Office of Audit, Risk, and Compliance
Fiscal Year 2025–26 Audit Plan
June 2, 2025

OVERVIEW

Internal Audit conducts risk-based assurance engagements, IT general controls 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. IT general controls reviews seek to align Internal Audit's assurance activities with the Information Technology Security Office's guidance and efforts to increase the overall efficiency and effectiveness of IT risk coverage across the institution on an on-going basis. The nature and scope of management advisory service activities add value and improve the university's governance, risk management, and control processes without the internal auditor assuming management responsibility. Investigations are initiated from various sources, including the Office of Audit, Risk, and Compliance (OARC) managed Hokie Hotline, and are coordinated through the institutional compliance program with support from Internal Audit, as appropriate.

RISK ASSESSMENT PROCESS

Enterprise Risk Assessment

The institution's Enterprise Risk Management (ERM) program provides enhanced visibility into the university's risks and aligns strategic planning with risk awareness. OARC facilitates the ERM program by working with university leadership to establish and maintain the framework for collectively identifying, assessing, and managing 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, Internal Audit leveraged this complimentary process as an element of the traditional annual risk assessment in support of audit plan development.

OARC Audit Planning Risk Assessment

Departments and administrative operations were grouped into approximately 175 auditable entities 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
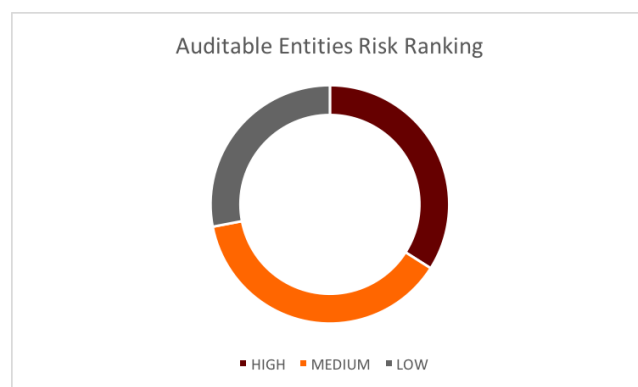
The chart depicts the results of the risk assessment classifications. The risk assessment results were consistent with previous risk assessments conducted by OARC.

IT Risk Assessment

Internal Audit 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 institution's IT security foundation. 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 is bifurcated into two processes. First, the risk assessment contemplates topical audits to gain a better understanding and provide confidence on the university-wide control environment. Second, each senior management area receives a dedicated information technology general controls review to assess compliance with the institution's Minimum Security Standards on a cyclical basis. Beginning with this audit plan, Internal Audit will accelerate its prior five-year review cycle to a three-year cycle.

CORE AUDIT PLAN

Internal Audit 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 compliance risk and complex operations. These entities are Athletics, Human Resources, Research, and University Scholarships and Financial Aid. While most years these four entities receive audit coverage, this is subject to external coverage and evaluated in light of the comprehensive risk assessment.

FISCAL YEAR 2025–26 AUDIT PLAN

The audit plan focuses on delivering value to the institution 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 2025–26 audit plan includes 34 projects, and Internal Audit'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
Affiliated Corporations	The institution maintains an extensive relationship with a matrix of affiliate corporations. These efforts seek to ensure selected corporations are meeting fiduciary responsibilities and appropriately managing risks. These efforts are coordinated with the Controller's Office and first started in 2025.	Operational – Financial Management
Air Transportation Services	Air Transportation Services, a unit within the Division of Auxiliary and Business Services, provides safe, on-demand air transportation for employees, or employees of university-related corporations, on official university business. The department is staffed by five pilots and supported by a flight operations manager and operates from a hangar located at the Virginia Tech Montgomery Executive Airport. The last audit was conducted in 2011.	Compliance – Operations
Animal Care and Resources	The Animal Resources and Care division provides resources and expertise to support scientifically sound animal research and teaching activities using healthy animals in the appropriate environment. By applying current veterinary standards and animal welfare practices that meet or exceed regulatory requirements, the division ensures humane animal care and use. The last audit was conducted in 2018.	Compliance - Research
Athletics *	The Department of Athletics, an approximately $120 million enterprise, sponsors 22 athletic teams at the NCAA Division I level. A component of Athletics is typically 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 was conducted in 2019.	Financial – Financial Management
Capital Construction Audit Program	The institution has maintained an on-going capital construction audit program for all capital projects utilizing the guaranteed maximum price contracting methodology. Executed by third-party construction auditing experts and overseen by Internal Audit, these reviews are a partnership with the divisions of Facilities and Finance.	Financial – Facilities
Clery Act Compliance	The Clery Act requires all colleges and universities that participate in federal financial aid programs to keep and disclose information about crime on and near their respective campuses, including timely warnings of crimes that may represent a serious or ongoing threat to the safety of students or employees. A review of this activity has not been previously conducted.	Compliance – Safety and Security

Planned Engagement	Overview	Risk Area
College of Veterinary Medicine Research	Virginia-Maryland College of Veterinary Medicine has a robust research program that spans basic biomedical sciences in infectious (viral, bacterial, and parasitic) and non-infectious (immune-mediated and oncologic) diseases to veterinary clinical research to translational and public health. The program's overall goal is to apply research to improve the lives of pets and people. The last audit was conducted in 2015.	Operational – Academic
Controlled Substances	Controlled substances are drugs or chemicals whose production, possession, and use are regulated by the government. These substances are often categorized into schedules based on their potential for abuse, accepted medical use, and potential for addiction. The regulatory compliance requirements of these substances can be complex to manage and mitigate. A review of these activities has not been previously conducted.	Compliance – Safety and Security
Data: Student Residency Status	The establishment of residency status is an important step in student processing. This data centric review will seek to look at data to identify potential errant or inconsistent residency processes. The last audit was conducted in 2014.	Compliance – Enrollment Management
Facility & Event Safety	The institution operates a variety of venues and events where patron safety is high risk. The processes and procedures for managing these events are most often a hybrid effort across multiple offices. A review of these activities has not been previously conducted.	Operational – Safety and Security
Fire Code Compliance	The institution is subject to compliance requirements with the Virginia Statewide Fire Prevention Code and has policies and procedures deployed to comply and mitigate the identified risks. The last audit was conducted in 2018.	Compliance – Facilities and Operations
Health and Counseling Centers	The Cook Counseling Center and Schiffert Health Centers provide comprehensive mental and physical health services for students. Supported primarily by a student health fee, students are provided free or reduced cost access to these facilities. The last audit was conducted in 2015.	Operational – Student Services
Human Resources – Leave Accounting *	The institution offers an array of leave benefits to allow time off to meet various employee needs. Additionally, Human Resources is responsible for various federal and state leave programs such as FMLA and disabilities. The last audit was conducted in 2016.	Compliance – Financial Management
Immigration Services - Employees	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. The student components of these efforts were reviewed in 2025.	Compliance – Human Resources
Industrial and Systems Engineering	The Grado Department of Industrial and Systems Engineering, within the College of Engineering, engages a wide range of research including manufacturing systems, human factors and ergonomics, and management systems. The research enterprise seeks to positively influence society by providing new knowledge, and train students to develop into independent researchers who will continue to advance the forefront of science and technology. The last audit was conducted in 2009.	Operational – Academic
Internal Controls Monitoring	This review will establish an updated framework to review and report out on common internal controls across the entire institution. Utilizing the previous Policy Compliance Review framework, and in partnership with distribute control owners, we seek to develop an aggregated look at the level of compliance with basic control parameters across all senior management areas.	Compliance

Planned Engagement	Overview	Risk Area
IT: Centralized Logging and Monitoring	The institution's logging services collect and store logs from various campus systems in a secure, centralized location. This allows the institution to monitor activity, detect security incidents, and troubleshoot issues efficiently. The last audit was conducted in 2020.	Operational – Information Technology
IT: Data Backup and Recovery	Data backup and recovery are critical components to ensure the institution is positioned to respond to operational interruptions. Data loss, system failure, or cyberattacks are all events that warrant robust backup and recovery processes and tools. A dedicated review of these activities has not been previously conducted.	Operational – Information Technology
IT: Low-Risk Procurement Compliance	Department Heads or above are delegated the authority to sign contracts and make procurements of low-risk software and information technology services, including "click-through" agreements, that do not go through Procurement. The institution has deployed a standard and procedures to track these purchases. This review will seek to ensure units are adhering to these requirements. A review of these activities has not been previously conducted.	Compliance – Information Technology
Office of Sponsored Programs *	Office of Sponsored Programs (OSP) provides a comprehensive array of support services for faculty and staff as they pursue and manage external funding projects. OSP also functions as the steward of the institution's research portfolio and its staff are responsible for ensuring that all research proposals and projects comply with university, federal, and sponsor regulations, policies, and procedures. A component of Research, often in OSP, is typically included in the audit plan each year.	Operational – Research
School of Neuroscience	The School of Neuroscience, within the College of Science, aspires to be at the forefront of research and training in Neuroscience. The school was founded in 2016. This school has not been previously reviewed.	Operational – Academic
Virginia Cooperative Extension and 4-H Programs	Virginia Cooperative Extension (VCE) offers a comprehensive collection of resources, programs, and services that are research-proven, accessible, and contain actionable information that supports the success and resilience of individuals and communities throughout the Commonwealth of Virginia and beyond. Additionally, VCE coordinates the Commonwealth's 4-H youth program. This review will be conducted across the five divisional units. A review of this nature has not been previously conducted.	Operational – Off-Campus Locations

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

<u>Reimagining Policy Compliance Reviews and Accelerated IT General Controls Reviews</u>
Internal Audit will reimagine its traditional policy compliance review program to focus on two efforts. First, the traditional operational elements (e.g. financial, human resources, vehicle management) of the reviews will be reenvisioned as university-wide internal control environment reviews with a single report on compliance by senior management area. By doing so, the comprehensive report will provide senior leadership with a wider view of basic compliance with core internal controls to help focus compliance efforts and identify significant areas for attention.

Next, in accordance with the Board of Visitors request, each senior management area will receive an information technology general controls review which seeks to assess conformance with the institution's Minimum Security Standards once every three years, an acceleration from the current five-year cycle. Internal Audit will seek to align this activity with the Information Technology Security Office's risk assessment and monitoring efforts to

increase the overall efficiency and effectiveness of institution-wide coverage of this critical risk area. The scheduled areas for this year's review are noted below.

Planned Engagements
College of Science
Office of the Executive Vice President & Chief Operating Officer and Selected Related Areas
Office of the Executive Vice President & Provost
Office of the President
Pamplin College of Business
Vice President for Facilities
VTC School of Medicine

Management Advisory Services

Planned Engagements	Overview	Risk Area
CMMC Readiness Review	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
Endpoint Management Processes	The Division of Information Technology is interested in identifying the various processes and software deployed across the decentralized information technology units to comply with the institution's standards for encryption, malware, and patching. Additional inquiry could include decentralized backup and recovery processes.	Operational – Financial Management
IT Procurement Processes	The Procurement Office is interested in reviewing information technology procurement processes. In addition to core policy and process review, the institution recently moved information technology procurement from the Division of Information Technology to Procurement within the Vice President for Finance's portfolio.	Operational – Information Technology
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

Miscellaneous Activities

Activity	Overview
Annual Risk Assessment and Audit Plan Development	Participate in the annual institutional risk assessment process, coordinated from OARC's ERM program, and develop the annual audit plan.
Audit Follow-Up	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.
Special Projects	Investigate fraud, waste, and abuse allegations.

AUDIT RESOURCES

The fiscal year 2025–26 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. The FTE calculation includes the continuation of the student internship program in which two Virginia Tech students are employed, and the use of outsourced consultants for some information technology and construction audit engagements.

Approximately 77 percent of Internal Audit'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. Internal Audit 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:
- 58 percent of Internal Audit'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.
- 8 percent to conduct investigations into fraud, waste, and abuse allegations.
- 10 percent for employee professional development, internal quality improvement projects, and other internal administrative functions.
- 13 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 10 of 23 risk areas. Specific risk areas include: