Management of Risk (International)

The IT Compliance Environment

Figure 20 displays the percentage of total respondents who agreed with the corresponding statements.

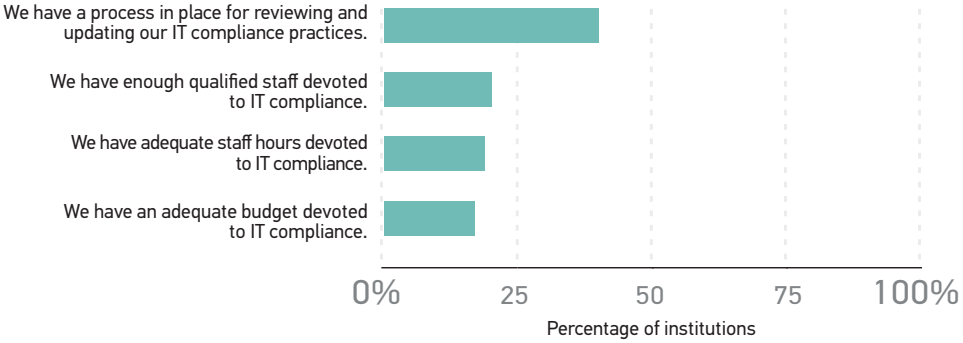


Figure 20. Percentage of Respondents Who Agree with Aspects of the IT Compliance Environment

Only one in five respondents feel there is adequate budget or staffing devoted to IT compliance. Closing this resource gap is one way to facilitate the maturity of IT compliance programs. In addition, the items in figure 20 are all associated with having *either* a formal risk management *or* a formal compliance program in place (either institution-wide or IT-specific).[14] In other words, institutions with a formal risk management or a formal compliance program are more likely to agree that the compliance items in figure 20 are in place.

Which type of program leads to the best IT compliance environment? Further analysis reveals that in a direct comparison of enterprise risk management, IT risk management, institutional compliance, and IT compliance programs, it is best to have an IT compliance program in place for optimal investment in IT compliance. In addition, a program devoted specifically to IT compliance makes it more likely to have a process in place for reviewing and updating IT compliance practices.[15] Therefore, the ideal scenario would be to have a specific program dealing with IT compliance in place to ensure adequate attention to IT compliance processes. However, for institutions with limited resources looking to get started, beginning with risk management may be more realistic, since both risk management and compliance outcomes are more effective with a risk management program in place.

About half (51%) of respondents agreed that the regulatory environment is too complex. Which compliance rules and laws are most difficult to address? Respondents were asked about the level of difficulty their institution was experiencing in addressing specific compliance issues (figure 21). The most difficult compliance issue is the Payment Card Industry Data Security Standard (PCI DSS).[16] This may be because PCI requirements are contractual in nature and the contract elements can change regularly without higher education input, requiring more technical investment. The contract elements for PCI DSS are also relatively more complex than for many of the others. Respondents rated the Family Educational Rights and Privacy Act as the least difficult compliance issue, which may be because FERPA is considered the oldest existing privacy regulation, and IT processes that deal with FERPA data are more integrated into the enterprise. In addition, FERPA is far less "liability rich" than other laws regulating sensitive data.

Figure 21. Difficulty in Addressing the Various Compliance Rules and Laws

PCI DSS: Payment Card Industry Data Security Standard
FISMA: Federal Information Security Management Act
ITAR: International Traffic in Arms Regulations
HIPAA: Health Insurance Portability and Accountability Act
GLBA: Gramm-Leach-Bliley Act
FACTA: Fair and Accurate Credit Transactions Act
FERPA: Family Educational Rights and Privacy Act

Difficulty with compliance rules and laws is not associated with having either a formal institutional or IT compliance program in place. It is, however, related to risk management maturity (discussed later). Therefore, institutions seeking to reduce the difficulty of addressing compliance rules and regulations may look to ensure they have a solid risk management program in place.

Institutions seeking to reduce the difficulty of addressing compliance rules and regulations may look to ensure they have a solid risk management program in place.

The IT Governance Environment

Figure 22 displays the percentage of institutions that involve various units in IT governance for (1) budget/spending decisions and (2) other decisions, broken out by whether they have an ITGB in place.

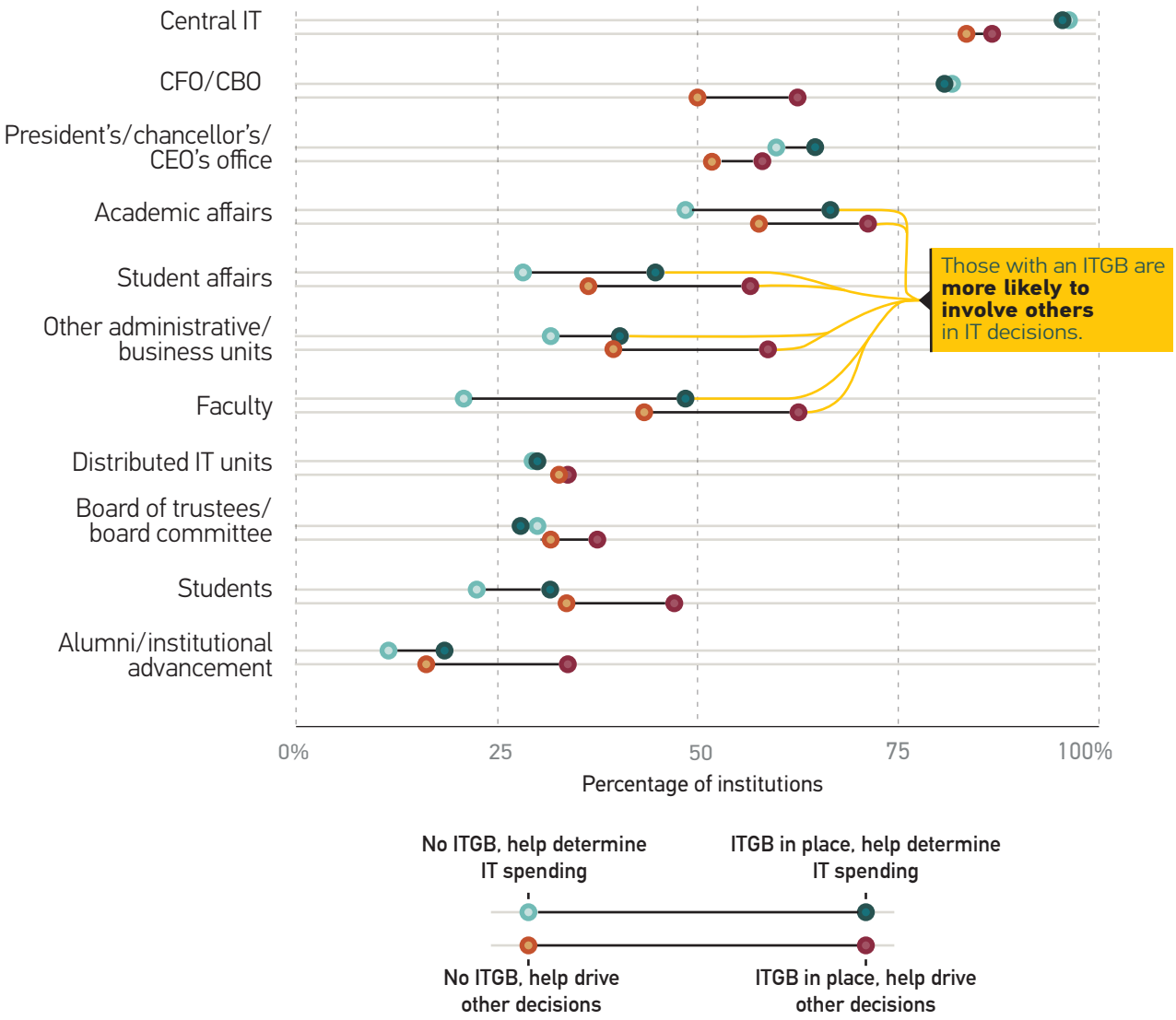


Figure 22. Percentage of Institutions Involving Various Units in IT Governance, Based on Whether an IT Governance Body (ITGB) Is in Place

It makes sense that for most institutions, central IT, the CFO/CBO, and senior leaders are more involved in IT budgeting and spending decisions than they are with other IT governance decisions, and this tends to be true regardless of whether there is an ITGB in place. Those with an ITGB in place, however, are more likely to involve others—particularly faculty, students, and alumni—in both IT budgeting and other IT governance decisions. Involving others in IT decisions can have important ramifications for advocating and communicating IT issues. This increased communication and discussion may influence the culture of acceptance of IT risk management, discussed later in this report.

Respondents were asked how strongly they agreed with a number of statements about IT governance at their institution. Mean responses (on a scale from 0 to 100) are depicted in figure 23, broken down by whether the institution has a formal IT governance body in place.

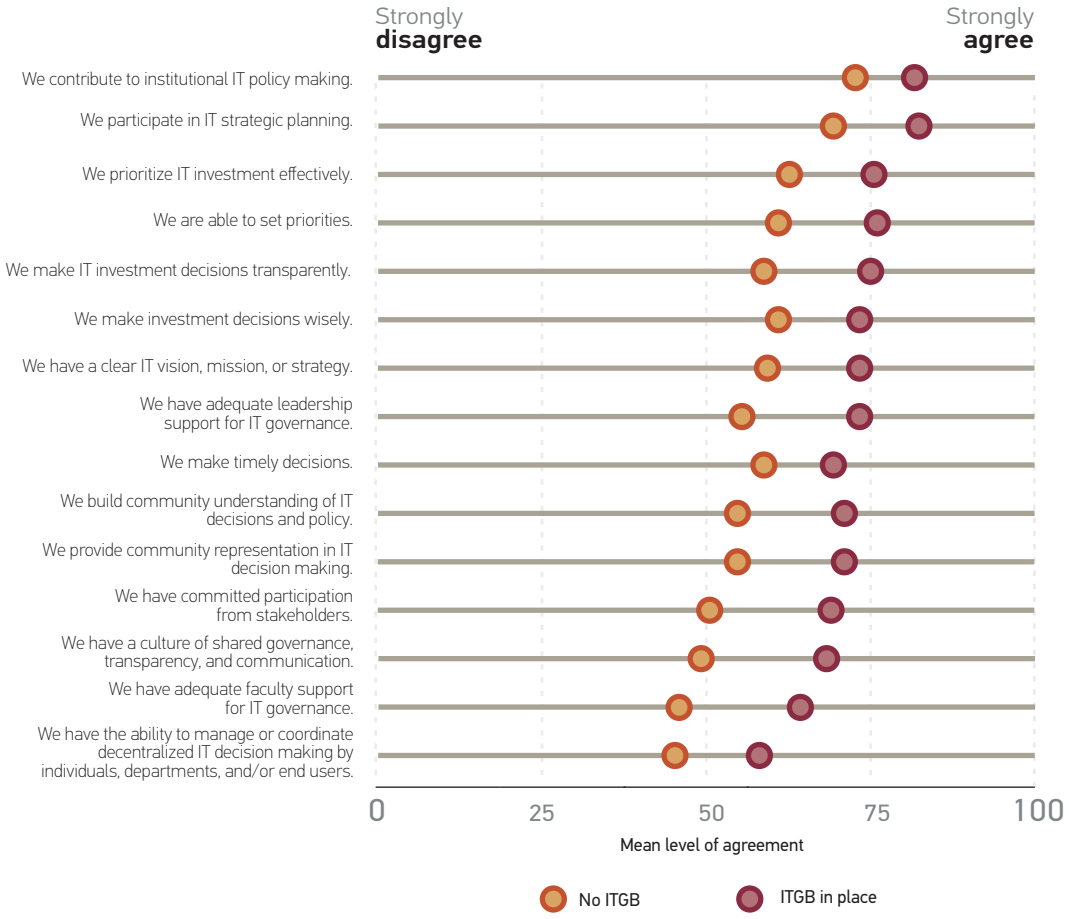


Figure 23. Mean Agreement Ratings for IT Governance Activities

For every governing issue listed, those institutions with a formal ITGB were significantly higher in agreement than those without an ITGB.[17] It appears that IT governance bodies in general are relatively strong on core functions of policy making, strategizing, prioritizing, and investment decisions. Having a formal ITGB makes a significant difference in key IT governance functions.

Figure 24 shows the percentage of institutions using formal frameworks for IT governance. One-third use at least one IT governance framework.

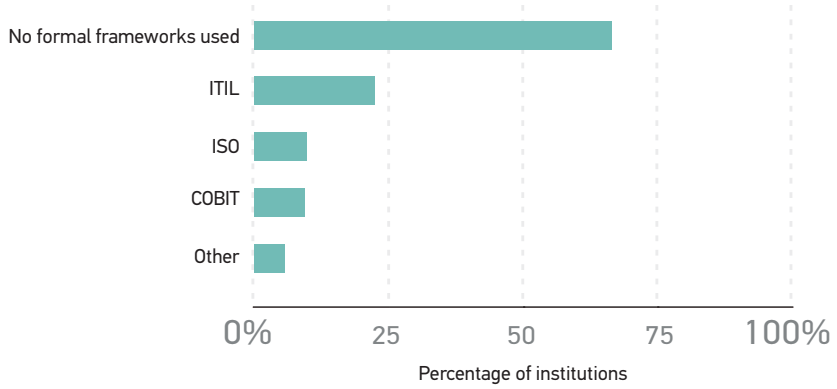


Figure 24. Frameworks Used for IT Governance (Multiple Responses Possible)

ITIL: Information Technology Infrastructure Library
ISO: International Organization for Standardization
COBIT: Control Objectives for Information and Related Technology

Those using a formal framework (any framework) view themselves as significantly more progressive on a number of governance issues (figure 25).[18]

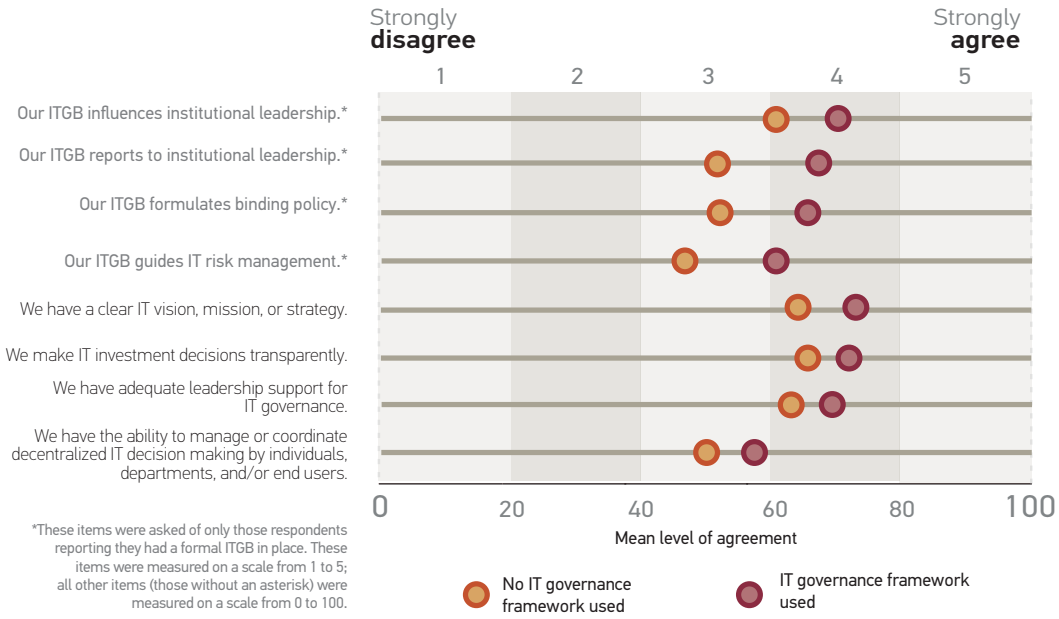


Figure 25. Mean Agreement Ratings for IT Governance Activities, Based on Whether a Governance Framework Is Used

Note: ITGB = IT Governance Body

Maturity in Higher Education IT Risk Management

The maturity indices developed by ECAR serve three functions: First, a maturity index can provide a starting point for institutional leaders to identify the necessary capabilities for progress in an area and to determine the investments needed to achieve a level of progress that aligns with institutional strategy. Second, a maturity index can be used intrainstitutionally to benchmark progress across time or across departments. Third, a maturity index can be used interinstitutionally to provide peer comparisons of progress.

When it comes to IT governance, risk, and compliance efforts, maturity in IT risk management is especially important. Effective technological changes to an institution's delivery of services to students and staff require an interwoven procedure to address potential uncertainty—namely risk assessment, risk mitigation, and risk controls. The "R" in GRC thus becomes a focal point of most institutional efforts. Determining the appetite for risk—the risk culture of an institution—may be the most transparent action any institution can take. The result can affect further actions in response to risk. In addition, an institution can accept a known risk through inaction. Identifying, mitigating, or accepting known risks, intentionally, requires maturity.

Even the "G" in GRC, governance, is—at its essence—implemented to reduce the risk of competing or misaligned strategies. The "C" in GRC, compliance, is a program or effort that not only reduces the risk of an institution's violating a law or regulation but also helps identify whether policies implemented by an institution to reduce a certain risk are actually working. Therefore, it is posited that when seeking to improve maturity in IT GRC, institutions should focus first on maturity in IT risk management.

The survey for this study included multiple items designed to measure maturity in IT risk management. Statistical analyses identified four dimensions: Communication/End-User Management, Acceptance, Risk Assessment/Management, and Investment.[19] The following section reports on maturity scores derived from the items on the GRC survey measuring maturity. Figure 26 displays the means for each of the maturity dimensions that were derived from a factor analysis of the survey items. The survey questions sought the degree of agreement with a number of items on a 5-point scale ranging from 1 (strongly disagree) to 5 (strongly agree). These means represent the risk management maturity of higher education institutions in general.[20]

When seeking to improve maturity in IT GRC, institutions should focus first on maturity in IT risk management.

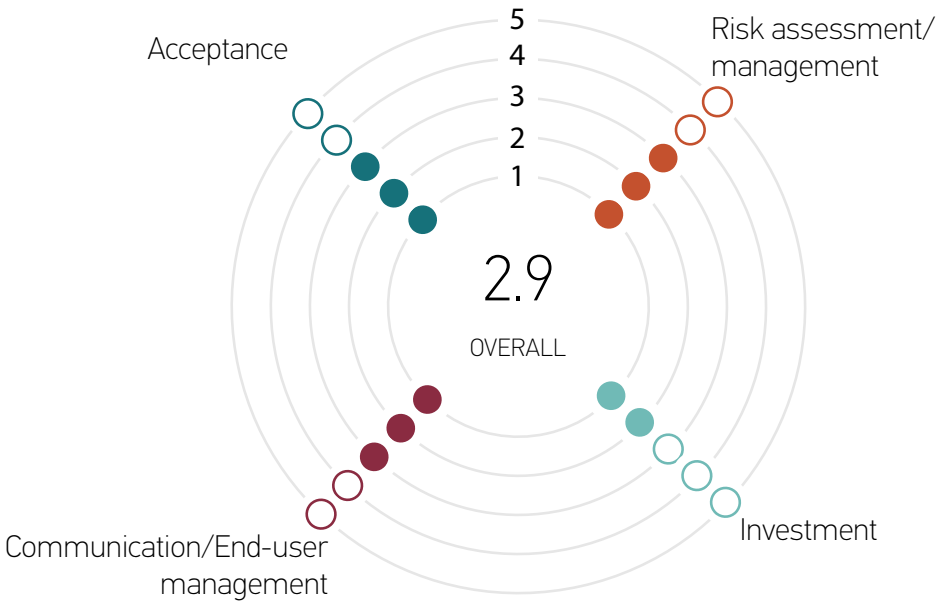


Figure 26. Dimensions of IT Risk Management Maturity

Communication/End-User Management

Figure 27 displays the percentage of respondents who agree or strongly agree with the items making up the Communication/End-User Management dimension. In general, institutions are most mature on this dimension. Four out of five of the items are in place at more than half of responding institutions. However, fewer than half of respondents stated that they effectively communicate about IT risks.

This dimension may be especially important in light of the prominent media attention invariably given to data and security breaches, some among higher education institutions. The role of the IT risk management lead in identifying and mitigating such risks—as well as the reporting line and scope of authority of the IT risk management lead—may be changing in light of this increased media attention. The time may be right to propose new IT risk management programs or processes that extend the authority of the IT risk management lead in managing enterprise and endpoint security, as well as improving communication efforts.

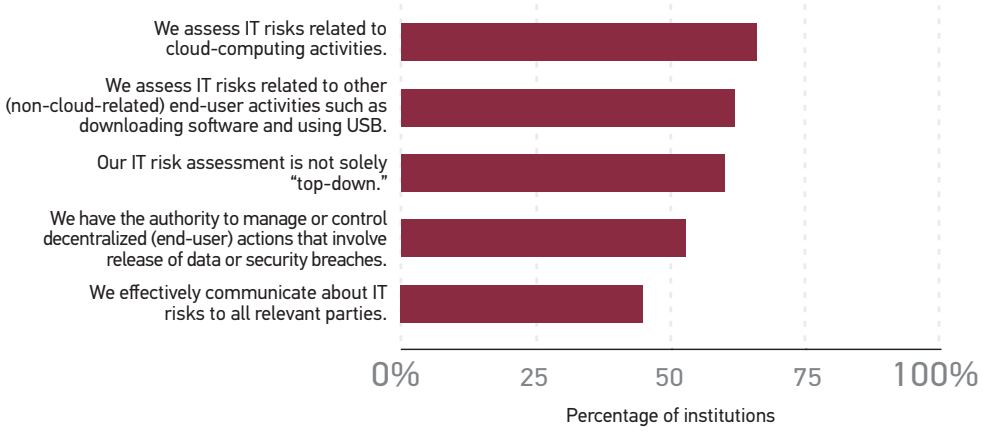


Figure 27. Percentage of Respondents Agreeing That Items Used to Measure the Communication/End-User Management Dimension Are in Place at Their Institution

Acceptance

Figure 28 displays the percentage of respondents who agree or strongly agree with the items making up the Acceptance dimension.[22] Fewer than one-fifth say that either staff or administration is resistant to IT risk management efforts. Faculty acceptance is perceived to be lower; still, a minority of respondents (42%) agree that faculty are resistant to IT risk management. Raising user awareness of IT risk management issues is an important first step toward breaking down acceptance barriers, and it may be the case that better communication about IT risk in general would result in greater acceptance of IT risk management. Indeed, higher scores on the Communication/End-User Management dimension are associated with greater Acceptance ($r = .31$, $p < .001$).

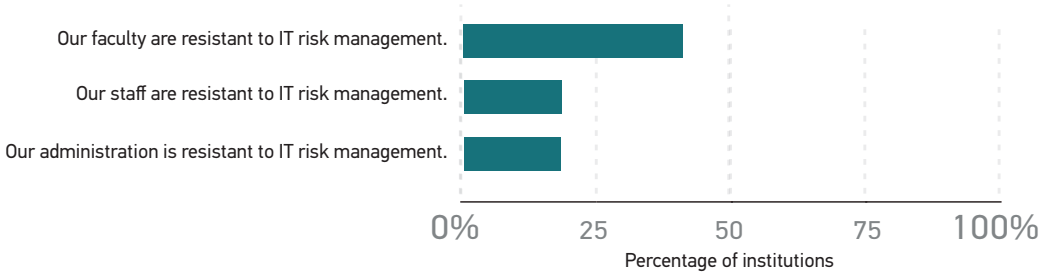


Figure 28. Percentage of Respondents Agreeing with Items Used to Measure the Acceptance Dimension

Risk Assessment/Management

Figure 29 displays the percentage of respondents who agree or strongly agree with the items making up the Risk Assessment/Management dimension. The majority of respondents (60% or more) agree they implement policies and controls in response to IT risk analysis and that IT effectively participates in institutional risk assessment. The remaining items, however, are not in place at the majority of institutions. For example, fewer than half of institutions effectively track and report IT risks (45%) or have a formal procedure for identifying IT risks (44%). This indicates that higher education institutions in general have many areas in which to advance their assessment and management of IT risk.

Figure 29. Percentage of Respondents Agreeing That Items Used to Measure the Risk Assessment/Management Dimension Are in Place at Their Institution

Investment

Figure 30 displays the percentage of respondents who agree or strongly agree with the items making up the Investment dimension. When it comes to risk management maturity, institutions in general are least mature on the Investment dimension. Results show that investment in people and services for IT risk management is generally lacking. Only 1 in 10 institutions report having an adequate budget devoted to IT risk management. These data are consistent with most institutions' lack of inclusion of risk management in the strategic plan and the preponderance of informal risk management programs.

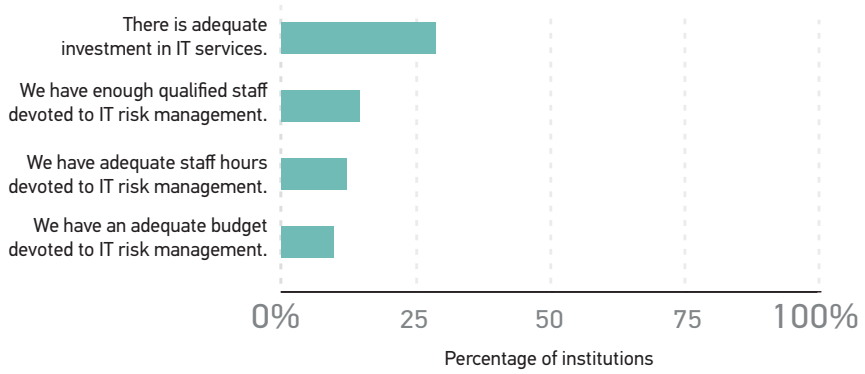


Figure 30. Percentage of Respondents Agreeing That Items Used to Measure the Investment Dimension Are in Place at Their Institution

Relations between Maturity Dimensions and Aspects of the GRC Environment

In this section, we discuss how maturity in risk management is associated with the following:

- Having formal programs in GRC
- The scope of authority of the risk management lead
- The balance between risk control and functionality/openness
- The use of frameworks for risk management
- Effectiveness in addressing specific risks
- IT compliance activities
- Difficulty in addressing compliance rules and laws
- IT governance activities

In general, maturity in risk management is shown to be associated with better practices in all areas of GRC.

IT Risk Management

Institutions with *either* an enterprise risk management program *or* an IT risk management program have higher scores on all four maturity dimensions: Risk Assessment/Management, Investment, Communication/End-User Management, and Acceptance. In addition, those explicitly listing IT risk management as a goal or objective in their institution's strategic plan are more mature in Risk Assessment/Management and Communication/End-User Management.

The scope of authority of the IT risk management lead correlates significantly with Risk Assessment/Management ($r = .37$, $p = .001$), Communication/End-User Management ($r = .24$, $p = .040$), and Acceptance ($r = .35$, $p = .002$). This suggests that institutions that allow risk management leads a broader scope of authority are more mature in their risk assessment and management efforts, are more successful in managing end-user activities, and have greater acceptance of risk management efforts within the institution.

Institutions allowing risk management leads a broader scope of authority are more mature in their risk assessment and management efforts, are more successful in managing end-user activities, and have greater acceptance of risk management efforts within the institution.

When it comes to balancing IT risk control and functionality or openness, the same three maturity dimensions relate: Risk Management/Assessment ($r = –.27$, $p < .001$), Communication/End-User Management ($r = –.26$, $p < .001$), and Acceptance ($r = .15$, $p = .031$). This suggests that those institutions tipping the scale more toward IT risk control than functionality and openness are more mature in risk assessment and management, have more control over end-user activities, and have greater acceptance of risk management.

When institutions not using a framework for risk management were compared with those who used a framework (any framework or multiple frameworks), institutions using a framework were more mature on the dimensions of Risk Assessment/Management ($t = 7.17$, $p < .001$); Investment ($t = 3.43$, $p = .001$); and Communication/End-User Management ($t = 4.20$, $p < .001$). No differences were found for the Acceptance dimension.

All four maturity dimensions are significantly related to the effectiveness with which institutions perceive themselves to be addressing the specific IT risks mentioned earlier (table 1). This finding enhances our confidence in the validity of these maturity dimensions. Institutions seeking to improve the effectiveness with which they address these specific risks will be able to find concrete steps toward progressing in risk management in ECAR's forthcoming Risk Management Maturity Index, which will be based on these dimensions.[23]

Table 1. Correlations between Maturity Dimensions and Perceived Effectiveness in Addressing Specific Risks

Type of IT Risk	Communication/ End-User Management	Acceptance	Risk Assessment/ Management	Investment
Information security	.51***	.25***	.43***	.38***
Physical security of IT resources	.38***	.19***	.30***	.22***
Identity/access management	.30***	.17***	.26***	.23***
Disaster planning and recovery systems; business continuity	.43***	.25***	.46***	.29***
Data privacy/confidentiality	.39***	.27***	.38***	.26***
Insufficient strategic funding of IT	.31***	.18***	.30***	.40***
Compliance with laws and regulations	.38***	.27***	.39***	.30***
Personnel malfeasance	.37***	.17***	.40***	.25***
Asset management	.44***	.14***	.40***	.23***
Information systems acquisition, development, and maintenance	.45***	.23***	.37***	.31***
Unique risks posed by cloud computing	.44***	.30***	.37***	.26***

****p < .001; n = 239–245*

IT Compliance

All of the IT compliance variables listed in figure 20 and here again in table 2 are associated with all four dimensions of risk management maturity. In other words, having a solid IT risk management program is associated with adequate investment in IT compliance and having processes for reviewing and updating IT compliance practices. This may be because, as stated in the Introduction, compliance acts as a risk control, since violations of laws, regulations, or internal policies are risk issues.

Table 2. Correlations between Maturity Dimensions and Compliance Activities

Aspects of IT Compliance Environment	Communication/ End-User Management	Acceptance	Risk Assessment/ Management	Investment
We have a process in place for reviewing and updating our IT compliance practices.	.53***	.22***	.65***	.44***
We have adequate staff hours devoted to IT compliance.	.49***	.27***	.51***	.53***
We have enough qualified staff devoted to IT compliance.	.43***	.31***	.52***	.57***
We have an adequate budget devoted to IT compliance.	.44***	.28***	.48***	.63***

****p ≤ .001; n = 239–243.*

As mentioned previously, difficulty with compliance rules and laws is not associated with having either a formal institutional or IT compliance program in place. In other words, having a formal institutional or IT compliance program does not reduce the difficulty in addressing compliance issues. This difficulty is, however, related to maturity in risk management, particularly the Acceptance and Investment dimensions (table 3).[24] The greater the acceptance of risk management within the institution and the greater the investment in risk management, the less difficult it is to address compliance issues. Again, communication about IT risk (as well as associated compliance issues) may be the key to expanding acceptance. This is more evidence that getting one's risk management ducks in a row should be the priority when initiating or enhancing GRC programs.

Table 3. Correlations between Maturity Dimensions and Difficulty in Addressing Compliance Rules and Laws

Compliance Rules and Laws	Communication/ End-User Management	Acceptance	Risk Assessment/ Management	Investment
PCI DSS	–.14*	–.26**	–.11	–.30**
U.S. state privacy and data protection laws	–.20**	–.16*	–.17*	–.24**
FISMA	–.10	–.23**	–.10	–.14
Your institution's IT policies	–.31**	–.16*	–.19**	–.17**
HIPAA Security Rule	–.11	–.20**	.02	–.15*
GLBA	–.14	–.19*	–.05	–.16*
HIPAA Privacy Rule	–.11	–.17*	–.00	–.15*
FACTA Red Flags Rule	–.10	–.20*	–.03	–.17*
FERPA	–.18**	–.28**	–.11	–.12

**p < .05; **p < .01; n = 160–241*
PCI DSS: PCI Data Security Standard
FISMA: Federal Information Security Management Act
HIPAA: Health Insurance Portability and Accountability Act
GLBA: Gramm-Leach-Bliley Act
FACTA: Fair and Accurate Credit Transactions Act
FERPA: Family Educational Rights and Privacy Act

IT Governance

Leadership influence is strongly associated with maturity in risk management. All four risk management maturity dimensions (Communication/End-User Management, Acceptance, Risk Assessment/Management, and Investment) are associated with the extent to which the ITGB influences leadership (table 4). In fact, all of the items in figure 23 are associated with maturity in risk management. Good IT governance and good IT risk management clearly go hand in hand.

Table 4. Correlations between Maturity Dimensions and Governance Activities

Statements about IT Governance	Communication/ End-User Management	Acceptance	Risk Assessment/ Management	Investment
We contribute to institutional IT policy making.	.36**	.25**	.28**	.08
We participate in IT strategic planning.	.37**	.33**	.33**	.16*
We prioritize IT investment effectively.	.47**	.31**	.36**	.23**
We are able to set priorities.	.45**	.29**	.35**	.25**
We make IT investment decisions transparently.	.46**	.22**	.34**	.16*
We make investment decisions wisely.	.42**	.28**	.34**	.20**
We have a clear IT vision, mission, or strategy.	.33**	.38**	.30**	.25**
We have adequate leadership support for IT governance.	.37**	.40**	.38**	.38**
We make timely decisions.	.36**	.28**	.33**	.20**
We build community understanding of IT decisions and policy.	.37**	.38**	.36**	.23**
We provide community representation in IT decision making.	.22**	.17**	.19**	.08
We have committed participation from stakeholders.	.42**	.42**	.44**	.31**
We have a culture of shared governance, transparency, and communication.	.37**	.37**	.34**	.26**
We have adequate faculty support for IT governance.	.29**	.40**	.29**	.31**
We have the ability to manage or coordinate decentralized IT decision making by individuals, departments, and/or end users.	.29**	.40**	.29**	.31**

**p < .05; **p < .01; n = 235–245*

Conclusions

Formal IT GRC programs are in the beginning stages of development in higher education. Although institutional governance bodies are common, IT governance is less so, and although informal methods of dealing with IT risk and compliance are found at many institutions, formal IT risk management and compliance programs are the exception rather than the rule. Managing IT governance, risk, and compliance issues is generally under the purview of the CIO and/or the CISO, though the maturity of IT GRC practices potentially impacts the entire institution.

GRC in higher education can better unite institutional strategy with IT execution. Investment in purposeful risk management activities can reduce vulnerabilities that attend any new technology, thereby reducing the risk profile. Merging IT execution with institutional strategy can require transparency in known risks as well as an attendant risk control plan, best achieved with a formal risk management program.

The rudiments of a GRC program may already exist within any enterprise. Most institutions have an institutional governance body in place, and more than half have an IT governance body. In addition, nearly half have either (or both) a formal IT risk management or a formal IT compliance program. These programs may lay the groundwork for an institution trying to move toward a common vision of GRC process. Institutions looking to create or enhance formal GRC programs may look to the factors in this report that point toward success:

- Better communication about IT risk throughout the institution, which may result in a less resistant risk management culture and enhanced end-user management
- The institution of effective processes to identify, track, report, prioritize, and respond to IT risks
- The involvement of leadership in IT GRC efforts
- Adequate investment in budgets and staff behind GRC programs

In addition, consider the following steps in getting started with IT GRC:

- Assess existing governance, risk, and compliance efforts and determine how they might be combined or leveraged to create efficiency and value.
- If certain GRC policies are already in place (e.g., to protect data or require certain types of security at the end-user stage), assess how compliance with those policies is measured. Assess whether an IT GRC framework or program may help measure the effectiveness of risk-reactive policies like this that are already in place. These types of assessments help establish the value of using IT GRC frameworks or establishing IT GRC programs.

- Start with risk management. The language of risk management is familiar to most in higher education, even those without formal training. A solid risk management program can provide the framework for other IT governance and compliance efforts.[25]
- Take steps to ensure leadership buy-in for GRC efforts. It may help to take a page from ECAR's report on analytics: Start with a strategic problem.[26] This may involve showing leadership the consequences of not having a formal risk management determination and how these consequences may impact the institution's strategic initiatives.[27]
  - Example 1: A researcher buys health data (containing millions of data points) with a grant. The insurance companies he purchases from have not verified that the data are de-identified or de-individualized. What risks are there to the institution? How does the assessment and management of these risks impact the institution's reputation or other strategic initiatives?
  - Example 2: Your state has passed student success legislation or an accreditation agency is insisting on proof of student success, which mandates that your institution show how institutional benchmarks are achieved for each student or program. Your counseling department has reviewed and proposed the purchase of an integrated planning and advising service (IPAS) system that requires a significant extract of student data, including personally identifiable information, to be uploaded to a cloud provider on a weekly basis. What governance process is in place that will approve or reject this proposed system? How will any associated risks be assessed and controlled?
- Assess your institution's risk management maturity with ECAR's forthcoming Risk Management Maturity Index.[28]

Recommendations

- **When embarking on IT GRC initiatives, priority should be given to establishing or strengthening the risk management program.** Maturity in risk management is associated with stronger IT compliance and governance processes.
- **CIOs have the opportunity to leverage their positions as IT governance leads to convey the importance of initiating and developing formal IT risk and compliance programs.** Formal programs in risk and compliance are associated with more investment and better practices in IT risk and compliance.
- **Give risk management leads a broad scope of authority by providing leadership support in managing institutional response to risk.** A broad scope of authority is associated with more-mature risk assessment and management, better end-user control, and less resistance to risk management efforts.
- **Bring IT risk into the institution's strategic planning discussion.** Most institutions do not include IT risk in the strategic plan, and this lack of inclusion creates a gap between institution strategy and IT execution. Inclusion may improve acceptance of IT risk management efforts across the institution.
- **Take steps to improve communication efforts regarding IT risks to all relevant parties.** Better communication may result in greater acceptance of IT risk management across the institution.
- **Gauge your institution's awareness and acceptance of IT risk.** Surveys are a valid form of awareness training; a survey, among other awareness activities, may reveal current perceptions or the level of risk acceptance.
- **Invest in formal frameworks for IT GRC efforts.** Institutions using a framework (any framework, e.g., ITIL, NIST, ISO, COBIT, HEISC) show more progress in their risk management efforts. They are also more likely to formulate binding policy, guide IT risk management, and report to and influence institutional leadership.
- **Institute a formal IT governance body.** Those institutions with formal ITGBs are more effective in their IT governance activities and involve others more in IT governance decisions, enhancing communication and awareness of IT governance issues.

Methodology

The survey data reported are based on 246 respondents, except where indicated. Survey invitations were sent to all EDUCAUSE primary representatives with instructions to solicit input from leads for risk management, compliance, or governance programs where applicable. Table A summarizes respondents by Carnegie Classification and institution size. Data collection took place during the first quarter of 2014. The margin of error for the survey is 6%.[29]

Table A. Survey Respondents

		Carnegie Classification									Total
		AA	BA Public	BA Private	MA Public	MA Private	DR Public	DR Private	Other	International	
Student FTE	Unknown	1	1	1	1	0	0	1	9	24	38
	Less than 2,000	4	2	25	0	7	0	1	3	0	42
	2,000–3,999	9	1	23	2	18	0	2	3	0	58
	4,000–7,999	8	1	0	9	8	2	4	0	0	32
	8,000–14,999	6	0	0	8	1	7	6	0	0	28
	15,000+	8	0	0	4	1	30	5	0	0	48
Total		**36**	**5**	**49**	**24**	**35**	**39**	**19**	**15**	**24**	**246**

Acknowledgments

This report resulted not only from the efforts of the co-authors but also from the contributions of several individuals both within and outside EDUCAUSE. The subject matter experts for this study, **Cathy Hubbs** (Chief Information Security Officer, American University), **Joanna Grama** (Director of DRA Operations, IT GRC and Cybersecurity Programs, EDUCAUSE), **Steve McDonald** (General Counsel, Rhode Island School of Design), and **Madelyn Wessel** (Associate General Counsel, University of Virginia), helped shape the content of the survey and report through their constructive feedback. The ECAR review team of **Eden Dahlstrom**, **Ron Yanosky**, and **Susan Grajek** provided many substantive comments and edits that improved the report immensely. **Ben Shulman** reviewed or provided the statistical analyses for the report. **Kate Roesch** created or stylized all graphics. **Gregory Dobbin** provided much assistance with editing and content changes for publication. Finally, **Ashlan Sarff** and **Lisa Gesner** worked to promote the survey and the report.

Notes

1. "Elephant and the Blind Men," traditional Jain story, http://www.jainworld.com/literature/story25.htm.
2. John A. Wheeler, *Hype Cycle for Governance, Risk, and Compliance Technologies, 2013*, report (Stamford, CT: Gartner, 2013), available from https://www.gartner.com/doc/2557320/hype-cycle-governance-risk-compliance.
3. Diana Oblinger, "Getting Your Ducks in a Row: Governance, Risk, and Compliance," *EDUCAUSE Review* 48, no. 6 (November/December 2013), http://www.educause.edu/ero/article/getting-your-ducks-row-governance-risk-and-compliance.
4. For all private versus public comparisons, private for-profit institutions are excluded because their sample size (n = 6) was too small for comparison. Therefore, references to "private" institutions refer to private not-for-profit institutions only.
5. The difference between the percentage of public and private institutions having formal IT risk management programs is only marginally significant, $p = .053$.
6. All of the Euler (Venn) diagrams used in this report were created using euler*APE*. See Luana Micallef and Peter Rodgers, euler*APE*: Drawing Area-Proportional 3-Venn Diagrams Using Ellipses, PLoS ONE, 2014, http://www.eulerdiagrams.org/eulerAPE.
7. These data roughly correspond to findings from the 2013 EDUCAUSE Core Data Service.
8. The non-IT officer most often specified was an elected or appointed chair, many times a faculty member.
9. There may be slight differences from data reported elsewhere in the report due to rounding.
10. Jacqueline Bichsel, *Analytics in Higher Education: Benefits, Barriers, Progress, and Recommendations*, research report (Louisville, CO: ECAR, 2012), http://www.educause.edu/library/resources/2012-ecar-study-analytics-higher-education.
11. For more information on the importance of soft skills in higher education IT, see Jacqueline Bichsel, *Today's Higher Education IT Workforce*, research report (Louisville, CO: ECAR, 2014), http://www.educause.edu/library/resources/today%E2%80%99s-higher-education-it-workforce.
12. Importance ratings were higher than effectiveness ratings for all risks.
13. The origins of GRC activity in IT are evident in organizations outside higher education. In a study of GRC-related activities in industry, the majority of organizations reported that GRC activities "started within the IT function" and that GRC activities were "primarily contained within the IT function." See Ponemon Institute, *The Role of Governance, Risk Management & Compliance in Organizations: Study of GRC Practitioners*, research report (Travis City, MI: Ponemon Institute, May 2011), http://www.emc.com/collateral/about/news/ponemon-report-egrc.pdf.
14. All four programs were significantly correlated with all four outcomes.
15. Beta weights for each of the four types of programs were compared in a multiple regression analysis for each compliance outcome measure.

16. For more information on PCI DSS, see the PCI Security Standards Council website, https://www.pcisecuritystandards.org/security_standards/.

17. Analyzed with multiple t-tests, $p < .001$ for each test except the nonsignificant item, where $p = .86$.

18. For more information on how frameworks can help with IT governance, see Eugene Wessels and Johan van Loggerenberg, "IT Governance: Theory and Practice" (proceedings of the Conference on Information Technology in Tertiary Education, Pretoria, South Africa, September 18–20, 2006), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.2838&rep=rep1&type=pdf.

19. Dimensions identified with a principal component analysis, Varimax rotation with Kaiser normalization. One identified dimension measuring technology was dropped because it didn't provide increased predictive value, it contained only two items, and it explained relatively little of the overall variance in risk management maturity.

20. Means for each dimension were obtained by calculating the average score (for all institutions) for the items making up that dimension. The overall mean is an average of the dimensional means: Communication/End-User Management = 3.46, Acceptance = 3.17, Risk Assessment/Management = 3.11, Investment = 2.30.

21. For example, Target has elevated the position of its new CIO after its recent well-publicized data breach. See Howard Baldwin, "The Other Shoe Drops for Target's CIO," *Forbes*, March 11, 2014, http://www.forbes.com/sites/howardbaldwin/2014/03/11/the-other-shoe-drops-for-targets-cio/.

22. Scores on the Acceptance dimension were reversed to make them comparable with the direction of the other dimensions (1 = least mature; 5 = most mature).

23. "ECAR Risk Management Maturity Index for Higher Education," maturity index (Louisville, CO: ECAR, forthcoming).

24. International data-protection laws and ITAR (International Traffic in Arms Regulations) were excluded from these analyses because of their relatively low *N*.

25. For more information on getting started in risk assessment, see Joanna L. Grama, *Legal Issues in Information Security* (Sudbury, MA: Jones & Bartlett Learning, 2011); Judith A. Pirani, *Learning While Doing: Two Institutions' Practical IT Risk Management Experiences*, research bulletin (Louisville, CO: ECAR, July 29, 2013), http://www.educause.edu/library/resources/learning-while-doing-two-institutions%E2%80%99-practical-it-risk-management-experiences; and Patrick J. Feehan, "Higher Education IT Compliance through the Prism of Risk Controls," *EDUCAUSE Review* 48, no. 6 (November/December 2013), http://www.educause.edu/ero/article/higher-education-it-compliance-through-prism-risk-controls.

26. Bichsel, *Analytics in Higher Education*.

27. For other ideas on how to discuss IT risk with leadership, see Janice M. Abraham, *Risk Management: An Accountability Guide for University and College Boards* (Washington, DC: AGB Press, 2013), 41–43, http://agb.org/store/risk-management-accountability-guide-university-and-college-boards.

28. "ECAR Risk Management Maturity Index."

29. Margin of error is based on estimating proportions/percentages for a sample size of 246.