Getting Your Ducks in a Row: Governance, Risk, and Compliance

Information technology is critical to higher education. But unless aligned with the institution's goals and based on 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.

In their introduction to this theme issue of EDUCAUSE Review, Joanna Lyn Grama and Rodney Petersen provide the rationale for GRC programs: “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.”

First is governance. “IT governance means ensuring that the campus IT strategy is aligned with the institution's strategic plan,” according to Grama and Petersen. In “Speaking the Same Language,” Mike Chapple illustrates alignment through a data governance model: “First, placing ‘Access to Data’ at the top of the model communicates a clear end-goal of the program: providing individuals who have legitimate business needs with the ability to access the data they need in a timely, effective manner. Second, placing ‘Technology’ at the base of the model conveys that data governance programs are not all about technology. Although technology may serve as a foundational tool for the development of strong data practices, these remain business processes that are supported by technology,” Chapple adds: “Data governance cannot be successful without IT leadership.” The first duck in the row is governance.

Second is risk. Risk management helps an IT organization identify its risks and address them in a way that is aligned with the institution's goals. Managing risk is about optimizing the institution. “Allocating resources to manage the risks in the right places allows campus administrators to spend their limited resources on the things that are critical to the institution's mission and to the achievement of its plans,” according to Janice M. Abraham, Robert Baird, and Frank Neugebauer. In “Leveraging Enterprise Risk Management,” the coauthors also remind us: “Institutional leaders are evaluating not only the downside of risk (i.e., what could go wrong) but also the upside—the opportunities presented by taking on additional risk.” Boards may ask, for example, “Is the institution taking enough risk with its IT strategies?” However, IT risk isn't only about information technology. The scope of enterprise risk management programs is broad, encompassing the strategic, operational, financial, legal, and reputational risks associated with information technology. Information security, for example, depends on human behavior; it is not just about technology. The second duck in the row is risk.

Risk leads to the third component, compliance. As Patrick J. Feehan writes in the final feature article: “IT compliance begins with risk. . . . [We must] understand the risks that we seek to manage down the path of IT compliance.” We comply with laws and regulations to avoid risk and penalties. IT compliance ensures that the institution's IT resources and systems are operated in a way that meets laws and regulations and that complies with institutional policy. Compliance goes beyond the usual acronyms such as FERPA, HIPAA, and PCI. It is complicated by the cloud, BYOD, third-party apps, and people. It can consume an enormous amount of time and resource. And, when not done well,
it poses significant risk. Thus, as Feehan warns: “The risk assessment of any proposed technology-centric activity has to have a broad vision, be collaborative, and not be limited to technology.” The third duck in the row is compliance.

If information technology is to advance higher education, governance programs must align information technology with institutional missions, goals, processes, and procedures to ensure the best outcomes. Doing so means avoiding unnecessary risks while taking on those that could bring value. And it means having an integrated, holistic, and proactive system that ensures compliance—not just with rules but also with the values that undergird the academy. GRC can be a compass that we use to guide our plans, decisions, and actions.

As Abraham, Baird, and Neugebauer explain: “Identifying and managing future risk is not a matter of clairvoyance. Rather, it involves the diligent exercise of watching what’s happening elsewhere.” The same is true for the entire GRC process: it’s about getting your ducks in a row.

**Diana G. Oblinger** (doblinger@edugcause.edu) is President and CEO of EDUCAUSE.

© 2013 Diana G. Oblinger. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs (by-nc-nd) 3.0 Unported License (http://creativecommons.org/licenses/by-nc-nd/3.0/).