



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

### No. 3350

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

**Last Revision Date:**  
11/18/2019

**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 an internal audit function to assist in the effective discharge of their fiduciary responsibilities in assessing the effectiveness internal control environment.

The Office of Audit, Risk and Compliance (OARC) performs independent internal audits, plans and oversees the university risk management process, and oversees the institutional compliance program. The OARC's mission is to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight as follows:

1. *Audit*: Provide independent, objective assurance and advisory activity designed to add value and improve university operations. It 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.
2. *Risk Management*: Provide oversight of the enterprise risk management (ERM) program by creating and maintaining the framework to identify, assess, and manage risk.
3. *Compliance*: Provide oversight of the institutional compliance program (ICP) and the distributed processes that support compliance across the university.

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

The scope of OARC work is to determine whether Virginia Tech's 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.
- Significant financial, managerial and operating information is accurate, reliable and timely.
- Compliance with policies, procedures, standards, laws, and regulations.
- Measures are taken to foster continuous improvement in control processes.
- Resources are acquired, managed, and protected in an economical, efficient, and effective manner.



## 2.2 Independence and Objectivity

Independence is essential to enable the internal audit function to accomplish its purpose. Accordingly, the Executive Director of Audit, Risk, and Compliance reports functionally to the CAR committee and also serves in a staff role to the committee. For day-to-day operations, the Executive Director of Audit, Risk, and Compliance reports administratively to the President. These reporting relationships allow for direct and unrestricted access to the President and the CAR Committee of the Board of Visitors.

All work will be conducted in an objective and independent manner. Staff will maintain an impartial attitude in selecting and evaluating evidence and in reporting results. Independence in fact and appearance enables unbiased judgments essential to the proper conduct of the department's scope of work. OARC staff have the responsibility to maintain high standards of conduct, professionalism, independence, and character to carry out proper and meaningful internal auditing within the university.

Internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, internal auditors will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that would normally be audited. Therefore, internal audit review and appraisal procedures do not in any way substitute for the responsibilities assigned to other persons in the organization.

## 2.3 Authority

OARC has unrestricted access to all university departments, records, reports, activities, property, and personnel that they deem necessary to discharge their audit responsibilities. OARC will exercise discretion in the review of records to assure the necessary confidentiality of matters that come to its attention.

OARC will allocate resources, set frequencies, select subjects, determine scopes of work, apply techniques required to accomplish audit objectives, and issue reports. OARC will also obtain assistance for specialized services from within or outside the university in order to complete engagements.

## 2.4 Auditing Standards

The internal audit function will conduct its activities in accordance with the Institute of Internal Auditors' International Professional Practices Framework including the Core Principles for the Professional Practice of Internal Auditing, Code of Ethics, the International Standards for the Professional Practice of Internal Auditing, and the Definition of Internal Auditing.

## 2.5 Systems Planning and Development

Management will consult OARC during the planning, development, and modification of major financial or operating systems and procedures (manual and automated) to ensure that:

- Reasonable and adequate internal controls exist.
- Systems or procedural documentation is complete and appropriate.
- An adequate audit trail exists.

OARC's participation will be designed to: (a) help ensure safeguarding of information assets and compliance with appropriate procedures, and (b) aid management efficiency by avoiding costly systems or procedural changes at later dates.



## 2.6 Responsibilities of the Executive Director of Audit, Risk, and Compliance

The Executive Director of Audit, Risk, and Compliance has primary responsibility for the proper maintenance and management of OARC to ensure that the work fulfills the purposes and responsibilities established in this policy statement. The Executive Director of Audit, Risk, and Compliance is specifically charged with the following responsibilities:

- Coordinating all auditing activities to provide a central source of information for management and the CAR Committee of the Board of Visitors regarding all audit activities and to provide comprehensive, cost-effective audit coverage for the university.
- Facilitating the university's efforts regarding enterprise risk management (ERM) on behalf of senior management and the CAR Committee of the Board of Visitors.
- Coordinating the university's Institutional Compliance Program (ICP) to be a resource and serve as a catalyst for the achievement of university best practices in compliance-related subject matter areas.
- Establishing written policies and procedures for OARC and directing its technical and administrative functions.
- Developing, submitting for approval, and executing comprehensive risk-based annual audit plans to carry out departmental responsibilities.
- Maintaining a professional audit staff with sufficient knowledge, skills, experience, and professional certifications to meet the requirements of this charter, and provide information on the sufficiency of department resources.
- Recommending improvements in controls designed to increase efficiency, safeguard university resources, and ensure compliance with government laws and regulations.
- Issuing an annual summary report of activities to the CAR Committee of the Board of Visitors.
- Appraising the adequacy of the action taken by management to correct significant reported internal control weaknesses and deficient conditions, and reporting this information at least quarterly to the responsible Vice Presidents and the university's Chief Business Officer, or their designees.
- Establishing and maintaining a Quality Assurance and Improvement Program to evaluate the operations of the department, including periodic internal self-assessments and external peer reviews at least once every five years by qualified persons who are independent of the university, the results of which will be presented to senior management and the Board of Visitors.
- Communicating directly with the CAR Committee of the Board of Visitors any matters considered to warrant its attention as appropriate, including trends and emerging issues that could impact the university.
- Performing sufficient tests and examinations to determine and report to management, the CAR Committee of the Board of Visitors, and the appropriate authorities the extent of any fraud, waste, and abuse detected by audit or otherwise and to identify the weaknesses in control procedures that may have allowed the fraudulent activity to occur. The investigation of the specific event with the objective or recovery and/or prosecution is the responsibility of the appropriate law enforcement agency and Commonwealth's Attorney based on jurisdiction.



## 2.7 Audit Reports

OARC will issue audit reports and/or memoranda in all audit activities performed. The format and style of the report will be determined by the Executive Director of Audit, Risk, and Compliance, depending upon the nature and conditions surrounding the audit. Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans. The formulation of overall opinions requires consideration of the engagement results and their significance. All reports on engagements scheduled in the annual audit plan will be issued to the members of the CAR Committee of the Board of Visitors; the President; appropriate senior management; and other appropriate personnel as deemed necessary by the Executive Director of Audit, Risk, and Compliance. In addition, reports approved at open meetings of the committee shall be made available to the public in accordance with state statutes. In certain circumstances, the Executive Director of Audit, Risk, and Compliance may decide, with the approval of the Chair of the CAR Committee of the Board of Visitors, to restrict the issuance of an audit report to certain members of management and/or the committee.

## 2.8 Responsibility for Corrective Action

Senior management to whom the audited department, activity, or agency reports organizationally is responsible for the issuance of a written response to recommendations made or deficient conditions reported by the internal audit function. The responses should be submitted to the Executive Director of Audit, Risk, and Compliance for inclusion in the issued audit report. At each meeting, the committee will receive status updates of recommendations in the process of implementation.

## 2.9 Coordination with External Auditing Agencies

The Executive Director of Audit, Risk, and Compliance will coordinate the department's 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. Duplication of work will be avoided as much as possible.

## 2.10 Special Projects

The Executive Director of Audit, Risk, and Compliance is empowered to conduct special audit projects, reviews, advisory services, or investigations at the request of the President, Vice Presidents or their designee, and the CAR Committee of the Board of Visitors to assist management in meeting its objectives, promoting economy and efficiency in the administration of, or preventing and detecting fraud, waste, and abuse in its programs and operations, examples of which may include facilitation, training, and advisory services.

## 3.0 Procedures

Principal guidance and direction on how OARC accomplishes its mission and responsibilities is provided to the audit staff through an office procedures manual. The manual promotes adherence to the International Professional Practice Framework developed by the Institute of Internal Auditors



## 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 resources, as well as the extravagant or excessive use of one's position or authority. Abuse can occur in financial or nonfinancial settings.

### **Add Value**

The internal audit function adds value to the organization (and its stakeholders) when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management, and control processes.

### **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 the internal auditor 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.

### **Code of Ethics**

The Code of Ethics of The Institute of Internal Auditors (IIA) are principles relevant to the profession and practice of internal auditing, and rules of conduct that describe behavior expected of internal auditors. The purpose of the Code of Ethics is to promote an ethical culture in the global profession of internal auditing.

### **Compliance**

Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

### **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.

### **Executive Director of Audit, Risk, and Compliance**

The individual who serves as the chief audit executive and is responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the IIA's Definition of Internal Auditing, the Core Principles, the Code of Ethics, and the *Standards*.

### **Engagement**

A specific internal audit 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.

### **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 the internal audit function to carry out internal audit responsibilities in an unbiased manner.

### **Internal Audit Function**

The department, division, team of advisors, or other practitioner(s) that provides independent, objective assurance and advisory services designed to add value and improve an organization's operations.





### **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: (1) mandatory and (2) strongly recommended.

### **Objectivity**

An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others.

### **Risk**

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

### **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.

### **Scope**

A statement that specifies the focus, extent, and boundary of a particular audit. The scope can be specified by defining the physical location of the audit, the organizational units that will be examined, the processes and activities that will be included, and the time period that will be covered.

### **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.

### **Standards**

A professional pronouncement that delineates the requirements for performing a broad range of internal audit activities, and for evaluating internal audit performance.

### **Waste**

The careless expenditure, consumption, mismanagement, use, or squandering of university. 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, 2018 edition.

The Institute of Internal Auditors' International Professional Practices Framework, including the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the *International Standards for the Professional Practice of Internal Auditing (Standards)*, and the Definition of Internal Auditing, revised in 2016 and effective 2017.



## 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.





## Virginia Polytechnic Institute and State University

- 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.