The Evolution of Enterprise Risk Management – A Case Study

By Seth Kornetsky, CIA, CFE

It was at a May 2001 audit committee meeting when I first heard Tufts' external auditor mention Enterprise Risk Management (ERM). I remember the perplexed look on the faces of the senior managers and audit committee members as the audit partner valiantly tried to extol ERM's virtues, walking us through a 20-page handout which explained the theory behind it. According to the partner, ERM was the wave of the future; a systematic, focused approach to anticipating and managing the operating, compliance, reputational and strategic risks that our university would likely face in the years ahead. Perhaps the timing was bad (we were still battle-fatigued from our university-wide effort to avert "Y2K" disaster on January 1, 2000), but the concept of ERM was not a big sell among the group. By the end of the meeting, and based on comments afterward, it was evident senior management and the audit committee members had concluded that ERM was yet another attempt by the external auditor to increase consulting income by promoting the latest management improvement technique (TQM was not yet a distant memory). It was enough of a challenge to provide the required administrative resources to support the academic enterprise and research; there was no time to assess probabilities and impacts and contemplate risk appetites! Besides, when necessary, a committee or task force could be easily convened to address any significant challenge or crisis.

> First, we had to get our own house in order by implementing a more formal risk-based approach to our audit planning process.

Fast forward almost a decade to a cultural shift. Slowly, risk assessment is becoming part of Tufts management's lexicon as ERM is becoming more prevalent among institutions of higher education. How did the university get to this point? Several years ago, realizing that a top-down directive to incorporate a structured risk assessment process with the university's strategic and operational planning was unlikely any time soon, we decided that Internal Audit would at least plant the seed by becoming an early adopter of ERM in terms of our auditing approach. If we were successful, we could lead the way for others within the university community to adopt concepts of ERM as part of their management activities. First, we had to get our own house in order by implementing a more formal risk-based approach to our audit planning process. To accomplish this objective, we developed a database designed to capture our institution's audit universe and incorporate a risk-based ranking model that would inform the annual audit plan. The database records, encompassing approximately 200+ distinct areas of audit focus, comprise Tufts University's financial, regulatory and research administrative processes, operations and information management systems. The records also include major departments and centers with significant assets or that receive considerable amounts of federal, state or private funding. We ranked (and continue to update) each database record relative to two major risk components which also incorporate five risk drivers:

- **Inherent Risk**, which addresses the likelihood and impact of an adverse event occurring absent any internal controls designed to manage, transfer or eliminate the risk. The following risk drivers help to assess the degree of inherent risk within a particular area or activity:
  1. Degree to which the operating unit, business process or information system supports a major Tufts administrative activity and/or the institution's research or academic mission
  2. The risk of fraud
  3. The risk that the University's reputation (based on the organization's external visibility) could be tainted due to non-compliance with state or federal regulations or the failure to demonstrate good business ethics
- **Residual Risk**, which addresses the likelihood and significance of the same adverse event occurring after evaluating the effectiveness of the internal controls designed to mitigate or eliminate the inherent risk. The following risk drivers are used to assess the degree of residual risk within a particular area or activity:
  4. The quality of controls based on the results of the last audit
  5. The date of the last audit (areas not audited for some time are assumed to have a potentially higher risk profile; accounting for this as an assumption, this risk driver is weighted only 50%)

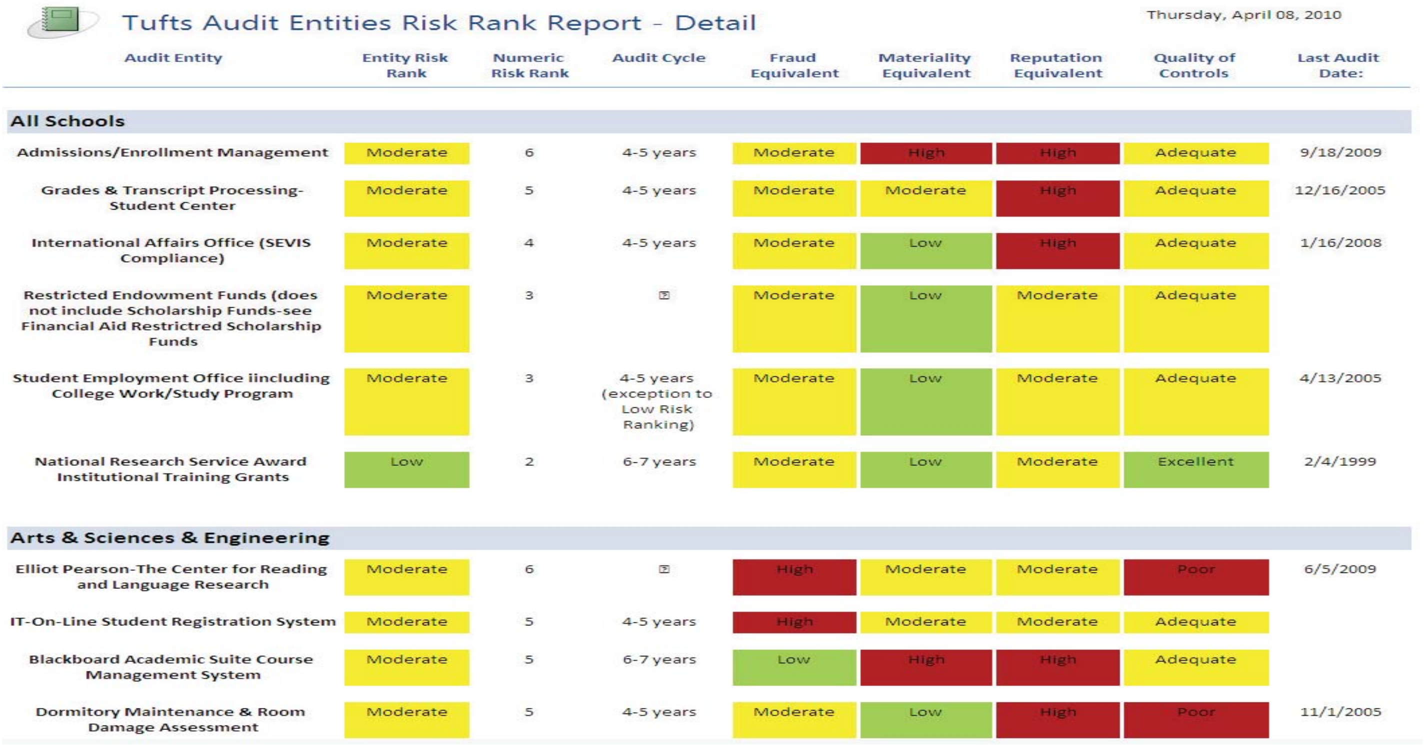
Using a ranking formula, the impact of the above-mentioned criteria results in an audit plan score that falls into a risk range of 'high,' 'medium' or 'low.' The higher the score, the greater the risk noted. Areas that score in the high and medium range are prioritized for internal audits.

ABOUT THE AUTHOR

***Seth Kornetsky**, CIA, CFE has served as Director of Audit & Management Advisory Services at Tufts University for the past 12 years. He has held several ACUA board positions and is a past president. Seth has also chaired the Professional Education Committee and been a past presenter at the Annual Conference. He has certification as a CIA and CFE. Seth has a Masters of Business Administration from Babson College. When not tending to audit matters he tends to his vegetable garden in western Massachusetts.*

(continued on page 17)

(continued from page 16)



Tufts Audit Entities Risk Rank Report - Detail

Thursday, April 08, 2010

Audit Entity	Entity Risk Rank	Numeric Risk Rank	Audit Cycle	Fraud Equivalent	Materiality Equivalent	Reputation Equivalent	Quality of Controls	Last Audit Date:
All Schools								
Admissions/Enrollment Management	Moderate	6	4-5 years	Moderate	High	High	Adequate	9/18/2009
Grades & Transcript Processing-Student Center	Moderate	5	4-5 years	Moderate	Moderate	High	Adequate	12/16/2005
International Affairs Office (SEVIS Compliance)	Moderate	4	4-5 years	Moderate	Low	High	Adequate	1/16/2008
Restricted Endowment Funds (does not include Scholarship Funds-see Financial Aid Restrictred Scholarship Funds	Moderate	3	⍰	Moderate	Low	Moderate	Adequate	
Student Employment Office iincluding College Work/Study Program	Moderate	3	4-5 years (exception to Low Risk Ranking)	Moderate	Low	Moderate	Adequate	4/13/2005
National Research Service Award Institutional Training Grants	Low	2	6-7 years	Moderate	Low	Moderate	Excellent	2/4/1999
Arts & Sciences & Engineering								
Elliot Pearson-The Center for Reading and Language Research	Moderate	6	⍰	High	Moderate	Moderate	Poor	6/5/2009
IT-On-Line Student Registration System	Moderate	5	4-5 years	High	Moderate	Moderate	Adequate	
Blackboard Academic Suite Course Management System	Moderate	5	6-7 years	Low	High	High	Adequate	
Dormitory Maintenance & Room Damage Assessment	Moderate	5	4-5 years	Moderate	Low	High	Poor	11/1/2005

Snapshot of Risk Database

BABY STEPS TO ERM

Subsequent to improving our approach to risk-based audit planning, we embarked on a dual strategy to promote the practice of risk assessment throughout the university. Given the existing complex, decentralized culture, we deliberately chose an incremental approach. We sensed that the executive management in place at the time was not yet persuaded of the need to participate in a structured forum where higher level operating and strategic risks might be discussed. Instead, on a one-to-one basis, we informally engaged Tufts vice presidents, senior managers and executive deans of administration in what the consultants refer to as a "risk conversation." We used these meetings as an opportunity to describe the risk model we were using and within this context, sought their input concerning the areas they perceived as at risk and "audit-worthy." We continue to use these annual meetings to educate our colleagues about the components of risk and prompt them to express any concerns about their schools or divisions in terms of strategic, operational and reputational risk probability and impact.

Concurrent with this strategy we developed an approach to promoting ERM on a local level by offering to facilitate risk assessment forums for clusters of academic department administrators at each of Tufts' schools. Department chairpersons were also encouraged to participate in the risk assessment forums. We realized that the majority of our clients would more easily identify with the concepts of ERM by applying them to their daily administrative responsibilities such as grants administration, regulatory compliance oversight, budget monitoring and reporting, personnel management, information security, records retention, etc. We still offer this option; each risk assessment forum is broken into two sessions of no more than 2-3 hours each. The first session is used to identify the top 5-10 inherent risks which the participating departments commonly share that could have a negative impact on successfully managing operations, regulatory compliance obligations, funding streams, environmental safety and other administrative activities. After identifying these risks, the participants are asked about the policies, procedures and other internal controls they currently employ in their departments to effectively manage or eliminate the identified risks. At the second session, weaknesses identified in current administrative practices pertaining to the identified risks lead to discussions and brainstorming concerning recommendations to address the issues. The recommendations are summarized in a report to senior school management as collectively addressed from the group. The risk assessment process is periodically offered as an alternative to a traditional audit; thereby leveraging resources and allowing for a more collective assessment by the individuals whose administrative practices are being reviewed.

TAKING ERM TO THE NEXT LEVEL

With the two strategies taking hold in modeling the concepts of ERM, it was time to take it up a notch by taking advantage of an established meeting structure that included all Tufts vice presidents, members of the Office of the Provost and the executive administrative deans from each of the schools. Known as the Administrative Council, the group meets monthly to discuss topics of interest and exchange information to promote administrative excellence and academic support. The Council represented an excellent opportunity to promote ERM at a higher administrative level to identify certain strategic and key operating risks and evoke discussion on how they might be managed. However, to obtain buy-in among the members, we needed a "champion" and found it in our executive vice president who chairs the Council. Having conducted a similar exercise with her previous employer, the executive vice president appreciated the value of risk assessment and was willing to place it on the agenda of a planned retreat and encourage participation. It was also critical to have a good facilitator available; one participant

Higher Education

(continued on page 18)

(continued from page 17)

on the Council serves as Tufts' director of Organizational Development and Training and she fit the bill.

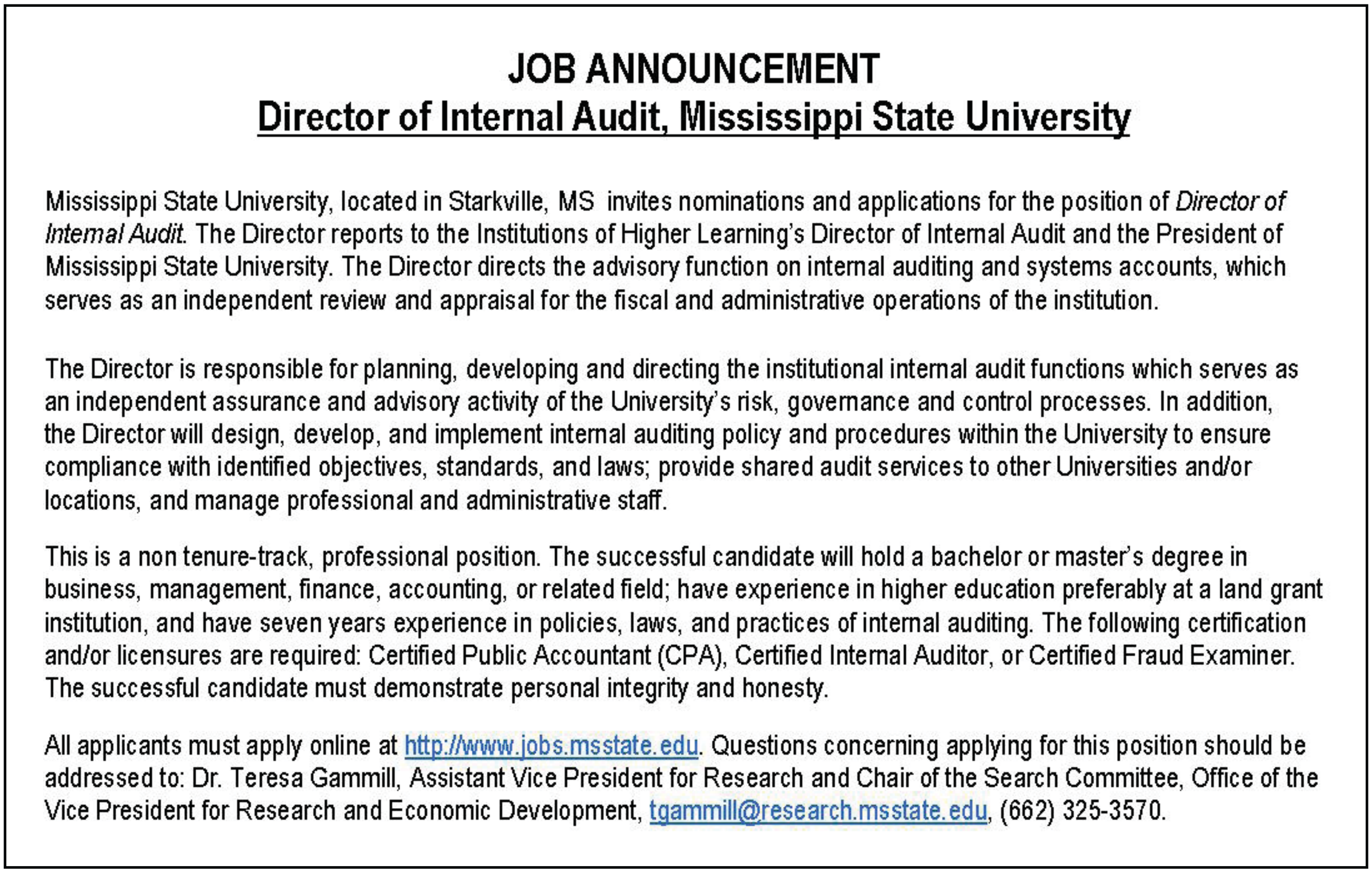
In advance of the session, a memorandum which contained a primer on concepts of ERM was sent to all Council members. Association of Governing Boards (AGB) recommendations for improving risk management at colleges and universities and examples of strategic, financial, operational, compliance and reputational risks at a hypothetical university were also provided. Council members were then asked to complete a Risk Reporting Form to identify higher level risks pertinent to their individual divisions and schools. The survey results were used to identify several risk "themes" for discussion and ranking at the Council retreat.

THE MOMENT OF TRUTH

At the retreat, I was tasked with introducing the risk assessment exercise. Admittedly, I was a little nervous and sensed a bit of skepticism amongst the group. I began my introductory remarks by stating that "for me, convening the Council for a discussion about enterprise risks was a dream-come-true." My comment elicited laughter and a few auditor wise cracks, but the ice was broken and what followed was a lively discussion about Tufts' more prevalent risks. By the end of the session, we agreed on four particular risks which were deemed relevant and impactful. The risks pertained to continuing to attract a high caliber of students and faculty, enhancing diversity, increasing collaboration among our schools and administrative divisions and maintaining good regulatory compliance. Within this context, we assessed the Council's current and future leadership ability to effectively address each of the identified risk areas.

THE FUTURE OF ERM AT TUFTS

Enterprise risk management at Tufts continues to evolve. Admittedly, not every step was followed at the Administrative Council retreat that a true ERM process might dictate; however, the process used was appropriate to engaging the Council and introducing them to a more formal risk assessment than they were accustomed to. Based on this experience, for any ERM activity to be successful, you must remain flexible. An early and integral step to success is to evaluate your management's comfort level about actively participating in a structured discussion about financial, operational, compliance and reputational risks and adjust your approach accordingly. For certain ACUA members, rolling out an ERM process will be relatively easy if the directive comes from an influential board member or senior executive. For other member institutions, it may require a more patient and methodical approach, similar to the process we deemed appropriate for Tufts. ■



JOB ANNOUNCEMENT

Director of Internal Audit, Mississippi State University

Mississippi State University, located in Starkville, MS invites nominations and applications for the position of *Director of Internal Audit*. The Director reports to the Institutions of Higher Learning's Director of Internal Audit and the President of Mississippi State University. The Director directs the advisory function on internal auditing and systems accounts, which serves as an independent review and appraisal for the fiscal and administrative operations of the institution.

The Director is responsible for planning, developing and directing the institutional internal audit functions which serves as an independent assurance and advisory activity of the University's risk, governance and control processes. In addition, the Director will design, develop, and implement internal auditing policy and procedures within the University to ensure compliance with identified objectives, standards, and laws; provide shared audit services to other Universities and/or locations, and manage professional and administrative staff.

This is a non tenure-track, professional position. The successful candidate will hold a bachelor or master's degree in business, management, finance, accounting, or related field; have experience in higher education preferably at a land grant institution, and have seven years experience in policies, laws, and practices of internal auditing. The following certification and/or licensures are required: Certified Public Accountant (CPA), Certified Internal Auditor, or Certified Fraud Examiner. The successful candidate must demonstrate personal integrity and honesty.

All applicants must apply online at http://www.jobs.msstate.edu. Questions concerning applying for this position should be addressed to: Dr. Teresa Gammill, Assistant Vice President for Research and Chair of the Search Committee, Office of the Vice President for Research and Economic Development, tgammill@research.msstate.edu, (662) 325-3570.