OLD DOMINION UNIVERSITY
University Policy

Policy #3016
UNIVERSITY RESPONSIBILITY FOR ENTERPRISE RISK MANAGEMENT

Responsible Oversight Executive: Vice President for Administration and Finance
Date of Current Revision or Creation: March 15, 2024

A. PURPOSE

The purpose of this policy is to establish the University's framework for Enterprise Risk Management (ERM) with the goal of identifying enterprise-level risk, which if not mitigated would impact the achievement of strategic business objectives, and to define the responsibilities of the Risk Advisory Council (RAC), Vice Presidents, and individuals in meeting and maintaining ERM standards.

B. AUTHORITY

Code of Virginia Section 23.1-1301, as amended, grants authority to the Board of Visitors to make rules and policies concerning the institution. Section 7.01(a)(6) of the Board of Visitors Bylaws grants authority to the President to implement the policies and procedures of the Board relating to University operations.

Agency Risk Management and Internal Control Standards, published by the Commonwealth Office of the Comptroller, establishes Committee on Sponsoring Organizations (COSO) based objectives and principles to facilitate implementation of the Commonwealth's agency risk management and internal control standards.

C. DEFINITIONS

Affiliates and Affiliated Organizations – Those organizations that are separate entities established to benefit the University through an operating agreement and include but are not limited to the Foundations, the Community Development Corporation, and the Alumni Association.

Compliance Requirements - Federal and State laws, rules, regulations, standards and institutional policies and procedures that University employees, students, volunteers, and vendors are expected to be aware of and in compliance with.

Compliance Risk - The organization's potential exposure to legal penalties, financial forfeiture, and material loss resulting from its failure to act in accordance with industry laws and regulations, internal policies or prescribed best practices.

Enterprise Level Risks - Risks that may impact the achievement of strategic business objectives needing to be identified and assessed.

Enterprise Risk Management (ERM) - The commitment to managing risk as an integral component of an entity's operations to maximize opportunities and minimize setbacks to the entity's mission, strategies, and objectives.

Financial Risk – The risk potential for losing money on an investment or having a negative business outcome.

Enterprise Risk Management Registry (ERM Risk Registry) - A database of ERM requirements that includes a description of the risk, responsible vice-presidential area, responsible office, responsible position number and title, risk rating, and status of the risk.

Governance and Culture Risk – The risk created when there is misalignment between an organization's values and leader actions, employee behaviors, or organizational systems.

Office of Risk Management (ORM) - The unit responsible for Environmental Health and Safety.

Operational Risk - The risk of loss from ineffective or failed internal processes, people, systems, or external events that can disrupt the flow of business operations.

Reputational Risk – The risk that develops when the expectations of stakeholders - such as customers, employees, third party suppliers, investors, donors, alumni, and regulatory bodies - are higher than the reality of what the business delivers.

Risk Advisory Council (RAC) – A University-wide group made up of key individuals knowledgeable of ERM issues, whose chair is the Vice President for Administration and Finance, or designee.

Risk Appetite - The amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style.

Risk Tolerance - The acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as those used to measure the related objective. In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Operating within risk tolerances helps ensure that the entity remains within its risk appetite and, in turn, that the entity will achieve its objectives.

Strategic Risk - The internal and external events that may make it difficult, or even impossible, for an organization to achieve its objectives and strategic goals. These risks can have severe consequences that impact organizations in the long term.

Vendors - Those individuals and entities who have a relationship with the University by virtue of a contract.

Volunteers – Those individuals who perform services in support of the University's mission without promise, expectation, or receipt of compensation for services rendered.

D. SCOPE

This policy applies to all employees, students, volunteers, and vendors. Employees include all staff, administrators, faculty, full- or part-time, and classified or non-classified persons paid by the University. Students include all persons admitted to the University who have not completed a program of study for which they were enrolled; student status continues whether the University's programs are in session. Volunteers include individuals who perform services in support of the University's mission without promise, expectation, or receipt of compensation for services rendered.

E. POLICY STATEMENT

Enterprise Risk Management (ERM) deals with compliance risks, governance and culture risk, financial risks, operational risks, reputational risks, and strategic risks facing the University. Compliance risks are assessed, monitored, and reported by the responsible compliance officer from the Office of Risk Management and shall follow a modified version of the COSO framework model for ERM Compliance. Culture, financial, operational, reputational, and strategic risk are assessed, monitored, and reported on by the responsible risk analyst and shall follow a modified version of the COSO Enterprise Risk Management framework. ERM compliance and ERM risk staff report to the Office of Risk Management (ORM) within the organization of the Vice President for Administration and Finance.

This policy outlines the University's ERM responsibilities in its commitment to fostering an institutional culture of adherence to ERM principles for identification, assessment, mitigation, monitoring, and reporting on enterprise-level risk to senior leadership and the Board of Visitors. University ERM is a shared responsibility among all employees, students, volunteers, vendors, and the Risk Advisory Council, whose responsibilities are described below.

F. PROCEDURES

1. Vice Presidents are responsible for promoting ERM awareness and responsibilities within their respective organizations; maintaining a current inventory of all enterprise-level risks; developing mitigation requirements for units within their organizations; and developing programs, processes, and controls to ensure ERM requirements are being met.

2. University employees, students, volunteers, and vendors are also responsible for being cognizant of any changes in the risk environment that may impact these responsibilities and, where applicable, cooperating with other affected units of the University to ensure requirements are met for the University as a whole.

3. The role of the Risk Advisory Council is to promote ERM awareness among the University's academic and administrative units. These duties include:

    a. Promoting effective communication and collaboration among those responsible for ERM;
    b. Monitoring emerging enterprise-level risk trends and disseminating information as needed;
    c. Serving as a resource in developing or improving ERM-related processes;
    d. Working with the University's Policy Review Committee to incorporate into policies any required ERM practices and procedures; and
    e. Making recommendations to senior management as to any resources or actions required for University ERM success.

4. The Vice President for Administration and Finance (or designee) will chair the Risk Advisory Council (RAC) and will consult with the other Vice Presidents to appoint members of the Council. The chair determines the scope and frequency of meetings of the Council in the fulfillment of its duties as outlined in this policy. The RAC shall be convened no less than quarterly.

5. The Vice Presidents, working with the ORM, will develop and maintain an inventory of all enterprise-level risks for the units within their organizations. The inventory should include the position number and title of the employee(s) responsible for each enterprise-level risk and any associated reporting requirements. The risk inventories will be submitted to the RAC at the Chair's request, and as risks are identified for addition or removal. The risk inventories submitted by the Vice Presidents will be used to update the ERM Risk Registry maintained by the RAC. Vice Presidents should ensure that position descriptions for those employees who have been identified as responsible for meeting ERM requirements include ERM as a core responsibility that is evaluated during the annual evaluation process. On an annual basis as determined by the RAC, Vice Presidents working with the ORM staff will submit an annual status report on enterprise-level risk identified as impacting the achievement of strategic goals and objectives within their organizations.

6. The Vice President for Administration and Finance (or designee) will report on the activities of the Risk Advisory Council to the Board of Visitors Administration and Finance Committee on a periodic basis.

7. The RAC Chair shall bring developing enterprise-level risk concerns to the RAC as needed to analyze their potential impact to the University's strategic plans, mission, and vision.

8. The Administration and Finance Committee of the Board of Visitors establishes the University's risk appetite and risk tolerance and makes ERM-related recommendations to the full Board as deemed necessary by the committee.

9. An ERM Risk Assessment Guide, based on the COSO models described in Section E, shall be developed by the Risk Advisory Council documenting the ERM framework to address compliance, governance and culture, financial, operational, reputational, and strategic risks.

10. The University Enterprise Risk Analyst/Officer shall assist the Executive Director of Risk Management in administering this policy.

G. RETENTION

Applicable records must be retained and then destroyed in accordance with the Commonwealth's Records Retention Schedules.

H. RESPONSIBLE OFFICER

Executive Director of Risk Management

I. RELATED INFORMATION

University Enterprise Risk Management Website
Policy #1003 University Responsibility for Compliance
Policy #6023 Policy for the Use of Non-Research Related Volunteers

POLICY HISTORY

****

Policy Formulation Committee (PFC) & Responsible Officer Approval to Proceed:

/s/ Robert Wells — February 26, 2024
Responsible Officer — Date

Policy Review Committee (PRC) Approval to Proceed:

/s/ Donna Meeks — October 24, 2023
Chair, Policy Review Committee (PRC) — Date

Executive Policy Review Committee (EPRC) Approval to Proceed:

/s/ Chad A. Reed — March 5, 2024
Responsible Oversight Executive — Date

University Counsel Approval to Proceed:

/s/ Allen T. Wilson — March 12, 2024
University Counsel — Date

Presidential Approval:

/s/ Brian O. Hemphill, Ph.D. — March 15, 2024
President — Date

Policy Revision Dates: March 15, 2024

Scheduled Review Date: March 15, 2029