Governance, Risk, and Compliance:

Why Now?

By Joanna Lyn Grama and Rodney Petersen

Governance, risk, and compliance (GRC) issues are increasingly pervading the IT space, with these concepts transcending silos such as central and distributed IT units, information security, and service management. As campus investment in information technology and campus reliance on information systems have grown, so has the need for reliable structures and measures to ensure success and minimize failure. GRC programs intend to do just that: they develop a framework for the leadership, organization, and operation of the institution’s IT areas to ensure that those areas support and enable the institution’s strategic objectives. As EDUCAUSE President and CEO Diana Oblinger notes, GRC programs are about “getting your ducks in a row.” GRC programs align institutional activities with the larger institutional goals (i.e., governance) and allow the identification of challenges and opportunities (i.e., risk). When internal requirements and external mandates are lined up (i.e., compliance), institutional activities have the best chance for success—especially in stormy weather or where danger lurks.
This issue of EDUCAUSE Review is devoted to better understanding the role of GRC programs in higher education IT organizations.

Governance
At its core, a governance program ensures that all institutional activities are aligned with the institution’s business goals. For higher education IT organizations, IT governance means ensuring that the campus IT strategy is aligned with the institution's strategic plan. Information technology thus becomes a strategic partner in the institutional mission.

Governance is not a new concept for information technology, yet many colleges and universities still struggle with effective governance. The 2013 EDUCAUSE Center for Applied Research (ECAR) report on measuring IT costs in higher education found that only 10 percent of the responding institutions reported very effective IT governance programs; 61 percent of institutions reported having an ineffective or only somewhat effective IT governance program. Many institutions have information security governance, data governance, enterprise system governance, and identity governance programs. What is unique about IT governance, as opposed to these specialized governance areas, is that it looks at top-level IT goals, assigns responsibilities for meeting those goals, and assesses the results within the context of the institutional strategic plan.

Risk
Colleges and universities have a history of equating risk management with its insurance practices—that is, of identifying certain types of risk and then purchasing insurance to mitigate the impact of those risks. Common risks to insure against include accidents in the workplace, theft, mechanical failure, and natural disasters. IT organizations also have a history of risk management practice, most notably in the information security practice area. Risk identification, prioritization, and response activities (together called “risk assessment”) are foundational concepts in risk management practices.

Enterprise IT risk management helps an institution identify the risks that it faces with regard to its IT resources and systems and affirmatively address those risks in a way that satisfies its overall goals. Enterprise IT risk management programs move beyond information security risks and look at the strategic, financial, legal, operational, and reputational risks inherent in operating IT systems.

KPMG International conducted a survey of C-suite industry executives in late 2012. Almost half of the C-level executives responding to that survey indicated that risk management is essential for adding business value to their organizations, and nearly 40 percent of the respondents said that risk management considerations are often factored into the organization’s overall strategic planning decisions. There is a gradual movement at colleges and universities to embrace enterprise IT risk management as a more holistic approach to understanding a variety of risks across the institution and prioritizing strategic resource allocation accordingly.

Compliance
An enterprise compliance program is generally defined as a formal program that specifies the organizational activities designed to help prevent and detect violations of applicable laws and regulations. For higher education IT organizations, compliance means ensuring that the institution’s IT resources and systems are operated in a way that meets the laws and regulations impacting those systems and that also complies with institutional policy.

Increased regulatory requirements and renewed enforcement efforts that scrutinize college and university practices are a sign of the times. In May 2013, for example, a state university agreed to pay $400,000 to the U.S. Department of Health & Human Services (HHS) to settle alleged violations of Health Insurance Portability and Accountability Act (HIPAA) regulations.

The future of the profession is going to require new backgrounds and new experiences that enable IT professionals to apply a GRC lens to IT decision-making.
of 1996 (HIPAA) Security Rule due to a breach of unsecured electronic protected health information at an outpatient clinic operated by the university.1

Ironically, legislative, regulatory, and contractual compliance issues are burdening colleges and universities at the same time that higher education institutions are under increased pressure to reduce costs. To add to this complexity, IT compliance may be but one element of a multi-faceted institutional compliance program.

The Importance of a Concerted GRC Effort Now

Various independent activities within EDUCAUSE have addressed and continue to address GRC topics. For instance, the EDUCAUSE Resource Library has a number of IT governance resources, and the topic was the subject of a 2008 ECAR study. The Higher Education Information Security Council (HEISC) was early to recognize the need for a risk management framework to guide institutional risk management efforts in information security. And EDUCAUSE policy activities have long been conducted in partnership with other organizations to study and advise on the laws and regulations that might inform institutional compliance activities. These independent efforts have been successful and strong.²

In the summer of 2013, EDUCAUSE conducted a survey asking our members how important GRC is currently and how important it will become. We knew, going into the survey, that governance issues are very important to higher education IT leaders. For instance, since 2000, strategic IT governance themes have been present every year in the EDUCAUSE annual list of “Top-10 IT Issues”: funding IT strategically (2000–2013); strategic planning / integrating IT into institutional decision making (2000–2007, 2010–2012); institution-wide IT governance (2004–2012); and cloud strategy (2004–2013).³

From the survey, we learned that our members think GRC is an important area for EDUCAUSE to emphasize. Our members also indicated that they would find toolkits, frameworks, templates, topical training, and whitepapers most useful to inform their own GRC programs. Through discussions with members of the EDUCAUSE IT Issues Panel and in conversations with our members, we learned that the need for IT governance may continue to grow—especially as IT organizations are tasked with demands to use information technology to support strategic missions, as they face greater regulatory mandates and increased fines for noncompliance, and as they address the requirement to constrain or reduce costs at the same time. We have also heard that the need for effective governance and risk management programs is becoming part of “business as usual” for higher education IT leaders, yet our data illustrate a gap between this need and what is currently in place. In short, the stakes are high for the effective operation of higher education IT organizations. IT GRC programs can help level the playing field, and higher education needs resources and support to introduce these programs.

In 2014, EDUCAUSE will build on its already well-established and successful programs and will more keenly focus on IT GRC topics to build a suite of resources for higher education IT professionals. Initial efforts will concentrate on defining IT GRC in a way that makes sense for higher education institutions. After that, EDUCAUSE will work to strengthen its reservoir of best practices, toolkits, and case studies to help institutions define and implement IT GRC activities on their own campuses. EDUCAUSE will also study and benchmark how higher education institutions are currently approaching IT GRC practices.

Historically, job requirements for IT professionals have emphasized computer skills, technical competencies, and/or academic degrees in computer science or engineering. The future of the profession, however, is going to require new backgrounds and new experiences that enable IT professionals to apply a GRC lens to IT decision-making. By exploring how to build effective IT GRC programs, EDUCAUSE can help these leaders, managers, and users of information technology as they shape strategic IT decisions at every level within higher education.

Notes
© 2013 Joanna Lyn Grama and Rodney Petersen. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs (by-nc-nd) 3.0 Unported License.

Joanna Lyn Grama (jgrama@educause.edu) is Director of IT GRC and Cybersecurity Programs for EDUCAUSE.

Rodney Petersen (rpetersen@educause.edu) is Senior Policy Advisor for SecuriCORE.

© 2013 Joanna Lyn Grama and Rodney Petersen. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs (by-nc-nd) 3.0 Unported License.