

Virginia Tech
Risk and Compliance Governance Framework
Charter

Purpose

Virginia Polytechnic Institute and State University (Virginia Tech) manages a wide range of risks to ensure the institution can continue to serve all members of the Hokie community, in the spirit of our motto, *Ut Prosim* (That I May Serve). By strategically managing risk, Virginia Tech can fulfill its mission and vision as a land-grant institution dedicated to improving the quality of life and the human condition, while protecting the institution's resources. Furthermore, Virginia Tech is committed to integrity, a culture of compliance, and the promotion of the highest ethical standards for all employees.

In 2017, the Board of Visitors charged the Office of Audit, Risk, and Compliance (OARC) with the development of institutional-level programs for risk and compliance efforts. Virginia Tech's Enterprise Risk Management (ERM) program and Institutional Compliance Program (ICP), led by the Vice President for Audit, Risk, and Compliance & Chief Risk Officer, are executed through significant collaboration from a number of departments and offices across the university.

Enterprise Risk Management (ERM) is a process applied in strategy-setting and across the enterprise that is designed to identify potential events that may affect the university, manage those risks to be within the entity's risk tolerance, and support the achievement of Virginia Tech's mission and objectives. ERM is a university-wide approach to address the full spectrum of the organization's internal and external risks and manage the impact of those risks as an interrelated risk portfolio. Enterprise risks are entity-level risks which cut across the institution, crossing units and functional areas, which, if not properly identified, assessed and managed, can result in the potential for a greater combined impact to the university.

The Institutional Compliance Program (ICP) coordinates the university's compliance efforts and serves as a resource to help the institution proactively meet its compliance obligations and manage compliance risks.

The mission of the Risk & Compliance Steering Committee (Steering Committee) and the Risk & Compliance Advisory Committee (Advisory Committee) is to support the implementation and execution of the ERM and ICP programs, as well as provide oversight and guidance for strategic decision making and effective resource allocation. These two groups help to set program priorities and promote an institution-wide perspective related to risk and compliance. The Steering Committee and Advisory Committee are essential components of the ERM and ICP program.

Responsibilities

The Steering Committee will perform the following responsibilities:

- support and promote a culture of ethics and integrity at all levels of the university;
- provide direction on strategic priorities based on the university's overall risk appetite;
- contribute to the assessment of risks, and the development and coordination of risk mitigation strategies;
- provide guidance on strategic direction and resource allocation;
- promote linkages between identified enterprise risks and compliance risk areas with Virginia Tech's Strategic Plan, Beyond Boundaries.

The Advisory Committee will perform the following responsibilities:

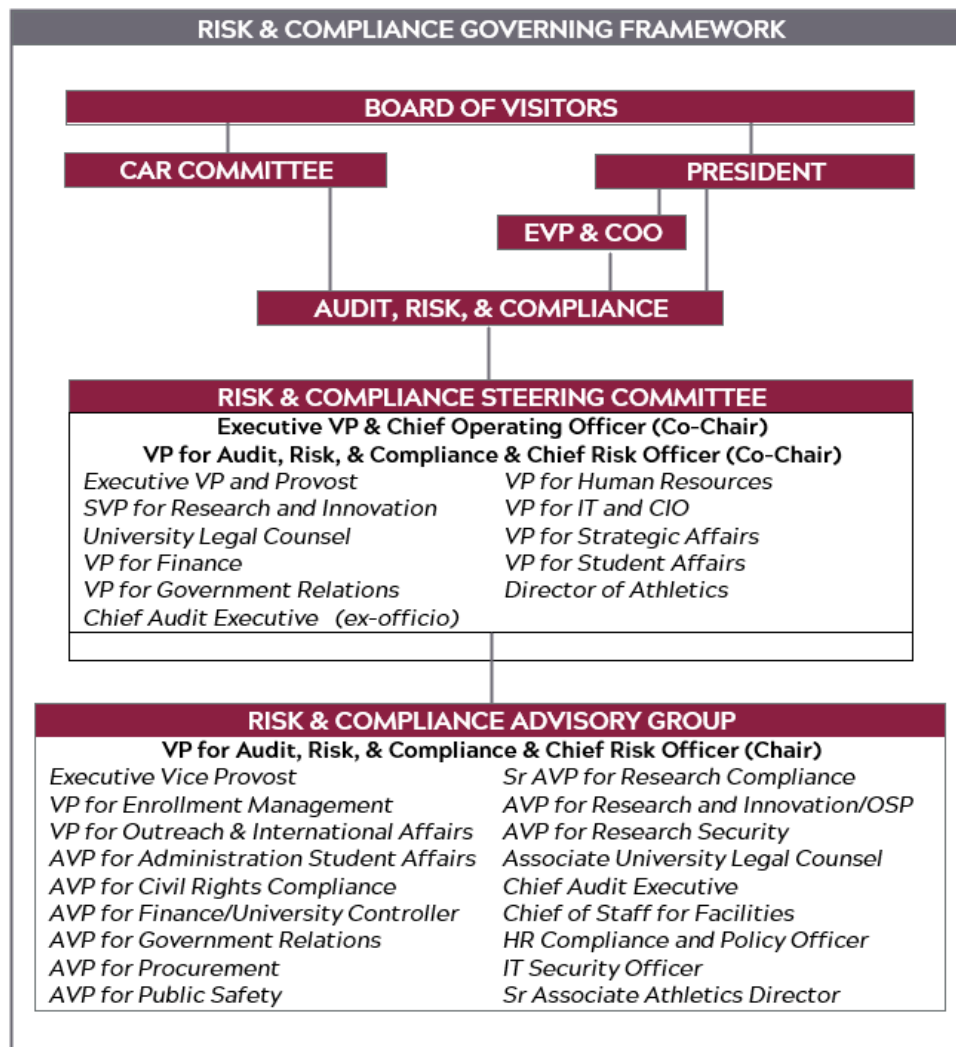
- support the university by promoting a culture of ethics and integrity including adherence to compliance-related policies and controls;
- continually seek to identify risks in their areas of operation that may be discussed with the Advisory Committee for insights and to identify potential efficiencies;
- review risk assessment results and propose university priorities and risk mitigation strategies;
- identify opportunities for continuous improvement including with respect to policies, training, and education needs in areas of noted risk;
- ensure appropriate ownership and accountability by risk and compliance owners including development of risk mitigation plans.

Risk and Compliance Owners

A risk and compliance owner is an accountable point of contact for a risk or compliance area. Owners are responsible for coordination of risk mitigation and compliance operations, including ensuring:

- risk assessments are periodically performed, including clearly articulating risk statements;
- internal stakeholders are assigned responsibility for each of the sub-risks identified within risk and compliance areas;
- regulatory changes are identified, assessed, managed, and monitored;
- adequate controls are in place and are integrated into daily activities, such as policies, training, and monitoring;
- gaps in mitigation and monitoring activities are identified and remediated;
- the status of mitigation and monitoring efforts are communicated to the Risk and Compliance Advisory Committee.

Framework Structure and Membership



Reporting and Accountability

The activities of the Steering Committee and Advisory Committee will be reported via their respective chairs to the Compliance, Audit, and Risk Committee of the Board of Visitors, shared with executive leadership, and included in an annual report as appropriate.

Meetings and Attendance

The Steering Committee and the Advisory Committee will each meet quarterly or more frequently as needed. Other members of the Virginia Tech community may be invited to attend meetings as needed. Certain agenda topics, special reports, or emerging issues may require conversations to be held under attorney-client privilege and such determination will be made by the University Counsel or designee.

Charter Revision Process

This charter will be periodically reviewed and amended as needed.