Title: Enterprise Risk Management System Policy Policy: 5110

Purpose

The University and its management are committed to the effective support of its stakeholders and require that robust risk management processes and procedures are adopted.

The purposes of establishing this risk management policy are to:

- provide a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to risk management;
- take into account business and legal or regulatory requirements, and contractual obligations;
- align risk management with the university's strategic context in which the establishment and maintenance of the enterprise risk management system will take place;
- establish criteria against which risk will be evaluated;
- specify how risk management performance will be measured and reported;
- ensure necessary resources are available to assist those accountable and responsible for managing risk;
- ensure that all risk management activities are conducted and implemented in an agreed and controlled manner; and
- achieve a risk management capability that meets changing business needs and is appropriate to the size, complexity and nature of the university

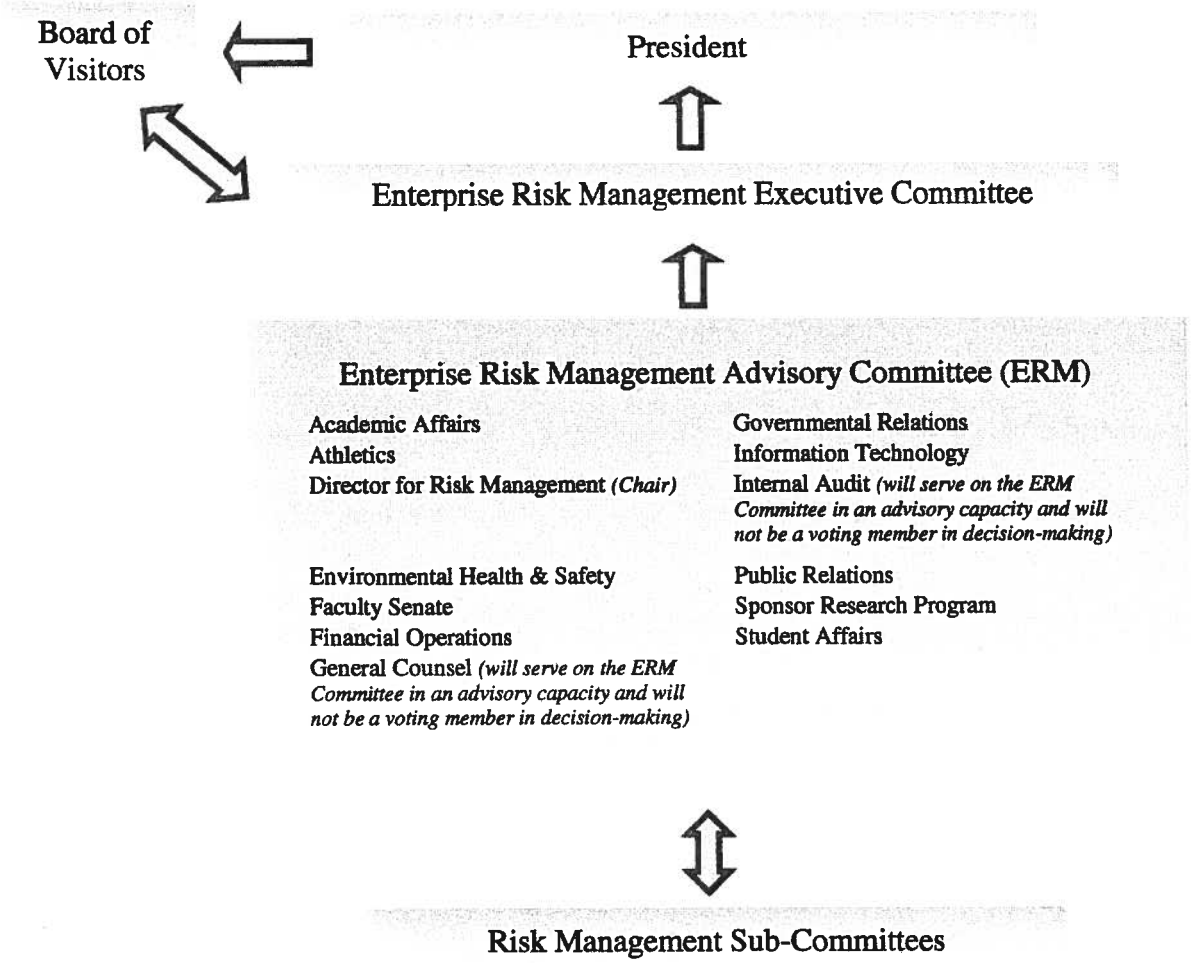
This Policy also specifies the activities for establishing an enterprise risk management capability, incorporating these capabilities into specifications, constructing end-to-end designs, and finally implementing the process.

This Policy shall also specify the ongoing management and maintenance of the enterprise risk management capability, including:

- assigning of accountabilities and responsibilities at appropriate levels within the organization;
- ensuring that the necessary resources are allocated to risk management;
- embedding of risk management within the organization by communicate the benefits of risk management to all stakeholders;
- exercising of risk treatment plans regularly;
- updating and communicating of the risk treatment plans – particularly when there is significant change in premises, personnel, process, market, technology or organizational structure; and
- ensuring that the framework for managing risk continues to remain appropriate

Authority, Responsibility, and Duties

A suitable risk management structure shall be created and operated for the purpose of planning, executing, monitoring, and improving the organization's risk management processes:



Board Members

University governors such as the Board of Visitors shall:

- Develop, prove, and maintain competence in the principles, methods, processes, and standards incorporated in and referenced by this Policy;
- Determine strategic approach to risk and set risk appetite;
- Establish and approve the structure for risk management;
- Understand the most significant risks;
- Manage the organization in a crisis;
- Overall responsibility for risk management;
- Ensure risk management in accordance with the university's approved risk management process methodology is embedded into all processes and activities; and
- Review group risk profile

President
The President provides risk direction and ensures that strategic, operational, financial and compliance risks are effectively managed. The President will embed risk considerations into the strategic planning. The President will hold management accountable for managing enterprise risk.

Enterprise Risk Management Executive Committee
The Enterprise Risk Management Executive Committee maintains oversight of the risk management process and approves risk strategies. The ERM Executive Committee is an established committee that includes Vice President of Administration and Finance, Director of Risk Management and a member from the Academic Affairs and Technology Services. The ERM Executive Committee will receive and review recommendations from the ERM Advisory Committee, and provide recommendations to the University President. The President will have the final responsibility and authority for all program decisions

Enterprise Risk Management Advisory Committee
A strategic-level ERM Advisory Committee shall create, oversee, and maintain risk management, establish the plan for the risk documents, determine the expected contents of these documents, and acquire acceptance from any relevant stakeholders. The committee shall:

- Develop, prove, and maintain competence in the principles, methods, processes, and standards incorporated in and referenced by this Policy;
- Assist in the planning of any organizational change, which may change the university's risk context
- Handle any risk problems that may arise
- Consider improvements arising from following implementation and measurement of risk management
- Give strategic direction to the risk program (both during the implementation project and in operation), and
- Liaise between senior management and the Risk Management Sub-Committee.

Risk Management Sub-Committee
Risk Management Sub-Committee are necessary to address development of risk management systems and related controls for risks that are of a specific nature, but tend to affect risk owners, processes, and assets throughout the enterprise. Risk Management Sub-Committee/managing functions shall:

- Develop, prove, and maintain competence in the principles, methods, processes, and standards incorporated in and referenced by this Policy;
- Assist the university in establishing specialized risk policies, such as for compliance, information security, and business continuity, in accordance with the university's approved risk management risk assessment and risk treatment methodology;
- Develop specialized contingency and recovery plans;
- Keep up to date with developments in the specialized area; and
- Support investigations of incidents and near misses

University Risk Manager
The Risk Manager shall:

- Develop, prove, and maintain competence in the principles, methods, processes, and standards incorporated in and referenced by this Policy;
- Develop the risk management policy and keep it up to date

- Document the internal risk policies and structures in accordance with the university's approved risk management policy and process methodology;
- Co-ordinate the risk management (and internal control) activities; and
- Compile risk information and prepare reports for the Board

University Department Manager
It is the responsibility of the manager of each support department and unit to develop, maintain, review, and test controls for risk management in accordance with the university's approved risk management process methodology and documented control objectives.

It is equally the responsibility of the manager of each support department and unit to assess and manage risk on a day-to-day basis, and to consider material risk issues when considering the development of any new product, service, or project. University Department Managers shall:

- Develop, prove, and maintain competence in the principles, methods, processes, and standards incorporated in and referenced by this Policy;
- Build risk aware culture within the department;
- Agree on risk management performance targets;
- Ensure implementation of risk improvement recommendations;
- Identify and report changed circumstances / risks;
- Produce specific policy statements, as necessary;
- Prepare and update the university department risk register;
- Set risk priorities for university department;
- Monitor projects and risk improvements;
- Prepare reports for Risk Management Sub-Committee; and
- Manage control risk self-certification activities.

Advisory Roles
Internal Audit and University Legal Counsel shall serve as an advisor and consult to the University administration in the development and implementation of the Enterprise Risk Management program and for the purpose of assisting the Board of Visitors in its fiduciary role for risk management.

Individual University Employees

- Understand, and assist in the action of appropriate implement risk management processes
- Co-operate with sub-committee management on risk management incident investigations

Definitions

Enterprise Risk Management: Is a process, affected 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.

Risk: is the potential of loss (an undesirable outcome, however not necessarily so) resulting from a given action, activity and/or inaction. The notion implies that a choice having an influence on the outcome sometimes exists (or existed). Potential losses themselves may also be called "risks". Any human endeavor carries some risk, but some are much riskier than others.

Risk Management: is the identification, assessment, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives, whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events[1] or to maximize the realization of opportunities. Risks can come from uncertainty in financial markets, threats from project failures (at any phase in design, development, production, or sustainment life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attack from an adversary, or events of uncertain or unpredictable root-cause.

Risk Management Framework: set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

Risk Management Process: systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, valuating, treating, monitoring and reviewing risk.

Stakeholder: person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

External Context: external environment in which the organization seeks to achieve its objectives. External context can include: — the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; — key drivers and trends having impact on the objectives of the organization; and — relationships with, and perceptions and values of external stakeholders.

Internal context: internal environment in which the organization seeks to achieve its objectives. Internal context can include: governance, organizational structure, roles and accountabilities; policies, objectives, and the strategies that are in place to achieve them; the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies); information systems, information flows and decision making processes (both formal and informal); relationships with, and perceptions and values of internal stakeholders; the organization's culture; standards, guidelines and models adopted by the organization; and form and extent of contractual relationships.

Risk Criteria: is a term of reference against which the significance of a risk is evaluated. Risk criteria are based on organizational objectives, and external and internal context. Risk criteria can be derived from standards, laws, policies and other requirements.

Risk Assessment: is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard).

Risk Identification: is a process of finding, recognizing and describing risks, Risk identification involves the identification of risk sources, events, their causes and their potential consequences

Risk Description: structured statement of risk usually containing four elements: sources, events, causes and consequences.

Risk Owner: is a person or entity with the accountability and authority to manage a risk.

Risk Analysis: is a process to comprehend the nature of risk and to determine the level of risk

Probability: measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty.

Frequency: number of events or outcomes per defined unit of time or to potential future events, where it can be used as a measure of likelihood probability

Risk Matrix: tool for ranking and displaying risks by defining ranges for consequence and likelihood

Risk Evaluation: process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

Risk Attitude: organization's approach to assess and eventually pursue, retain, take or turn away from risk

Risk Appetite: amount and type of risk that an organization is willing to pursue or retain

Risk Tolerance: is an organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives.

Risk Avoidance: informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular.

Risk Register: record of information about identified risks

Risk Profile: description of any set of risks that relate to the whole organization, part of the organization, or as otherwise defined.

Risk Management Audit: systematic, independent and documented process for obtaining evidence and evaluating it objectively in order to determine the extent to which the risk management framework, or any selected part of it, is adequate and effective

Policy Statements

Accountability

Enhanced risk management includes comprehensive, fully defined and fully accepted accountability for risks, controls and risk treatment tasks. Designated individuals shall fully accept accountability, shall be appropriately skilled and shall have adequate resources to check controls, monitor risks, improve controls and communicate effectively about risks and their management to external and internal stakeholders. This can be facilitated by:

- identifying risk owners that have the accountability and authority to manage risks;
- identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;
- identifying other responsibilities of people at all levels in the organization for the risk management process;
- establishing performance measurement and external and/or internal reporting and escalation processes; and
- ensuring appropriate levels of recognition

Risk accountability shall be recorded in job/position descriptions, databases or information systems.

The definition of risk management roles, accountabilities and responsibilities shall be part of all the organization's induction programs, as well as any contracted arrangements with third-party service providers. The organization commits to ensuring that those who are accountable are equipped to fulfill that role by providing them with the authority, time, training, resources and skills sufficient to assume their accountabilities.

Integration into Organizational Strategy and Governance
Risk management shall be viewed as central to the organization's management processes, such that risks are considered in terms of effect of uncertainty on objectives. The governance structure and process are based on the management of risk. Effective risk management shall be regarded by managers as essential for the achievement of the organization's objectives.

This is evidenced by managers' language and important written materials in the organization when using the term "uncertainty" in connection with risks. This attribute is also normally reflected in the organization's statements of policy, particularly those relating to risk management. This attribute shall be verified through interviews with managers and through the evidence of their actions and statements.

Integration into Organizational Processes
Risk management shall be embedded in all the organization's practices and processes in a way that it is relevant, effective and efficient. The risk management process shall become part of, and not separate from, those organizational processes. In particular, risk management shall be embedded into the policy development, business and strategic planning and review, and change management processes.

All decision making within the organization, whatever the level of importance and significance, shall involve the explicit consideration of risks and the application of risk management to some appropriate degree. This shall be indicated by records of meetings and decisions to show that explicit discussions on risks took place. In addition, all components of risk management are represented and evidenced within key processes for decision making in the organization, e.g. for decisions on the allocation of capital, on major projects and on re-structuring and organizational changes.

For these reasons, soundly based risk management shall be seen within the organization as providing the basis for effective governance.

There shall be an organization-wide risk management plan to ensure that the risk management policy is implemented and that risk management is embedded in all of the organization's practices and processes. The risk management plan can be integrated into other organizational plans, such as strategic plans.

The requirements, context, scope, risk criteria, definitions, and approach of the organizations risk management system specified within this Policy document and it supporting documents shall provide the structure and approach for specialized risk management processes, including , but not limited to information security, business continuity, disaster recovery, occupational health and safety, environmental risk management.

Resources
The organization shall allocate and budget for appropriate resources for risk management. Consideration should be given to the following:

- people, skills, experience and competence;
- resources needed for each step of the risk management process;
- the organization's processes, methods and tools to be used for managing risk;
- documented processes and procedures;
- information and knowledge management systems; and
- training programs

Policy Communication
Enhanced risk management includes continual communications with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance, as part of good governance.

Communication with stakeholders is an integral and essential component of risk management. Communication is rightly seen as a two-way process, such that properly informed decisions can be made about the level of risks and the need for risk treatment against properly established and comprehensive risk criteria.

Comprehensive and frequent external and internal reporting on both significant risks and on risk management performance contributes substantially to effective governance within an organization.

Establishing Internal Communication and Reporting Mechanisms
The organization shall establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk. These mechanisms should ensure that:

- key components of the risk management framework, and any subsequent modifications, are communicated appropriately;
- there is adequate internal reporting on the framework, its effectiveness and the outcomes;
- relevant information derived from the application of risk management is available at appropriate levels and times; and
- there are processes for consultation with internal stakeholders

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

Establishing External Communication and Reporting Mechanisms
The organization shall develop and implement a plan as to how it will communicate with external stakeholders. This should involve:

- engaging appropriate external stakeholders and ensuring an effective exchange of information;
- external reporting to comply with legal, regulatory, and governance requirements;
- providing feedback and reporting on communication and consultation;
- using communication to build confidence in the organization; and
- communicating with stakeholders in the event of a crisis or contingency

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

Implementing the Framework (System) for Managing Risk
In implementing the organization's framework for managing risk, the organization shall:

- define the appropriate timing and strategy for implementing the framework;
- apply the risk management policy and process to the organizational processes;
- comply with legal and regulatory requirements;
- ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;
- hold information and training sessions; and
- communicate and consult with stakeholders to ensure that its risk management framework remains appropriate

Implementing the Risk Management Process
Risk management shall be implemented by ensuring that the risk management process outlined in the organization's Risk Management Process Methodology is applied through a risk management plan at all relevant levels and functions of the organization as part of its practices and processes.

Risk monitoring
Ongoing monitoring and review is necessary to ensure that the context, the outcome of the risk assessment and risk treatment, as well as management plans, remain relevant and appropriate to the circumstances. The organization should make sure that the risk management process and related activities remain appropriate in the present circumstances and are followed. Any agreed improvements to the process or actions necessary to improve compliance with the process should be notified to the appropriate managers to have assurance that no risk or risk element is overlooked or underestimated and that the necessary actions are taken and decisions are made to provide a realistic risk understanding and ability to respond.

Additionally, the organization shall regularly verify that the criteria used to measure the risk and its elements are still valid and consistent with business objectives, strategies and policies, and that changes to the business context are taken into consideration adequately during the risk management process.

This monitoring and review activity should address (but not be limited to):

- Legal and environmental context
- Competition context
- Risk assessment approach
- Asset value and categories
- Impact criteria
- Risk evaluation criteria
- Risk acceptance criteria
- Total cost of ownership
- Necessary resources

The organization shall ensure that risk assessment and risk treatment resources are continually available to review risk, to address new or changed threats or vulnerabilities, and to advise management accordingly.

Continual improvement
An emphasis shall be placed on continual improvement in risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.

This shall be supported by the existence of explicit performance goals against which the organization's and individual manager's performance is measured. The organization's performance shall be published and communicated. Normally, there shall be at least an annual review of performance and then a revision of processes, and the setting of revised performance objectives for the following period.

This risk management performance assessment shall be an integral part of the overall organization's performance assessment and measurement system for departments and individuals.

References

ISO 31000 (Risk Management System Framework)
ISO 31010 (Risk Assessment Approach)
ISO Guide 73 (Risk management vocabulary)
ISO 27005 (Supporting the Risk Assessment Approach)
ISO 27003 (Supporting the establishment of an Enterprise Risk Management System)
ISO 19011 (Supporting auditing of management systems)
Commonwealth of Virginia, Information Technology Resource Management, "Information Technology Security Standard", SEC 501-07 January 28, 2013
Commonwealth of Virginia, Information Technology Resource Management, "Information Technology Risk Management Guideline", SEC 506-01, December 11, 2006

Approval By: _____
President

Date: 12/19/13