VCU

Virginia Commonwealth University

Enterprise Risk Management White Paper

Prepared by VCU Staff

Presented to the
Board of Visitors
Audit and Compliance Committee
May 11, 2012

Copyright – 2012 - VCU

Enterprise Risk Management

Enterprise Risk Management (ERM) is a new way of thinking, planning and strategizing.

Traditionally, businesses and universities have identified and managed risks individually or transactionally. Some examples are information technology breaches or failures, legal issues, and carrying traditional fire and other types of insurance. This can, at times, create a "silo" approach to risk management that may create a lack of coordination that could fail to identify strategic and reputational risks.

Risk is always a part of any business and not all risk is detrimental or must be eliminated. Successful organizations are those that can identify and manage risks in advance of those risks transforming into actualities. Unexpected occurrences can drive a business to react in a non-proactive manner and/or create significant liabilities.

Establishing an organizational Enterprise Risk Management ("ERM") process and structure can help to cover gaps by creating a holistic organization-wide approach to risk management that increases communication and integrates risk management with strategic planning. Additionally, ERM can help to position an organization to not only identify and mitigate traditional risks, but also to manage risk and, whenever possible, turn risk into opportunities.

Traditional risk mitigation involves one-time organizational action to try to avoid or reduce risk. Examples of risk mitigation include purchasing fire insurance, installing computer intrusion software, and/or instituting a policy prohibiting a certain type of activity. However, ERM institutes active and on-going identification and *management* of risks. An organization with an effective ERM process will continually work to identify and prioritize its risks across the business and develop a process to manage and monitor those risks.

• • •

"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

COSO/Treadway Commission

Enterprise Risk Management is a Best Practice in Business.

The control framework developed by the Committee of Sponsoring Organizations (COSO) states that risk management is an essential part of strong controls by ensuring that risk appetite aligns with management's decisions and an organization's strategy. A recent report by Ernst & Young noted that companies that made risk management practices part of their corporate culture tended to do better financially than those that did not. ("Turning Risk into Results," Ernst & Young Global Management 2012)

The Sarbanes-Oxley Act requires businesses to utilize a control framework in their internal control assessments. (Sarbanes-Oxley Act of 2002, Section 404) Many opted for the COSO Framework, which includes a risk assessment element. NYSE corporate governance rules require listed companies to "discuss policies with respect to risk assessment and risk management." (NYSE Listed Company Manual Section 303A Part 7. (c) (iii) (D)) Most recently, corporate debt rating agencies have started reviewing risk management in its company evaluation process. When properly implemented, ERM integrates the concepts of internal control, Sarbanes–Oxley, and strategic planning; all recognized as best practices.

Can Enterprise Risk Management Improve How Universities Operate?

Current trends point towards increasing pressure to transform risk management for universities:

- Fierce competition for faculty, students, staff, and financial resources.
- Pressure for increased productivity, responsiveness, and accountability while reducing costs.
- Increased external scrutiny from government, governing boards, and the public demanding accountability.
- New technologies that require investment of both financial and human capital resources.
- Rapidly increasing entrepreneurial ventures beyond the traditional educational venues that create stresses and strains on traditional administrative and financial infrastructures.
- Increased competition in the marketplace.

ERM focuses on an institution's achievement of its objectives or mission in the following four areas:

- *Strategic – high-level goals that are aligned with and support the institution's mission*
- *Operational – ongoing management process*
- *Financial – protection of the institution's assets*
- *Compliance – the institution's adherence to applicable laws and regulations*

Additionally, this framework helps a university manage one of its most important, overarching risks – reputational risk. The importance of reputational risk for a university cannot be over emphasized. There is not a single activity at a university that is not touched by potential or actual reputational risk. From academic quality to degree awarding, from research to instruction; a university's reputation is always a factor in customer and stakeholder decisions. If an incident were to occur to diminish a university's reputation, the financial and strategic repercussions could be devastating and have a long-term impact.

Using an ERM framework, management can review pressures and risks on an organization-wide basis and determine which risks may or could affect the ability to meet the university's strategic goals. ERM can also clarify the role of the board and senior management in risk management and decide whether the university should take on new risks or reduce its current risks. Although higher education has lagged behind the for-profit business sector in implementing ERM, it is now widely accepted in higher education as a best practice in strategic organizational management. Given the university's goals in education, research, and public service; implementation of ERM is one of the best ways to assist VCU to meet its strategic vision.

Why Should Virginia Commonwealth University Implement Enterprise Risk Management?

As a part of the state-required ARMICS process, the university has annually completed an "agency-wide risk assessment." (Update on Agency Risk Management and Internal Control Standards (ARMICS) - Presentation to Finance, Investment and Property Committee, VCU Board of Visitors, August 24, 2011) That assessment has identified challenges and opportunities for the university and has identified ways to improve the control environment. The university currently has wide-ranging policies and procedures to actively manage many of its financial, compliance and operational risks. However, some financial policies may need to be written, revised or updated. Implementing ERM to expand upon the current risk assessment processes will create opportunities to identify and manage risks and controls to include strategic and reputational risks. This could present an opportunity for VCU to lead among its peers.

ERM is an important step in implementing the overall strategic plan that identifies, analyzes, and strategically mitigates risks across a wide range of sources. Without ERM, implementation of a strategic plan like *Quest for Distinction* could be analogized to driving on a freeway without routinely checking one's mirrors for other cars and related risks. ERM helps the board members understand how management knows that the important risks to the university will be identified and managed.

Quest for Distinction identifies VCU as forward looking and future planning. Successful implementation of ERM would complement the strategic plan by focusing on those risks that could keep the university from successfully reaching the *Quest for Distinction* goals. The first step for any strategic plan is to focus on implementing those activities that help to achieve those goals. A similarly important parallel step is to identify and manage those risks that may prevent reaching the goals. Additionally, other risks may be identified that do not directly relate to *Quest for Distinction*, but relate to the university's mission statement and core values.

What would ERM look like at VCU?

From the very beginning, the President must promote the importance of ERM to the university, lend his sponsorship to the ERM project, and lead the ERM process. Through its support and monitoring of the ERM project, the board sets the tone for risk management on campus. Senior management, including the Board of Visitors and the President, must demonstrate the importance of ERM to VCU by making time to add their expertise to the process and by making the ERM project a time and budget priority.

The next step, as with most projects, is to put someone in charge. The most important indicator of success in this project will be having an individual whose responsibility is to continually maintain the momentum of the process. This project director would be someone reporting either to the President, Vice President for Finance and Administration, or Executive Director of Assurance Services. The project director would assist in developing a framework that would guide the process and identify resources necessary to make the project successful and further refine the map that the university will continuously follow to meet its strategic goals. The Department of Assurance Services would be a valuable resource in assisting in the direction of this project.

Similar to strategic planning, ERM is not a one-time process that develops a discrete inventory of risks that is then placed on the shelf for decoration or occasional reference. ERM must become part of the living culture and

strategic planning processes for the university. Whenever priorities are set or decisions are made, enterprise risk management must become part of the process. An important part of ERM is education and how to make risk assessment part of the decision-making process and vocabulary on campus and create a culture that supports setting priorities and responsible risk-taking.

We will need to build on VCU's current risk management processes to identify, analyze, evaluate, treat, and monitor the university's current processes and strategic goals. In a large multi-faceted university with many schools, activities, research grants, foundations, associations, and a teaching hospital; this could be a daunting task. Similar to strategic planning, full implementation of ERM could involve many employees and stakeholders to tap the creativity necessary to identify all the university's risks.

As ERM began in the for-profit business sector, it used a process-control approach that focused on key business processes and managing risk events by using consistency across the business processes. This approach used the COSO framework to comprehensively review each process creating detailed control documentation and comprehensive reporting. This approach requires an extensive amount of initial effort to catalog, document, and analyze all the risks.

Some universities have embraced a measurement-driven approach that focuses on identifying the key risk factors and understanding their materiality and probability of occurrence. Risk mitigation activities are focused on the most material risks with appropriate mitigation strategies. This creates risk management as a tool that can be used for budgetary as well as strategic planning. This approach has been successfully implemented at Emory University in Atlanta (a 14,000-student university with a teaching hospital) and Cornell University in New York (a 22,000-student public land grant university with a teaching hospital).

We have reviewed and evaluated these two ERM approaches. We have seen that the most successful models implemented by universities have used the measurement-driven approach similar to that implemented at Emory and Cornell Universities. This model is one that we believe would fit well with VCU and involves staff throughout the university to identify, prioritize, and manage risks. There may be opportunities to involve internal or external experts to assist in tailoring this or another ERM model to VCU.

Selected Universities that have implemented ERM

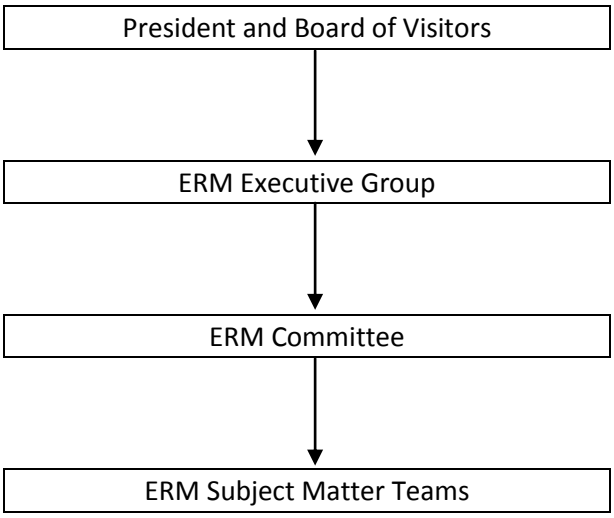
- Drexel University
- University System of Georgia
- NC State University
- Penn State University
- Emory University
- University of North Carolina
- University of California System
- University of Texas System
- Texas A&M University
- University of Maryland
- Ohio University
- Western Carolina University
- University of Notre Dame
- Stanford University
- University of Pennsylvania
- University of South Florida
- California Institute of Indiana State University
- Lehigh University
- University of Washington
- University of Wisconsin

Source: United Educators and other research

How Can VCU Identify and Prioritize its Risks?

Interviews, group discussions, surveys, or other methods would be used by facilitators to guide the risk identification and evaluation process. An important part of the ERM process is for the user groups to have significant input in risk identification and evaluation. This process should identify those risks that the senior management and the board need to focus on, not trivial risks.

Possible ERM Structure



One common way to identify and rate risks is through the use of facilitated meetings. VCU faculty, staff, and other stakeholders with different backgrounds and responsibilities would collaborate and brainstorm with the assistance of a facilitator trained in group dynamics and familiar with ERM goals. These groups would be organized around subject matters such as: Finance, Safety and Facilities, Human Resources, Information Technology, Governance, Academics, Student Affairs, and Research. Risks would be scored as to both severity and likelihood, emphasizing severity. Certain areas could be reviewed for risk first because they have higher risks, have greater importance as strategic initiatives, or have higher exposure to affect the university's reputation.

This process will identify many more risks than can be actively managed by senior management. After a broad range of risks are identified through this initial process, an ERM Committee (probably individuals at the Assistant Vice President level) would be tasked with grouping and prioritizing the risks. Establishing a cross-functional ERM committee is an opportunity to advance some real thinking and truth-telling about the risks various individuals on campus see. Staff from Finance and Administration as well as Assurance Services would be key members of this ERM Committee due to their risk analysis experience. This committee would then decide how many of these risks could be actively managed at one time, the Key Risks. Generally, it may be difficult for senior management to be involved in managing more than 50 risks annually. Management could individually decide whether certain other risks should be managed by department managers outside of this ERM project.

How are the Risks Managed?

After the ERM Committee identifies those Key Risks, each risk would be assigned to a Process Owner. That individual may or may not be responsible for owning that risk or implementing action to mitigate that risk. The Process Owner would be responsible for ensuring that the risk is managed and to report on that risk to the ERM Executive Group (probably individuals at the President's Cabinet level). The Process Owner would have to work closely with those responsible for actually managing that risk (the Risk Owners), both to identify the details of the risk and to develop practical ways to mitigate the risk. The Risk Owners need to use their risk management and mitigation plans in budget development and clearly identify those budget requests that mitigate Key Risks.

The ERM Executive Group would meet for a few hours quarterly to review Key Risks. Each Key Risk would be reviewed annually. The Process Owner would present the status of that risk, steps being taken to manage the risk, the planned operational response to an occurrence of that risk, and the planned communication response to an occurrence. In order to keep the meeting direct and concise, the Process Owner would be given approximately five minutes to present and a similar amount of time to answer questions. A rigid timetable ensures that the scheduled risks are addressed within the allotted time.

Of course, the implementation is not complete until a monitoring procedure is in place to revisit the risk assessment process periodically and bring the process full circle by re-assessing risk and evaluating methods of risk control. The ERM Committee would periodically meet to decide whether there are new risks that may need to be managed as Key Risks and whether any Key Risks are so well managed that they no longer need to be managed by the ERM Executive Group.

Annually, the project director would update the appropriate committees of the Board of Visitors on the status of risk management. This update would summarize important risk management activities, identify important risks that have not been sufficiently managed, and ask for the board members' input on their assessment of risks that may need to be considered.

How Much is Enterprise Risk Management Going to Cost VCU?

As previously noted, the university currently reviews enterprise level risk as a part of the ARMICS procedures. Implementing ERM would build upon this process and culture to make the process more formal, involve management more deeply, and integrate risk assessment into strategic planning and decision-making. The university may want to engage internal or external experts in developing the ERM framework and in facilitating risk identification and scoring; this may involve the budgeting of resources. Additional costs and meeting time will be required to educate and inform those involved of the background, process, and goals of the project.

However, most of the cost to the university will be "soft costs" in that individual staff members will be asked to make time in their regular work duties to fulfill ERM tasks. After some initial start-up and organizational meetings, the ERM Executive Group would meet for three quarterly. The ERM Committee may need to meet for two or three days to initially review and prioritize the Key Risks. The facilitated meetings to identify the risks may involve eight meetings of ten individuals lasting three to four hours. Initially, the individual identified as the project director may find that organizing and monitoring the project takes a significant amount of his or her workload. After the initial phase, the project director should find that maintaining the momentum of the project is less burdensome.

The Process Owners and the managers in the identified risk areas will be performing tasks that are integral to their regular duties. We believe that many of these staff members are already identifying and working to mitigate risks in their assigned areas. Formalizing their procedures and then reporting their results to management annually should not be a significant additional burden.

How Will the Implementation of Enterprise Risk Management Benefit VCU?

Adoption and implementation of Enterprise Risk Management at VCU will give management and the board knowledge that, as a whole, the university is doing what it can to be ready for the future. We may have limited ability to affect or even predict the future, but if we are ready for the future then we can continue to direct our path through the future, instead of having the future direct us.

A strong risk assessment with related mitigation strategies will increase the university's reputation as a leader in active governance by both the board and senior management. The university will be seen as a proactive steward of its resources by state government, donors, the bond market, and other stakeholders.

ERM can help in management's efforts to:

- Sustain its competitive advantage
- Solidify its integrity and reputation
- Respond effectively when a significant event occurs
- Avoid financial surprises
- Mitigate future liabilities
- Effectively manage all of its resources

Should an event occur that has been a part of the risk management process, the university's response can be quick, decisive and resilient, because it has been anticipated. Even if an event occurs that had not been part of the process, the university will be seen as having been active in risk management and had just not thought of the unthinkable and the risk management process may aid in mitigating future liabilities.

Primarily, implementation of risk management will be another tool to successfully implement the themes of *Quest for Distinction* and lead VCU into its second 50 years as a premier urban, public research university distinguished by its commitments to education, research, human health, and engagement.