

Enterprise Risk Management
Keith R. Bushey
George Mason University

In many instances risk assessment projects conducted at higher institutions of learning are elaborate paper drills designed primarily to satisfy an outside audience, such as an auditor. In a system driven by centralized review of risk, it makes sense to summarize and prioritize so that decisions can be made that address the “most critical” risks to the enterprise as a whole. Unfortunately, this approach can leave the concerns of many individual departments, schools or even colleges out of the final risk analysis. George Mason University recently took a different approach to evaluating risk by implementing a series of in depth personal interviews with key stakeholders whose operations were determined to present the highest risk to the university should they fail or be severely compromised.

Introduction of the Organization

George Mason University has locations in three Virginia counties: Arlington, Fairfax, and Prince William. In 2005 the university began offering courses in a fourth county, Loudoun, and opened a campus in the United Arab Emirates in the fall of 2006. While each campus has a distinctive academic focus, the Fairfax Campus offers the majority of courses and is the only location that offers resident housing. Founded in 1972, the public university is considered a major educational force both regionally and nationally and has a reputation as an innovative, entrepreneurial institution. Mason has received national distinction in a range of academic fields. The university is accredited by the Commission on Colleges of the Southern Association of Colleges and Schools to award bachelors, masters and doctoral degrees. Enrollment at Mason passed the 30,000 student enrollment mark in fall 2006.

Problem/Initiative

University risk assessment projects are often driven by a need to satisfy an external requirement, such as an auditor's report. While reams of documents or an exhaustive collection of "plans" may satisfy an external audience, they are generally impractical to implement without a significant investment of resources. Additionally, large sets of plans prepared by people with very different viewpoints tend to overwhelm with mind numbing detail those who attempt to evaluate them, or conversely are subject to such generalizations as to make them of limited practical use. In the usual university-wide risk assessment project, department heads may devote significant time and effort to fill out myriad forms, yet their unit level problems never make it to the top of the priority list.

High priority items given funding are frequently the central ones, rather than those identified by the units, because they affect more people and processes. When an institution has limited resources to dedicate to risk remediation, it makes sense to give the highest priority to the “most critical” risks to the enterprise as a whole. Unfortunately this approach can have at the very least the appearance, if not in fact the reality, of leaving the concerns of many individual departments, schools, and even colleges out of the final risk analysis.

The challenge of collecting interpretable data from a diverse group of individuals is quite difficult. Department heads understand the university’s need to address risk as well as their own responsibility in that mission. However, they are not highly motivated to invest their time in completing forms that traditionally result in little direct benefit to their units.

To address this issue Mason’s President established the Executive Enterprise Risk Management Group (EERMG) under the leadership of the Senior Vice President for Finance and Administration. The EERMG was charged to assess risks in the area of information technology, physical risks and risks from departmental procedures and processes. Its membership reflects these charges. The Senior Vice President for Finance and Administration has an enterprise view of a variety of administrative offices as well as auxiliary enterprises, such as the book store, housing, and athletics. The Vice President for Information Technology and Chief Information Officer (CIO) is also the University’s Chief Security Officer. The Chief Safety Officer is responsible for emergency preparedness planning and for physical security. The Director of Internal Audit and Management Services is responsible for ensuring good business practices are followed.

The Controller is responsible for effective financial controls and the Executive Director of the ITU Security and Project office, who reports to the CIO, is responsible for cyber security policies and planning.

Design

Rather than require every department in the University to fill out risk assessment forms, the EERMG members first dedicated their own time and energy to identifying which departments were most relevant to business continuity. The group then prioritized the list of departments and developed a timeline by which the top fourteen departments would be assessed. They also established a four year review cycle, during which all fourteen departments and associated subdivisions would be assessed. Throughout the cycle, departments where significant risks are identified will be revisited to monitor progress on remediation of those risks.

Implementation

The Chief Safety Officer and the IT Security Coordinator head up the risk assessment team. Their assessment includes an investigation of physical, process, and personnel security, as well as IT security. The process is iterative. It begins with the distribution of a standard 20 page risk assessment questionnaire, followed by at least one two-hour interview. The team is available to assist the department head in completing the questionnaire before the scheduled interview.

The risk assessment questionnaire begins with the office's mission and a request for the office to list critical assets. Questions follow under the categories of physical security, including staffing, building, and workplace procedures, while electronic security covers account and password management, virus protection, data backup and recovery,

operating systems and application software. In addition, confidentiality and protection of sensitive data, security awareness and education, the Gramm Leach Bliley Act (GLBA) and Family Education Rights Privacy Act (FERPA) requirements are reviewed.

The two members of the risk assessment team visit each department and conduct interviews to clarify questions and conduct on site security assessments. By engaging the various department heads and their senior staff members in a discussion about the answers to the questionnaire, the two interviewers are able to concentrate on identifying not only specific risks, but also general themes that could affect the university as a whole.

The personal approach allows the interviewers to make suggestions for addressing problems at the time of the interview rather than assign blame for deficiencies, as so often happens in an impersonal report. Because of the length and the complexity of some of the questions, a second interview session is initially scheduled for approximately two weeks following the first interview. While the second session is not always used, it does allow for additional work to be done by the department to address questions not fully answered during the first interview. The feedback from department heads has been very positive.

Benefits

The direct interaction between the interview team and the department heads allows immediate clarification of questions and provides instant feedback on findings. It also encourages frank discussion of issues in a non threatening environment. These are factors that are not present when using a paper based process.

With the support of the EERMG, when a risk is identified that should be quickly corrected, the interview team can request resource allocations to address the issue outside

the normal budget process. That capability obviously has a positive impact on the way department heads view the interview process. Several examples where the team provided assistance include improvements in building access control, installation of fire suppression equipment and changes in work hours to provide greater personnel security.

Because of their training and experience, the team is also able to make suggestions in regards to procedures. These procedural tweaks usually cost nothing to implement, but can quickly correct deficiencies or otherwise improve the unit's risk profile.

Retrospect

If we were to begin anew, we would conduct a pilot study to validate the questions. During the first few interviews we determined that several questions were difficult to understand or perhaps too esoteric from the interviewee's perspective. The original version also included questions that turned out to be redundant or contradictory. Changes were made before the third departmental interview, so in essence the first two departments served as our "pilot" study.

Since part of the process included educating department heads in areas they were not familiar with, it would have been beneficial to have provided some basic background readings to acquaint them with any new concepts before asking them to complete the questionnaire. Sometimes their "education" was accomplished in a phone conversation before the first interview and sometimes it was part of the actual interview process. By establishing a common knowledge base via the readings we could have immediately

addressed the actual issues and spent less time on establishing a basic knowledge level during the interview.