IT Governance, Risk, and Compliance at Case Western Reserve University

ECAR

SNAPSHOT | August 6, 2014

Thomas Siu, ~~Sheriff~~ Chief Information Security Officer

What does IT GRC look like at your institution?

Our core IT governance committee is the Information Technology Services Planning and Advisory Committee (ITSPAC), put into place about a decade ago. This committee has subcommittees, including Security, IT Policy, Compliance, and various other groups that represent other schools and departments, which push content to the Priority Review Board and the Executive Steering Committee. This method of governance helps prioritize what IT does for the university; brings into alignment the IT initiatives put forward by each of the schools; and links these efforts to the university objectives. We gain traction in getting cooperation on our IT policies by involving faculty in ITSPAC and asking for feedback, as opposed to merely announcing policies. These processes also help increase efficiency and reduce costs across the university; for example, when we see that multiple departments require the same service, we can contract from a single vendor and get better rates than we would if each department contracted individually.

Describe ownership and authority in each of the areas of IT GRC.

ITSPAC is currently headed by the chief academic technology officer, who reports to the CIO. The Executive Steering Committee consists of the CIO, the CFO, the chief administrative officer, and the provost. Security and IT Policy are subcommittees of ITSPAC headed by the CISO (me). We also have a compliance officer who works in legal counsel. Risk is managed by both legal counsel and treasury. The CISO, however, works cooperatively with these departments on issues of risk and compliance. In general, IT GRC officers, including the CISO, have a broad scope of authority. For example, I have the authority to deny someone IT services. It's a big hammer that is used rarely, but it is indicative of the scope of authority I am allowed to ensure compliance. The CISO reports to the CIO, who has in-depth involvement with ITSPAC.

How does your institution prioritize IT GRC concerns?

IT prioritizing for major projects occurs at the level of the Executive Steering Committee. For smaller projects, the various committees representing ITSPAC are involved with setting priorities. Assessment of priorities often involves assessment of risk. As the CISO, I prioritize IT risks, as well as define the taxonomy and the methods used to address these risks. I help coordinate non-IT risks, as well. As a private university, Case Western takes an approach to IT compliance that can be more flexible than that of public institutions. For example, we don't have to adhere to laws mandating IT security training for faculty. However, there are enough compliance rules and laws we do have to comply with, the specifics of which often conflict with one another. Here, risk assessment comes into play as well. Our institutional values determine our risk umbrella, which tell us, for example, when and to whom to disclose certain

EDUCAUSE

information. Some types of risk are easily quantified (e.g., in terms of monetary loss), but much of IT risk is qualitative in terms of measuring value. For example, value is realized when you have made people happy with a new policy or purchasing decision, and that is difficult to quantify.

Do you use any specialized software or system for any or all of the GRC functions?

We do not use specialized software or systems for IT GRC, but we've started to use SPARTA for research compliance. SPARTA is a planning tool for proposal writers that allows them to see who else is writing in the same area to possibly form collaborations. It also provides a more comprehensive picture of certain details (e.g., who is involved in research, who has or needs training, which research projects are dealing with sensitive information) to better address research risk, compliance, and security issues.

What factors are used to determine which risks are addressed and how much risk is acceptable?

We have a security risk management policy that determines which risks are high, medium, and low. The language in the policy also prescribes actions to take. We assess the level of threat and decide whether to accept, watch, research, or mitigate the risk. Security risks generally take priority; for other IT risks, it's really a matter of negotiation between our IT leaders in terms of how risks are addressed. For example, there can be huge risks in outsourcing, but we have decided to take more of these risks because there is a consensus among our IT leaders that there is real value in outsourcing that is worth the risk. The value is assessed by how well outsourcing aligns with our key strategies.

What are the pain points of your institution's GRC strategies, programs, and processes?

I wish there were more people involved on our ITSPAC committees; for example, I would like to see more faculty participation. It has been difficult to convey to them their stake in IT GRC. One of the biggest problems is departments that procure IT hardware or software on their own through various vendors and then expect to be supported. We have begun to address this issue by forming better relationships with these departments and keeping them more informed. My wish list for IT GRC would include more people as well—specifically, staff who can help integrate outsourced products and processes into our IT environment. I would also like to see more proactive risk management instead of reactive risk management. Risk management should not be problem management; rather, it's the probability of a problem happening, and you need experienced people who can make that determination.

What do you see as the future of IT GRC at your institution?

I don't see us going toward tools at present, though they could help us quantify risks better. The mind-set of our institution is leaning toward accepting more risks, so I am focused on thinking about the really bad things that can happen in each situation and mitigating the risk if possible. I see us developing more comprehensive and cooperative plans and strategies for proactively dealing with and evading risk. Part of that will be having more conversations about our values and integrating those into our risk equation.

For more information, visit the following web pages

- ITSPAC IT Governance at Case Western Reserve University 2014
- ITSPAC Subcommittees 2014
- IT Policies
- Information Security: Risk Management Policy
- University Compliance Program
- Office of Risk Management and Insurance (focus on insurance and financial risk)