# Charter for the Office of Audit, Risk, and Compliance

**No. 3350**

**Policy Effective Date:**
2/9/1989

**Last Revision Date:**
11/19/2024

**Policy Owner:**
President Sands

**Policy Author:**
*(Contact Person)*
Sharon Kurek

1.0 Purpose
2.0 Policy
3.0 Procedures
4.0 Definitions
5.0 References
6.0 Approval and
Revisions

## 1.0 Purpose

This policy outlines the policies and procedures covering the Office of Audit, Risk, and Compliance (OARC) at Virginia Polytechnic Institute and State University and serves as a charter for the department.

## 2.0 Policy

It is the policy of the Compliance, Audit, and Risk (CAR) Committee of the Board of Visitors and the management of Virginia Polytechnic Institute and State University to support the maintenance of audit, risk, and compliance functions to assist in the effective discharge of their fiduciary responsibilities in assessing the effectiveness of the internal control environment.

The Office of Audit, Risk, and Compliance (OARC) performs comprehensive assurance services through independent internal audit and advisory activities, the university risk management process, and the institutional compliance program. OARC helps the university accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. OARC's mission is to enhance value through providing strategic insight, enabling informed decisions, and promoting integrity and compliance.

1. *Audit*: Provide independent, objective assurance and advisory activities designed to add value and improve university operations.
2. *Risk Management*: Provide oversight of the enterprise risk management (ERM) program by identifying, assessing, and managing risk by working with risk owners within the ERM process.
3. *Compliance*: Provide oversight of the institutional compliance program and the distributed processes that support compliance across the university by working with subject matter experts and compliance risk owners.

### 2.1 Scope of the Office of Audit, Risk, and Compliance

The scope of OARC's work is to determine whether Virginia Tech's network of risk management, internal controls, compliance activities, and governance processes, as designed and represented by management, are adequate and functioning in a manner to ensure:

- Programs, plans, and strategic objectives are achieved.
- Risks are appropriately identified, managed, and considered in institutional decision making.
- Processes for the collection and administration of significant financial, managerial, and operating information provide management with accurate, reliable, and timely data.

- Compliance with policies, procedures, standards, laws, regulations, contracts, or other requirements.

- Significant legislative or regulatory changes impacting the compliance activities are recognized and addressed properly.

- Resources are acquired, managed, and protected in an economical, efficient, and effective manner.

- Integrity, quality, and continuous improvement are fostered in the university's culture and control processes.

## 2.2 Accountability

The Vice President for Audit, Risk, and Compliance and Chief Risk Officer shall be accountable to senior leadership and the CAR Committee of the Board of Visitors to:

- Supervise the leaders responsible for Internal Audit and Institutional Compliance.

- Provide assessments on the adequacy and effectiveness of the university's processes for controlling its activities and managing its risks in the areas set forth under the mission and scope of work.

- Report significant issues related to the processes for controlling the activities of the university, including potential improvements to those processes, and provide information concerning such issues through resolution.

- Periodically provide information on the status and results of the annual audit plan, university compliance and risk management activities, and the sufficiency of department resources.

- Coordinate with, and provide oversight of, other compliance, control, and monitoring functions by working with subject matter experts and compliance risk owners.

## 2.3 Independence, Objectivity, and Professionalism

To provide for OARC's objectivity and professionalism, including the highest level of ethics and integrity, and maintain Internal Audit's independence:

- The Vice President for Audit, Risk, and Compliance and Chief Risk Officer reports to the President and the CAR Committee, and for day-to-day administrative oversight to the Executive Vice President and Chief Operating Officer.

- The Chief Audit Executive reports functionally to the CAR Committee and administratively to the Vice President for Audit, Risk, and Compliance and Chief Risk Officer.

- The Chief Compliance Officer reports to the Vice President for Audit, Risk, and Compliance and Chief Risk Officer and is accountable to the CAR Committee.

OARC personnel will exhibit the highest level of professional objectivity and integrity in gathering, evaluating, and communicating information about the activity or process being examined. OARC assessments will consider all relevant facts and circumstances, and OARC staff will not be influenced by their own personal interests or by others interests in forming judgments.

The internal audit function conducts its activities in accordance with the Institute of Internal Auditors' International Professional Practices Framework, which are the Global Internal Audit Standards and Topical Requirements. The Chief Audit Executive will report annually to the CAR Committee and senior management regarding Internal

Audit's conformance with the Global Internal Audit Standards, including maintaining its independence and objectivity, which will be assessed through an ongoing quality assurance and improvement program.

## 2.4 Authority

OARC is authorized to:

- Have unrestricted access, consistent with applicable law to all university functions, data, records, information, physical property, and personnel that they deem necessary to carry out their responsibilities. OARC will exercise discretion in their review and will remain accountable for confidentiality and safeguarding records and information.
- Have direct and unrestricted access to the President and the CAR Committee of the Board of Visitors.
- Allocate resources, set frequencies, select subjects, determine scope of work, and apply techniques, and issue communications to accomplish OARC objectives.
- Obtain assistance for specialized services from within or outside the university to complete engagements.

As Internal Audit is an independent function, OARC staff assigned to its mandate are not authorized to:

- Have direct operational responsibility or authority over any of the procedures, systems, or activities audited.
- Initiate or approve accounting transactions external to OARC.
- Direct the activities of any employee not employed by OARC, except to the extent such employees have been appropriately assigned to assist with OARC engagements or activities.

## 2.5 Responsibility

OARC has the responsibility to enhance and protect organizational value by:

*General:*

- Evaluating and assessing existing significant functions and new or changing services, processes, operations, and control processes coincident with their development, implementation and/or expansion of the university.
- Conducting investigations of suspected fraudulent and non-compliant activities and appropriately notifying relevant university management, the CAR Committee, and the appropriate authorities.
- Communicating directly with the CAR Committee on any matters considered to warrant its attention as appropriate, including trends and emerging issues that could impact the university.
- Maintaining a professional staff with sufficient knowledge, skills, experience, and professional certifications to meet the requirements of this charter.

*Enterprise Risk Management:*

Enterprise Risk Management, under the direction of the Vice President for Audit, Risk, and Compliance and Chief Risk Officer, provides services including, but not limited to:

- Planning, facilitating, and overseeing the university's efforts ERM processes.

- Executing the periodic university risk assessment process and advising risk owners in their identification, monitoring, and effectiveness of their mitigation activities.
- Ensuring risk management plans are maintained and university risk assessment results are reported to senior management and the CAR Committee.

### *Internal Audit:*

Internal Audit, under the direction of the Chief Audit Executive, provides services including, but not limited to:

- Coordinating audit activities to provide a central source of information for management and the CAR Committee regarding all audit activities and to provide comprehensive, cost-effective audit coverage for the university.
- Developing, submitting for approval, and executing a comprehensive risk-based annual audit plan that considers the input of the CAR Committee and senior management.
- Adjusting the internal audit plan, as necessary, in response to changes in the institution's risk, operations, programs, systems, and controls, and communicating significant changes to the plan with the CAR Committee and senior management.
- Performing, documenting, and communicating internal audit engagements in accordance with the Global Internal Audit Standards.
- Appraising the adequacy of actions taken by management to correct significant reported internal control weaknesses and deficient conditions, and reporting this information to the CAR Committee and responsible senior manager as appropriate.
- Establishing and maintaining a quality assurance and improvement program to evaluate Internal Audit's conformance with the Global Internal Audit Standards, including internal assessments (both ongoing and periodic) and external assessments conducted at least once every five years by a qualified, independent assessor or assessment team, the results of which will be presented to senior management and the CAR Committee.

### *Institutional Compliance:*

Institutional Compliance, under the direction of the Chief Compliance Officer, provides services including, but not limited to:

- Providing oversight of the institutional compliance program and the distributed processes that support compliance across the university by working with subject matter experts and compliance risk owners.
- Conducting periodic risk assessments to identify potential areas of compliance vulnerability and risk, and ensuring management ownership for monitoring and managing compliance risks.
- Advising institutional compliance risk owners and decentralized compliance risk management leadership.

## 2.6 Coordination with External Auditing Agencies

To ensure appropriate coordination and completeness of the CAR Committee reporting responsibilities, senior managers should promptly notify OARC of any external audits or reviews. OARC will coordinate its audit efforts with those of the Auditor of Public Accounts or other external auditing agencies by participating in the planning and definition of the scope of proposed audits, so the work of all auditing groups is complementary, and their combined efforts provide comprehensive, cost-effective audit coverage for the university. The Vice President for Audit, Risk, and Compliance and Chief Risk Officer, in consultation with the Chief Audit Executive, will work

with the appropriate members of management to determine the level of involvement of OARC, if any, in the performance of each external audit. Duplication of work will be avoided as much as possible.

# 3.0 Procedures

Principal guidance and direction on how OARC accomplishes its mission and responsibilities is provided to the staff through an office procedures manual. The manual promotes adherence to the Global Internal Audit Standards.

# 4.0 Definitions

**Abuse**
The excessive or improper use of a thing or policy, or employment of something in a manner contrary to the natural or legal rules for its use. Abuse includes the destruction, diversion, manipulation, misapplication, mistreatment, or misuse of university resources, as well as the extravagant or excessive use of one's position or authority. Abuse can occur in financial or nonfinancial settings.

**Advisory Services**
Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without assuming management responsibility.

**Assurance**
An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

**Charter**
The charter is a formal document that defines OARC's purpose, authority, and responsibility. The charter establishes the office's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities.

**Compliance**
Activities that support coordination, management, and monitoring of the risks associated with federal, state, and institutional laws, regulations, and policies.

**Conflict of Interest**
Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest could prejudice an individual's ability to perform his or her duties and responsibilities objectively.

**Control**
Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

**Control Environment**
The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control (e.g. integrity and ethical values; management's philosophy and operating style; organizational structure; and the assignment of authority and responsibility).

**Control Processes**
The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.

**Engagement**
A specific assignment, task, or review activity, such as an internal audit, control self-assessment review, fraud examination, or consultancy. An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.

**Enterprise Risk Management**
A process applied in strategy-setting and across the enterprise that is designed to identify potential events that may affect the entity, manage risk to be within the entity's risk tolerance, and support the achievement of entity objectives.

**Fraud**
The intentional misrepresentation or concealment of information in order to deceive, mislead, or acquire something of value. Fraud is an intentional deception perpetrated to secure an unfair advantage or personal benefit.

**Governance**
The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives. The governance process includes: promoting appropriate ethics and values within the organization; ensuring effective organizational performance management and accountability; communicating risk and control information to appropriate areas of the organization; and coordinating the activities of and communicating information among the board, external and internal auditors, and management.

**Independence**
The freedom from conditions that threaten the ability of a function to carry out its responsibilities in an unbiased manner.

**International Professional Practices Framework**
The conceptual framework that organizes the authoritative guidance promulgated by the Institute of Internal Auditors. Authoritative guidance is comprised of two categories including mandatory guidance (Global Internal Audit Standards, Topical Guidance) and supplemental guidance (global practice guides).

**Objectivity**
An unbiased mental attitude that allows individuals to make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments. Objectivity requires that individuals do not subordinate their judgment on matters to others.

**Risk**
The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is commonly measured in terms of impact, likelihood, and velocity.

**Risk Management**
A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

**Significance**
The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors, such as magnitude, nature, effect, relevance, and impact. Professional judgment assists internal auditors when evaluating the significance of matters within the context of the relevant objectives.

**Waste**
The careless expenditure, consumption, mismanagement, use, or squandering of university resources. Waste also includes incurring unnecessary costs due to inefficient or ineffective practices, systems, or controls.

## 5.0 References

Section 2.1-155.3 of the *Code of Virginia*, enacted in 1984.

*State Fraud, Waste, and Abuse Hotline Policies and Procedures Manual*, Office of the State Inspector General, Commonwealth of Virginia, 2023 edition.

The Institute of Internal Auditors' International Professional Practices Framework, including the Global Internal Audit Standards, effective January 2025.

## 6.0 Approval and Revisions

- Revision 0

  Approved February 9, 1989, by the Director of Internal Audit, David C. Goodyear.

- Revision 1
  Annual review. Section 2.8 - changed so that reports "approved" by the Finance and Audit Committee of the Board of Visitors shall be available to the public.

  Approved March 29, 1990, by the Director of Internal Audit, David C. Goodyear.

- Revision 2
  Changes were made to eliminate minor discrepancies between the audit manual and the policy statement as presented to the Board of Visitors.

  Approved November 3, 1995, by the Director of Internal Audit, David C. Goodyear.
  Annual review, November 5, 1998, by Office of the Executive Vice President. No revisions.

- Revision 3
  Policy updated to reflect review by the Finance and Audit Committee of the Board of Visitors. Policy serves as a charter for the Internal Audit Department.

Approved March 29, 2004 by the Executive Vice President and Chief Operating Officer, Minnis E. Ridenour.
Approved March 29, 2004 by the Finance and Audit Committee of the Board of Visitors.

- Revision 4
  Policy updated to reflect review by the Finance and Audit Committee of the Board of Visitors, in conjunction with the Internal Audit Department's quality assurance review.

  Approved March 14, 2005 by the Executive Vice President and Chief Operating Officer, James A. Hyatt.
  Approved March 14, 2005 by the Finance and Audit Committee of the Board of Visitors.

- Revision 5 April 1, 2008:
  Updates to position titles and/or responsibilities due to university reorganization.

- Revision 6
  - Policy title changed from "Internal Audit Department" to "Internal Audit Charter."
  - Section 2.2 revised to reflect change in Director of Internal Audit reporting relationship.
  - Sections 2.5 and 2.7 revised to clarify the role of Internal Audit and the standards under which it conducts its activities.
  - Section 2.9 revised to clarify the process for senior management areas submitting corrective action plans.

  Approved November 7, 2011 by the university President, Charles W. Steger.
  Approved November 7, 2011 by the Finance and Audit Committee of the Board of Visitors.

- Revision 7
  - Full technical review correcting grammatical, punctuation, word usage, sentence structure, and minor content and/or format inconsistencies. The charter was also revised to incorporate the concept of objectivity, and to include applicable procedures and definitions.
  - Policy title changed from "Internal Audit Charter" to "Charter for the University's Internal Audit Function."

  Approved November 9, 2015 by the Finance and Audit Committee of the Board of Visitors and President, Timothy D. Sands.

- Revision 8
  Revised to address the reorganization of the Board of Visitors' committee structure and additional responsibilities with regard to risk management and compliance. Additional revisions were made to reflect revised guidance from the Institute of Internal Auditors.

  Approved November 5, 2017 by the Compliance, Audit, and Risk Committee of the Board of Visitors and President, Timothy D. Sands.
- Revision 9
  Revisions from technical review correcting grammatical, punctuation, word usage, sentence structure, and minor content and/or format inconsistencies.

  Approved November 18, 2019 by the Compliance, Audit, and Risk Committee of the Board of Visitors and President, Timothy D. Sands.

- Revision 10

  Revisions from technical review correcting grammatical, punctuation, and minor format inconsistencies. Additionally, section 2.9 was revised to clarify expectations on OARC's responsibility for coordinating external audits and reviews.

  Approved November 15, 2020 by the Compliance, Audit, and Risk Committee of the Board of Visitors and President, Timothy D. Sands.

- Revision 11

  Revised to delineate the roles and responsibilities for internal audit, enterprise risk management, and the institutional compliance program. Additional revisions were made to streamline for consistency.

  Approved November 14, 2022 by the Compliance, Audit, and Risk Committee of the Board of Visitors and President, Timothy D. Sands.

- Revision 12

  Updates to position titles and reporting lines due to university reorganization.

  Approved June 5, 2023 by the Compliance, Audit, and Risk Committee of the Board of Visitors and President, Timothy D. Sands.

- Revision 13

  Updates to Internal Audit mandate throughout to align with updated Global Internal Audit Standards.

  Approved November 19, 2024 by the Compliance, Audit, and Risk Committee of the Board of Visitors and President, Timothy D. Sands.