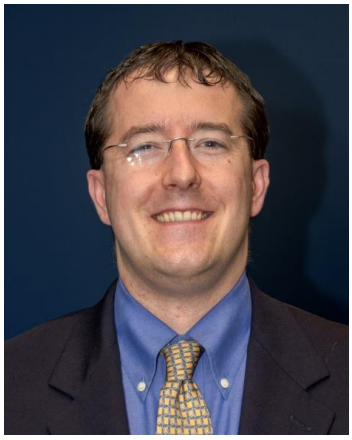
IT Governance, Risk, and Compliance at Saint Louis University

ECAR

SNAPSHOT | August 6, 2014

Nick Lewis, Director, IT Security and Compliance



What does IT GRC look like at your institution?

IT governance is managed through our Executive Technology Advisory Committee (ETAC), led by Vice President and CIO David Hakanson. The committee works on IT strategy for the university and IT governance decision making. A number of groups across campus report to ETAC, including the IT Security and Compliance Committee, which is made up of representatives from Academic Affairs, the Compliance Office, General Counsel, Human Resources, the Research Office, Risk Management, the Office of the University Registrar, and IT. The focus of this committee is on IT security and compliance risk, and we are currently working on a risk management plan, which entails defining acceptable risk, increasing awareness of risks, and outlining risk that needs to be supported. Although no formal enterprise risk management program exists, there is a person who oversees risk management for the university, and that person works closely with the IT Security and Compliance Committee. A university compliance program (largely focused on HIPAA, billing, and research compliance) is also represented on the committee.

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

ETAC is led by the vice president and CIO. I lead the IT Security and Compliance Committee and report to the deputy CIO. These groups triage GRC issues and report them to the CFO, the president's office, and other executive staff, where the authority resides to ensure compliance. Our recent interim president was general counsel, who supported more funding and positions for IT GRC, which is improving and broadening the scope of IT GRC.

How does your institution prioritize IT GRC concerns?

The IT Security and Compliance Committee helps prioritize risk issues and decide which of them need to be forwarded to ETAC or the executive staff committee, which includes the president and vice presidents. In the planning stages are new methods of quantifying risks and losses, determining who can accept a risk, and developing a risk management plan that would mitigate risks and losses. We are also planning to include more representatives from across campus in these discussions.

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

We use the NIST (National Institute of Standards and Technology) framework for risk management. We've had discussions about using COBIT and other frameworks. Our philosophy is that it is not so important which framework you use but that you choose something and stick with it. We did try some software at one point for GRC, but we discovered that the software was designed for GRC programs that

were more mature than ours. We have recently decided to seek a tool that better fits our institution, and we plan to implement that in the near future. We are hoping that a tool will help us address GRC communication and management efforts across the institution. For example, if a compliance law changes, we need a tool that will help us identify all the areas that are affected by this change, the updates that need to be made, and the costs involved, as well as manage the necessary changes.

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

There are two areas of the university where we have been doing formal risk assessment: (1) a research area with a formal requirement for a risk assessment, and (2) our medical center, which involves specific legal risks and policies associated with electronic health records. We identify the gaps that exist and prioritize based on those gaps. Then we identify which security and controls need to be implemented. This is mostly done on a case-by-case basis. If there is an issue (e.g., we think a department or researcher is accepting too much risk or that the proposal they're offering for addressing risk is not adequate), then we address it at the level of the IT Security and Compliance Committee. What we are still finalizing in our IT security risk management plan is documenting this process in the risk register, including the level of risk and whether we think the plan for addressing it is acceptable. If we don't agree that the proposal for risk management is acceptable, we will address it at the department or individual level first before taking it to the executive leadership level; often, what is needed is simple communication and information about the consequences of not addressing particular risks. Frequently, which risks are addressed also depends on the sensitivity of the information involved.

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

We need more coordination between our GRC committees and better processes for triaging and addressing IT security risk issues. We also need to improve the processes for "reporting up" risks to leadership. We need more formal documented processes in place to ensure leadership involvement, particularly with a new president. The real challenge for us right now is communication and general agreement on the processes used to address IT GRC issues. We also need greater awareness of the risks associated with dealing with or sharing certain types of sensitive data. For example, we have researchers dealing with health data they have been amassing over long periods of time. We need to better convey to researchers, research departments, the IRB, and others that, when dealing with these types of sensitive data, they need to be in communication with us, and we will then determine what needs to be communicated to ensure they are addressing the risks associated with this data for their own and the institution's protection.

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

Our previous method of assessing IT risk was based purely on a financial model, which was not a good model and method for us. We are restarting efforts in this area and working on a formal IT risk management framework that will document who is qualified to assess and accept risk, as well as how we will quantify some risks. We are also working on formal processes that will identify and document the data we have. This is not for monitoring purposes per se, but so we can better identify areas in which we need to focus our security efforts.