Virginia Tech

Office of Audit, Risk, and Compliance
Fiscal Year 2024–25 Audit Plan
June 10, 2024

OVERVIEW

The Office of Audit, Risk, and Compliance (OARC) conducts risk-based assurance engagements, policy compliance reviews, management advisory services, and investigations. The risk-based assurance engagement is an objective examination of evidence to provide an independent assessment of governance, risk management, and the control systems within the university. The objective of the policy compliance review is to ensure all senior management areas (even low risk) receive periodic reviews from OARC every five years to perform tests of compliance with major university business policies. The nature and scope of management advisory service activities, developed through agreement with the client, add value and improve the university's governance, risk management, and control processes without the internal auditor assuming management responsibility.

RISK ASSESSMENT PROCESS

Enterprise Risk Assessment

The university instituted an Enterprise Risk Management (ERM) initiative during fiscal year 2017–18 to provide enhanced visibility into the university's risks and to align strategic planning with the resulting risk awareness. OARC facilitates the ERM program by working with university leadership to establish and maintain the framework for collectively identifying and assessing risks across the enterprise. The ERM program intends to strengthen the university's ability to achieve its mission and strategic objectives by:

- Obtaining a holistic view of the most critical risks to the achievement of Virginia Tech's mission and objectives;
- Creating a risk-aware culture, including the management of risks to an appropriate level;
- Improving focus and perspective on both internal and external risks and opportunities, including emerging risks and value drivers;
- Enhancing decision making and alignment with strategic goals; and
- Improving efficiency and optimizing allocation of resources through risk prioritization.

University leadership provided feedback to the ERM process by identifying risks and assessing the risks in terms of likelihood of occurrence, significance of impact, and velocity of onset, all grouped by the categories depicted below:

ERM RISK CATEGORIES	ALTITUDES OF RISK
Strategic	Systemic and Existential
Financial	Institutional
Compliance	Unit-Level
Operational	
Reputational	

In order to maximize efficiency and engagement from university senior leadership, OARC leveraged this complimentary process as an element of the traditional annual risk assessment in support of audit plan development.

OARC Audit Planning Risk Assessment

University departments and administrative operations were grouped into approximately 175 auditable entities or responsibility centers based on common missions and the existing organizational structure. For each auditable entity, OARC reviewed financial data, including expenditures, revenues, cash receipts, federal contracts and grants, and total employees. The relative risk was assessed on a judgmental basis for the following qualitative and quantitative factors.

RISK FACTORS
Quality and Stability of Control Environment
Business Exposure (Materiality and Liquidity of Operational Resources)
Public and Political Sensitivity
Compliance Requirements
Information Technology and Management Reporting

Elements considered within these factors included:

- Management's awareness of internal controls;
- Stability and expertise of management;
- Interval since the last audit review;
- Complexity of operations and technology applications;
- Materiality or financial impact to the university;
- Potential impact to reputation;
- Impact of noncompliance with internal and external policy, procedure, regulatory, and statutory requirements; and
- Reliance on information and management reporting for operating decisions, monitoring performance, providing services, and allocating resources.

Auditable Entities Risk Ranking

■ HIGH ■ MEDIUM ■ LOW
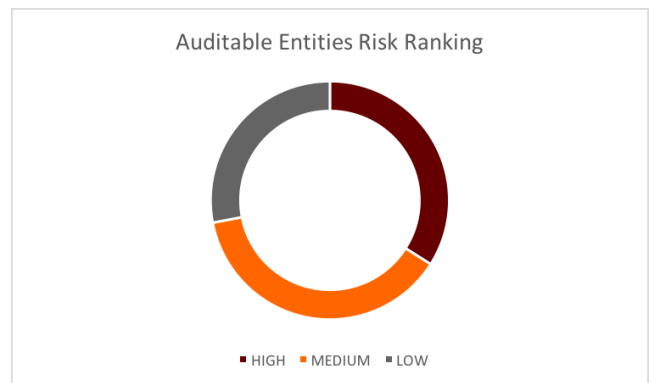
The chart depicts the results of the risk assessment classifications. The risk assessment results were consistent with previous risk assessments conducted by OARC.

IT Risk Assessment

OARC has also created a university-wide information technology (IT) risk-based audit plan mapped to the ISO 27002 standard, a best practice for developing and maintaining enterprise-wide IT security that is also referenced by university policies. OARC consulted with key IT personnel to ensure that audit coverage is maximized and properly targeted.

The IT risk assessment is driven by the Center for Internet Security's Critical Security Controls and Virginia Tech's Minimum Security Standards, which lay the IT security foundation for the university. OARC considers these controls and the relative risk of the decentralized computing environment as it identifies the topical audits in the plan. Careful consideration is made to ensure coverage includes administrative, academic, and research computing.

The IT audit approach includes a variety of topical audits to gain a better understanding of the university-wide environment instead of narrowly focusing on the performance of individual departments. This approach also allows OARC to maintain current knowledge of the IT security and operating conditions in a dynamic industry through the constant evaluation and reassessment of planned audit engagements.

CORE AUDIT PLAN

OARC has identified certain critical areas for inclusion in the core audit plan to ensure that adequate coverage is provided over a reasonable time. To obtain additional insight and to validate the plan, OARC management conducted surveys and discussions with senior leadership to identify reputation factors, regulatory changes, organization shifts, new initiatives, and deployment of new systems or technology tools.

The critical areas for core audit plan inclusion are:
- Academic Units
- Auxiliary Enterprises and Athletics
- Campus Safety and Security
- Enrollment Services
- Facilities and Operations
- Financial Management
- Human Resources
- Information Technology
- Off-Campus Locations
- Research
- Student Services

The core audit plan includes several multi-year audits that will allow for ongoing reviews of selected components of entities with high external compliance risk and complex operations. These entities are Athletics, Human Resources, Research, and University Scholarships and Financial Aid.

FISCAL YEAR 2024–25 AUDIT PLAN

The audit plan focuses on delivering value to Virginia Tech with an emphasis on the following risk areas: strategic, operational, financial, compliance, and IT. If new topics emerge during the audit plan period that require more immediate attention, reconfiguration of the plan can be undertaken to accommodate these changes. The fiscal year 2024–25 audit plan includes 30 projects, and OARC's goal is to complete 85 percent of the audit plan. As each audit is undertaken, risks will be re-evaluated to ensure proper audit coverage with consideration of confidentiality, integrity, and availability.

Risk-Based Assurance

Planned Engagement	Overview	Risk Area
Athletics *	The Department of Athletics, an approximately $121.8 million enterprise, sponsors 22 athletic teams at the NCAA Division I level. A component of Athletics is included in the audit plan each year.	Compliance - Athletics
Bursar	The specific responsibilities of the Office of the University Bursar (OUB) include: providing timely and accurate billings to students and general users of the university's services and ensuring that payments and credits are received and properly applied to each customer's account in a timely manner, receipt and timely application of all other cash payments made to the university, and disbursement of payroll, all university payables, and collection of delinquent accounts and notes receivable. The last audit of the OUB was in 2019.	Financial – Financial Management
Data Analytics: Subscription Services	This review will seek to look across the various procurement avenues and analyze data looking for ongoing or continuous subscriptions, be that for technology or other services. The premise is to identify efficiencies where multiple subscriptions could be combined for savings, instances where university pricing is not being leveraged, or places where unnecessary subscriptions are being utilized. A review has not previously been completed.	Operational – Financial Management
Electrical and Computer Engineering	The Bradley Department of Electrical and Computer Engineering (ECE) is one of the country's larger ECE departments. ECE offers bachelor, masters, and doctoral degrees in electrical and computer engineering with education and research opportunities in diverse areas, including control systems, computers, communications, electronics, electromagnetics, and power. ECE was last reviewed in 2015.	Operational – Academic
Environmental Health and Safety	Environmental Health and Safety provides institutional support and oversight for departments in maintaining regulatory requirements of laboratory safety and chemical hygiene. Department personnel perform routine inspections of areas both on and off campus. Additionally, the department provides training mandated by many federal and state agencies. The department was last reviewed in 2015.	Operational – Safety and Security
Human Resources: Benefits *	Human Resources administers the Commonwealth benefits program and provides benefit management and guidance for approximately 7,500 faculty and staff. The benefits program is an integral part of the university's employee compensation package and includes health insurance, leave, legal resources, retirement plans through the Virginia Retirement System, tuition assistance, and workers compensation. This function was last reviewed in 2019.	Operational – Human Resources

Planned Engagement	Overview	Risk Area
Immigration Services	As a global land-grant university, the institution teaches and employs a diverse set of international faculty, staff, and students. To assist these individuals in navigating the complex regulatory immigration environment, the institution has established several offices to provide support and to ensure compliance requirements are being met. Various components of these efforts have previously been reviewed in 2018.	Compliance – Human Resources and Student Services
IT: Cloud Services	Cloud service provider risk encompasses concerns such as data security, compliance issues, service reliability, and vendor lock-in. The institution faces challenges related to data protection, downtime, and dependency on a single provider. To mitigate these risks, the institution conducts risk assessments and security reviews. This engagement will assess these practices and evaluate controls for ongoing oversight. This was last reviewed in 2013.	Operational – Information Technology
IT: Network Infrastructure and Services	Network Infrastructure and Services (NI&S) provides and manages the university's data, voice, and video networks and related services. A component of NI&S, network security, was last reviewed in 2017.	Operational – Information Technology
IT: Security Operations Center	The institution recently engaged with OmniSOC, a shared security operation center (SOC) that specializes in higher education and research institutions. OmniSOC delivers critical security alerts through ongoing monitoring 24/7. As a new risk mitigation and control strategy, it has never been reviewed.	Operational – Information Technology
National Security Institute	The National Security Institute (NSI), founded in September 2021, is aspiring to become the nation's preeminent academic organization at the center of research, technology, policy, and talent development to advance national security. As one of the university's thematic institutes, NSI will further the interdisciplinary faculty with unique research infrastructure to answer practical national security issues. This institute has never been reviewed.	Operational – Research
Programs for Minors	Educational programming and activities involving minors are integral to the institution's engagement mission. The university recognizes that ensuring the safety and well-being of minors on campus is imperative. Formed in 2020, the Office of Youth Protection, within the College of Agriculture and Life Sciences, is responsible for the oversight and operating standards for programs involving minors on campus. These processes were last reviewed in 2019.	Compliance – Safety and Security
Recreational Sports	Recreational Sports provides opportunities for students, faculty, and staff to engage in physical activities to create healthy lifestyle habits. A department within the Division of Student Affairs, Recreational Sports deploys many strategies and manages multiple facilities to meet its goals. This department was last reviewed in 2017.	Operational – Student Services
Research: Cost Sharing	Cost sharing is the portion of a project or program cost that is not reimbursed by the sponsor. In a proposal or an award, cost sharing represents a commitment by the university. Cost sharing can be both mandatory, in which the sponsor requires the sharing as a condition of the award, or voluntary, wherein it is not required by the sponsor but the university offers cost sharing to be more competitive. Compliance with federal cost accounting standards requires that cost sharing expenses be treated in a consistent and uniform manner. The last cost sharing review was in 2015.	Compliance – Research

Planned Engagement	Overview	Risk Area
School of Plant and Environmental Sciences	The School of Plant and Environmental Sciences, within the College of Agriculture and Life Sciences, seeks to train the next generation of professionals in the fields of plant breeding and genetics, agronomic and horticulture crop production, plant protection, soil and water systems management, agricultural technologies, environmental restoration, and agro-environmental stewardship. The school had an advisory review in 2019.	Operational – Academic
Subrecipient Monitoring	Federal regulations require prime recipients to monitor subawards and to assure subrecipients meet their obligations and are in compliance with federal requirements. The Office of Sponsored Programs has established policies and procedures that outline responsibilities and actions that must occur in the subrecipient processes. These controls were last reviewed in 2019.	Compliance – Research
Undergraduate Admissions	Undergraduate Admissions seeks to attract, recruit, and enroll a highly qualified, talented, and diverse student body. In addition to hosting thousands of prospective students each year, undergraduate admissions reviews over 45,000 applications through partnerships across the campus community. This department was last reviewed in 2020.	Compliance – Enrollment Services
University Building Official	The University Building Official, an office within the Division of Campus Planning, Infrastructure, and Facilities, has primary responsibility for the proper management for, and enforcement of, the Virginia Uniform Statewide Building Code to ensure that construction projects conducted on university property are completed in compliance with code, related laws, and regulations. The office serves as the primary liaison with outside regulatory agencies. This department was last reviewed in 2019.	Operational – Facilities and Operations
VT India	The institution has had a presence in South Asia countries since 2009, with research ties going back further. In 2023, the institution inaugurated a new satellite office in the IIT Madras Research Park in Chennai. The university maintains several collaborative partnerships across India. These activities have never been reviewed.	Operational – Off-Campus Locations

* Entity receives an annual audit on different components of their operation.

University Policy Compliance Reviews

OARC will continue its program of limited scope reviews of senior management areas. These reviews evaluate major aspects of a department's administrative processes using internal control questionnaires and limited testing that provides broad audit coverage ensuring compliance with university policies on campus.

Planned Engagement	Risk Area
Agricultural Research and Extension Centers: Hampton Roads, Middleburg, Reynolds, Southwest Virginia, Tidewater	Operational
College of Liberal Arts and Human Sciences	Operational
College of Natural Resources and Environment	Operational
Vice President and Dean for Graduate Education	Operational
Vice President for Information Technology	Operational

Management Advisory Services

Planned Engagement	Overview	Risk Area
Central Funds	The university maintains a series of centrally managed funds for a variety of purposes. This project will review the controls utilized to ensure appropriate oversight and use of these funds.	Operational – Financial Management
CMMC Readiness	The Department of Defense is nearing the end of a lengthy rule-making process called the Cybersecurity Maturity Model Certification (CMMC). Once implemented, the goal is to reinforce cybersecurity safeguards across sensitive unclassified information. While the exact regulatory timeline is unknown, this project will review the steps taken by the institution to prepare for this regulation.	Compliance – Information Technology
Corps of Cadets Armory	This review will ensure critical controls are included as the Corps of Cadets establishes its first armory.	Compliance – Safety and Security
Data Analytics: Research Compliance Dashboard	Over the past several years, Internal Audit has increased the depth and breadth of its research data analytics capabilities. This project seeks to formalize these efforts into routine processes and dashboards to provide a more robust and routine look at common research compliance risks.	Compliance – Research
Research Accounting Processes – HERD	The National Science Foundation's Higher Education Research and Development (HERD) survey is the primary source of information on research and development expenditures at U.S. colleges and universities. The survey collects information on research expenditures by field of research and source of funds and gathers information on types of research, expenses, and headcounts of personnel. The survey is an annual census of institutions. At the university, the survey is a collaboration of processes that is spearheaded by the Controller's Office. This review will look at processes and procedures used to compile and review the survey for accuracy.	Operational – Financial Management
Research: Post-Award Processes	The Office of Sponsored Programs has recently updated certain post-award processing efforts and has changed the way information flows across the department. This project seeks to assist management in understanding the flow of information and identify any potential effectiveness or efficiencies that can be gained within the updated processes.	Compliance - Research

Special Projects and Annual Audit Activities

Activity	Overview
Special Projects	Investigate fraud, waste, and abuse allegations.
Annual Audit Activities (Follow-up, Inventory)	Conduct follow-up audit procedures to ensure that management is implementing controls as described within their responses to audit report recommendations.
External Audit Coordination	Manage and serve as the liaison for all external audit services, including contracted and regulatory-imposed audits.

AUDIT RESOURCES

The fiscal year 2024–25 audit plan is based on professional staffing of 12 full-time equivalents (FTEs). This plan includes a small adjustment to reflect historic trends of some turnover and extended family leave within the fiscal year. Staffing will continue to be augmented by the continuation of the student internship program in which two Virginia Tech students are employed.

Approximately 75 percent of OARC's available resources are committed to the completion of planned audit projects, management advisory reviews, and investigations. The annual audit plan is designed to provide appropriate coverage utilizing a variety of audit methodologies, including audits of individual units, functional and process audits, university-wide reviews, and information system projects. OARC conducts follow-up audit procedures throughout the year to ensure that management is implementing controls as described within their responses to audit report recommendations.

Audit resources are allocated as follows:
- 55 percent of OARC's available resources are committed to the completion of planned audit projects and follow-up audit procedures.
- 11 percent to accommodate requests from management and consultations with university departments.
- 7 percent to conduct investigations into fraud, waste, and abuse allegations.
- 12 percent for employee professional development, internal quality improvement projects, and other internal administrative functions.
- 15 percent for compensated absences such as annual, sick, and holiday leave.

AUDIT PLAN MAPPED TO ERM

As part of the ERM program, university leadership has identified key residual risks across six thematic areas. This year's plan spans all six thematic areas and 11 of 23 risk areas. Specific risk areas include:
- Athletics
- Employee Recruitment & Retention
- Enrollment Management
- Facilities
- Global Engagement
- Health, Safety, & Security
- Legal & Regulatory
- Research Compliance
- Resource Diversification & Management
- Student Wellness & Experience
- Technology & Security