

## Committee Minutes

### COMPLIANCE, AUDIT, AND RISK COMMITTEE

Roanoke Hotel, Roanoke, Virginia

8:30 a.m.

August 26, 2018

#### Closed Session

**Committee Members Present:** Mr. Mehmood Kazmi (chair), Ms. Anna James, Mr. Robert Mills, Jr., Mr. Horacio Valeiras

**Board Members Present:** Mr. Dennis Treacy (rector), Mr. Preston White

**VPI & SU Staff:** Dr. Cyril Clarke, Mr. Brian Daniels, Ms. Kay Heidbreder, Ms. Elizabeth Hooper, Ms. Sharon Kurek, Ms. Kim O'Rourke, Dr. Dwayne Pinkney, Dr. Timothy Sands, Mr. M. Dwight Shelton, Jr.

#### Compliance, Audit, and Risk Closed Session

1. **Motion for Closed Session:** Motion to begin closed session.
2. **Update on Fraud, Waste, and Abuse Cases:** The Committee received an update on outstanding fraud, waste, and abuse cases.
3. **Executive Director of Audit, Risk, and Compliance Performance Review:** The Committee provided an annual performance review to the Executive Director of Audit, Risk, and Compliance (OARC).
4. **Discussion with the Executive Director of Audit, Risk, and Compliance:** The Executive Director discussed audits of specific departments and units where individual employees were identified.

#### Open Session

**Committee Members Present:** Mr. Mehmood Kazmi (chair), Ms. Anna James, Mr. Robert Mills, Jr., Mr. Horacio Valeiras

**Board Members Present:** Mr. Edward Baine, Ms. Greta Harris, Mr. Charles C.T. Hill, Ms. Tish Long, Mr. Chris Petersen, Ms. Debbie Petrino, Mr. Dennis Treacy (rector), Mr. Jeffrey Veatch, Mr. Preston White, Dr. John Ferris, Mr. Robert Sebek, Ms. Rachel Iwicki

**VPI & SU Staff:** Mr. Omar Banks, Mr. Bob Broyden, Ms. Lori Buchanan, Dr. Cyril Clarke, Ms. Shelia Collins, Mr. Al Cooper, Mr. David Crotts, Mr. Brian Daniels, Mr. Corey Earles, Dr. Jack Finney, Dr. Lance Franklin, Ms. Kay Heidbreder, Mr. Tim Hodge, Ms. Elizabeth Hooper, Ms. Sharon Kurek, Dr. Lisa Lee, Dr. Theresa Mayer, Ms. Nancy Meacham, Dr. Scott Midkiff, Mr. Ken Miller, Ms. April Myers, Ms. Kim O'Rourke, Mr. Mark Owczarski, Dr. Patty Perillo, Mr. Charlie Phlegar, Dr. Dwayne Pinkney, Dr. Scot Ransbottom, Dr. Timothy Sands, Mr. M. Dwight Shelton Jr., Dr. Ken Smith, Mr. Steve Vantine, Ms. Tracy Vosburgh, Dr. Lisa Wilkes, Dr. Sherwood Wilson

**Guests:** Ms. Ashley Deihl (Baker Tilly), Ms. Cassandra Walsh (Baker Tilly)

### **Compliance, Audit, and Risk Open Session**

1. **Motion to Reconvene in Open Session:** Motion to begin open session.
2. **Welcome and Introductory Remarks:** The chair of the Compliance, Audit, and Risk Committee provided opening remarks.
3. **Consent Agenda:** The Committee approved and accepted the items listed on the Consent Agenda.
  - a. **Approval of Minutes of the June 3, 2018 Meeting:** The Committee reviewed and approved the minutes of the June 3, 2018 meeting.
  - b. **Update of Responses to Open Internal Audit Comments:** The Committee reviewed the university's update of responses to all previously issued internal audit reports. As of March 31, 2018, the university had eight open recommendations. Three audit comments were issued during the second quarter of the fiscal year. As of June 30, 2018, the university had addressed seven comments, leaving four open recommendations in progress.
  - c. **Internal Audit Reports:** The following internal audit reports were issued by OARC since the June 3, 2018 meeting. Where applicable, management developed action plans to effectively address the issues in the report with a reasonable implementation timeframe. As noted above, OARC conducts follow-up on management's implementation of agreed upon improvements for previously issued audit recommendations.

- i. **Advancement Compliance Review:** The audit received a rating of improvements are recommended. Audit recommendations were issued to management where opportunities for further improvement were noted in the areas of leave reporting, expenditures, and funds handling.
    - ii. **IT: Employee Access Life Cycle:** The audit received a rating of improvements are recommended. An observation with university-wide impact was noted with respect to controls and processes for provisioning and deprovisioning employees for the Enterprise Directory and Banner.
    - iii. **University Scholarships and Financial Aid:** The audit received an effective rating.
  - d. **Status Update of the Audit of the University's Financial Statements:** This report provided the current status of the audit of the university's financial statements for 2017-18.
  - e. **Statewide Reviews and Special Reports:** This report provided the current status of ongoing and forthcoming statewide reviews. Virginia Tech is subject to reviews by a variety of Commonwealth agencies, including the Auditor of Public Accounts, Office of the State Inspector General, and Virginia Department of Veterans Services.
4. **OARC Annual Report:** The Committee reviewed and accepted the Annual Report for OARC. Acceptance of this report documented the Committee's review of the effectiveness of the internal audit function, including staffing resources, financial budget, training, objectivity, and reporting relationships as required by the Committee's Charter. In addition to conducting scheduled audits, policy compliance reviews, and advisory services, the department participated in annual audit activities, fraud investigations, and professional development activities. Twenty-six audit projects, or 92 percent of the audits on the fiscal year 2017-18 amended audit plan, were completed.

In addition to operating the audit function, OARC designed and implemented an Enterprise Risk Management (ERM) framework and Institutional Compliance Program (ICP).

5. **Internal Audit Reports:** The following internal audit reports were issued by OARC since the June 3, 2018 meeting. Where applicable, management developed action plans to effectively address the issues in the report with a reasonable

implementation timeframe. As noted above, OARC conducts follow-up on management's implementation of agreed-upon improvements for previously issued audit recommendations.

- a. **Global Activities:** The audit received a rating of improvements are recommended. An observation with university-wide impact was noted with respect to the organizational structure of providing immigration and visa services to students and employees. Additionally, a low-priority recommendation of a less significant nature was noted in the area of contingency plans and incident management.
  - b. **Athletics Compliance Review:** The audit received a rating of significant improvements are needed. Audit recommendations were issued to management where opportunities for further improvement were noted in the areas of fiscal responsibility, wage payroll, leave reporting, P14 appointments, expenditures, fixed assets, and funds handling.
6. **Audit Plan for Fiscal Year 2018-19:** The Committee reviewed and approved the annual audit plan for fiscal year 2018-19. OARC conducted the annual risk assessment after reviewing financial and operational data and seeking input from senior management. In addition, a university-wide information technology risk assessment and audit plan were created in accordance with industry standards. For fiscal year 2018-19, more than 20 audit projects are proposed given current staffing levels, with approximately 75 percent of available resources committed to the completion of planned projects.
  7. **Enterprise Risk Management Program:** The Committee received an update on the ERM program, including planned activities for the next several years and the long-term vision for ERM.
  8. **Institutional Compliance Program:** The Committee received an update on the institutional compliance program, including convening the newly established compliance oversight committee to coordinate best practices regarding maintenance of a compliance matrix of applicable regulations and authoritative guidance with responsible parties, risk assessment, and monitoring activities.
  9. **Discussion of Future Topics:** The Committee discussed topics to be covered in future committee meetings.

There being no further business, the meeting adjourned at 10:50 a.m.

## Update of Responses to Open Audit Comments

### COMPLIANCE, AUDIT, AND RISK COMMITTEE

**June 30, 2018**

As part of the internal audit process, university management participates in the opening and closing conferences and receives copies of all final audit reports. The audited units are responsible for implementing action plans by the agreed upon implementation dates, and management is responsible for ongoing oversight and monitoring of progress to ensure solutions are implemented without unnecessary delays. Management supports units as necessary when assistance is needed to complete an action plan. As units progress toward completion of an action plan, the Office of Audit, Risk, and Compliance (OARC) performs a follow-up visit within two weeks after the target implementation date. OARC is responsible for conducting independent follow up testing to verify mitigation of the risks identified in the recommendation and formally close the recommendation. As part of management's oversight and monitoring responsibility, this report is provided to update the Compliance, Audit, and Risk Committee on the status of outstanding recommendations. Management reviews and assesses recommendations with university-wide implications and shares the recommendations with responsible administrative departments for process improvements, additions or clarification of university policy, and inclusion in training programs and campus communications. Management continues to emphasize the prompt completion of action plans.

The report includes outstanding recommendations from compliance reviews and audit reports. Consistent with the report presented at the March Board meeting, the report of open recommendations includes three attachments:

- Attachment A summarizes each audit in order of final report date with extended and on-schedule open recommendations.
- Attachment B details all open medium and high priority recommendations for each audit in order of the original target completion date, and with an explanation for those having revised target dates or revised priority levels.
- Attachment C charts performance in implementing recommendations on schedule over the last seven years. The 100 percent on-schedule rate for fiscal year 2018 reflects closing 30 of 30 recommendations by the original target date.

The report presented at the June 3, 2018 meeting covered audit reports reviewed and accepted through March 31, 2018 and included eight open medium and high priority recommendations. Activity for the quarter ended June 30, 2018 resulted in the following:

Open recommendations as of March 31, 2018	8
Add: medium and high priority recommendations accepted June 3, 2018	3
Subtract: recommendations addressed since March 31, 2018	7
Remaining open recommendations as of June 30, 2018	<u>4</u>

While this report is prepared as of the end of the quarter, management continues to receive updates from OARC regarding auditee progress on action plans. The remaining open recommendations are progressing as expected and are on track to meet their respective target due dates. Management continues to work conjointly with all units and provides assistance as needed to ensure action plans are completed timely.

## ATTACHMENT A

## Open Recommendations by Priority Level

## COMPLIANCE, AUDIT, AND RISK COMMITTEE

March 31, 2018

Report Date	Audit Name	Audit Number	Total Recommendations					
			ISSUED	COMPLETED	OPEN			
					Extended		On-schedule	
			High	Medium	High	Medium	Open	
28-Feb-18	Vice President for Research and Innovation	18-1392	1				1	1
16-May-18	Controller's Office: Risk Management	18-1369	1				1	1
16-May-18	Telecommunications Operations	18-1379	1				1	1
18-May-18	Biochemistry	18-1364	1				1	1
<b>Totals:</b>			<b>4</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>4</b>	<b>4</b>

**ATTACHMENT B****Open Audit Recommendations****COMPLIANCE, AUDIT, AND RISK COMMITTEE****June 30, 2018**

Report Date	Item	Audit Number	Audit Name	Recommendation Name	Priority		Target Date		Follow Up Status	Status of Recommendations with Revised Priority / Target Dates
					Original	Revised	Original	Revised		
28-Feb-18	1	18-1392	Vice President for Research and Innovation	Fiscal Responsibility	Medium		30-Aug-18		1	
18-May-18	2	18-1364	Biochemistry	Oversight of Lab Safety Training	Medium		01-Oct-18		2	
16-May-18	3	18-1369	Controller's Office: Risk Management	Large Event Insurance Coverage	Medium		15-Nov-18		2	
16-May-18	4	18-1379	Telecommunications Operations	ATLAS Systems Controls	Medium		31-Jan-19		2	

Follow Up Status

- 1 As of June 30, 2018, management confirmed during follow up discussions with the Office of Audit, Risk, and Compliance (OARC) that actions are occurring and the target date will be met. OARC will conduct testing after the due date to confirm that the Management Action Plan is implemented in accordance with the recommendations.
- 2 Target date is beyond current calendar quarter. Management has follow-up discussions with the auditor to monitor progress, to assist with actions that may be needed to meet target dates, and to assess the feasibility of the target date.

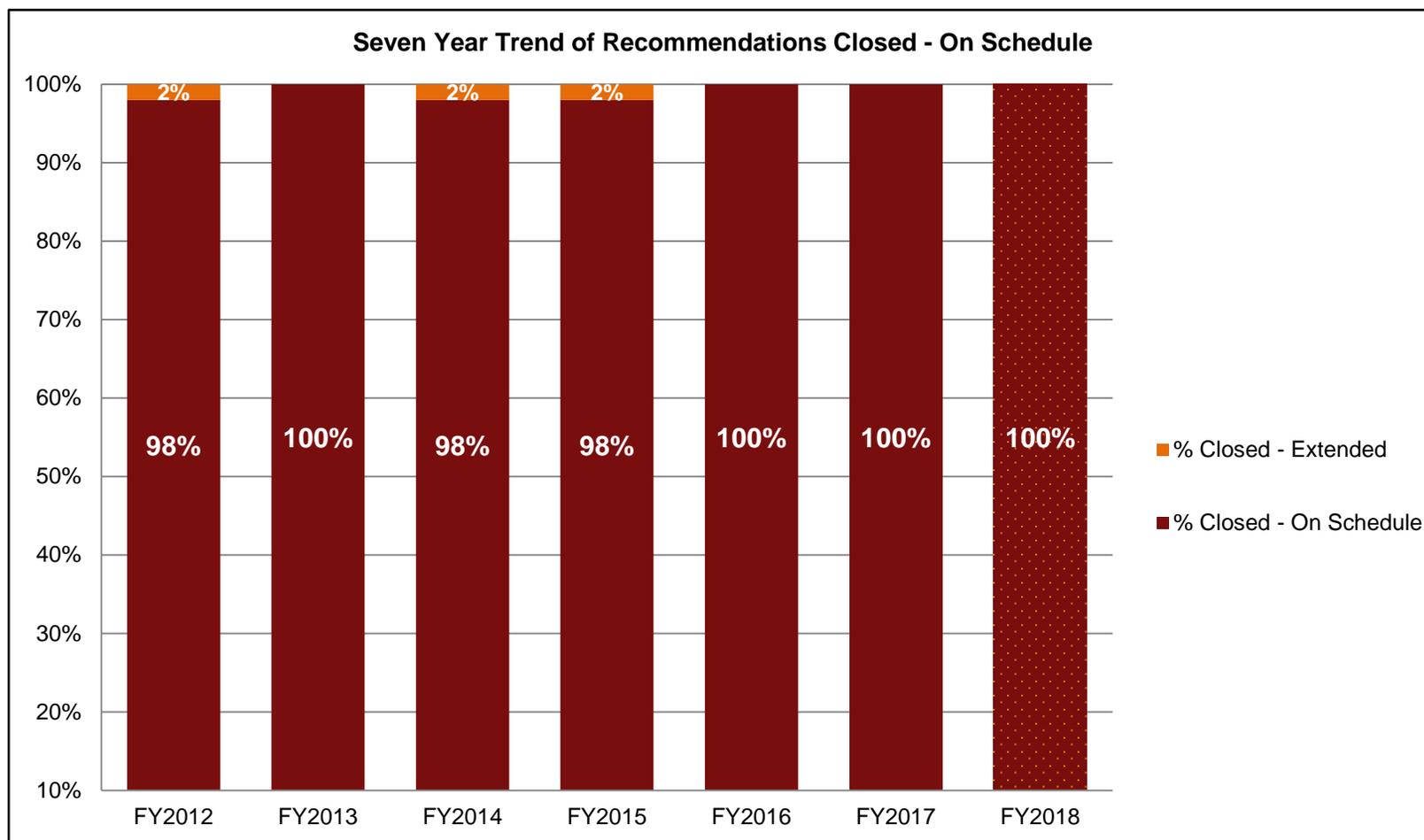
For Open Detail Report: "current calendar quarter" is used to refer to the current working quarter instead of the quarter being reported on.

### ATTACHMENT C

## Management Performance and Trends Regarding Office of Audit, Risk, and Compliance Recommendations

### COMPLIANCE, AUDIT, AND RISK COMMITTEE

June 30, 2018



**Internal Audit Reports**  
**COMPLIANCE, AUDIT, AND RISK COMMITTEE**  
**August 26, 2018**

**Background**

This report provides a summary of audit ratings issued this period and the full rating system definitions. The following reviews have been completed during this reporting period. The Office of Audit, Risk, and Compliance has made a concerted effort to ensure progress on the annual audit plan.

<b>Consent Agenda Reports</b>	<b>Rating</b>
Advancement Compliance Review	Improvements are Recommended
IT: Employee Access Lifecycle	Improvements are Recommended
USFA	Effective
<b>Report for Discussion</b>	<b>Rating</b>
Global Activities	Improvements are Recommended
Athletics Compliance Review	Significant Improvements are Needed

**Summary of Audit Ratings**

The Office of Audit, Risk, and Compliance's rating system has four tiers from which to assess the controls designed by management to reduce exposures to risk in the area being audited. The auditor can use professional judgment in constructing the exact wording of the assessment in order to capture varying degrees of deficiency or significance.

### Definitions of each assessment option

**Effective** – The audit identified opportunities for improvement in the internal control structure, but business risks are adequately controlled in most cases.

**Improvements are Recommended** – The audit identified occasional or isolated business risks that were not adequately or consistently controlled.

**Significant or Immediate Improvements are Needed** – The audit identified several control weaknesses that have caused, or are likely to cause, material errors, omissions, or irregularities to go undetected. The weaknesses are of such magnitude that senior management should undertake immediate corrective actions to mitigate the associated business risk and possible damages to the organization.

**Unreliable** – The audit identified numerous significant business risks for which management has not designed or consistently applied controls prior to the audit. Persistent and pervasive control weaknesses have caused or could cause significant errors, omissions, or irregularities to go undetected. The weaknesses are of such magnitude that senior management must undertake immediate corrective actions to bring the situation under control and avoid (additional) damages to the organization.

### **RECOMMENDATION:**

That the internal audit reports listed above be accepted by the Compliance, Audit, and Risk Committee.

August 26, 2018

**Statewide Reviews and Special Reports**  
**COMPLIANCE, AUDIT, AND RISK COMMITTEE**  
**August 26, 2018**

**Background**

Virginia Tech is subject to reviews by a variety of Commonwealth agencies, including the Auditor of Public Accounts (APA), the Office of the State Inspector General (OSIG), and others. In addition to the annual audits of the university's financial statements and its Intercollegiate Athletics program conducted by the APA, Virginia Tech has been included along with other agencies in statewide reviews typically included as part of an agency's annual work plan. Due to the breadth of the programs and the dollar volume of activities at Virginia Tech, the university is often selected for inclusion in a variety of statewide reviews. The following report provides an analysis of statewide audit activities consistent with the university's planned approach to manage and report on these audit activities.

**OSIG Chemical Inventory Management**

In accordance with the Code of Virginia § 2.2-309 [A](10), OSIG conducts performance audits of executive branch state agencies, including colleges and universities, to ensure state funds are spent as intended and to evaluate the efficiency and effectiveness of programs. As previously reported, all higher education institutions, including Virginia Tech, were originally notified that OSIG will conduct a performance audit at a sampling of Virginia's colleges and universities during fiscal year 2017-18. Virginia Tech, among others, was notified in February 2018 of its inclusion for the planning phase of this project centered on chemical inventory management. Virginia Tech subsequently responded to a detailed survey provided by OSIG, but ultimately was not among the three agencies of varying size and focus selected for detailed assessment. Further involvement for Virginia Tech is not anticipated at this time.

**Virginia Department of Veterans Services (DVS)**

Virginia Tech received notice of its selection in a Compliance Survey, which will be conducted to ensure that schools, training establishments, and their approved courses are in compliance with all applicable provisions of the laws administered by the U.S. Department of Veterans Affairs and State Approving Agency (DVS). This limited scope review was to monitor compliance based on a review of records for a specific set of students. After initial delays, the onsite review was conducted in July 2018, and the university is awaiting the results.

## **Status Update of the Audit of the University's Financial Statements**

### **COMPLIANCE, AUDIT, AND RISK COMMITTEE**

**August 26, 2018**

The Auditor of Public Accounts (APA) began the audit of the university's financial statements for fiscal year 2017-18 with the entrance conference on May 14, 2018. The APA is currently in the initial stage of the audit where they review transactions and test internal controls over the university's financial processes. Through early August 2018, the audit seems to be progressing as planned and the APA has not provided any audit comments or recommendations for improvements. At this time, we are not aware of any issues that would prevent the successful completion of the fiscal year 2017-18 audit by the targeted deadline of October 31, 2018.

**OARC Annual Status Report  
For the Fiscal Year Ended June 30, 2018  
COMPLIANCE, AUDIT, AND RISK COMMITTEE**

**August 26, 2018**

**Mission Statement – Scope of Work**

---

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. 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. Audits help 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. **Enterprise Risk Management:** Provide oversight of the enterprise risk management (ERM) program by creating and maintaining the framework to effectively 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.

The internal audit function conducts its activities in accordance with the Institute of Internal Auditors' (IIA) International Professional Practices Framework (see appendix). Internal audit coverage encompasses reviews of all university operations and activities to appraise:

- the accuracy, reliability, and timeliness of significant financial, managerial, and operational information and the adequacy of the internal controls employed over the compilation and reporting of such information;
- compliance with policies, procedures, standards, laws, and regulations;
- risk identification and management;
- measures taken to safeguard assets, including tests of existence and ownership;
- the adequacy, propriety, and cost-effectiveness of accounting, financial, and other controls throughout the university, as well as compliance therewith;
- measures taken to foster continuous improvement in control processes;
- whether university resources are being acquired, managed, and protected in an economical, efficient, and effective manner; and
- the achievement of programs, plans, and objectives.

OARC reports functionally to the Compliance, Audit, and Risk (CAR) Committee of the Board of Visitors. For day-to-day operations, the Executive Director reports administratively to the President.

**OARC Annual Status Report  
For the Fiscal Year Ended June 30, 2018**

**Executive Summary – State of University’s Control Environment**

---

The university’s internal audit function within OARC continues to be a significant element of the university’s overall control structure and a positive influence on the control environment. During fiscal year 2017-18, OARC examined and tested the operations and systems of internal control within a number of university departments to assist management and the Board of Visitors in the discharge of their fiduciary responsibilities.

As a result of the audit, advisory, and investigative work performed during fiscal year 2017-18, no deficiencies representing material control weaknesses were identified; however, a number of areas requiring improvement were noted. The scope of audit work was not limited in any way by management or others, nor were there any instances where OARC considered its independence or objectivity to have been impaired. Management and others were found to be conscientious, cognizant, and accepting of their responsibility for internal control, as well as open, cooperative, and supportive of audit efforts.

Management has generally accepted audit findings and responded by developing action plans that address the concerns included in report recommendations. These statements are made with the understanding that no system of internal control provides absolute assurance that controls are functioning effectively. These statements are also not meant to imply that fraud and other irregularities do not exist or, if they do exist, are certain to be detected. Decisions as to the level of risk that is tolerable and should be accepted by the university are the responsibility of management. That said, based on the audit, advisory, and investigative work performed during fiscal year 2017-18, OARC did not identify any areas where management decided to accept a level of risk that we believed to be unacceptable.

**Summary Observations – Audit Program**

---

Audits were performed in accordance with the fiscal year 2017-18 annual audit plan at a level consistent with the resources of OARC. Eight audit and advisory projects have been completed since the June board meeting.

While the annual audit plan included 42 proposed projects, OARC had to defer or cancel 16 projects (38%) due to seven vacancies equivalent to over 4,500 hours of audit effort. The majority of these projects were simply deferred to next year’s audit plan. A risk-based audit of the utilization of endowed professorships and a policy compliance review of the College of Liberal Arts and Human Sciences are underway and will be carried forward into fiscal year 2018-19.

For fiscal year 2017-18, OARC completed 92 percent of its amended audit plan as depicted in Exhibit 1 on the following page.

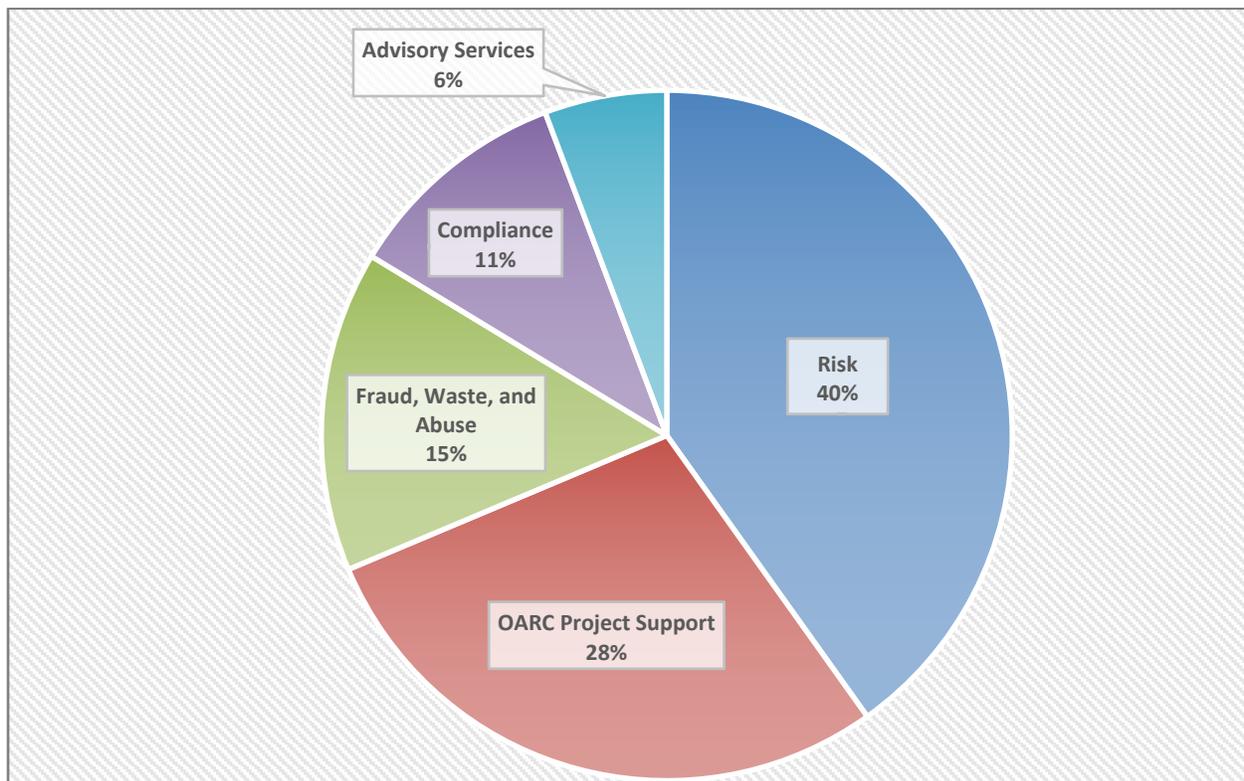
**OARC Annual Status Report  
For the Fiscal Year Ended June 30, 2018**

**Exhibit 1  
FY 2017-18 Completion of Audit Plan**

<b>Audits</b>	
Total # of <b>Audits</b> Planned	34
Total # of Supplemental <b>Audits</b>	1
Total # of Carry Forwards	7
Total # of Planned <b>Audits</b> Deferred and/or Canceled	16
<b>Total Audits in Plan as Amended</b>	<b>26</b>
Total <b>Audits</b> Completed	24
<b>Audits</b> - Percentage Complete	92%
<b>Audits</b> - Percentage Complete or Underway	100%
Note: Includes Policy Compliance Reviews and Advisory Services	

Exhibit 2 displays the distribution of direct audit hours (69%) by category. Indirect hours primarily for administration, computer/network support, training, and compensated absences (31%) are not included in this chart. OARC Project Support has increased as a percentage over previous years as a result of emerging ERM and ICP programs as well as vacancies for positions that would be focused on risk-based audits and compliance reviews.

**Exhibit 2  
FY 2017-18 Distribution of Direct Audit Hours**



**OARC Annual Status Report  
For the Fiscal Year Ended June 30, 2018**

The department was able to increase the amount of effort spent on advisory services with dedicated staff to focus on these important projects requested by management. Additionally, the overall percentage of effort spent on risk-based projects was lower as a result of the aforementioned vacancies.

Exhibit 3 below displays the status of the fiscal year 2017-18 audit plan as amended. As noted previously, only two projects remain in progress and will be carried forward to the fiscal year 2018-19 audit plan.

**Exhibit 3  
FY 2017-18 Audit Plan Status**

Audit Project	Risk Ranking	BOV Mtg
<b>Risk-Based Audit</b>		
Biochemistry	High	Jun-18
Biomedical Engineering and Mechanics (BEAM)	High	Mar-18
Chemistry	Medium	Mar-18
Controller's Office – Risk Management	High	Jun-18
Fire Safety Compliance	High	Mar-18
Global Activities	High	Aug-18
IT – Employee Access Life Cycle	High	Aug-18
IT – Mobile Device Security	High	Jun-18
Research – Animal Care and Use	High	Mar-18
Research – Lab Safety	High	Mar-18
Telecommunications Operations	High	Jun-18
University Scholarships and Financial Aid*	High	Aug-18
Utilization of Endowed Professorships	High	<i>Carry-Forward</i>
Virginia Cooperative Extension – Central District	Medium	Mar-18
<b>Policy Compliance Reviews</b>		
College of Engineering Compliance Review		Mar-18
College of Liberal Arts and Human Sciences Compliance Review		<i>Carry-Forward</i>
Department of Athletics Compliance Review*		Aug-18
Vice President for Advancement Compliance Review		Aug-18
Vice President for Research and Innovation Compliance Review		Mar-18
Virginia – Maryland College of Veterinary Medicine Compliance Review		Nov-17

\* Annual Audit on Different Components

**OARC Annual Status Report  
For the Fiscal Year Ended June 30, 2018**

Additionally, OARC responded to management's requests for advisory services and consultative guidance including the following areas:

- Sport Clubs – Sport clubs are administered by the Virginia Tech Department of Recreational Sports. Each club is comprised of students, who organize, fund, and promote their clubs with the ultimate goal of competing against other colleges and universities on both a regional and national level. The objective of this advisory review was to analyze the risk environment associated with the operation of the Sport Clubs program and assist in the identification of potential risk mitigation strategies. OARC identified and evaluated policies and practices that address the safety of students participating in these sport clubs. This review included extensive surveying and a benchmarking study of other universities' safety-related and operational practices.
- Controlled Unclassified Information (CUI) – CUI is defined as information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526. The objective of this advisory review was to assess the effectiveness of control design with respect to the Secure Research Environment (SRE) maintained by Collaborative Computing Solutions (CCS) and the COMPASS system maintained by the Office of Export and Secure Research Compliance (OESRC). This review involved an evaluation of the design and documentation of the controls implemented by CCS and OESRC to achieve compliance with federal requirements.
- Facilities and Administrative (F&A) Charges – The purpose of this engagement was to evaluate the university's accounting and utilization of F&A charges. Upon initiation of this engagement, we were notified of a parallel and proactive analysis to be performed in the Office of the University Controller on behalf of the Vice President for Finance and Chief Financial Officer and the Vice President for Research and Innovation. As a result, this advisory review served primarily to validate that effort, which was titled, "*Analysis of the Generation, Allocation, and Expenditure of Facilities & Administrative Cost Recoveries for Fiscal Years 2013 Through 2017.*"
- Marketing Study Abroad Program – While performing an advisory review at the Steger Center for International Scholarship (see below), OARC, in coordination with University Legal Counsel, visited Lugano, Switzerland to perform a control review of the study abroad program managed by a Marketing faculty member within the Pamplin College of Business.
- Steger Center for International Scholarship – The Steger Center for International Scholarship, located in Riva San Vitale, Switzerland, is the university's European campus center and the base for operations and support of its programs in the region. OARC visited the center and reviewed its operations from a financial and operational standpoint.

**OARC Annual Status Report  
For the Fiscal Year Ended June 30, 2018**

- Virginia Tech Carilion School of Medicine – The Virginia Tech Carilion School of Medicine represents a unique, public-private partnership between a top-tier research university and a major health care institution. The school has obtained its full accreditation from the Southern Association of Colleges and Schools Commission on Colleges and the Liaison Committee on Medical Education. Successful transition officially occurred on July 1, 2018 to incorporate the VTCSOM as the ninth college of Virginia Tech. OARC performed a multi-year review to advise on risk and related controls in preparation for the transition of the school’s operations to within Virginia Tech through service as an ex-officio member of the transition team.

**Management Corrective Actions (MCAs)**

---

OARC conducts follow-up on management’s implementation of agreed upon improvements for previously issued audit recommendations. Each audit recommendation—and its associated MCA—is given a rating of high, medium, or low priority by the auditors. This judgment is made in a local context, and items identified as high do not necessarily convey material deficiencies or risks beyond the operating environment in which they were found. A primary objective of this classification is to drive a greater sense of urgency in completing the corrective action and completion of audit follow-up. The CAR Committee receives the higher priority recommendations and associated MCAs. However, OARC and management closely monitor all outstanding recommendations to ensure they are adequately addressed by the responsible parties.

Of the 92 MCAs generated during audits issued in fiscal year 2017-18, OARC categorized two as high priority (2%). High-priority MCAs would include those that are systemic or have a broad impact; have contributed to a significant investigation finding; are reportable conditions under professional literature; create health or safety concerns; involve senior officials; create exposures to fines, penalties, or refunds; or are otherwise judged as significant control issues. Open MCAs at fiscal year-end have been outstanding an average of 163 days and are on track for completion. Audits for fiscal year 2017-18 resulted in recommendations with ratings of high, medium, or low MCAs as follows:

**Exhibit 4  
Inventory of MCAs**

Beginning # of MCAs	42
MCAs added	92
MCAs closed	<u>109</u>
Current open inventory of MCAs	25

Note: The open inventory above includes seven open MCAs from the reports presented to the CAR Committee at the August 26, 2018 meeting. In addition, 14 of the 25 open MCAs are categorized as either low-priority recommendations, recommendations resulting from advisory service reviews, or observations with university-wide impact or for central administration identified during audits that are excluded from status reports of previously issued recommendations shared with the CAR Committee.

## OARC Annual Status Report For the Fiscal Year Ended June 30, 2018

### Cost Containment and Revenue Enhancement Recommendations

---

OARC emphasized the identification of cost containment and revenue enhancement strategies in the performance of audit activities. OARC issued the following recommendations to management to assist with cost containment or revenue enhancement strategies:

- IT: Employee Access Life Cycle – A university-wide system for managing access to university applications and data was not fully implemented. Streamlining processes around the employee system access life cycle has the potential to increase operational efficiency by reducing employee downtime and to better secure university data. Timely provisioning of access requests will help support employee productivity. Prompt removal of access when no longer needed will help prevent unauthorized or inappropriate access to sensitive data.
- Virginia Tech Carilion Research Institute – A review of the process used by VTCRI for electronic payments for human behavior studies, which facilitated approximately 7,750 payments totaling \$247,715 during the scope period, revealed a lack of sufficient accountability and thorough monitoring to prevent misappropriation of funds. The process was decentralized and the respective lab personnel maintained complete responsibility for all participant activity and associated payments. This autonomous function created a potential fraud risk, which would permit an employee to create fictitious participant records and payments that may be undetected.
- Biochemistry – Controls were not in place to verify the identity of the purchaser who retrieved materials from the Biochemistry Service Center. This lack of controls led to either untimely or a lack of billing for four of 60 (7%) charges reviewed. Of the five billing cycles reviewed, consisting of approximately 60 transactions totaling \$8,521 in billable materials, four instances, consisting of two purchasers and approximately \$78 in material, were identified where Interdepartmental Service Requests were not provided by the purchaser and the person who signed the activity log was unidentifiable. After determining the identity of one of the two purchasers, Biochemistry billed the purchaser untimely, ranging from 172 to 312 days after dispensing the items from the service center, while the other purchaser remained unbilled at the time of the review, ranging from 337 to 387 days after dispensing the items from the service center.
- Telecommunications Operations – Of the initial \$89,175 in cellular and vendor charges reviewed, billing and rate discrepancies totaling \$3,438 (4%) were identified across eight of 1,725 charges reviewed. Additionally, there was a lack of preventive controls to validate the number of hard copy billing invoices created versus the number processed. Further, Network Infrastructure & Services (NI&S) has been unable to obtain the Virginia Information Technology Agency (VITA) non-cellular contract despite several attempts; therefore, the rates and associated charges for this contract could not be verified, although bills were paid timely and in accordance with stated balances. Finally, the NI&S website contained inactive

**OARC Annual Status Report  
For the Fiscal Year Ended June 30, 2018**

rates. The eight billing discrepancies identified resulted in over/under charges to NI&S and, subsequently, to the customer. Each was a result of human error that was not detected in the monthly review process. The monthly billing discrepancies continued nine to 24 months, averaging approximately 17 months, generating billing disparities totaling \$3,438. Approximately \$1,215 (35%) of that could be attributed to errors made by the vendor.

### **Recurring Audit Recommendations**

The same or similar recommendations noted below were identified in multiple audit reports issued in fiscal year 2017-18. The data in Exhibit 5 will be shared with leadership in the appropriate administrative departments so that they can establish education and/or monitoring programs that will reduce the recurrence of these issues in future years.

**Exhibit 5  
Recurring Audit Recommendations**

Recommendations	Occurrences	Audits
Health and Safety	7	Biochemistry Biomedical Engineering and Mechanics Chemistry Fire Safety Compliance (2) Research: Animal Care and Use Virginia Cooperative Extension: Central District
Wage Payroll	6	College of Engineering Controller's Office: Risk Management Department of Athletics Vice President for Research and Innovation Virginia Cooperative Extension Central District Virginia-Maryland College of Veterinary Medicine
Leave Reporting	6	College of Engineering Department of Athletics Vice President for Advancement Vice President for Research and Innovation Virginia Cooperative Extension: Central District Virginia-Maryland College of Veterinary Medicine
Fiscal Responsibility	5	College of Engineering Department of Athletics Vice President for Research and Innovation Virginia Cooperative Extension: Central District Virginia-Maryland College of Veterinary Medicine
Expenditures	5	Department of Athletics Vice President for Advancement Vice President for Research and Innovation Virginia Cooperative Extension: Central District Virginia-Maryland College of Veterinary Medicine
Funds Handling	4	Department of Athletics Vice President for Advancement Virginia Cooperative Extension: Central District Virginia-Maryland College of Veterinary Medicine

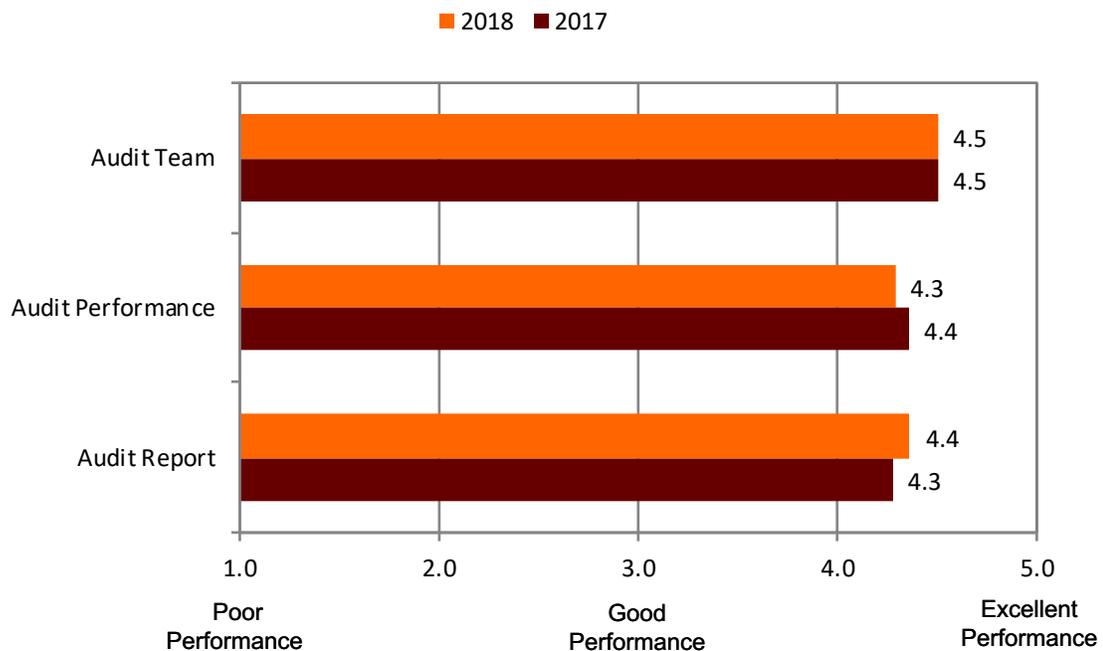
## OARC Annual Status Report For the Fiscal Year Ended June 30, 2018

### Results of Surveys for Evaluating OARC Services

Each audit and compliance review management contact is emailed a link to an online survey requesting their assistance in evaluating the quality of audit services provided by OARC. Feedback from the surveys is used to enhance the overall quality of university audits. The survey responses are grouped into three categories focused on the following areas:

<u>Audit Team</u>	Demonstrated technical proficiency, approached audit with objective and professional manner, and conclusions and opinions were logical.
<u>Audit Performance</u>	Discussed the preliminary audit objectives, scope, and timing of the audit, management concerns and suggestions were solicited and considered in the audit, and disruption of daily activities was minimized as much as possible during the audit.
<u>Audit Report</u>	Written clearly and contained adequate explanations for the observations, and recommendations improved or added value to the department's operation.

### Exhibit 6 Results of FY 2017-18 Surveys for Evaluating OARC Services



Overall, customer ratings were highly favorable as results ranged from good to excellent. Attaining a cumulative average score of 4.4 on a 5-point scale exceeded OARC's goal of a 4.0 rating on survey feedback. Comments provided by clients showed appreciation of the audit process and the courtesy, professionalism, flexibility, and thoroughness demonstrated by the audit team.

## OARC Annual Status Report For the Fiscal Year Ended June 30, 2018

### Fraud Waste and Abuse

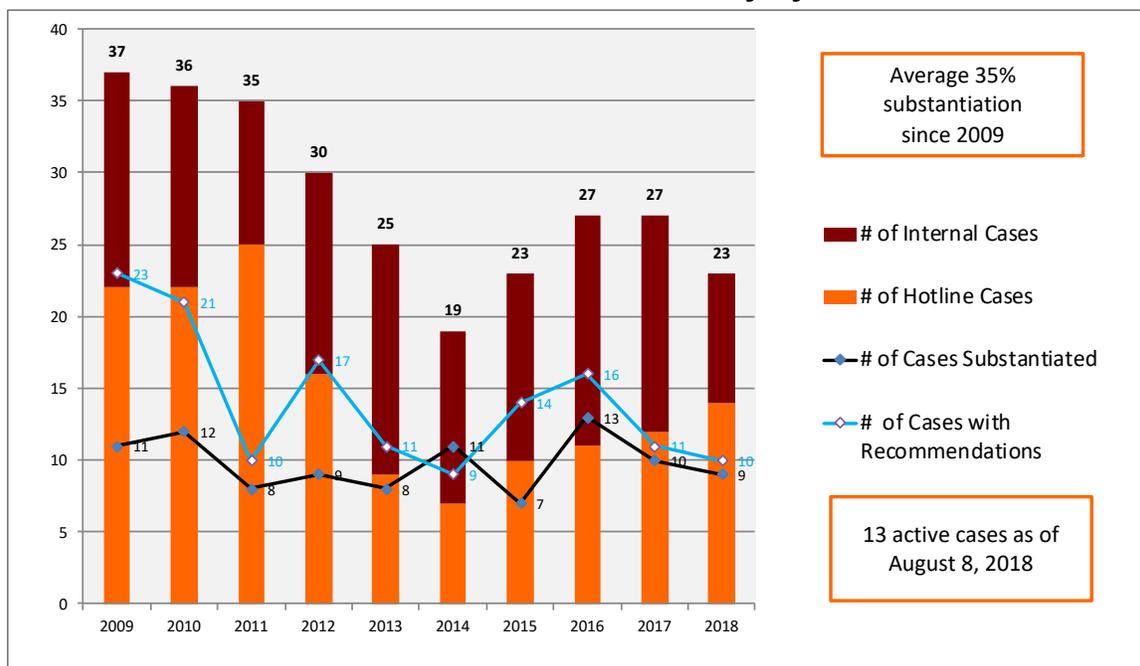
OARC conducts reviews of all state hotline and internal complaints alleging fraud, waste, and abuse. During fiscal year 2017-18, OARC received 23 cases, including 14 state hotline and nine internal complaints. Thirteen cases from fiscal year 2017-18 were closed, along with 12 cases from the prior fiscal year. For the 25 cases completed, three of the nine (33%) state hotline cases were substantiated and 12 of 16 (75%) internally reported cases were substantiated. Since 2008-09, approximately 51 percent of internally reported allegations have been substantiated, and 18 percent of state hotline cases have historically been substantiated, for a combined weighted average of 35 percent.

OARC makes recommendations of improvements related to business practices, communication, and management that improve the overall operating environment of the university. Over the previous 10 years, OARC made recommendations in 49 percent of fraud, waste, and/or abuse cases.

The number of reported cases decreased this year. However, OARC closed 36 percent more cases in fiscal year 2017-18 than the previous fiscal year. Since fiscal year 2008-09, 75 percent of the allegations investigated by OARC fall within five general categories: improper use of university resources, leave or time abuse, abuse of authority, misfeasance and waste, and conflict of interest.

Exhibit 7 displays the number of fraud, waste, and abuse reviews performed for hotline and internal complaints for fiscal years 2008-09 through 2017-18, the total number of cases, the number of substantiated cases, and the number of cases with recommendations for management.

**Exhibit 7**  
**FWA Historical Case Volume Summary by Fiscal Year**



## **OARC Annual Status Report For the Fiscal Year Ended June 30, 2018**

### **Quality Assurance and Improvement Program**

---

A comprehensive Quality Assurance and Improvement Program of the university's internal audit function is maintained in accordance with requirements set forth by the IIA International Standards for the Professional Practice of Internal Auditing (Standards). This program includes ongoing internal assessments, periodic self-assessments, and an independent external assessment that should be conducted at a minimum of every five years.

An external assessment was last completed during fiscal year 2015-16, when the internal audit function received the highest rating possible of "generally conforms." The next independent external assessment will be due in 2021. A formalized self-assessment will be conducted during fiscal year 2018-19.

### **Enterprise Risk Management Program**

---

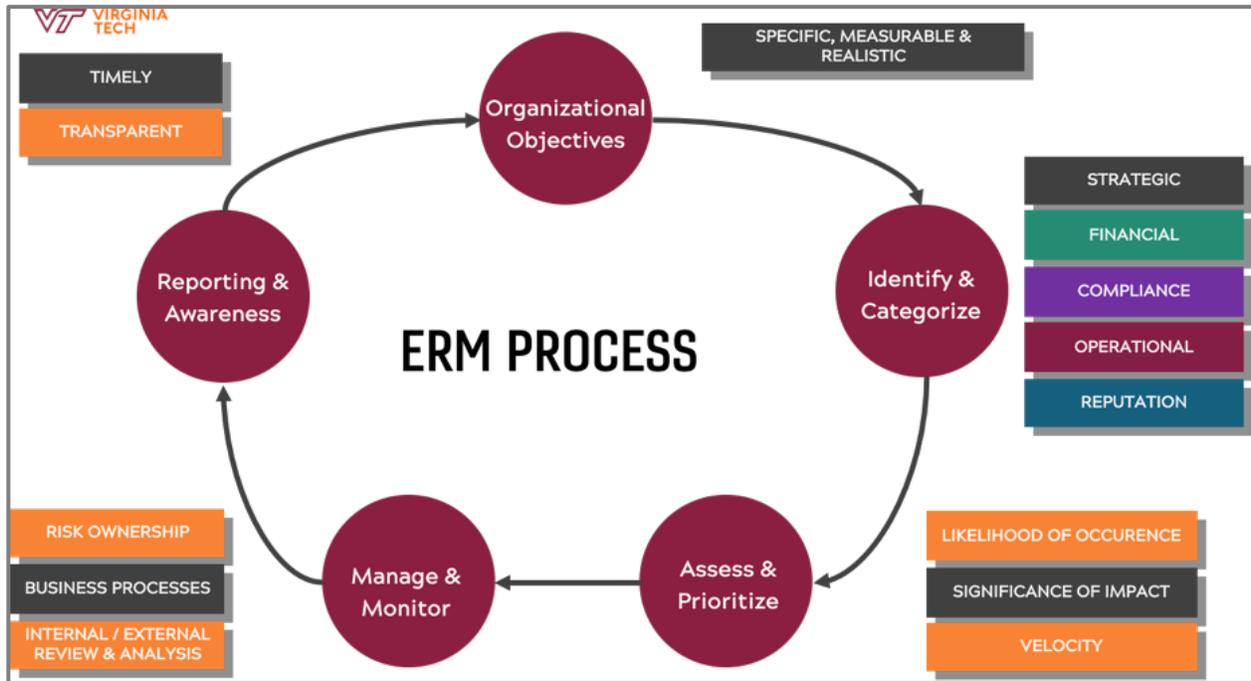
At the request of the Board of Visitors' CAR Committee and the President, OARC was charged last August with coordinating Virginia Tech's Enterprise Risk Management (ERM) Program. ERM is a process applied in strategy-setting and across the enterprise that is designed to identify potential events that may affect the entity, to manage risk to be within the entity's risk tolerance, and to support the achievement of entity mission and objectives. Articulated differently, risk management, as an essential part of a strong control environment, helps ensure that risk appetite aligns with management's decisions and an organization's strategy.

The purpose of the ERM program is to strengthen the university's ability to achieve its mission and strategic objectives. This is done by effectively managing key risks and seizing opportunities related to the achievement of strategic objectives. In this context, risk encompasses both negative events ("downside risk") and opportunities ("upside risk"). Benefits of an effective ERM program include:

- holistic view of the most critical risks to achievement of entity's mission and objectives;
- risk-aware culture, including the management of risks to an appropriate level of risk tolerance;
- improved focus and perspective on both internal and external risks and opportunities, including emerging risks and value drivers;
- enhanced decision making and alignment with strategic goals; and
- improved efficiency and optimized allocation of resources through risk prioritization.

The ERM program is implemented as a collaborative effort by various levels of the organization. OARC developed the ERM process, created an ERM framework, and facilitated discussions between senior leaders and their management teams to identify, categorize, and assess risks. OARC continues to promote communication and collaboration among risk management activities, including the identification of risk owners and development of risk snapshots. Additionally, OARC assists the committees in their duties and provides senior leaders with key information to make risk-informed decisions.

# OARC Annual Status Report For the Fiscal Year Ended June 30, 2018



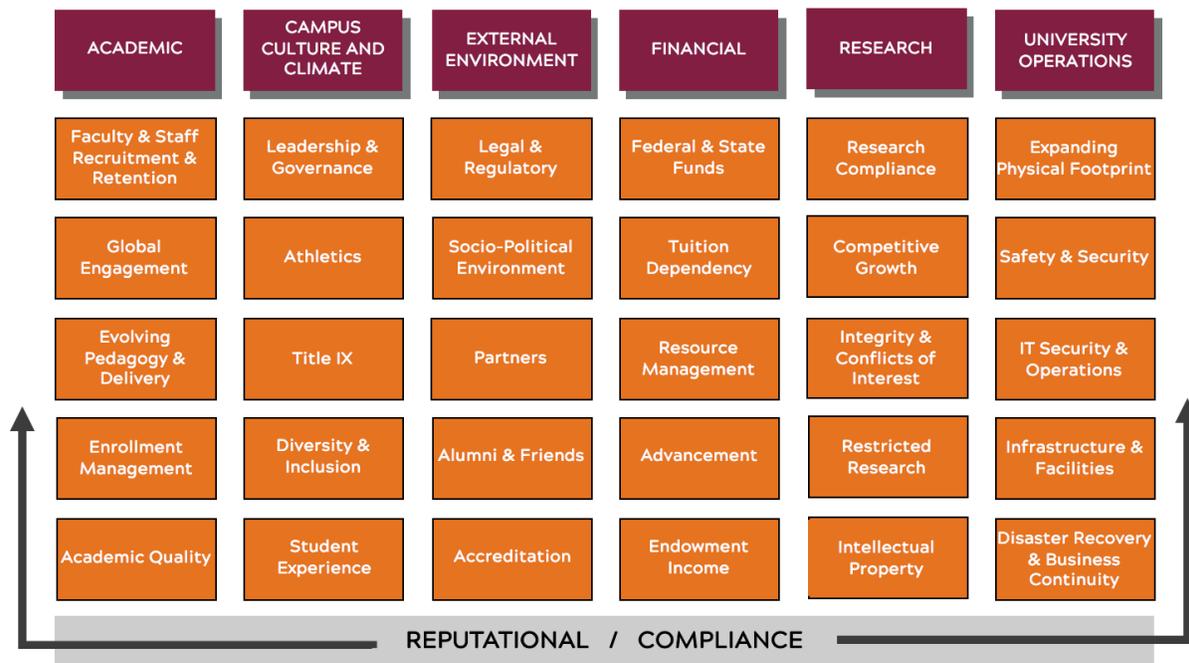
## OARC Annual Status Report For the Fiscal Year Ended June 30, 2018

The President's Leadership Team (PLT) serves as the Risk Advisory Committee. This group reviews the risks identified individually by senior leaders and further prioritized and assessed the risks to identify the university's top strategic risks. Members will continually seek to identify risks in their areas of operation and bring them to the PLT for evaluation in light of higher education or industry trends and national regulatory indicators. Also, this group ensures appropriate ownership and accountability of risks, including development of risk mitigation plans.

The President's Executive Staff+ serves as the ERM Committee. Executive Staff sets the university's risk appetite, contributes to the assessment of risks along with risk mitigation plans, and provides guidance on how to report key risks to the CAR. Executive Staff will incorporate information from the ERM program to guide strategic decision making and to effectively allocate resources.

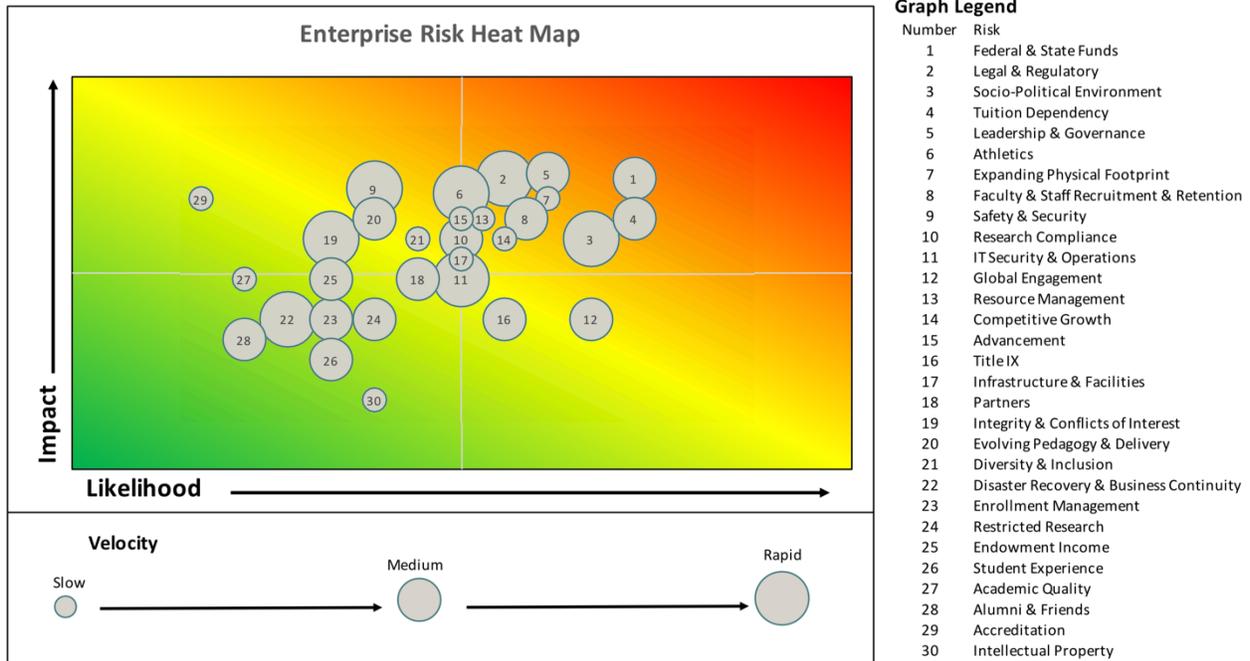
The initial ERM risk identification and assessment process was undertaken during fiscal year 2017-18 and resulted in university leadership's identification of key residual risks across six thematic areas, documented in the Enterprise Risk Landscape.

## ENTERPRISE RISK LANDSCAPE



In consideration of long-term and strategic organizational objectives, leadership assessed key risks in terms of likelihood of occurrence, significance of impact, and velocity, which was depicted in a heat map.

## OARC Annual Status Report For the Fiscal Year Ended June 30, 2018



The ERM program continued to move forward with OARC facilitating the identification of risk owners, development of risk snapshot templates for completion by risk owners, and the university's first ERM tabletop exercise.

### Institutional Compliance Program

Virginia Tech is committed to integrity, a culture of compliance, and the promotion of the highest ethical standards for all employees. As compliance with legal and regulatory requirements continue to increase in visibility and emphasis, OARC was charged in Fall 2017 with forming an Institutional Compliance Program (ICP) to promote and support a working environment that reflects this commitment. The ICP serves as a resource for Virginia Tech by helping the institution proactively meet its compliance obligations and manage compliance risks. The ICP structure is based on the eight elements of an effective compliance program identified by the Higher Education Compliance Alliance. A successful and effective compliance program should create a culture in which compliance is seen as everyone's job, not just a task dedicated to a specific office, and provide a positive focus that promotes an ethical, values-based environment that is consistent with the mission of higher education.



The primary focus of compliance with applicable laws and regulations is in the academic and administrative units throughout the university, where the authority for policy development and the responsibility for implementation of compliance reside. The compliance framework will include members of management with responsibility for key

## OARC Annual Status Report For the Fiscal Year Ended June 30, 2018

compliance areas and other appropriate officials. During fiscal year 2017-18, initial efforts began for OARC to leverage existing structures (including audit, ERM, hotline administration, legal counsel, and the policy office) to support compliance efforts.

The ICP has been implemented as a collaborative effort at various levels of the organization as depicted below.



### Institutional Compliance Function (OARC)

The charge from the President for the compliance function within OARC was to be a resource and serve as a catalyst for the achievement of university best practices in compliance-related subject matter areas. While OARC does not own any discrete compliance subject matter area, it will assist in promoting a culture of compliance and ethical behavior by:

- developing a compliance matrix of applicable regulations and authoritative guidance with responsible parties;

## **OARC Annual Status Report For the Fiscal Year Ended June 30, 2018**

- implementing the compliance risk assessment process as a component of the ERM program;
- facilitating the university compliance and ethics hotline;
- assisting the compliance committees in their various duties; and
- providing assistance in responding to external reviews and investigations.

### Executive Compliance Committee (ECC)

The charge of the ECC is to promote excellence in our compliance efforts to assure compliance with our legal, regulatory, and ethical responsibilities. The ECC is responsible for approving the university's compliance priorities and has oversight responsibility for the university's compliance efforts, including fulfillment of these priorities.

### Compliance Advisory Committee (CAC)

The charge of the CAC is to assist the ECC in promoting a culture and understanding of and adherence to applicable legal and regulatory requirements. The CAC will provide compliance leadership in the university's academic and administrative units and ensure effective communication and collaboration among those responsible for compliance by:

- fostering communication across campus on issues related to compliance;
- maintaining a university compliance matrix;
- reviewing the results of the compliance risk assessment and proposing university priorities;
- ensuring the development and implementation of corrective action plans as developed by responsible parties and approved by senior management; and
- reporting results to the ECC, including progress on plans and risks being assumed.

The success of Virginia Tech's ICP is predicated on leadership's embrace of a culture of compliance in alignment with our strategic goals. During fiscal year 2017-18, OARC developed the ICP framework and the program continues to emerge and evolve. Progress was made in the first year, including the establishment of the oversight committees and identification of almost 300 compliance areas and associated ownership by over 50 distributed compliance owners. The initial committee meeting was held to identify tasks and begin development of a more complete database of the various compliance requirements faced by the university.

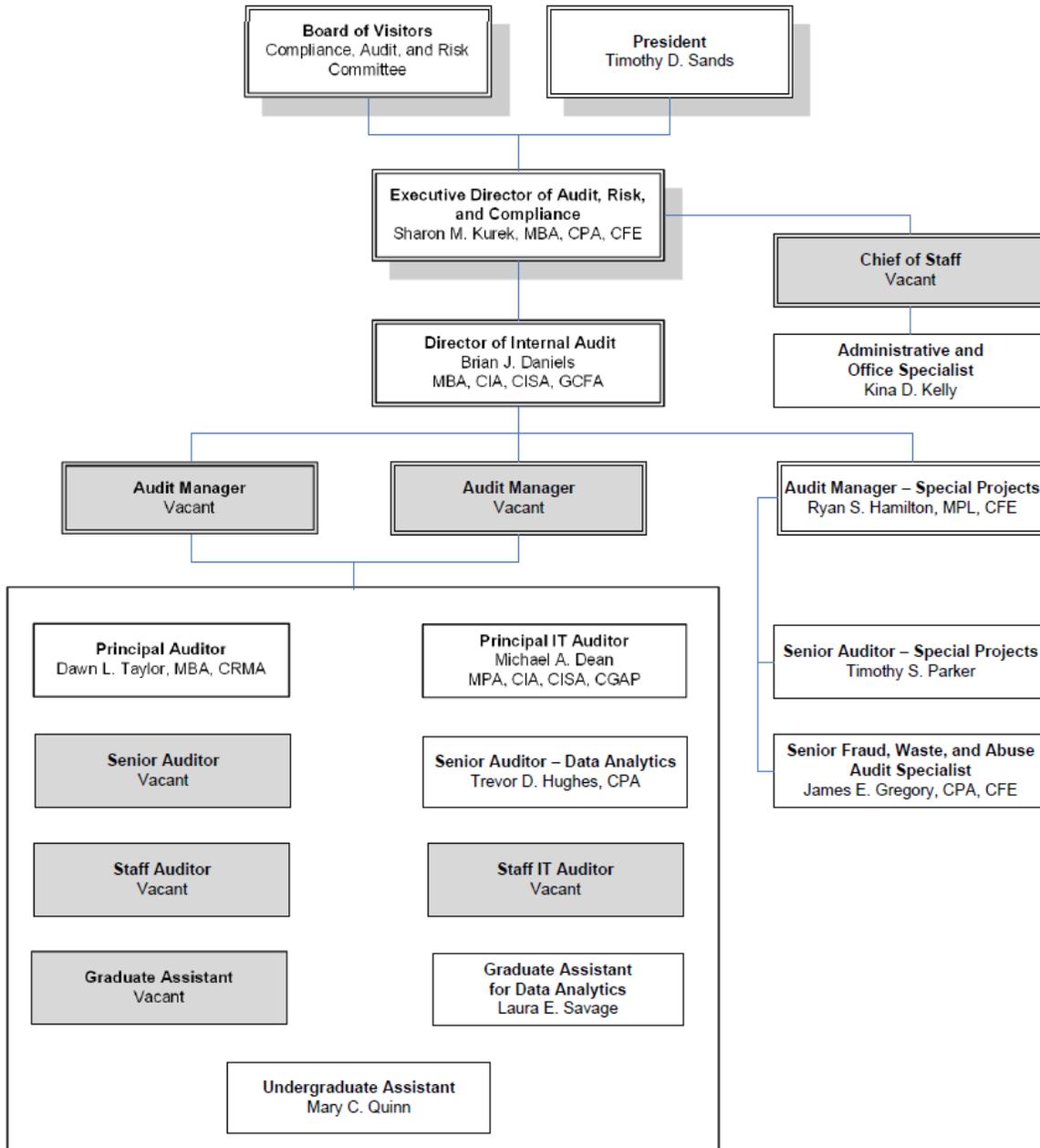
### **Staffing**

---

Current OARC staffing includes the Executive Director of Audit, Risk, and Compliance; Director of Internal Audit; an Audit Manager for Special Projects; a Chief of Staff; seven audit professionals; a part-time wage Senior Fraud Specialist; an Administrative and Office Specialist; two graduate assistants; and an undergraduate student wage employee. Two audit manager positions are being held vacant for budget purposes. Exhibit 8 on the following page shows OARC's organizational chart as of June 2018.

# OARC Annual Status Report For the Fiscal Year Ended June 30, 2018

## Exhibit 8 OARC Organizational Chart Office of Audit, Risk, and Compliance Virginia Tech



**Credential Legend:**  
 CPA – Certified Public Accountant  
 CIA – Certified Internal Auditor  
 CISA – Certified Information Systems Auditor  
 CFE – Certified Fraud Examiner  
 GCFA – GIAC Forensic Analyst  
 CGAP – Certified Government Auditing Professional  
 CRMA – Certification in Risk Management Assurance  
 MBA – Master’s of Business Administration  
 MPA – Master’s of Public Administration  
 MPL – Master’s of Policy Leadership

Organizational Structure  
June 2018

**OARC Annual Status Report  
For the Fiscal Year Ended June 30, 2018**

Sharon M. Kurek was elected as the Association of College and University Auditors (ACUA) President after serving as the Vice President and a Board Member-at-large on the governing board of the Association of College and University Auditors (ACUA). She remained a member of the ACUA Faculty Program, which is a resource to other associations or universities looking for talented speakers on topics such as risk, internal controls, auditing, compliance, and fraud. Additionally, Ms. Kurek completed the graduate course work for the Virginia Tech Pamplin College of Business professional MBA program. Furthermore, Ms. Kurek collaborated with peers from other institutions of higher education nationally while participating on an external quality assessment team for the University of Texas at Dallas' internal audit function.

Brian J. Daniels continues to join with peer institutions through the Virginia Alliance for Secure Computing and Networking (VASCAN) group in an effort to plan and organize the annual fall conference aimed at improving information security in the higher education arena within the commonwealth. Mr. Daniels served on the ACUA Membership Committee and performed an audit of ACUA and its management firm as part of his role on the Audit Committee. Additionally, Mr. Daniels collaborated with peers from other institutions of higher education nationally while participating on an external quality assessment team for the University of South Carolina System and Texas Tech University System. Mr. Daniels was elected by peer institutions to serve a multi-year term on the ACUA Board of Directors beginning in the fall of 2018.

Ryan S. Hamilton, Audit Manager for Special Projects, joined OARC late in the fiscal year after a distinguished career working with the Central Intelligence Agency in a similar audit and advisory capacity.

OARC leadership continued to participate actively within the College and University Auditors of Virginia (CUAV) organization, attending meetings with peer chief audit executives through the CUAV group to discuss best practices or issues. The Executive Director is a member of the CUAV Legislative Committee, which is proactively involved in the state legislative process with respect to laws and regulations pertinent to higher education internal audit and effective communication, thereof, to stakeholders.

OARC staff has more than 200 years of combined professional experience in accounting, auditing, compliance, and IT and over 60 years of service to Virginia Tech. The staff offers an extensive background with expertise in such functional areas as IT; fraud and forensics; environmental, health, and safety; NCAA bylaws; financial aid; research regulations; and general financial, compliance, and operational auditing. Additional expertise is in development related to Enterprise Risk Management and Institutional Compliance. Exhibit 9 shows the certifications and advanced degrees held by OARC staff at yearend.

**OARC Annual Status Report  
For the Fiscal Year Ended June 30, 2018**

**Exhibit 9  
Certification and Advanced Degrees held by OARC**

<b>Certification and Advanced Degrees</b>	
<b>Professional Certifications</b>	
3	Certified Public Accountants (CPA)
3	Certified Fraud Examiners (CFE)
2	Certified Information Systems Auditor (CISA)
2	Certified Internal Auditor (CIA)
1	Certified Government Auditing Professional (CGAP)
1	Certified Forensics Analyst (GCFA)
1	Project Management Professional (PMP)
1	Certification in Risk Management Assurance (CRMA)
<b>Advanced Degrees</b>	
3	Master of Business Administration (MBA)
1	Master of Policy Leadership (MPL)
1	Master of Public Affairs (MPA)

OARC ensures each staff member annually receives 40 hours of continuing professional education (CPEs) to meet professional certification requirements. General training topics included auditing practices and techniques, fraud detection techniques, data analytics, and regulatory items, such as Title IX and Payment Card Industry Standards.

### **Resources**

Exhibit 10 compares OARC's expenditures from fiscal year 2016-17 with expenditures for fiscal year 2017-18. The expenditures for salaries and benefits decreased mostly due to extended vacancies among staff members. As a result, training expenses were down by approximately 18 percent. Additionally, during fiscal year 2017-18, Baker Tilly was hired in a co-sourcing arrangement to lend expertise and assist with conducting an audit of a high-risk activity.

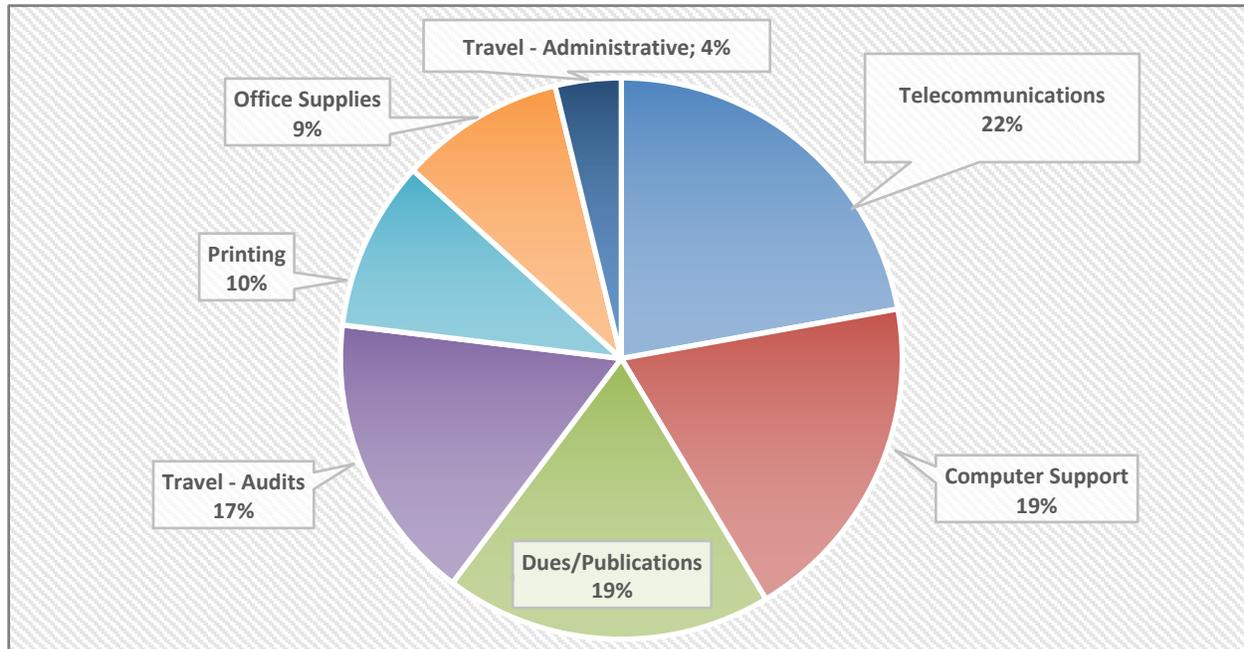
**Exhibit 10  
Analysis of Expenditures**

	<b>FY2017</b>	<b>FY2018</b>
Salaries and Benefits	1,553,925	1,480,551
Operating Expenses	43,157	38,394
Training	38,312	30,018
Audit Software	45,664	18,699
Professional Audit Services	-	4,812
Personnel Expenses	986	1,593
External Quality Assessment	9,202	-
<b>Total</b>	<b>\$1,691,246</b>	<b>\$1,574,067</b>

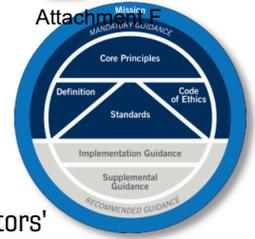
**OARC Annual Status Report  
For the Fiscal Year Ended June 30, 2018**

Exhibit 11 shows an analysis of operating expenses. Approximately 60 percent of operating expenses resulted from basic costs to support the department, including telecommunications, computer support, office supplies, and printing. Similarly, membership dues and publication expenses will remain an ongoing cost as leadership encourages and sponsors professional certification and organizational participation.

**Exhibit 11  
Analysis of Operating Expenses**



**OARC Annual Status Report Appendix  
For the Fiscal Year Ended June 30, 2018**



**Per Charter:**

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, Definition of Internal Auditing, Code of Ethics, and *International Standards for the Professional Practice of Internal Auditing*.

<b>MANDATORY GUIDANCE</b>	
<b>Core Principles</b>	<ul style="list-style-type: none"> <li>Demonstrates integrity.</li> <li>Demonstrates competence and due professional care.</li> <li>Is objective and free from undue influence (independent).</li> <li>Aligns with the strategies, objectives, and risks of the organization.</li> <li>Is appropriately positioned and adequately resourced.</li> <li>Demonstrates quality and continuous improvement.</li> <li>Communicates effectively.</li> <li>Provides risk-based assurance.</li> <li>Is insightful, proactive, and future-focused.</li> <li>Promotes organizational improvement.</li> </ul>
<b>Definition of Internal Auditing</b>	Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
<b>Code of Ethics</b>	<p>Internal auditors are expected to apply and uphold the following principles:</p> <ul style="list-style-type: none"> <li><b>Integrity</b> – The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.</li> <li><b>Objectivity</b> – Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments.</li> <li><b>Confidentiality</b> – Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.</li> <li><b>Competency</b> – Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services.</li> </ul>
<b>International Standards for the Professional Practice of Internal Auditing</b>	<p><b>Attribute Standards (1000 through 1300)</b></p> <p>1000 Purpose, Authority, and Responsibility</p> <p>1100 Independence and Objectivity</p> <p>1200 Proficiency and Due Professional Care</p> <p>1300 Quality Assurance and Improvement Program</p> <p><b>Performance Standards (2000 through 2600)</b></p> <p>2000 Managing the Internal Audit Activity</p> <p>2100 Nature of Work</p> <p>2200 Engagement Planning</p> <p>2300 Performing the Engagement</p> <p>2400 Communicating Results</p> <p>2500 Monitoring Progress</p> <p>2600 Communicating the Acceptance of Risks</p>

August 26, 2018

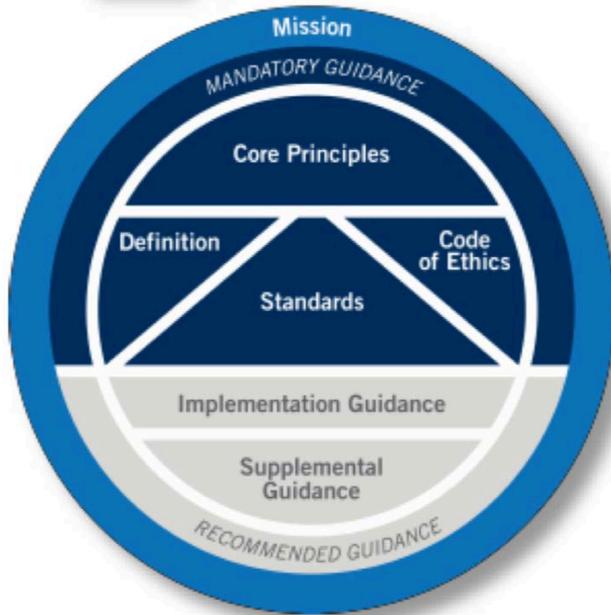
# OFFICE OF AUDIT, RISK, AND COMPLIANCE ANNUAL STATUS REPORT

*Sharon M. Kurek, CPA, CFE, MBA*  
*Executive Director of Audit, Risk, and Compliance*





International Professional  
Practices Framework



*The chief audit executive's reporting and communication to senior management and the board must include information about:*

- *The audit charter, including internal audit activity's purpose, authority, and responsibility.*
- *Independence of the internal audit activity.*
- *The audit plan and progress against the plan.*
- *Resource requirements.*
- *Results of audit activities.*
- *Conformance with the Code of Ethics and the Standards, and action plans to address any significant conformance issues (Quality Assurance & Improvement Program).*
- *Management's response to risk that, in the chief audit executive's judgment, may be unacceptable to the organization.*

# OARC MISSION

- *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. OARC's mission is to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight as follows:*

- *AUDIT - Provide independent, objective assurance and advisory activity designed to add value and improve university operations. Audits help the university accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*
- *ENTERPRISE RISK MANAGEMENT - Provide oversight of the enterprise risk management program by creating and maintaining the framework to effectively identify, assess, and manage risk.*
- *COMPLIANCE - Provide oversight of the institutional compliance program and the distributed processes that support compliance across the university.*

# STATE OF UNIVERSITY'S CONTROL ENVIRONMENT

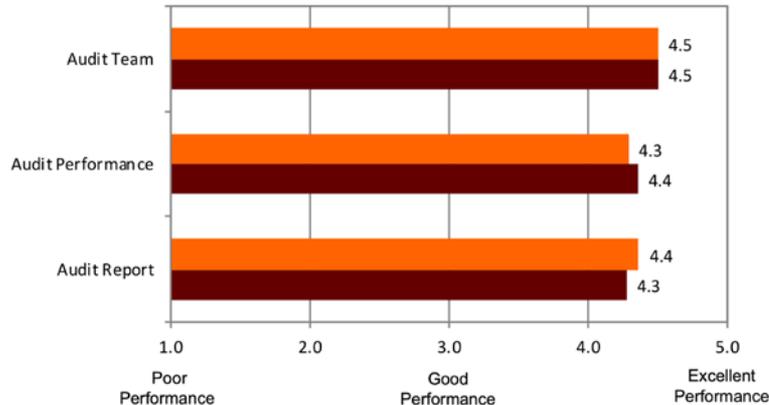
- *Management accepts their responsibility for internal control and is supportive of audit efforts*
- *Management generally accepts audit recommendations and responds by developing action plans to address concerns*
- *No material control weaknesses were identified; however, a number of areas requiring improvement were noted*
- *Work was not limited by management*
- *Independence/objectivity was not impaired*

## FY 2017-18 Completion of Audit Plan

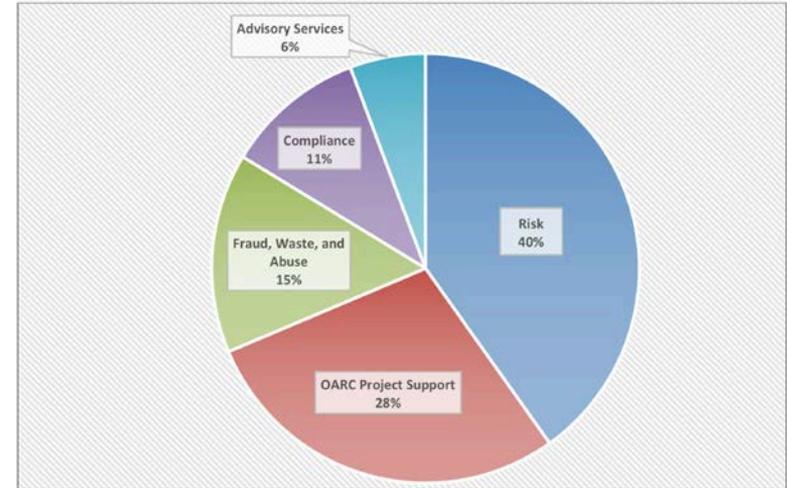
<b>Audits</b>	
Total # of <b>Audits</b> Planned	34
Total # of Supplemental <b>Audits</b>	1
Total # of Carry Forwards	7
Total # of Planned <b>Audits</b> Deferred and/or Canceled	16
<b>Total Audits in Plan as Amended</b>	<b>26</b>
Total <b>Audits</b> Completed	24
<b>Audits</b> - Percentage Complete	92%
<b>Audits</b> - Percentage Complete or Underway	100%
Note: Includes Policy Compliance Reviews and Advisory Services	

## Results of FY 2017-18 Surveys for Evaluating OARC Services

■ 2018 ■ 2017



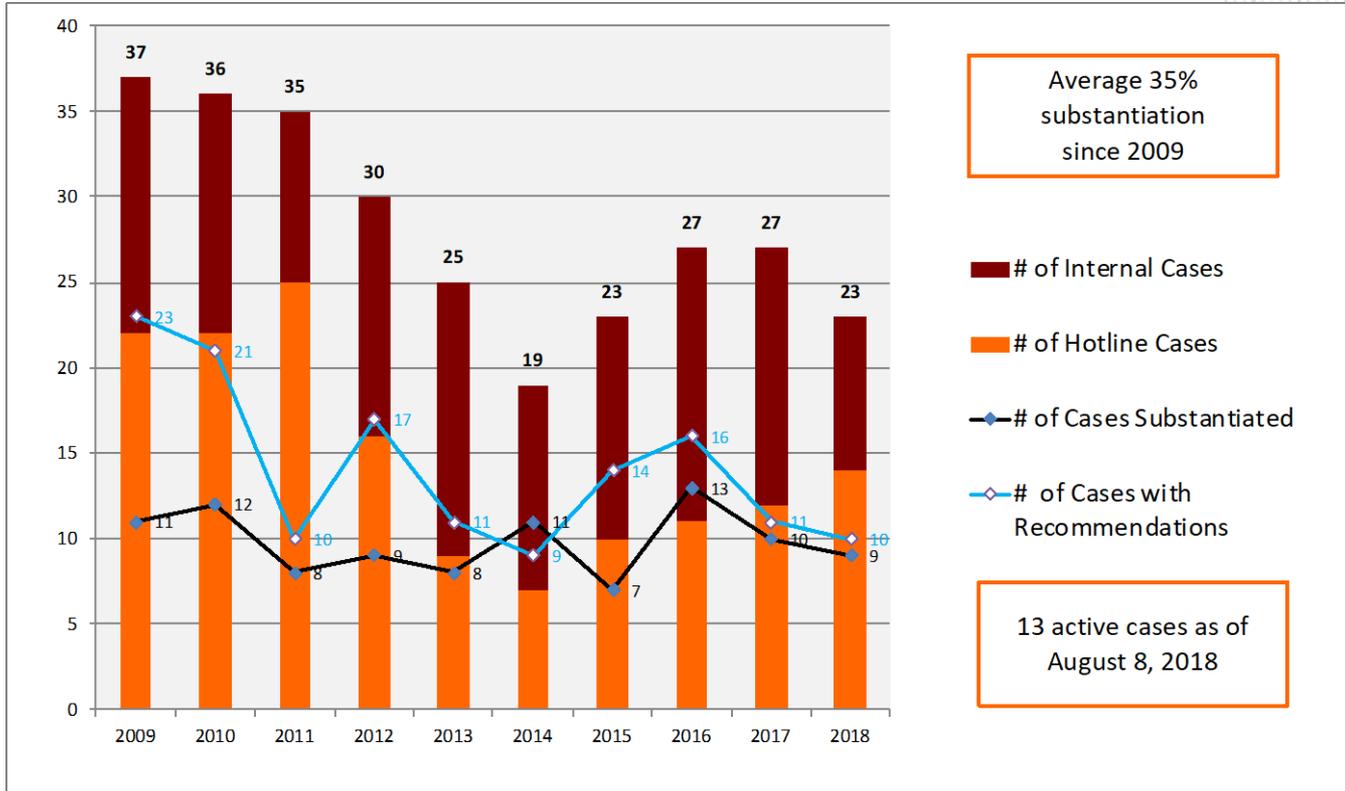
## FY 2017-18 Distribution of Direct Audit Hours

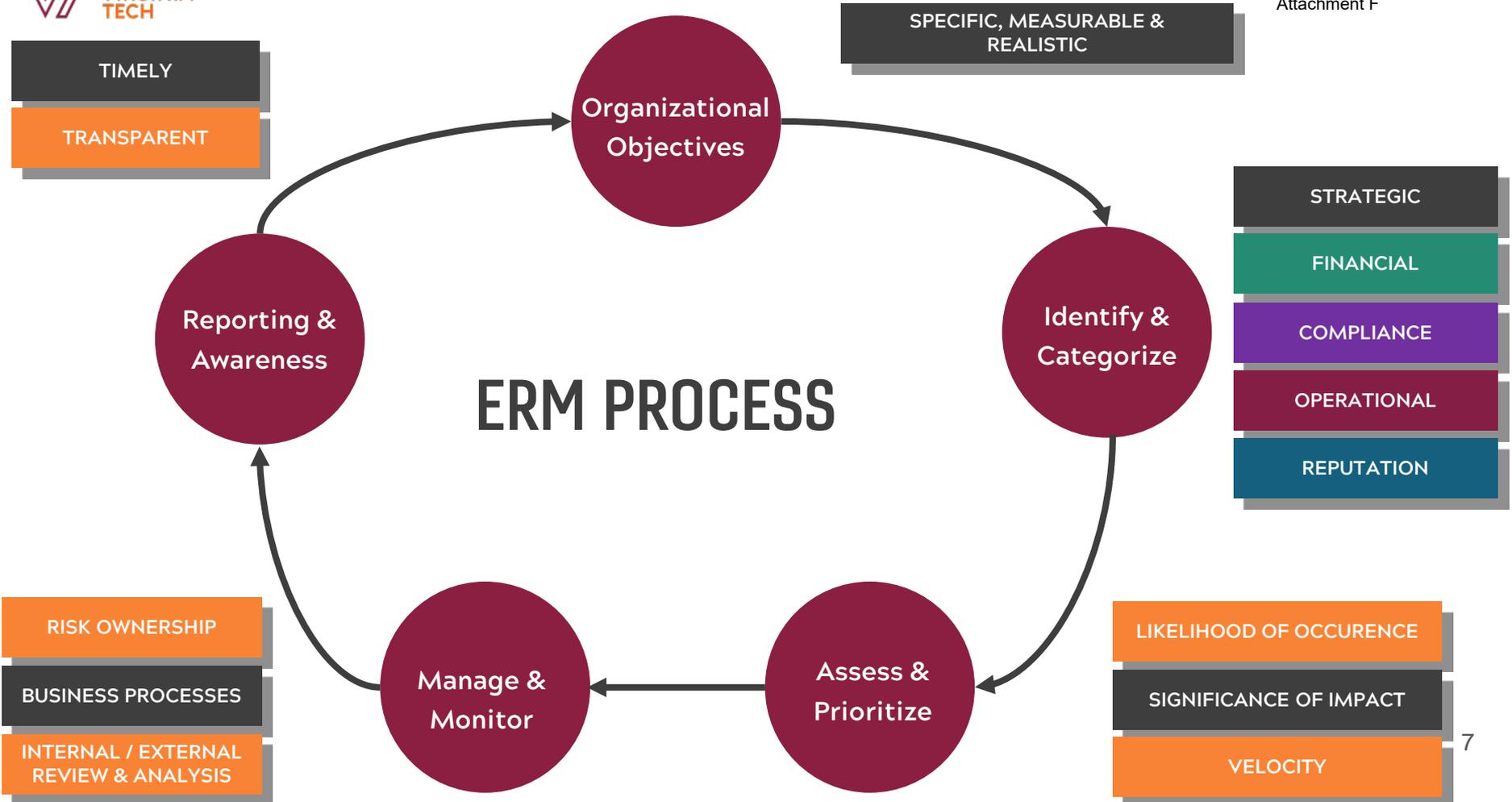


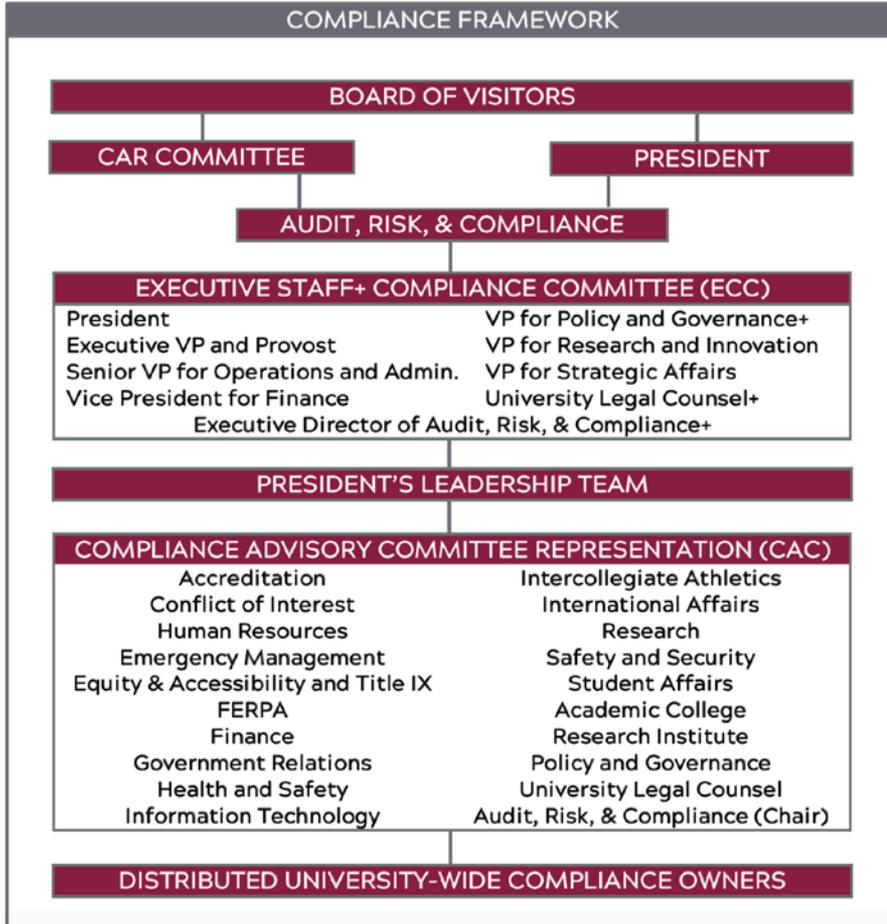
## Inventory of MCAs

Beginning # of MCAs	42
MCAs added	92
MCAs closed	<u>109</u>
Current open inventory of MCAs	25

# FRAUD, WASTE, AND ABUSE (FWA)

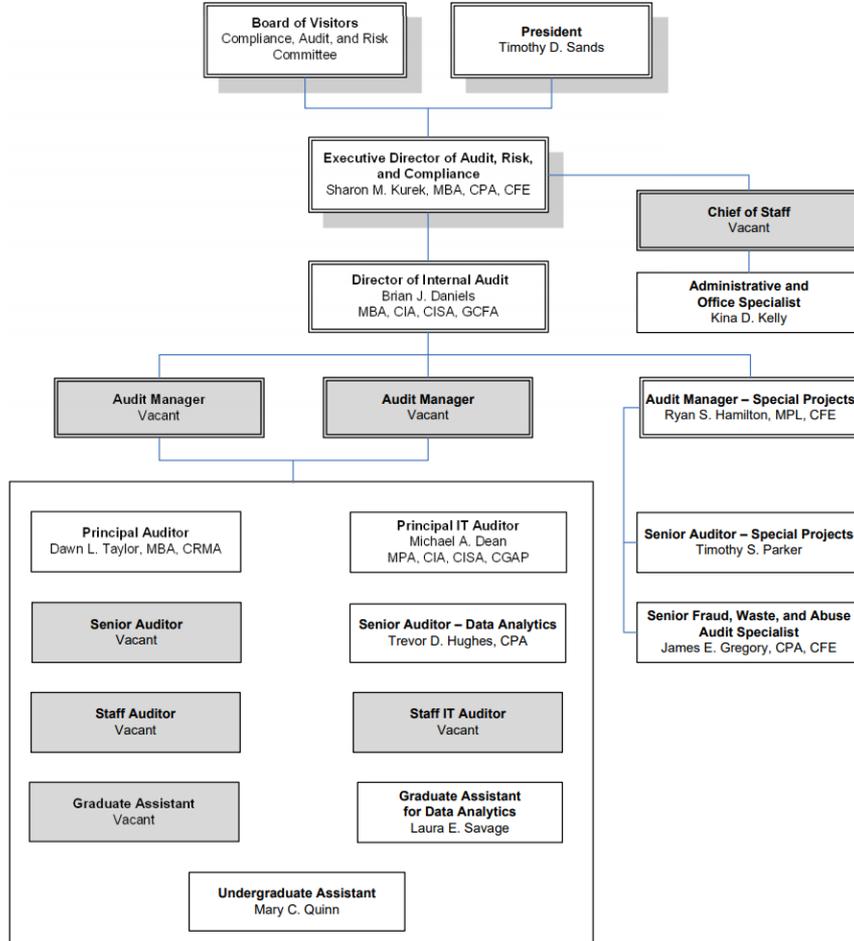






## STATISTICS

- *CAC – 20 Members*
- *56 Distributed Compliance Owners*
- *298 Regulations Initially Identified by OARC*



## Certification and Advanced Degrees held by OARC

Certification and Advanced Degrees	
<b>Professional Certifications</b>	
3	Certified Public Accountants (CPA)
3	Certified Fraud Examiners (CFE)
2	Certified Information Systems Auditor (CISA)
2	Certified Internal Auditor (CIA)
1	Certified Government Auditing Professional (CGAP)
1	Certified Forensics Analyst (GCFA)
1	Project Management Professional (PMP)
1	Certification in Risk Management Assurance (CRMA)
<b>Advanced Degrees</b>	
3	Master of Business Administration (MBA)
1	Master of Policy Leadership (MPL)
1	Master of Public Affairs (MPA)

## Analysis of Expenditures

	<b>FY2017</b>	<b>FY2018</b>
Salaries and Benefits	1,553,925	1,480,551
Operating Expenses	43,157	38,394
Training	38,312	30,018
Audit Software	45,664	18,699
Professional Audit Services	-	4,812
Personnel Expenses	986	1,593
External Quality Assessment	9,202	-
<b>Total</b>	<b>\$1,691,246</b>	<b>\$1,574,067</b>

# QUESTIONS?

# Virginia Tech

---

**Office of Audit, Risk, and Compliance**

Fiscal Year 2018-19 Audit Plan

August 26, 2018

## 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 (ERM)

The university began a new Enterprise Risk Management (ERM) initiative during fiscal year 2017-18 to provide enhanced visibility into the university's risks and align strategic planning with the resulting risk awareness. OARC began facilitating the ERM program by working with university leadership to establish the framework for collectively identifying and assessing risks across the enterprise. The ERM program will ultimately 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 of risk tolerance;
- 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
- Improve efficiency and optimized allocation of resources through risk prioritization.

University leadership provided feedback for the initial ERM process by assessing the risks in terms likelihood of occurrence, significance of impact, and the 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 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 business 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.

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 assessment of IT and business operations at the university identified four high-level risk domains intended to encapsulate the vast majority of the systems and computing environments within the university as follows:

- Student Systems;
- Finance and Administrative Systems;
- Human Resources Systems; and
- Research Systems.

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 validate the plan, one-on-one discussions were conducted 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 annual reviews of selected components of the entities with high external compliance risk and complex operations. These entities are University Scholarships and Financial Aid, Research, Human Resources, and Intercollegiate Athletics.

## **FISCAL YEAR 2018-19 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. 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. Annual expenditures and revenues referenced below reflect fiscal year 2016-17 data unless otherwise noted.

At the direction of the Board of Visitors, significant effort has gone in to the development of a more senior staff within the internal audit function. This effort has been generally successful; however, budgetary considerations have not necessarily kept pace with these efforts. This factor, combined with the continued general migration of audit staff to promotional opportunities in management across the university, requires the Draft Audit Plan to be tempered. As such, you will see the 21 projects we have on the audit plan for this year, as well as 8 projects that would have been included on the plan if the office were able to maintain its prior staffing levels.

### Risk-Based Assurance

Planned Engagement	Overview	Risk Area
Athletics *	The Department of Athletics (Athletics), with 22 varsity sports at the NCAA Division I level, monitors and supports more than 550 student-athletes each academic year. Athletics had operating revenues of approximately \$87.4 million and total operating expenses of approximately \$90.7 million. The Office of Audit, Risk, and Compliance conducts various components of a complete audit of Athletics over a five-year period.	Compliance – Athletics
Americans with Disabilities Act (ADA) Compliance	Virginia Tech is committed to equal opportunity in employment and education for individuals with disabilities and complies with the Americans with Disabilities Act, as amended, and Section 504 of the Rehabilitation Act of 1973. ADA and Accessibility Services consults with colleges and departments both on and off campus to ensure equal opportunity for individuals with disabilities. Employees with disabilities may be entitled to reasonable accommodations under Title 1 of the Americans with Disabilities Act. Given the applicability to students, the Services for Students with Disabilities office also has a role in helping to ensure reasonable accommodations and ADA compliance. ADA compliance has not previously received a focused review.	Compliance – Human Resources and Student Services
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 2011.	Operational – Human Resources
Hume Center	The mission of the Ted and Karyn Hume Center for National Security and Technology (Hume Center) is to cultivate the next generation of national security leaders by developing and executing curricular, extracurricular, and research opportunities to engage students. Jointly operating in the National Capital Region and the Blacksburg campuses, Hume Center research activities principally focus on cybersecurity, resilience, and autonomy challenges faced by the national security and homeland security communities. While not officially established in its current format until 2010, organizational oversight of the Hume Center has transitioned several times since inception. Research expenditures	Operational – Research

Planned Engagement	Overview	Risk Area
	totaled approximately \$6.6 million. Elements of the Hume Center's activity have been previously reviewed; however, there has not yet been a focused audit.	
IT: Controlled Unclassified Information (CUI) and Secure Research Environment (SRE)	CUI is defined as information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not deemed as classified. The federal security requirements apply only to components of nonfederal systems that process, store, or transmit CUI when it resides in nonfederal systems and/or organizations such as Virginia Tech. The offices of Collaborative Computing Solutions within the Division of IT and the Office of Export and Secure Research Compliance within the Division of Research and Innovation jointly developed the SRE to allow for sponsored research projects working with covered data sets to be processed, stored, and transmitted with appropriate and required security considerations in place. Although a previous advisory review was done during the establishment of this project, a dedicated review has not yet occurred.	Compliance – Research
IT: Industrial Control Systems	Industrial Control Systems (ICS) is a general term that encompasses several types of systems and instrumentation related to industrial processes. At Virginia Tech, this may include operations related to power generation and distribution among other areas. Given the growing complexity of industrial environments, it is important that organizations make an effort to adequately protect against digital threats. Doing so requires a multi-step approach that focuses on network security, server security, and device-level security. ICS has not previously received a dedicated review.	Information Technology
IT: Third-Party Access to University Data	In addition to mandatory submission of data to third parties, the university has procured entire systems and services through outsourcing agreements to host and process institutional data. Examples include an outsourced e-commerce system for procuring goods or services and systems intended to meet federal immigration requirements. In addition to these high-visibility centrally purchased systems, there may be departmental systems outside of the university environment that may have highly sensitive data, yet have not been approved by central administration due to long-term existence or relatively low financial impact. This audit is intended to identify and review the security of university data in outsourced systems as well as other third-party vendor access to data. The outsourced environment was last audited in 2013.	Information Technology
Maintenance Reserve	Maintenance Reserve work is described as any major repair or replacement with a cost of \$25,000 to \$1 million to a fixed component of existing physical plant or property intended to extend the useful life of an asset in its current form. The first priority of Maintenance Reserve is to maintain the integrity of a building envelop to prevent intrusion of weather and natural elements, which can quickly destroy a building beyond repair when allowed to progress unchecked. Thus, repairs of roofs, windows, and building skin are considered the first priority for the use of these resources. Maintenance Reserve projects are generally not intended to enhance, upgrade, or otherwise improve plant, property, or equipment. Maintenance Reserve is a significant	Operational – Facilities

Planned Engagement	Overview	Risk Area
	activity at the university, with more than \$27 million allocated from the commonwealth budget process over the current biennium. This activity has not previously received a dedicated review.	
Office of the University Bursar	The Office of the University Bursar (OUB) has the responsibility of 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. The specific responsibilities of this department 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, disbursement of payroll, all university payables, Perkin's loan fund repayment, collection of delinquent accounts and notes receivable, and administration of the Budget Tuition Program. The Office of the University Registrar also partners closely with University Scholarships and Financial Aid in the administration of scholarships for students. The last audit of OUB was in 2012.	Financial – Financial Management
Research: Grant Management *	In addition to safety and other compliance matters, the university's research portfolio requires significant fiscal oversight and management. Principal Investigators (PIs) are responsible for monitoring the day-to-day fiscal performance and technical progress of their sponsored award. Proper monitoring practices for PIs include: assuring salaries and equipment are charged accurately, tracking budget reports carefully, noting any restrictions placed by the sponsor on the expenditure of awarded funds. Additional considerations requiring active management and oversight from PIs and their departments include cost sharing, which is a financial commitment by the university to share in the funding of a sponsored activity. Various elements of this topic have been included in various distributed reviews, but this broad centralized approach will leverage data analysis in a manner not previously conducted.	Financial – Research
Research: Subrecipient Monitoring *	The Office of Sponsored Programs functions as the steward of Virginia Tech's research portfolio and is responsible for ensuring that all research proposals and projects comply with university, federal, and sponsor regulations, policies, and procedures. A Subrecipient refers to a recipient that receives a subaward or subcontract from a pass-through entity to carry out part of a program. Subrecipient monitoring guidelines and responsibilities are shared among PIs, departmental administrators, OSP personnel, and the OSP Subrecipient Monitoring Committee. This topic is a significant federal compliance area requiring close attention to ensure compliance and avoid significant financial or other penalties. This topic has not previously received a targeted review.	Compliance – Research
School of Public and International Affairs	The School of Public and International Affairs (SPIA), operating within the College of Architecture and Urban Studies, offers degree programs in the Center for Public Administration and Policy, Government and International Affairs, and Urban Affairs and Planning. Research initiatives are carried out by the Metropolitan Institute in the National Capital Region and the Institute for Policy	Operational – Academic

Planned Engagement	Overview	Risk Area
	and Governance at the Blacksburg campus. Total expenditures were approximately \$9.2 million, while revenue was just over \$2.2 million. SPIA has not previously received a dedicated review.	
Student Medical Insurance Reimbursement Program	The Student Medical Insurance office within Insurance and Risk Management has overseen the reimbursement of students related to overpayments for insurance premiums based on inflated rates charged to Virginia Tech students by third parties during the period of 2003-2011. Reimbursements have been based upon a percentage of each student's actual recorded payment toward their health insurance coverage. The university has worked with an outside entity to manage the repayment of affected individuals. This review will focus on the closeout of the reimbursement program.	Compliance – Financial Management
Title IX Compliance	Maintaining a campus free of sex discrimination, including sexual misconduct and sexual harassment, is important for all students and employees. Title IX of the Education Amendments (1972) prohibits discrimination on the basis of sex in any educational program or activity that receives federal financial assistance. Failure to comply with Title IX can include the termination of all or part of a university's federal funding. This includes grants, subsidies, and other program funds from the federal government. In addition to the loss of federal funds, universities may be sued by those seeking redress for violations of Title IX. It is essential that institutions receiving federal financial assistance operate in a nondiscriminatory manner. Although external reviews have occurred, this topic has not previously received a dedicated review.	Compliance – Campus Safety and Security
University Building Official	Virginia Tech has its own University Building Official serving as the authority having jurisdiction for projects governed by the Virginia Uniform Statewide Building Code and administered directly by the university on campus and the sites throughout the Commonwealth owned by the university. The Office of the University Building Official provides technical engineering and code related support and serves as the primary liaison with outside regulatory agencies, working closely with them on code issues that affect the design, construction, and ultimately the approval to occupy a new university facility or maintain existing facilities. The last dedicated review of this topic was in 2015.	Operational – Facilities
University Registrar	The Office of the University Registrar provides many services, including academic records maintenance for more than 33,000 current students across 250 undergraduate and graduate degree programs. Other areas of responsibility include data stewardship; data integrity; ensuring compliance with all agency, state, and federal regulations; and development of semester course offerings. The last dedicated review of this office was in 2012.	Operational – Enrollment Services
University Scholarships and Financial Aid*	The Office of University Scholarships and Financial Aid (USFA) supports the university's student access, enrollment, and retention goals by providing the financial means to encourage economic, social, cultural, and academic diversity in the student body. USFA provided or monitored approximately \$462 million in student financial assistance. A complete audit of the various activities within USFA is performed over a four-year period.	Compliance – Enrollment Services

\* 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 surveys review 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	Overview	Risk Area
College of Agriculture and Life Sciences	The College of Agriculture and Life Sciences, with 12 academic departments and more than 2,700 students, offers a diverse range of degree programs ranging from an associate's program in Agricultural Technology to doctoral programs. CALS had \$139.8 million in expenditures including \$44.3 million in sponsored research. The last policy compliance audit of this area was in 2014.	Operational
Vice President and Dean for Graduate Education	The Virginia Tech Graduate School is responsible for the development, administration, and evaluation of graduate education throughout the university and administers all graduate degrees. The Graduate School currently offers more than 150 master's and doctoral programs for over 7,000 students at multiple locations throughout the Commonwealth of Virginia, through partnerships with the University of Maryland and Wake Forest University, and at several international sites. The last policy compliance audit of this area was in 2014.	Operational
Vice President for Student Affairs	The Division of Student Affairs is committed to the growth, development, and achievement of students at Virginia Tech. This organization works closely with academic colleagues to support students as they learn to be successful and effective leaders in the emerging global community. The division employs approximately 3,600 faculty and staff. The last policy compliance audit of this area was in 2014.	Operational

## Management Advisory Services

Planned Engagement	Overview	Risk Area
School of Plant and Environmental Sciences	The School of Plant and Environmental Sciences will be a national and international leader for improving human well-being and quality of life through learning, discovery, and engagement in plant and environmental sciences. The school will integrate three existing departments that share certain mission elements: Crop and Soil Environmental Sciences; Horticulture; and Plant Pathology, Physiology, and Weed Science. These units, with \$8 million in research and \$23 million in total expenditures, already share cross-cutting interdisciplinary research and will be further connected through undergraduate curricula and linked graduate programs, as well as through statewide research, extension, and outreach activities. This review is intended to assess initial control structure for the operations of the new school as it continues establishment.	Operational – Academic
Youth Protection Activities	The university is committed to the safety and welfare of its students, employees, and visitors through the establishment of practices that support a safe and secure environment in all buildings and grounds owned, controlled, or leased by Virginia Tech, including satellite locations, as well as promoting safety through policies and programs. Administrators, employees, students, volunteers, and others working with minors (children under the age of 18) have a responsibility to promote their protection.	Operational – Campus Safety and Security

## 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. Assist management with year-end inventory counts for financial statement verifications.
External Audit Coordination	Manage and serve as the liaison for all external audit services including contracted and regulatory-imposed audits.
Quality Assurance	OARC will undergo a mid-cycle review of its Quality Assurance and Improvement program to assess operations and practices with applicable standards. Additional effort will go into internal assessment to ensure the most effective and efficient procedures are in place and identify means of improving overall performance.

## ADDITIONAL AUDIT COVERAGE PENDING RESOURCES

With additional resources, the following projects would have been included for the fiscal year 2018-19 audit plan. Otherwise, these projects will be considered for inclusion on the fiscal year 2019-20 plan.

Planned Engagement	Overview	Risk Area
College of Natural Resources and Environment	The College of Natural Resources and Environment (CNRE) is comprised of four academic departments containing eight undergraduate majors and is the only college specializing in natural resource education, research, and outreach in Virginia. CNRE had expenditures of \$33.9 million including \$16.5 million in sponsored research. The last policy compliance audit of this area was in 2014.	Operational
Contract Approval and Delegated Authority	The Vice President for Finance and Chief Financial Officer is designated as the university's Chief Contracting Officer by the Board of Visitors, but has also been authorized to delegate signature authority. All contractual agreements must be reviewed by University Legal Counsel prior to execution, and may also require a review from the IT Security Office. University policy delegates to department heads the authority to enact purchases of goods and services valued up to \$2,000 per transaction. Department heads are responsible for the correct exercise of delegated purchasing authority and must ensure that personnel are properly trained and supervised, that all rules and procedures are followed, and that prices being paid are fair and reasonable. A focused review of this topic had not previously been conducted.	Financial – Financial Management
Eastern Shore AREC	Virginia Tech's Eastern Shore Agricultural Research Extension Center (AREC) is committed to supporting commercial vegetable and agronomic crop production. The center sits on a 226-acre farm that hosts an office complex, laboratories, equipment buildings, garages, a greenhouse, graduate student housing, a large freshwater pond, and woodland areas. More than 25 agricultural crops are grown annually for research and extension studies. This unit has not previously received a dedicated review.	Operational – Off-Campus Locations
GDPR	The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU. This advisory review will develop a	Compliance – Information Technology

Planned Engagement	Overview	Risk Area
	more complete understanding of the applicability and impact to the university and assess the continuing efforts by various university constituents.	
Graduate Education	The Virginia Tech Graduate School is responsible for the development, administration, and evaluation of graduate education throughout the University, and administers all graduate degrees. The Graduate School currently offers more than 150 master's and doctoral programs for over 7,000 students at multiple locations throughout the Commonwealth of Virginia, through partnerships with the University of Maryland and Wake Forest University, and at several international sites. The last dedicated review was in 2013.	Operational – Enrollment Services
IT: Windows Server Security	Servers are used widely to perform a variety of tasks, from network attached file storage or collaborative database hosting to processing email or print requests. As such, servers often present significant risks when not properly secured. A large percentage of the university's servers operate on the Windows platform. Focus will be on Windows Server security across the university including distributed locations, in various administrative, academic, and research departments. Windows Server security was last audited in 2014.	Information Technology
Licensing and Trademarks	University Relations, within the Division of Advancement, promotes and protects the Virginia Tech brand through appropriate use of the university's trademarks. Licensing and Trademarks approves internal use of trademarks and administers a licensed collegiate merchandise program through a partnership with IMG Licensing. Licensing and Trademarks had revenues of \$1.8 million and was last reviewed in 2009.	Financial – Auxiliary
Parking and Transportation	Virginia Tech has more than 16,400 parking spaces, a motorist assistance program, a fleet of approximately 300 vehicles, and a robust and award-winning alternative transportation program that includes daily shuttles from the Blacksburg campus to the Virginia Tech Carilion Research Institute in Roanoke as well as to the National Capital Region. In addition to the 33,000 students and 13,000 employees, an estimated 60,000 alumni, parents, and community members visit the campus each year. This area had \$6.5 million in revenue and last received a dedicated review in 2014.	Operational – Auxiliary Enterprise

## AUDIT RESOURCES

The audit plan for fiscal year 2018-19 is based on professional staffing of 11 full-time equivalents (FTEs). This is a reduced figure from prior years with two positions held vacant to cover other unfunded expenses, as relative seniority for audit staff has been prioritized when filling positions at the urging of the audit committee. Staffing will continue to be augmented by the continuation of the student internship program in which 2-3 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.

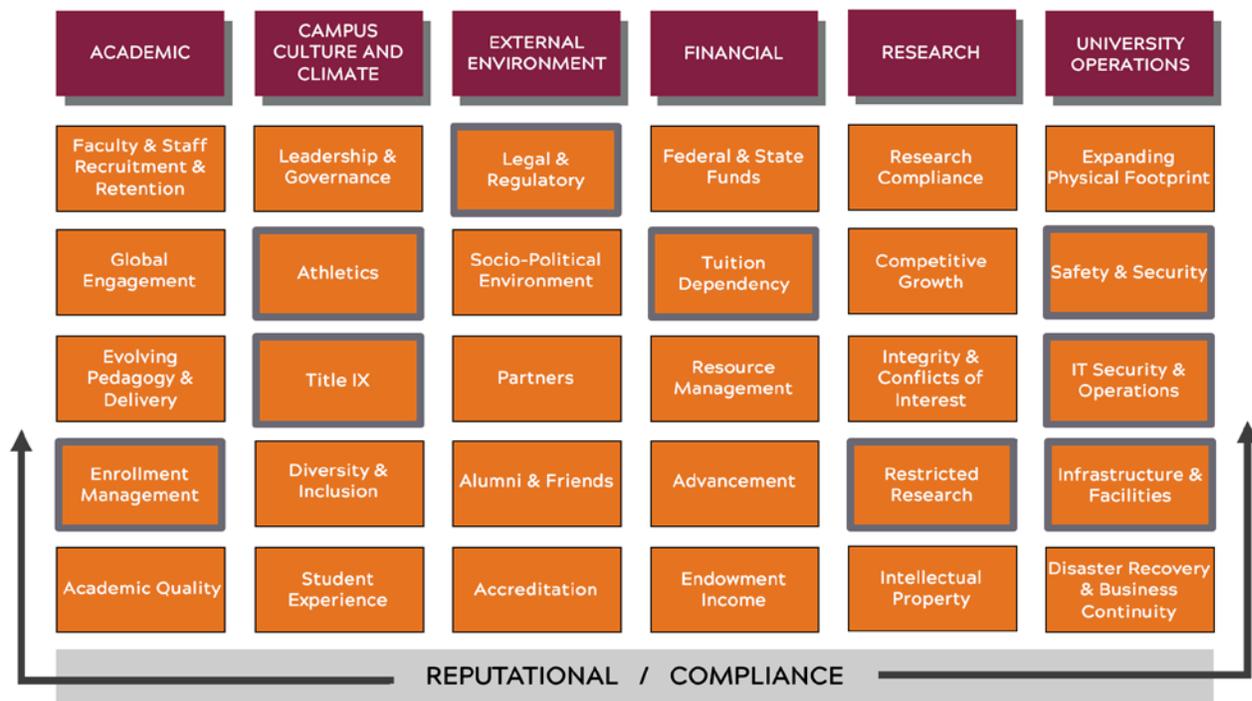
Audit resources are allocated as follows:

- 52 percent of the OARC's available resources are committed to the completion of planned audit projects and follow-up audit procedures.
- 10 percent to accommodate requests from management and consultations with university departments.
- 11 percent to conduct investigations into fraud, waste, and abuse allegations.
- 14 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 recently identified key residual risks across six thematic areas. The graphic below depicts how planned projects will provide audit coverage of enterprise risks.

## ENTERPRISE RISK LANDSCAPE



# OFFICE OF AUDIT, RISK, AND COMPLIANCE AUDIT PLAN Fiscal Year 2018-19

August 26, 2018

---

**Brian Daniels**

*Director of Internal Audit  
Office of Audit, Risk, and Compliance*

# OVERVIEW - ANNUAL AUDIT PLAN

The Office of Audit, Risk, and Compliance (OARC) conducts:

- Risk-Based Assurance Engagements
- Policy Compliance Reviews
- Management Advisory Services
- Investigations

Annual risk assessment process informs and guides the development of the audit plan for the next fiscal year

# OVERVIEW - ANNUAL 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. The critical areas for core audit plan inclusion are:

• Academic Units	• Human Resources
• Auxiliary Enterprises and Athletics	• Information Technology
• Campus Safety and Security	• Off-Campus Locations
• Enrollment Services	• Research
• Facilities and Operations	• Student Services
• Financial Management	

# RISK-BASED AUDIT PROJECTS

The audit plan focuses on strategic, operational, financial, compliance, and IT risks. The audit plan will be reconfigured as needed when new topics requiring more immediate attention emerge.

Athletics *	Research: Grant Management *
Americans with Disabilities Act (ADA) Compliance	Research: Subrecipient Monitoring *
Human Resources: Benefits*	School of Public and International Affairs
Hume Center	Student Medical Insurance Reimbursement Program
IT: Controlled Unclassified Information (CUI) and Secure Research Environment (SRE)	Title IX Compliance
IT: Industrial Control Systems	University Building Official
IT: Third-Party Access to University Data	University Registrar
Maintenance Reserve	University Scholarships and Financial Aid*
Office of the University Bursar	<i>* Entity receives an annual audit on different components of their operation</i>

# POLICY COMPLIANCE AUDITS

OARC will continue its program of limited scope reviews of senior management areas. These surveys review 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.

College of Agriculture and Life Sciences

Vice President and Dean for Graduate Education

Vice President for Student Affairs

# MANAGEMENT ADVISORY SERVICES

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.

School of Plant and Environmental Sciences

Youth Protection Activities

# ADDITIONAL AUDIT PROJECTS

With additional resources, the following projects would have been included for the fiscal year 2018-19 audit plan. Otherwise, these projects will be considered for inclusion on the fiscal year 2019-20 plan.

College of Natural Resources and Environment (Compliance Review)	Graduate Education
Contract Approval and Delegated Authority	IT: Windows Server Security
Eastern Shore AREC	Licensing and Trademarks
General Data Protection Regulation (GDPR) (Advisory Review)	Parking and Transportation

# QUESTIONS?

August 26, 2018

# *Future of ERM*

## *Steady State at Virginia Tech*

*Sharon M. Kurek, CPA, CFE, MBA*  
*Executive Director of Audit, Risk, and Compliance*



# AGENDA

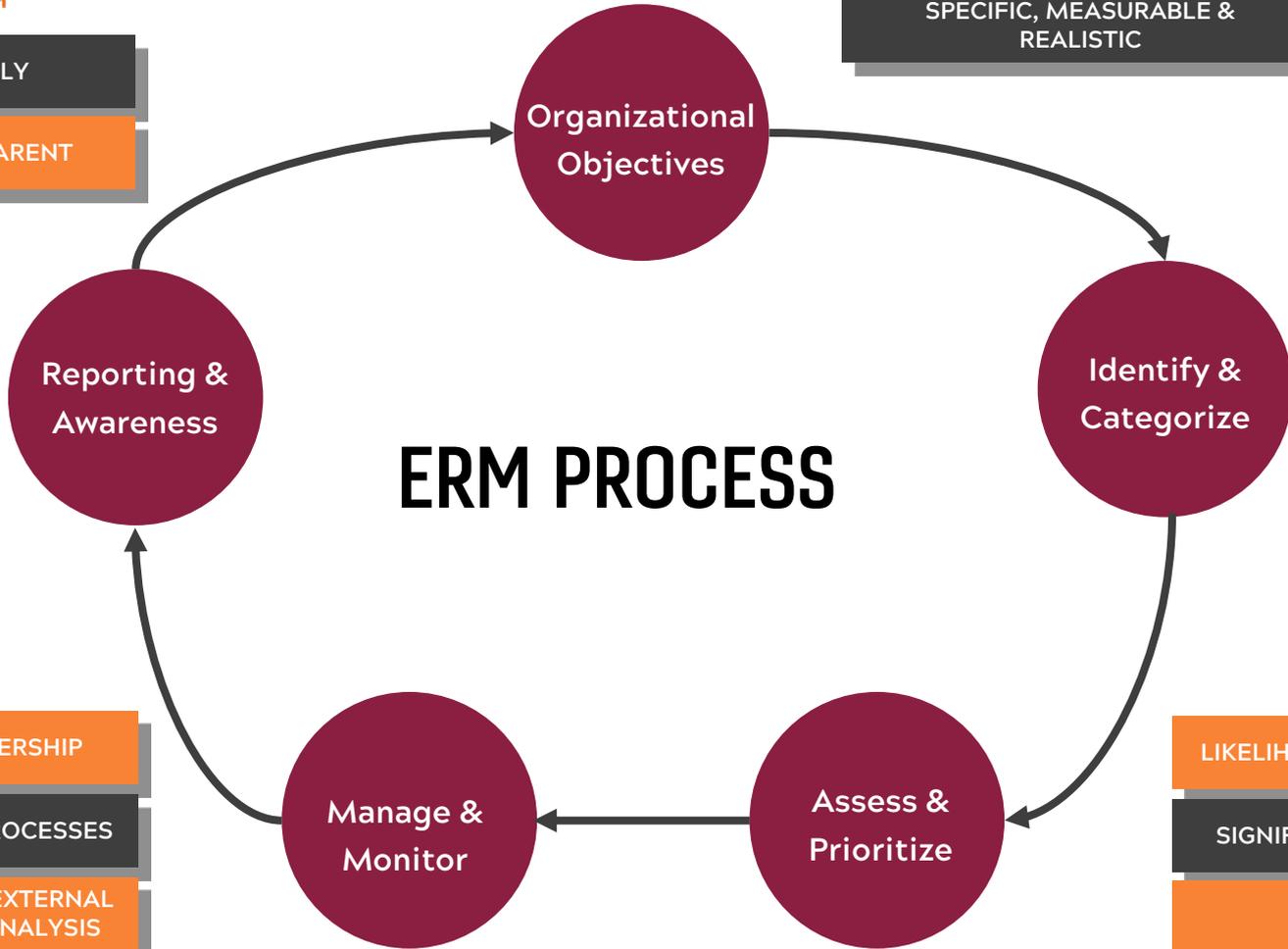
- 1. What has been achieved to date?*
- 2. What does a mature ERM program look like at Virginia Tech?*



TIMELY

TRANSPARENT

SPECIFIC, MEASURABLE & REALISTIC



# ERM PROCESS

STRATEGIC

FINANCIAL

COMPLIANCE

OPERATIONAL

REPUTATION

RISK OWNERSHIP

BUSINESS PROCESSES

INTERNAL / EXTERNAL REVIEW & ANALYSIS

LIKELIHOOD OF OCCURENCE

SIGNIFICANCE OF IMPACT

VELOCITY

# PLANS THROUGH 2020

- *Collection of Risk Snapshots from Risk Owners – Draft August & Final December*
  - *Refresh Risk Snapshots – Annually & As Needed starting 2019*
- *Tabletop Exercises – 4 times per year*
- *OARC Deep Dive of Risk Snapshots with Risk Owners – 3-5 per year (emphasis on top risks)*
- *President's Leadership Team ERM Discussions – Semi-Annually & As Needed*
- *Risk Owner Presentations to CAR Committee – Starting 2019*
- *Refresh Enterprise Risk Landscape & Heat Map - 2020*

# VISION FOR 2020 AND BEYOND

- *Periodic Reassessment of Overall Program - Continuous Improvement*
- *Refresh of Risk Snapshots - Annually & As-Needed*
- *Tabletop Exercises – 4 times per year*
- *OARC Deep Dive of Risk Snapshots with Risk Owners – 3-5 per year (emphasis on top risks)*
- *President's Leadership Team ERM Discussions – Semi-Annually & As Needed*
- *Risk Owner Presentations to CAR Committee – As Needed*
- *Refresh Enterprise Risk Landscape & Heat Map- Every 3 years after 2020*

## *Update since June*

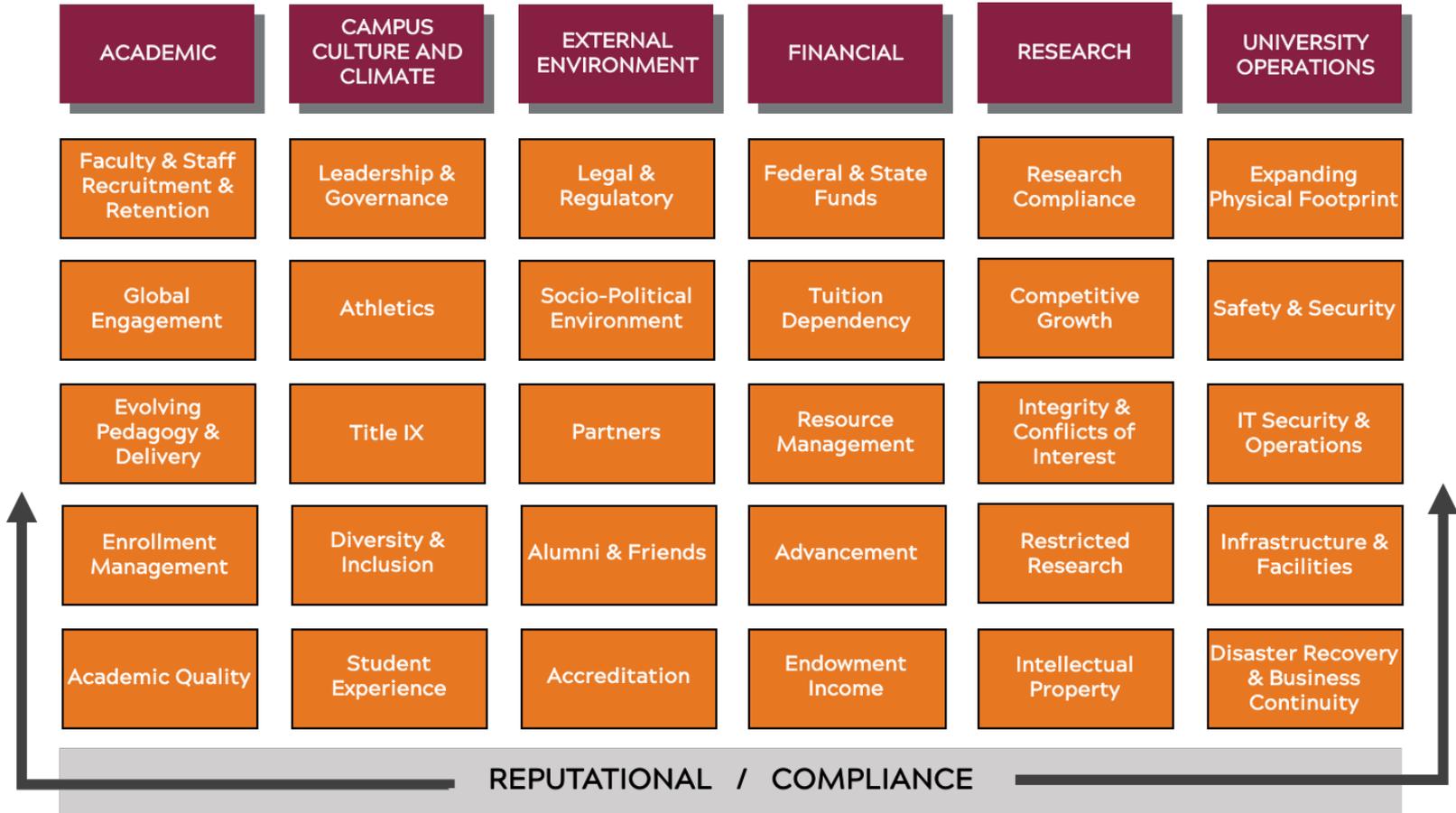
- *Assignment of Risk Ownership (see appendix in BOV Portal)*
- *Risk Owners are drafting Risk Snapshots that capture Risk Owner, Risk Statement, Sub-risks, Current Key Processes, Mitigation Action Plans, etc.*
- *President's Leadership Team and BOV participated in a Tabletop Exercise on budget reduction risk scenario*

## *Going Forward*

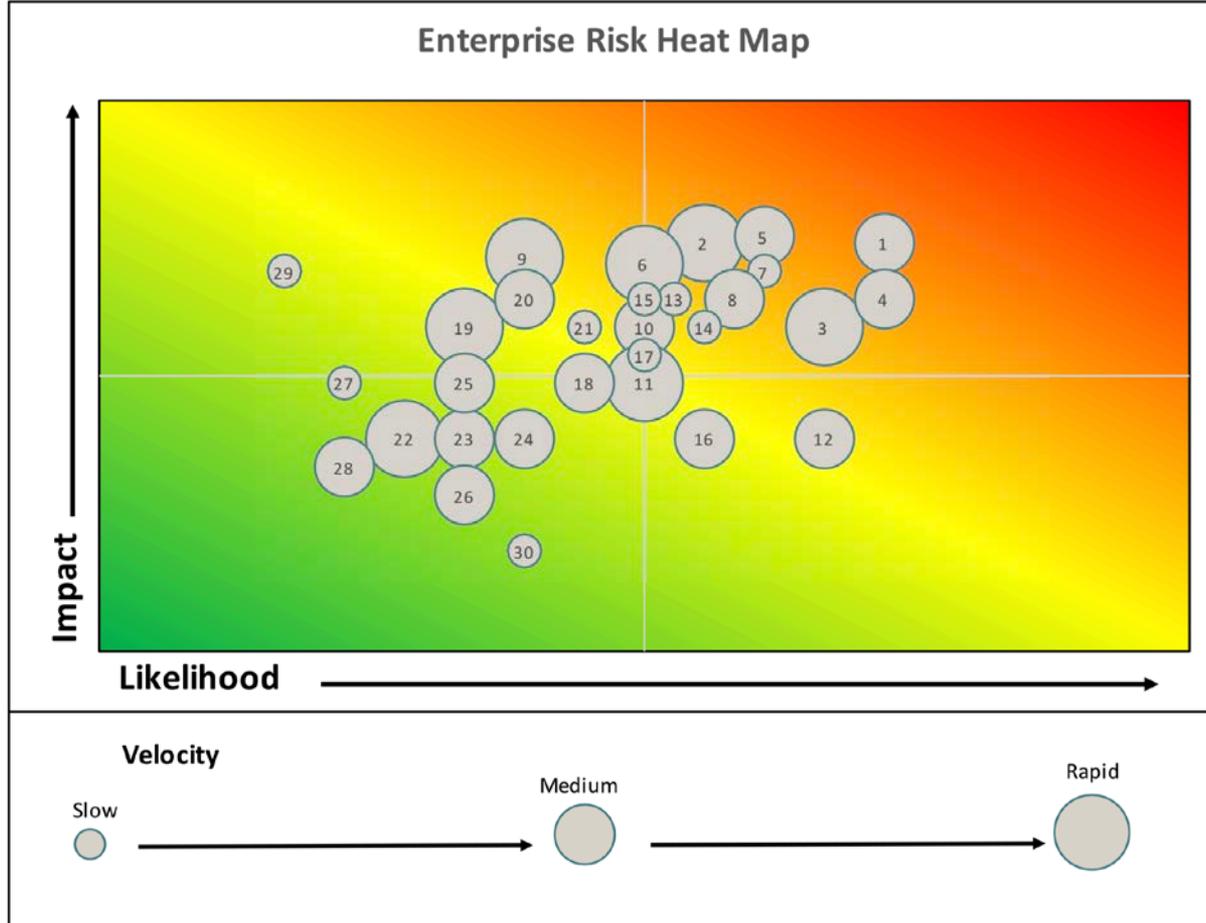
- *Finalize Risk Snapshots for each enterprise risk*
- *Periodic Tabletop Exercises*
- *Analysis of Current Processes*
- *Periodic Reporting to OARC and ERM Committees*
- *Risk Owners Periodically Brief BOV*
- *Refresh Enterprise Risk Landscape & Heat Map*

# QUESTIONS?

# Enterprise Risk Landscape



# Enterprise Risk Heat Map



## Graph Legend

Number	Risk
1	Federal & State Funds
2	Legal & Regulatory
3	Socio-Political Environment
4	Tuition Dependency
5	Leadership & Governance
6	Athletics
7	Expanding Physical Footprint
8	Faculty & Staff Recruitment & Retention
9	Safety & Security
10	Research Compliance
11	IT Security & Operations
12	Global Engagement
13	Resource Management
14	Competitive Growth
15	Advancement
16	Title IX
17	Infrastructure & Facilities
18	Partners
19	Integrity & Conflicts of Interest
20	Evolving Pedagogy & Delivery
21	Diversity & Inclusion
22	Disaster Recovery & Business Continuity
23	Enrollment Management
24	Restricted Research
25	Endowment Income
26	Student Experience
27	Academic Quality
28	Alumni & Friends
29	Accreditation
30	Intellectual Property

# ERM Risk Owners

ACADEMIC		
Risk Category	Risk Owner	Name
Faculty & Staff Recruitment	VP HR	Lisa Wilkes
	Provost	Cyril Clarke
	Vice Provost	Jack Finney
Global Engagement	Provost	Cyril Clarke
	VP OIA	Guru Ghosh
Evolving Pedagogy & Delivery	Provost	Cyril Clarke
	Vice Provost	Don Taylor
	Vice Provost	Rachel Holloway
Enrollment Management	Provost	Cyril Clarke
	Vice Provost	Luisa Havens Gerardo
Academic Quality	Provost	Cyril Clarke
	Vice Provost	Rachel Holloway
	VP Grad. Educ.	Karen DePauw

CAMPUS CULTURE AND CLIMATE		
Risk Category	Risk Owner	Name
Leadership & Governance	President	Tim Sands
Athletics	Athletics Director	Whit Babcock
Title IX	VP HR	Lisa Wilkes
Diversity & Inclusion	Provost	Cyril Clarke
	Vice Provost	Menah Pratt-Clarke
Student Experience	Provost	Cyril Clarke
	VP Student Affairs	Patty Perillo

EXTERNAL ENVIRONMENT		
Risk Category	Risk Owner	Name
Legal and Regulatory	Legal Counsel	Kay Heidbreder
Socio-Political Environment	President	Tim Sands
Partners	VPRI	Theresa Mayer
	Provost	Cyril Clarke
Alumni & Friends	VP Advancement	Charlie Phlegar
Accreditation	Provost	Cyril Clarke
	Vice Provost	Don Taylor

# ERM Risk Owners

FINANCIAL		
Risk Category	Risk Owner	Name
Federal & State Funds	SVPOA VPF & CFO Exec. Dir.	Dwayne Pinkney Dwight Shelton Chris Yianilos
Tuition Dependency	SVPOA VPF & CFO Provost	Dwayne Pinkney Dwight Shelton Cyril Clarke
Resource Management	SVPOA VPF & CFO Provost	Dwayne Pinkney Dwight Shelton Cyril Clarke
Advancement	VP Advancement	Charlie Phlegar
Endowment Income	VPF & CFO	Dwight Shelton

RESEARCH		
Risk Category	Risk Owner	Name
Research Compliance	VPRI	Theresa Mayer
Competitive Growth	VPRI Provost	Theresa Mayer Cyril Clarke
Integrity & Conflicts of Interest	VPRI	Theresa Mayer
Restricted Research	VPRI	Theresa Mayer
Intellectual Property	VPRI	Theresa Mayer

OPERATIONS		
Risk Category	Risk Owner	Name
Expanding Physical Footprint	VPRI Provost SVPOA VP NCR VP HS&T	Theresa Mayer Cyril Clarke Dwayne Pinkney Steve McKnight Mike Friedlander
Safety and Security	SVPOA VP Operations	Dwayne Pinkney Sherwood Wilson
IT Security & Operations	VPIT & CIO	Scott Midkiff
Infrastructure and Facilities	SVPOA VP Operations VPIT & CIO	Dwayne Pinkney Sherwood Wilson Scott Midkiff
Disaster Recovery & Business Continuity	SVPOA VP Operations VPIT & CIO	Dwayne Pinkney Sherwood Wilson Scott Midkiff

# INSTITUTIONAL COMPLIANCE PROGRAM (ICP) UPDATE

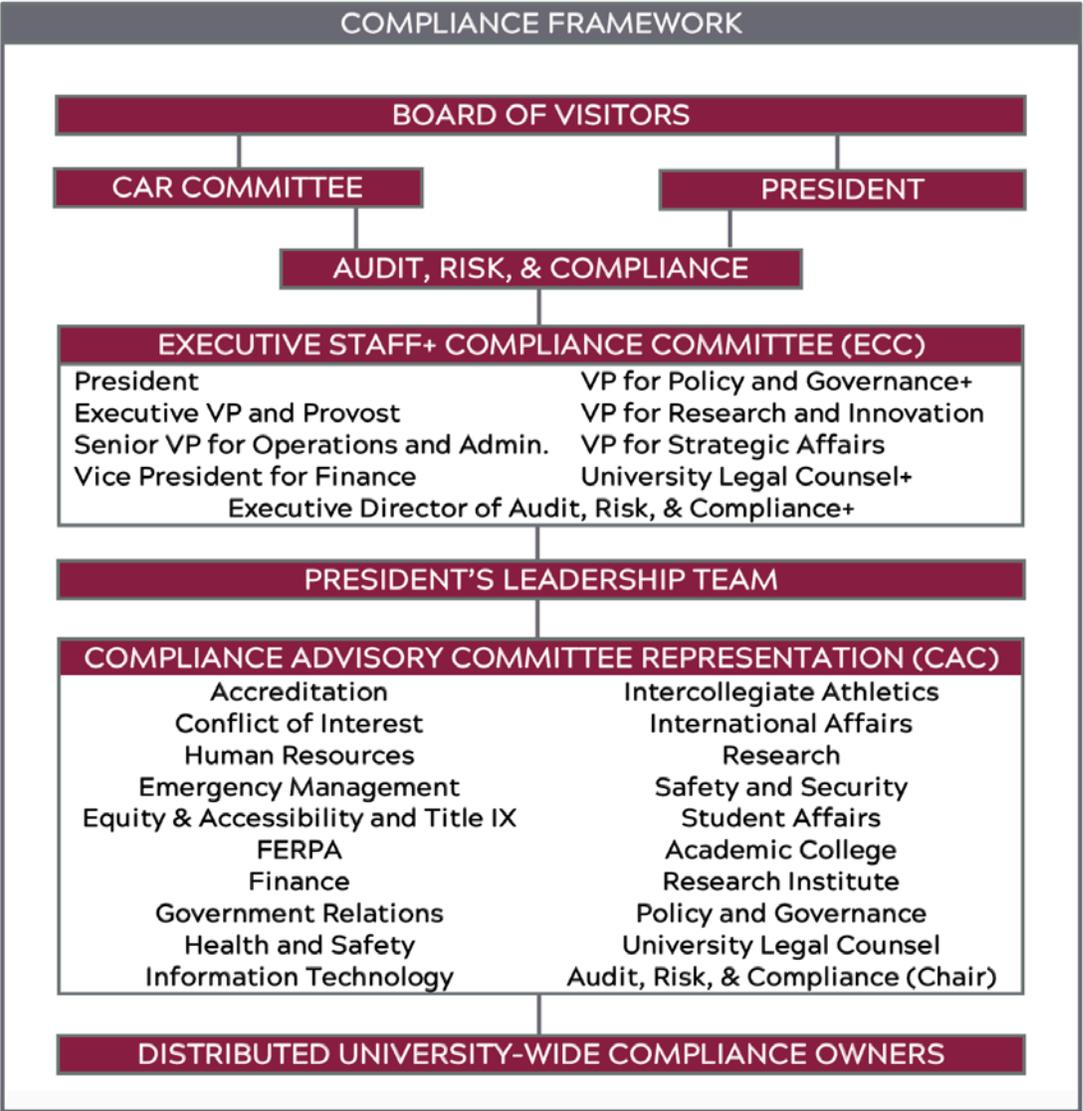
August 26, 2018

---

**Sharon Kurek**

*Executive Director of Audit, Risk, and Compliance*

# COMPLIANCE FRAMEWORK



## STATISTICS

- CAC - 20 Members
- 56 Distributed Compliance Owners
- 298 Regulations Initially Identified by OARC

# ICP SUMMARY

## *Update since June*

- *Establishment of Compliance Advisory Committee (CAC) Representation*
- *Initial CAC meeting held with more than 20 compliance owners and designees present to discuss the function and purpose of the committee*
- *Distributed database of compliance requirements to CAC members*

## *Going Forward*

- *Divide CAC into subgroups for analysis of database content for accuracy and completeness*
- *CAC members will provide input on future compliance risk assessment to be completed by 50+ compliance owners*
- *CAC will subsequently review results of university-wide compliance risk assessment*

# QUESTIONS?

# 8 ELEMENTS OF AN EFFECTIVE COMPLIANCE PROGRAM

High-level personnel exercising oversight

Written policies and procedures

Training and Education

Lines of Communication

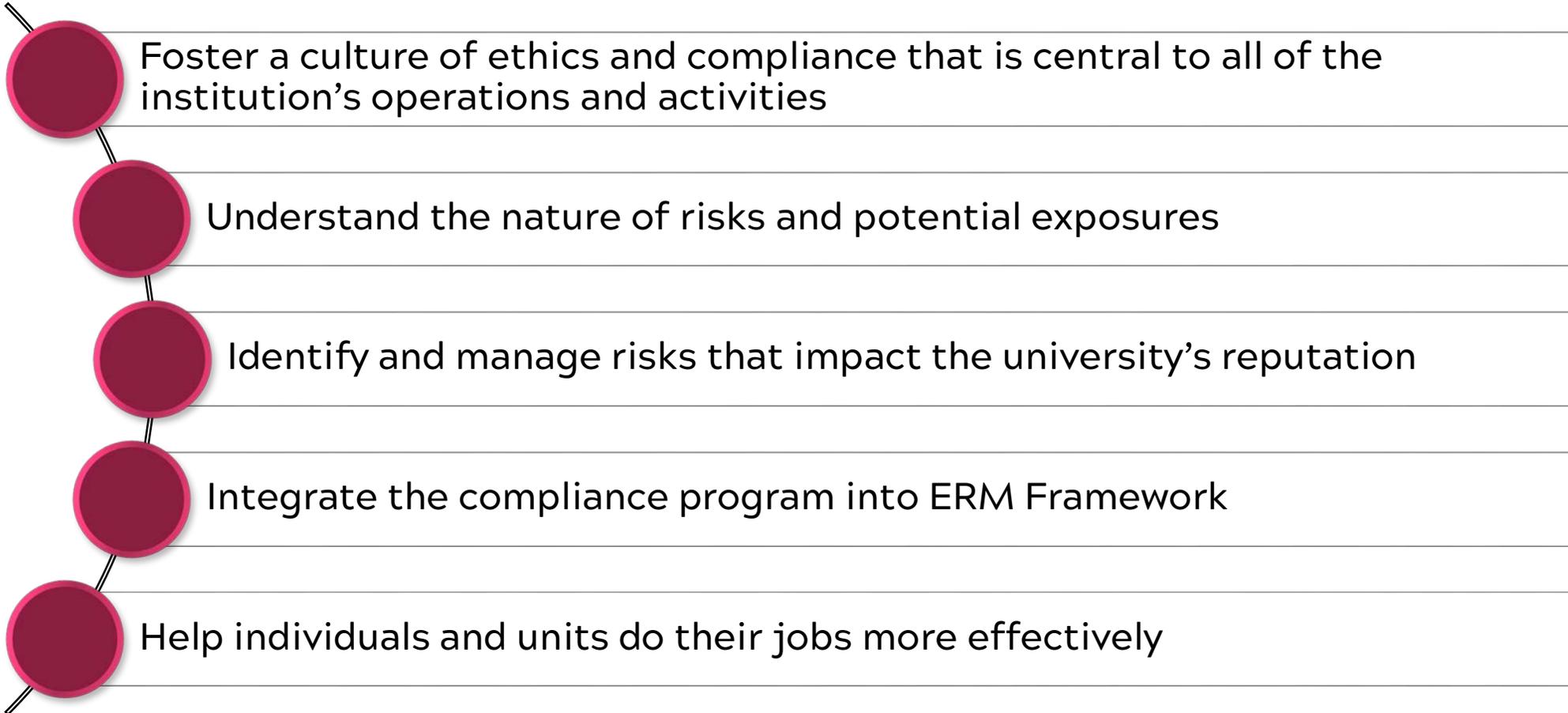
Well publicized disciplinary guidelines

Internal compliance monitoring

Response to detected offenses

Perform periodic compliance risk assessments

# COMPLIANCE PROGRAM BENEFITS: A Coordinated Effort

- 
- Foster a culture of ethics and compliance that is central to all of the institution's operations and activities
  - Understand the nature of risks and potential exposures
  - Identify and manage risks that impact the university's reputation
  - Integrate the compliance program into ERM Framework
  - Help individuals and units do their jobs more effectively

# Common Higher Education Compliance Areas

- Access/Disability Services
- Accreditation
- Athletics
- Conflicts of Interest
- Discrimination / Harassment
- Donors and Gifts
- Emergency Preparedness
- Environmental Health & Safety
- Export Control
- FERPA / Education Records
- Financial Aid
- Fiscal Management
- Global Operations
- HIPAA Privacy and Security
- Human / Animal Subjects
- Human Resources / Equal Opportunity
- Immigration
- Intellectual Property /Technology Licensing
- Research Administration
- Safety / Security
- Scientific Misconduct
- Tax Compliance