

Committee Minutes

COMPLIANCE, AUDIT, AND RISK COMMITTEE

The Inn at Virginia Tech

10:00 a.m.

November 17, 2019

Closed Session

Committee Members: Anna James (chair), Letitia Long, Sharon Brickhouse Martin, Dennis Treacy

Other Board Members: Greta Harris, Mehul Sanghani, Horacio Valeiras (rector), Preston White

VPI & SU Faculty and Staff: Cyril Clarke, Ryan Hamilton, Kay Heidbreder, Sharon Kurek, Justin Noble, Kim O'Rourke, Dwayne Pinkney, Timothy Sands

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. **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: Anna James (chair), Sharon Brickhouse Martin, Letitia Long, Dennis Treacy

Other Board Members: Edward Baine, Greta Harris, Charles C. T. Hill, Mehul Sanghani, Horacio Valeiras (rector), Preston White

Representatives to the Board: Ryan King, Tammie Smith, Madelynn Todd

VPI & SU Faculty and Staff: Charity Boyette, Ashley Campbell (student), Cyril Clarke, Al Cooper, Tiffany Cunningham, Jon Deskins, Kari Evans, Lance Franklin, Ryan Hamilton, Kay Heidbreder, Sharon Kurek, Nancy Meacham, Scott Midkiff, Ken Miller, Justin Noble, Kim O'Rourke, Mark Owczarski, Patty Perillo, Dwayne Pinkney, Chris Rahmes, Jackson Ribler (student), Timothy Sands, Don Taylor, Tracy Vosburgh, Lisa Wilkes

Guests: DeeAnn Compton (APA), Meghan Finney (APA)

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 considered and approved the items listed on the Consent Agenda.
 - a. **Minutes for the August 25, 2019 Meeting:** The Committee reviewed and approved the minutes of the August 25, 2019 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 June 30, 2019, the university had five open recommendations. Eleven audit comments were issued during the fourth quarter of the fiscal year. As of September 30, 2019, the university had addressed two comments, leaving 14 open recommendations in progress.
 - c. **Audit Plan Status Report:** The committee reviewed the Audit Plan Status Report. The Office of Audit, Risk, and Compliance (OARC) has completed 9 percent of its audit plan, and 33 percent was underway, in accordance with the fiscal year 2019-20 annual audit plan.
 - d. **Internal Audit Reports:** The following internal audit reports were issued by the Office of Audit, Risk, and Compliance (OARC) since the August 25, 2019 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. **Research: Grant Management:** The audit received a rating of improvements are recommended. One observation was noted with respect to compliance with university requirements for the effort certification and submission process. Additionally, three low-priority recommendations of a less significant nature were noted and shared with management, with emphasis on enhancing financial monitoring, effort reporting, and training practices.
 - ii. **School of Public and International Affairs:** The audit received a rating of improvements are recommended. An observation was noted with respect to international travel. Additionally, a low-priority recommendation of a less significant nature was noted for management.
 - iii. **Vice President for Student Affairs Policy Compliance Review:** The audit received a rating of improvements are recommended. Audit recommendations were issued to management in the areas of fiscal responsibility, wage payroll, leave reporting, P-14 appointments, expenditures, and emergency preparedness. Additionally, an observation for central administration was made with respect to minimum annual vehicle mileage.
4. **Auditor of Public Accounts Financial Statement Audit and Management Letter:** The Committee received a report from Ms. Compton, Audit Director, Auditor of Public Accounts, on the status of the university's financial statement audit and management letter for the fiscal year ended June 30, 2019.
5. **Review and Approval of Audit Charters:** The Committee reviewed and approved the Compliance, Audit, and Risk Committee Charter and the Charter for the Office of Audit, Risk, and Compliance in accordance with professional standards. After conducting a thorough review, OARC recommended modifications to the charters reflecting the change in meeting frequency and minor technical corrections.
6. **Office of Audit, Risk, and Compliance's Quality Assurance and Improvement Program Periodic Self-Assessment:** The Committee reviewed and accepted the results of OARC's Quality Assurance and Improvement Program (QAIP) Periodic Self-Assessment. The objectives of the review were to

assess conformance with the Institute of Internal Auditors' (IIA) International Standards for the Professional Practice of Internal Auditing (Standards), evaluate the effectiveness of the university's internal audit function in carrying out its mission, and identify opportunities to improve its management and work processes. Results indicated that the internal audit function "generally conforms" with the IIA Standards, which is the highest rating.

The Standards require that internal audit functions implement a comprehensive Quality Assurance and Improvement Program. This program includes ongoing internal assessments, periodic self-assessments, and an independent external assessment that should be conducted at least every five years. The prescribed independent external assessment was last conducted in 2016 and is next due in 2021.

7. **ERM and IPC Program Updates:** The Committee received an update on the ERM and ICP programs. An update to the enterprise risk landscape and heat map was shared with the committee along with the timeline for next iteration of the ERM process. ICP developments with the university-wide compliance matrix and associated risk assessments, as well as the new anonymous fraud, waste, and abuse reporting hotline were also shared with the committee.
8. **Discussion of Future Topics:** The Committee briefly discussed topics to be covered in future committee meetings.

There being no further business, the meeting adjourned at 11:59 a.m.

COMPLIANCE, AUDIT, AND RISK COMMITTEE**September 30, 2019**

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 August 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 2020 reflects closing 2 of 2 recommendations by the original target date.

The report presented at the August 25, 2019 meeting covered audit reports reviewed and accepted through June 30, 2019 and included five open medium and high priority recommendations. Activity for the quarter ended September 30, 2019 resulted in the following:

Open recommendations as of June 30, 2019	5
Add: medium and high priority recommendations accepted August 25, 2019	11
Subtract: recommendations addressed since June 30, 2019	2
Remaining open recommendations as of September 30, 2019	<u>14</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. Through September 27, 2019, OARC has not closed any of the fourteen outstanding medium and high priority recommendations. 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

September 30, 2019

Report Date	Audit Name	Audit Number	Total Recommendations						
			ISSUED	COMPLETED	OPEN				
					Extended		On-schedule		Total
					High	Medium	High	Medium	Open
14-Mar-19	University Building Official	19-1434	2	1				1	1
15-May-19	Hume Center	19-1429	1				1		1
15-May-19	Industrial Control Systems	19-1438	2					2	2
25-Aug-19	College of Liberal Arts & Human Sciences	18-1387	3				1	2	3
25-Aug-19	Office of the University Registrar	19-1432	1					1	1
25-Aug-19	Athletics	19-1435	5					5	5
25-Aug-19	Research: Subrecipient Monitoring	19-1442	1					1	1
Totals:			15	1	0	0	2	12	14

Open Audit Recommendations

COMPLIANCE, AUDIT, AND RISK COMMITTEE

September 30, 2019

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		
15-May-19	1	19-1429	Hume Center	Computer Security	High		29-Nov-19		1	
25-Aug-19	2	19-1432	Office of the University Registrar	FERPA Training	Medium		31-Oct-19		1	
25-Aug-19	3	19-1435	Athletics	Drug-Testing Consent Form	Medium		15-Dec-19		1	
25-Aug-19	4	19-1435	Athletics	Concussion Consent Form	Medium		15-Dec-19		1	
8/25819	5	19-1435	Athletics	Equipment Room Inventory Management	Medium		15-Dec-19		1	
25-Aug-19	6	19-1435	Athletics	Equipment Room P-Card Sharing	Medium		15-Dec-19		1	
25-Aug-19	7	19-1435	Athletics	Drug-Testing Reconciliation	Medium		15-Dec-19		1	
14-Mar-19	8	19-1434	University Building Official	Monitoring Permit Expiration	Medium		31-Dec-19		1	
15-May-19	9	19-1438	Industrial Control Systems	Documentation of Policies and Procedures	Medium		31-Dec-19		1	
15-May-19	10	19-1438	Industrial Control Systems	Access Security Controls	Medium		31-Dec-19		1	
25-Aug-19	11	19-1442	Research:Subrecipient Monitoring	Subrecipient Risk Assessment	Medium		31-Mar-20		2	
25-Aug-19	12	18-1387	College of Liberal Arts & Human Sciences	Fiscal Responsibility	Medium		30-Apr-20		2	
25-Aug-19	13	18-1387	College of Liberal Arts & Human Sciences	Funds Handling	Medium		30-Apr-20		2	
25-Aug-19	14	18-1387	College of Liberal Arts & Human Sciences	Information Technology	High		31-Dec-20		2	

Follow Up Status

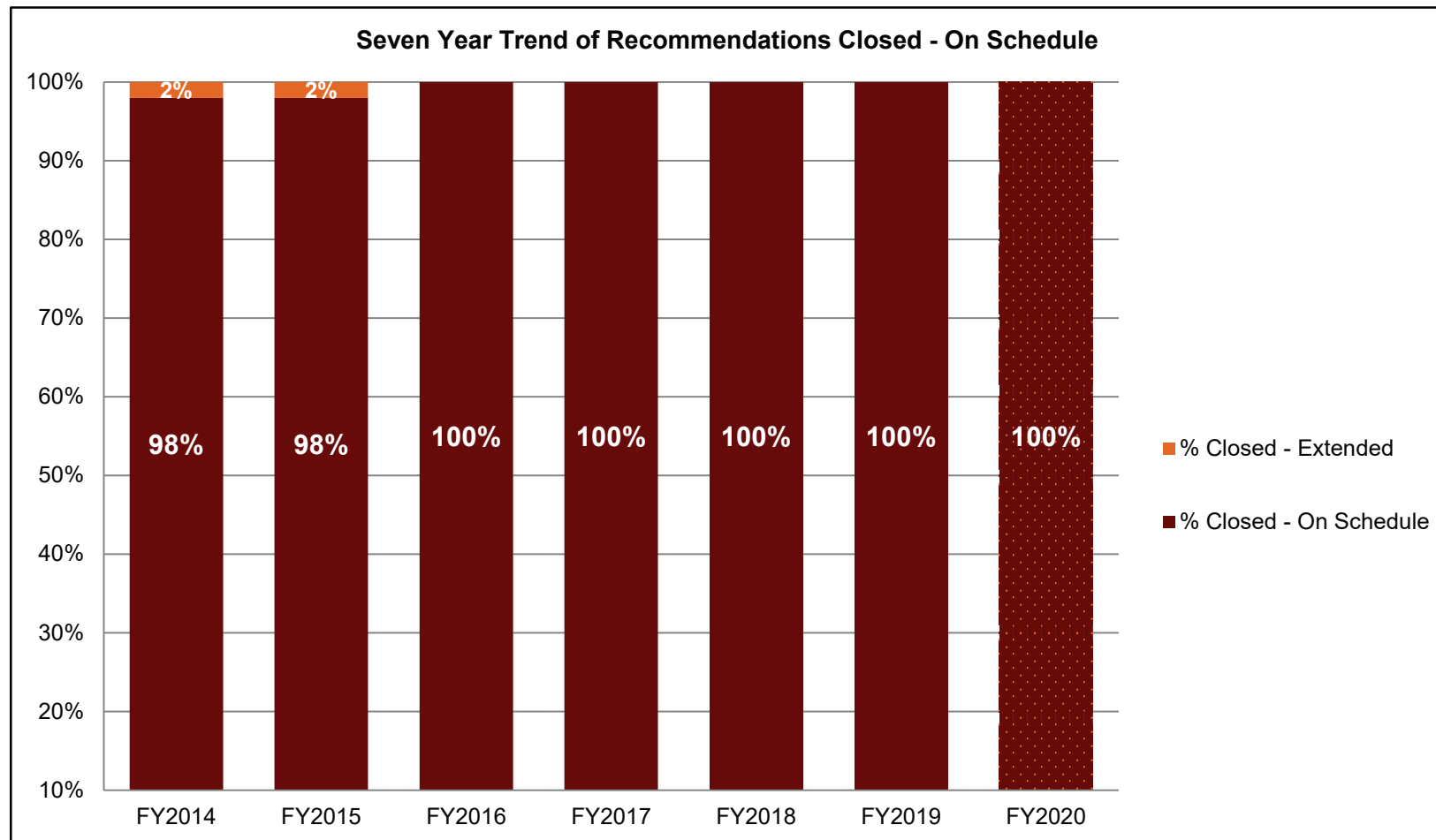
- 1 As of September 27, 2019, management confirmed during follow up discussions with the Office of Audit, Risk, and Compliance (OARC) that actions are occurring and the target date will be met. OARC will conduct testing after the due date to confirm that the Management Action Plan is implemented in accordance 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.

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

COMPLIANCE, AUDIT, AND RISK COMMITTEE

September 30, 2019



Audit Plan Status Report

COMPLIANCE, AUDIT, AND RISK COMMITTEE

November 17, 2019

Audit Plan Update

Audits were performed in accordance with the fiscal year 2019-20 annual audit plan at a level consistent with the resources of the Office of Audit, Risk, and Compliance (OARC). Two risk-based audits and one policy compliance review have been completed since the August board meeting.

The following eight audit projects are underway: Chemical Engineering, Graduate Education, HR: Payroll, IT: Log Management, Physical Security, University Scholarships and Financial Aid, VCE – Northern District, and the policy compliance review for the Vice President for Information Technology. Additionally, an advisory service project related to the research institutes is ongoing.

The policy compliance review for the Vice President for Diversity, Inclusion, and Strategic Affairs project has been deferred to the fiscal year 2020-21 audit plan as part of the President and Provost reviews.

So far in fiscal year 2019-20, OARC has completed 9% percent of its audit plan as depicted in Exhibit 1.

Exhibit 1 FY 2019-20 Completion of Audit Plan

Audits	
Total # of Audits Planned	31
Total # of Supplemental Audits	0
Total # of Carry Forwards	3
Total # of Planned Audits Canceled and/or Deferred	1
Total Audits in Plan as Amended	33
Total Audits Completed	3
Audits - Percentage Complete	9%
Audits - Percentage Complete or Underway	33%
Note: Includes Policy Compliance Reviews and Advisory Services	

Internal Audit Reports
COMPLIANCE, AUDIT, AND RISK COMMITTEE

November 17, 2019

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.

Consent Agenda Reports	Rating
Research: Grant Management	Improvements are Recommended
School of Public and International Affairs	Improvements are Recommended
Vice President for Student Affairs Policy Compliance Review	Improvements are Recommended

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.

November 17, 2019

Auditor of Public Accounts Financial Statement Audit and Management Letter
COMPLIANCE, AUDIT, AND RISK COMMITTEE

November 17, 2019

The Committee will receive an update on the status of
the Auditor of Public Accounts financial statement audit
and Management Letter
for the fiscal year ended June 30, 2019.

**VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
COMPLIANCE, AUDIT, AND RISK COMMITTEE OF THE BOARD OF VISITORS**

COMPLIANCE, AUDIT, AND RISK CHARTER

I. PURPOSE

The primary purpose of the Compliance, Audit, and Risk (CAR) Committee is to assist the Board of Visitors in fulfilling its fiduciary responsibilities related to oversight of:

- The university's enterprise risk management program, as an essential part of a strong control environment, to ensure that risk appetite aligns with management's decisions and strategy;
- Adherence to this charter, including reviewing audits conducted by the Office of Audit, Risk, and Compliance and external bodies and providing guidance on auditing concerns to the full Board;
- The university's compliance with all federal, state, and local laws and executive orders and policies promulgated by academic and athletic accrediting bodies, regulatory agencies, funding agencies, and the State Council of Higher Education for Virginia;
- The maintenance of effective systems of internal control, including the integrity of the university's financial accounting and reporting practices; and
- The performance of the university's internal and independent audit functions.

The function of the Committee is oversight. University management is responsible for the preparation, presentation, and integrity of the university's financial statements, fiscal plans, and other financial reporting. University management is also responsible for maintaining appropriate financial accounting and reporting policies, procedures, and controls designed to assure compliance with generally accepted accounting principles and applicable laws and regulations. The Office of Audit, Risk, and Compliance examines and evaluates the adequacy and effectiveness of the university's internal control systems. The university's external auditor, the state Auditor of Public Accounts, is responsible for planning and conducting the financial statement examination in accordance with generally accepted government auditing standards.

This document and the related meeting planner are intended to identify and document the Committee's oversight responsibilities in order that such sound practices will continue despite the turnover of Committee members. It also outlines the regularly scheduled review activities that will ensure that the university continues to have an independent and objective internal audit function and obtains the greatest possible benefit from its external audits.

II. MEETINGS

By statute, the Board of Visitors, including the CAR Committee, must meet once a year, but traditionally holds four meetings a year. Additional meetings may occur more frequently as circumstances warrant. The Committee Chair should discuss the agenda with the

Executive Director of Audit, Risk, and Compliance prior to each Committee meeting to finalize the meeting agenda and review the items to be discussed.

III. RESPONSIBILITIES

In performing its audit oversight responsibilities, the CAR Committee shall:

A. General

1. Adopt a formal written charter that specifies the Committee's responsibilities and practices. The charter should be reviewed annually and updated as necessary.
2. Maintain minutes of meetings.
3. Authorize audits within the Committee's scope of responsibilities.
4. Report Committee actions to the Board of Visitors with such recommendations as the Committee may deem appropriate.
5. Meet in closed session, consistent with state law, (without members of senior management present, when appropriate) with the external auditors and/or the Executive Director of Audit, Risk, and Compliance to discuss matters that the Committee or the auditors believe should be discussed privately. The Executive Director of Audit, Risk, and Compliance shall have a regularly scheduled opportunity to meet privately with the Committee at each of its four annual meetings.

B. Risk Management and Internal Control

1. Review the university's enterprise risk management (ERM) efforts including the program structure and the processes for assessing significant risk exposures and the steps management has taken to monitor and control such exposures, as well as the university's risk assessment and risk management policies.
2. Consider the effectiveness of the university's internal control systems, including those over information technology and financial reporting.
3. Understand the scope of internal and external audit reviews of internal control, and obtain reports on significant potential issues and recommendations, together with management's responses.
4. Review management's written responses to significant potential issues and recommendations of the auditors, including the timetable to correct the identified weaknesses in the internal control system.
5. Advise management that they are expected to provide a timely analysis of significant reporting issues and practices.

C. External Auditors

1. Make inquiries of management and the independent auditors regarding the scope of the external audit for the current year.
2. As necessary, discuss with the external auditors their processes for identifying and responding to key audit and internal control risks.

3. Review the coordination of internal and external audit procedures to promote an effective use of resources and ensure complete and efficient coverage of the university's risks.
4. Meet with external auditors at the completion of the financial statements audit to receive and discuss the audit report(s), and determine whether external auditors are satisfied with the disclosure and content of the financial statements, including the nature and extent of any significant changes in accounting principles.
5. Review the results and organizational response stemming from significant reviews by regulatory agencies or other external entities (non-financial statement audits).

D. Internal Auditors

1. Approve the charter for the Office of Audit, Risk, and Compliance. The charter should be reviewed annually and updated as necessary.
2. Review and approve the annual audit plan and any significant changes to the plan.
3. Review the effectiveness of the internal audit function, including staffing resources, financial budget, training, objectivity and reporting relationships.
4. Review completed audit reports and progress reports on executing the approved annual audit plan.
5. Review the results of the Office of Audit, Risk, and Compliance's Quality Assurance and Improvement Program (QAIP), including results of internal assessments (both ongoing and periodic) and external assessments conducted at least once every five years by a qualified, independent assessor or assessment team from outside the university.
6. Inquire of the Executive Director of Audit, Risk, and Compliance regarding any difficulties encountered in the course of the audits, including any restrictions on the scope of work or access to required information.
7. Review and concur in the appointment, replacement, reassignment, or dismissal of the Executive Director of Audit, Risk, and Compliance.
8. Evaluate the Executive Director of Audit, Risk, and Compliance's annual performance and make decisions regarding compensation.

E. Compliance, Ethics, and Business Conduct

1. Support leadership by promoting and supporting a university-wide culture of ethical and lawful conduct.
2. Require management to periodically report on procedures that provide assurance that the university's mission, values, and codes of conduct are properly communicated to all employees.
3. Review the programs and policies of the university designed by management to assure compliance with applicable laws and regulations and monitor the results of the compliance efforts.
4. Monitor the university's conflict of interest policies and related procedures.

The “CAR Agenda Meeting Planner” is an integral part of this document. If the Board of Visitors meets less frequently than anticipated, the Planner will be adjusted accordingly.

**Virginia Polytechnic Institute and State University
Compliance, Audit, and Risk Committee of the Board of Visitors
CAR Agenda Meeting Planner**

A=Annually; S=Scheduled BOV Meeting; AN=As Necessary	Frequency			Planned Timing			
	A	S	AN	Aug	Nov	Mar	Jun
A. General							
1. Review and update CAR Committee charter	X				X		
2. Approve and maintain minutes of previous meeting		X		X	X	X	X
3. Authorize audits within the Committee’s scope of responsibilities			X				
4. Report Committee actions to the Board of Visitors with recommendations deemed appropriate		X			X	X	X
5. Meet in closed session with Executive Director of Audit, Risk, and Compliance, and with external auditors, as needed		X		X	X	X	X
B. Risk Management and Internal Control							
1. Review the university’s ERM efforts including the program structure, processes, risk assessment, and risk management policies		X			X	X	X
2. Consider the effectiveness of the university’s internal control systems			X				
3. Understand the scope of internal and external audit reviews of internal control, and obtain reports on significant potential issues and recommendations, together with management’s responses		X			X	X	X
4. Review management’s written responses to significant potential issues and recommendations of the auditors, including the timetable to correct identified weaknesses in the internal control system		X			X	X	X
5. Advise management that they are expected to provide a timely analysis of significant current reporting issues and practices	X				X		
C. External Auditors							
1. Make inquiries of management and the independent auditors regarding the scope of the external audit for the current year	X						X
2. Discuss with the external auditors their processes for identifying and responding to key audit and internal control risks			X		X		
3. Review the coordination of internal and external audit procedures to promote an effective use of resources and ensure complete and efficient coverage of the university’s risks			X				

A=Annually; S=Scheduled BOV Meeting; AN=As Necessary	Frequency			Planned Timing			
	A	S	AN	Aug	Nov	Mar	Jun
4. Meet with external auditors at the completion of the financial statements audit to receive and discuss the audit report(s)	X				X		
5. Review results of other significant reviews from regulatory agencies or other external entities			X				
D. Internal Auditors							
1. Review and approve the charter for the Office of Audit, Risk, and Compliance, if changes are needed	X				X		
2. Approve the annual audit plan	X						X
3. Review the effectiveness of the internal audit function, including staffing resources, financial budget, training, objectivity, and reporting relationships	X				X		
4. Review the results of the QAIP, including internal and external assessments			X				
5. Review completed audit reports and progress reports on executing the approved annual audit plan		X			X	X	X
6. Inquire of the Executive Director of Audit, Risk, and Compliance regarding any difficulties encountered in the course of the audits, including any restrictions on the scope of work or access to required information		X		X	X	X	X
7. Review and concur in the appointment, replacement, reassignment, or dismissal of the Executive Director of Audit, Risk, and Compliance			X				
8. Evaluate the Executive Director of Audit, Risk, and Compliance's annual performance and make decisions regarding compensation	X						X
E. Compliance, Ethics, and Business Conduct							
1. Convey commitment to ethical conduct through periodic receipt of management reports on how the university's mission, values, and codes of conduct are properly communicated to all employees			X				
2. Review the programs and policies of the university designed to assure and monitor compliance		X			X	X	X
3. Monitor the university's conflict of interest policies and related procedures		X		X	X	X	X

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY COMPLIANCE, AUDIT, AND RISK COMMITTEE OF THE BOARD OF VISITORS

COMPLIANCE, AUDIT, AND RISK CHARTER

I. PURPOSE

The primary purpose of the Compliance, Audit, and Risk (CAR) Committee is to assist the Board of Visitors in fulfilling its fiduciary responsibilities related to oversight of:

- The university's enterprise risk management program, as an essential part of a strong control environment, to ensure that risk appetite aligns with management's decisions and strategy¹.
- Adherence to this charter, including reviewing audits conducted by the Office of Audit, Risk, and Compliance and external bodies and providing guidance on auditing concerns to the full Board¹.
- The university's compliance with all federal, state, and local laws and executive orders¹; and policies promulgated by academic and athletic accrediting bodies, regulatory agencies, funding agencies, and the State Council of Higher Education for Virginia¹.
- The maintenance of effective systems of internal control, including the integrity of the university's financial accounting and reporting practices¹; and
- The performance of the university's internal and independent audit functions.

The function of the Committee is oversight. University management is responsible for the preparation, presentation, and integrity of the university's financial statements, fiscal plans, and other financial reporting. University management is also responsible for maintaining appropriate financial accounting and reporting policies, procedures, and controls designed to assure compliance with generally accepted accounting principles and applicable laws and regulations. The Office of Audit, Risk, and Compliance examines and evaluates the adequacy and effectiveness of the university's internal control systems. The university's external auditor, the state Auditor of Public Accounts, is responsible for planning and conducting the financial statement examination in accordance with generally accepted government auditing standards.

This document and the related meeting planner are intended to identify and document the Committee's oversight responsibilities in order that such sound practices will continue despite the turnover of Committee members. It also outlines the regularly scheduled review activities that will ensure that the university continues to have an independent and objective internal audit function and obtains the greatest possible benefit from its external audits.

II. MEETINGS

By statute¹, the Board of Visitors, including the CAR Committee, must meet once a year, but traditionally holds four meetings a year. Additional meetings may occur more frequently as circumstances warrant. The Committee Chair should discuss the agenda with the

Executive Director of Audit, Risk, and Compliance prior to each Committee meeting to finalize the meeting agenda and review the items to be discussed.

III. RESPONSIBILITIES

In performing its audit oversight responsibilities, the CAR Committee shall:

A. General

1. Adopt a formal written charter that specifies the Committee's responsibilities and practices. The charter should be reviewed annually and updated as necessary.
2. Maintain minutes of meetings.
3. Authorize audits within the Committee's scope of responsibilities.
4. Report Committee actions to the Board of Visitors with such recommendations as the Committee may deem appropriate.
5. Meet in closed session, consistent with state law, (without members of senior management present, when appropriate) with the external auditors and/or the Executive Director of Audit, Risk, and Compliance to discuss matters that the Committee or the auditors believe should be discussed privately. The Executive Director of Audit, Risk, and Compliance shall have a regularly scheduled opportunity to meet privately with the Committee at each of its four annual meetings.

B. Risk Management and Internal Control

1. Review the university's enterprise risk management (ERM) efforts including the program structure and the processes for assessing significant risk exposures and the steps management has taken to monitor and control such exposures, as well as the university's risk assessment and risk management policies.
2. Consider the effectiveness of the university's internal control systems, including those over information technology and financial reporting.
3. Understand the scope of internal and external audit reviews of internal control, and obtain reports on significant potential issues and recommendations, together with management's responses.
4. Review management's written responses to significant potential issues and recommendations of the auditors, including the timetable to correct the identified weaknesses in the internal control system.
5. Advise management that they are expected to provide a timely analysis of significant reporting issues and practices.

C. External Auditors

1. Make inquiries of management and the independent auditors regarding the scope of the external audit for the current year.
2. As necessary, discuss with the external auditors their processes for identifying and responding to key audit and internal control risks.

3. Review the coordination of internal and external audit procedures to promote an effective use of resources and ensure complete and efficient coverage of the university's risks.
4. Meet with external auditors at the completion of the financial statements audit to receive and discuss the audit report(s), and determine whether external auditors are satisfied with the disclosure and content of the financial statements, including the nature and extent of any significant changes in accounting principles.
5. Review the results and organizational response stemming from significant reviews by regulatory agencies or other external entities (non-financial statement audits).

D. Internal Auditors

1. Approve the charter for the Office of Audit, Risk, and Compliance. The charter should be reviewed annually and updated as necessary.
2. Review and approve the annual audit plan and any significant changes to the plan.
3. Review the effectiveness of the internal audit function, including staffing resources, financial budget, training, objectivity and reporting relationships.
4. Review completed audit reports and progress reports on executing the approved annual audit plan.
5. Review the results of the Office of Audit, Risk, and Compliance's Quality Assurance and Improvement Program (QAIP), including results of internal assessments (both ongoing and periodic) and external assessments conducted at least once every five years by a qualified, independent assessor or assessment team from outside the university.
6. Inquire of the Executive Director of Audit, Risk, and Compliance regarding any difficulties encountered in the course of the audits, including any restrictions on the scope of work or access to required information.
7. Review and concur in the appointment, replacement, reassignment, or dismissal of the Executive Director of Audit, Risk, and Compliance.
8. Evaluate the Executive Director of Audit, Risk, and Compliance's annual performance and make decisions regarding compensation.

E. Compliance, Ethics, and Business Conduct

1. Support leadership by promoting and supporting a university-wide culture of ethical and lawful conduct.
2. Require management to periodically report on procedures that provide assurance that the university's mission, values, and codes of conduct are properly communicated to all employees.
3. Review the programs and policies of the university designed by management to assure compliance with applicable laws and regulations and monitor the results of the compliance efforts.
4. Monitor the university's conflict of interest policies and related procedures.

The “CAR Agenda Meeting Planner” is an integral part of this document. If the Board of Visitors meets less frequently than anticipated, the Planner will be adjusted accordingly.

**Virginia Polytechnic Institute and State University
Compliance, Audit, and Risk Committee of the Board of Visitors
CAR Agenda Meeting Planner**

A=Annually; QS=Scheduled BOV Meeting=Quarterly ; AN=As Necessary Q1, Q2, Q3, Q4 based on Fiscal Year (July – June)	Frequency			Planned Timing			
	A	QS	AN	Aug Q1	Nov Q2	Mar Q3	Jun Q4
				Aug	Nov	Mar	Jun
A. General							
1. Review and update CAR Committee charter	X				X		
2. Approve and maintain minutes of previous meeting		X		X	X	X	X
3. Authorize audits within the Committee’s scope of responsibilities			X				
4. Report Committee actions to the Board of Visitors with recommendations deemed appropriate		X		X	X	X	X
5. Meet in closed session with Executive Director of Audit, Risk, and Compliance, and with external auditors, as needed		X		X	X	X	X
B. Risk Management and Internal Control							
1. Review the university’s ERM efforts including the program structure, processes, risk assessment, and risk management policies		X		X	X	X	X
2. Consider the effectiveness of the university’s internal control systems			X				
3. Understand the scope of internal and external audit reviews of internal control, and obtain reports on significant potential issues and recommendations, together with management’s responses		X		X	X	X	X
4. Review management’s written responses to significant potential issues and recommendations of the auditors, including the timetable to correct identified weaknesses in the internal control system		X		X	X	X	X
5. Advise management that they are expected to provide a timely analysis of significant current reporting issues and practices	X				X		
C. External Auditors							
1. Make inquiries of management and the independent auditors regarding the scope of the external audit for the current year	X						X
2. Discuss with the external auditors their processes for identifying and responding to key audit and internal control risks			X		X	X	

A=Annually; <u>QS=Scheduled BOV Meeting=Quarterly</u> ; <u>AN=As Necessary</u> <u>Q1, Q2, Q3, Q4 based on Fiscal Year (July—June)</u>	Frequency			Planned Timing			
	A	<u>QS</u>	AN	<u>Aug Q1</u>	<u>Nov Q2</u>	<u>Mar Q3</u>	<u>Jun Q4</u>
3. Review the coordination of internal and external audit procedures to promote an effective use of resources and ensure complete and efficient coverage of the university's risks			X	<u>X</u>		<u>X</u>	
4. Meet with external auditors at the completion of the financial statements audit to receive and discuss the audit report(s)	X				X		
5. Review results of other significant reviews from regulatory agencies or other external entities			X				
D. Internal Auditors							
1. Review and approve the charter for the Office of Audit, Risk, and Compliance, if changes are needed	X				X		
<u>2.</u> <u>Review the draft annual audit plan</u>	<u>X</u>						<u>X</u>
<u>3.2.</u> Approve the annual audit plan	X			<u>X</u>			<u>X</u>
<u>4.3.</u> Review the effectiveness of the internal audit function, including staffing resources, financial budget, training, objectivity, and reporting relationships	X			<u>X</u>	<u>X</u>		
<u>5.4.</u> Review the results of the QAIP, including internal and external assessments			X				
<u>6.5.</u> Review completed audit reports and progress reports on executing the approved annual audit plan		X		<u>X</u>	X	X	X
<u>7.6.</u> Inquire of the Executive Director of Audit, Risk, and Compliance regarding any difficulties encountered in the course of the audits, including any restrictions on the scope of work or access to required information		X		X	X	X	X
<u>8.7.</u> Review and concur in the appointment, replacement, reassignment, or dismissal of the Executive Director of Audit, Risk, and Compliance			X				
<u>9.8.</u> Evaluate the Executive Director of Audit, Risk, and Compliance's annual performance and make decisions regarding compensation	X			<u>X</u>			<u>X</u>
E. Compliance, Ethics, and Business Conduct							
1. Convey commitment to ethical conduct through periodic receipt of management reports on how the university's mission, values, and codes of conduct are properly communicated to all employees			X				
2. Review the programs and policies of the university designed to assure and monitor compliance		X		<u>X</u>	X	X	X
3. Monitor the university's conflict of interest policies and related procedures		X		X	X	X	X



Virginia Polytechnic Institute and State University

Charter for the Office of Audit, Risk, and Compliance

No. 3350

Policy Effective Date:
2/9/1989

Last Revision Date:
11/17/2019

Policy Owner:
President Sands

Policy Author:
(Contact Person)
Sharon Kurek

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

1.0 Purpose

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

2.0 Policy

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

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

1. *Audit:* Provide independent, objective assurance and advisory activity designed to add value and improve university operations. It helps the university accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
2. *Risk Management:* Provide oversight of the enterprise risk management (ERM) program by creating and maintaining the framework to identify, assess, and manage risk.
3. *Compliance:* Provide oversight of the institutional compliance program (ICP) and the distributed processes that support compliance across the university.

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

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

- Programs, plans, and strategic objectives are achieved.
- Risks are appropriately identified, managed, and considered in institutional decision making.
- Significant financial, managerial and operating information is accurate, reliable and timely.
- Compliance with policies, procedures, standards, laws, and regulations.
- Measures are taken to foster continuous improvement in control processes.
- Resources are acquired, managed, and protected in an economical, efficient, and effective manner.



Virginia Polytechnic Institute and State University

2.2 Independence and Objectivity

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

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

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

2.3 Authority

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

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

2.4 Auditing Standards

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

2.5 Systems Planning and Development

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

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

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



Virginia Polytechnic Institute and State University

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

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

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



Virginia Polytechnic Institute and State University

2.7 Audit Reports

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

2.8 Responsibility for Corrective Action

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

2.9 Coordination with External Auditing Agencies

The Executive Director of Audit, Risk, and Compliance will coordinate the department's audit efforts with those of the Auditor of Public Accounts or other external auditing agencies by participating in the planning and definition of the scope of proposed audits so the work of all auditing groups is complementary, and their combined efforts provide comprehensive, cost-effective audit coverage for the university. Duplication of work will be avoided as much as possible.

2.10 Special Projects

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

3.0 Procedures

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



Virginia Polytechnic Institute and State University

4.0 Definitions

Abuse

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

Add Value

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

Advisory Services

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

Assurance

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

Charter

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

Code of Ethics

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

Compliance

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

Conflict of Interest

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

Control

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



Virginia Polytechnic Institute and State University

Control Environment

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

Control Processes

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

Executive Director of Audit, Risk, and Compliance

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

Engagement

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

Enterprise Risk Management

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

Fraud

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

Governance

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

Independence

The freedom from conditions that threaten the ability of the internal audit function to carry out internal audit responsibilities in an unbiased manner.

Internal Audit Function

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



Virginia Polytechnic Institute and State University

International Professional Practices Framework

The conceptual framework that organizes the authoritative guidance promulgated by the Institute of Internal Auditors. Authoritative guidance is comprised of two categories: (1) mandatory and (2) strongly recommended.

Objectivity

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

Risk

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

Risk Management

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

Scope

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

Significance

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

Standards

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

Waste

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

5.0 References

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

State Fraud, Waste, and Abuse Hotline Policies and Procedures Manual, Office of the State Inspector General, Commonwealth of Virginia, 2018 edition.

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



Virginia Polytechnic Institute and State University

6.0 Approval and Revisions

- **Revision 0**
Approved February 9, 1989, by the Director of Internal Audit, David C. Goodyear.
- **Revision 1**
Annual review. Section 2.8 - changed so that reports "approved" by the Finance and Audit Committee of the Board of Visitors shall be available to the public.
Approved March 29, 1990, by the Director of Internal Audit, David C. Goodyear.
- **Revision 2**
Changes were made to eliminate minor discrepancies between the audit manual and the policy statement as presented to the Board of Visitors.
Approved November 3, 1995, by the Director of Internal Audit, David C. Goodyear.

Annual review, November 5, 1998, by Office of the Executive Vice President. No revisions.
- **Revision 3**
Policy updated to reflect review by the Finance and Audit Committee of the Board of Visitors. Policy serves as a charter for the Internal Audit Department.
Approved March 29, 2004 by the Executive Vice President and Chief Operating Officer, Minnis E. Ridenour.
Approved March 29, 2004 by the Finance and Audit Committee of the Board of Visitors.
- **Revision 4**
Policy updated to reflect review by the Finance and Audit Committee of the Board of Visitors, in conjunction with the Internal Audit Department's quality assurance review.
Approved March 14, 2005 by the Executive Vice President and Chief Operating Officer, James A. Hyatt.
Approved March 14, 2005 by the Finance and Audit Committee of the Board of Visitors.
- **Revision 5 April 1, 2008:**
Updates to position titles and/or responsibilities due to university reorganization.
- **Revision 6**
 - Policy title changed from "Internal Audit Department" to "Internal Audit Charter."
 - Section 2.2 revised to reflect change in Director of Internal Audit reporting relationship.
 - Sections 2.5 and 2.7 revised to clarify the role of Internal Audit and the standards under which it conducts its activities.
 - Section 2.9 revised to clarify the process for senior management areas submitting corrective action plans.

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



Virginia Polytechnic Institute and State University

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

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

- Revision 8

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

Approved November 5, 2017 by the Compliance, Audit, and Risk Committee of the Board of Visitors and President, Timothy D. Sands.

- Revision 9

Revisions from technical review correcting grammatical, punctuation, word usage, sentence structure, and minor content and/or format inconsistencies.

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



Virginia Polytechnic Institute and State University

Red = Insertions
Blue = Deletions

Charter for the Office of Audit, Risk, and Compliance

No. 3350

Policy Effective Date:
2/9/1989

Last Revision Date:
11/5~~17~~/201~~7~~2019

Policy Owner:
President Sands

Policy Author:
(Contact Person)
Sharon Kurek

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

1.0 Purpose

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

2.0 Policy

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

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

1. *Audit*: Provide independent, objective assurance and advisory activity designed to add value and improve university operations. It helps the university accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
2. *Risk Management*: Provide oversight of the enterprise risk management (ERM) program by creating and maintain~~ing~~ 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.

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

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

- Programs, plans, and strategic objectives are achieved.
- Risks are appropriately identified, managed, and considered in institutional decision making.
- Significant financial, managerial and operating information is accurate, reliable and timely.
- Compliance with policies, procedures, standards, laws, and regulations.
- Measures are taken to foster continuous improvement in control processes.
- Resources are ~~being~~ acquired, managed, and protected in an economical, efficient, and effective manner.



Virginia Polytechnic Institute and State University

2.2 Independence and Objectivity

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

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

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

2.3 Authority

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

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

2.4 Auditing Standards

The internal audit function will conduct its activities in accordance with the Institute of Internal Auditors' International Professional Practices Framework including the Core Principles for the Professional Practice of Internal Auditing, Code of Ethics, the International Standards for the Professional Practice of Internal Auditing, and the Definition of Internal Auditing. ~~Generally accepted auditing standards promulgated by the American Institute of Certified Public Accountants and government auditing standards issued by the United States Government Accountability Office will be referenced as appropriate.~~

2.5 Systems Planning and Development

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

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



Virginia Polytechnic Institute and State University

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

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

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

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



Virginia Polytechnic Institute and State University

or recovery and/or prosecution is the responsibility of the appropriate law enforcement agency ~~police departments~~ and Commonwealth's Attorney based on jurisdiction.

2.7 Audit Reports

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

2.8 Responsibility for Corrective Action

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

2.9 Coordination with External Auditing Agencies

The Executive Director of Audit, Risk, and Compliance will coordinate the department's audit efforts with those of the Auditor of Public Accounts or other external auditing agencies by participating in the planning and definition of the scope of proposed audits so the work of all auditing groups is complementary, and their combined efforts provide comprehensive, cost-effective audit coverage for the university. Duplication of work will be avoided as much as possible.

2.10 Special Projects

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

3.0 Procedures

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



Virginia Polytechnic Institute and State University

~~resource to external parties such as the Compliance, Audit, and Risk Committee of the Board of Visitors, senior management, external auditors, and quality assurance parties.~~

4.0 Definitions

Abuse

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

Add Value

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

Advisory Services

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

Assurance

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

Charter

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

Code of Ethics

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

Compliance

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

Conflict of Interest

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



Virginia Polytechnic Institute and State University

Control

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

Control Environment

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

Control Processes

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

Executive Director of Audit, Risk, and Compliance

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

Engagement

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

Enterprise Risk Management

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

Fraud

The intentional misrepresentation or concealment of information in order to deceive, mislead, or acquires something of value. Fraud is an intentional deception perpetrated to secure an unfair advantage ~~deception perpetrated by an individual or individuals, or an organization or organizations, either internal or external to the university, which could result in a tangible or intangible benefit to themselves, others, or the Commonwealth or could cause detriment to others or the Commonwealth. Fraud includes a false representation of a matter of fact, whether by words or by conduct, by false or misleading statements, or by concealment of that which should have been disclosed, which deceives and is intended to deceive.~~

Governance

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



Virginia Polytechnic Institute and State University

Independence

The freedom from conditions that threaten the ability of the internal audit function to carry out internal audit responsibilities in an unbiased manner.

Internal Audit Function

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

International Professional Practices Framework

The conceptual framework that organizes the authoritative guidance promulgated by the Institute of Internal Auditors. Authoritative guidance is comprised of two categories—(1) mandatory and (2) strongly recommended.

Objectivity

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

Risk

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

Risk Management

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

Scope

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

Significance

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

Standards

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

Waste

The ~~intentional or unintentional, thoughtless or~~ careless expenditure, consumption, mismanagement, use, or squandering of ~~Commonwealth-university resources to the detriment or potential detriment of the Commonwealth.~~ Waste also includes incurring unnecessary costs due to inefficient or ineffective practices, systems, or controls.



Virginia Polytechnic Institute and State University

5.0 References

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

State Fraud, Waste, and Abuse Hotline Policies and Procedures Manual, Office of the State Inspector General, Commonwealth of Virginia, [2014-2018](#) edition.

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

6.0 Approval and Revisions

- Revision 0
Approved February 9, 1989, by the Director of Internal Audit, David C. Goodyear.
- Revision 1
Annual review. Section 2.8 - changed so that reports "approved" by the Finance and Audit Committee of the Board of Visitors shall be available to the public.
Approved March 29, 1990, by the Director of Internal Audit, David C. Goodyear.
- Revision 2
Changes were made to eliminate minor discrepancies between the audit manual and the policy statement as presented to the Board of Visitors.
Approved November 3, 1995, by the Director of Internal Audit, David C. Goodyear.

Annual review, November 5, 1998, by Office of the Executive Vice President. No revisions.
- Revision 3
Policy updated to reflect review by the Finance and Audit Committee of the Board of Visitors. Policy serves as a charter for the Internal Audit Department.
Approved March 29, 2004 by the Executive Vice President and Chief Operating Officer, Minnis E. Ridenour.
Approved March 29, 2004 by the Finance and Audit Committee of the Board of Visitors.
- Revision 4
Policy updated to reflect review by the Finance and Audit Committee of the Board of Visitors, in conjunction with the Internal Audit Department's quality assurance review.
Approved March 14, 2005 by the Executive Vice President and Chief Operating Officer, James A. Hyatt.
Approved March 14, 2005 by the Finance and Audit Committee of the Board of Visitors.
- Revision 5 April 1, 2008:
Updates to position titles and/or responsibilities due to university reorganization.



Virginia Polytechnic Institute and State University

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

Approved November 7, 2011 by the university President, Charles W. Steger.

Approved November 7, 2011 by the Finance and Audit Committee of the Board of Visitors.

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

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

- Revision 8

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

Approved November 5, 2017 by the Compliance, Audit, and Risk Committee of the Board of Visitors and President, Timothy D. Sands.

- Revision 9

Revisions from technical review correcting grammatical, punctuation, word usage, sentence structure, and minor content and/or format inconsistencies.

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



Office of Audit, Risk, and Compliance
300 Turner Street NW
North End Center, Suite 3200
Blacksburg, Virginia 24061
P: 540-231-5883
www.audit.vt.edu

October 15, 2019

Sharon M. Kurek
Executive Director, Audit, Risk, and Compliance
North End Center
300 Turner Street NW, Suite 3200
Blacksburg, Virginia 24061

Ms. Kurek:

This memorandum is to report the outcome of the internal quality assurance review (QAR) conducted as part of the ongoing Quality Assurance and Improvement Program. The objectives of this QAR were to determine whether the Office of Audit, Risk, and Compliance (OARC) is in compliance with the International Professional Practices Framework (IPPF) promulgated by the Institute of Internal Auditors (IIA) and to assess the quality of ongoing performance and identify opportunities to improve OARC policies, procedures, and processes.

In my opinion, OARC **generally conforms** with the IIA Standards. The IIA's *Quality Assessment Manual for the Internal Audit Activity* provides a scale of three ratings, "Generally Conforms," "Partially Conforms," and "Does Not Conform." According to the manual, "Generally Conforms" is the highest rating and indicates that the relevant structure, policies, and procedures of the internal audit activity, as well as the processes by which they are applied, conform with the requirements of the Standards and the Code of Ethics in all material respects. In addition, OARC effectively executes its mission as set forth in the audit charter.

During the QAR, opportunities were identified to improve OARC policies, procedures, and processes. Those opportunities included: enhancing onboarding procedures, establishing procedures to track continuing professional education, enhancing ongoing monitoring activities, completing revisions of office policies and procedures, and instructing staff regarding audit documentation requirements.

I appreciate the courtesies extended during this review.

Sincerely,

A handwritten signature in blue ink that reads 'Ryan S. Hamilton'.

Ryan S. Hamilton
Audit Manager for Special Projects

cc: Anna H. James
Timothy D. Sands
Horacio A. Valeiras

Virginia Tech

Internal Quality Assurance Review

Quality Assurance and Improvement Program
October 15, 2019



OFFICE OF AUDIT, RISK,
AND COMPLIANCE
VIRGINIA TECH.

Engagement Overview

Objectives

The objectives of this internal quality assurance review (QAR) were to:

- ❖ Determine whether the Office of Audit, Risk, and Compliance (OARC) is in conformance with the International Professional Practices Framework (IPPF) promulgated by the Institute of Internal Auditors (IIA).
- ❖ Assess the quality of ongoing performance and identify opportunities to improve OARC policies, procedures, and processes.

Scope

The scope of this QAR included fiscal year 2017-18 and 2018-19 audit engagements completed as of February 26, 2019 and all OARC policies, procedures, and processes.

Methodology

This QAR was conducted using the IIA's *Quality Assurance and Improvement Program Practice Guide* (2012), as well as the *Quality Assessment Manual for the Internal Audit Activity* (2017) published by the Internal Audit Foundation.¹ To accomplish the objectives, the following activities were performed:

- ❖ Reviewed the mandatory elements of the IPPF (2017 edition), which comprises the Code of Ethics, the Core Principles for the Professional Practice of Internal Auditing, the Definition of Internal Auditing, and the International Standards for the Professional Practice of Internal Auditing (Standards).
- ❖ Reviewed previous internal and external quality assurance reports and actions taken in response to recommendations.
- ❖ Evaluated internal (audit staff) and external (auditee) survey results.
- ❖ Obtained and reviewed information provided by OARC relevant to this QAR, including audit charter, audit manual, organizational chart, risk assessments, audit plans, etc.
- ❖ Reviewed Board of Visitors (BOV) Compliance, Audit, and Risk Committee charter, meeting minutes, and submitted meeting materials.
- ❖ Selected and reviewed a random sample of five audit engagements.
- ❖ Reviewed continuing professional education (CPE) credits for audit staff personnel.
- ❖ Interviewed a sample of audit staff personnel.
- ❖ Interviewed the Executive Director, Audit, Risk, and Compliance (i.e., chief audit executive).

¹ The Internal Audit Foundation is a nonprofit organization operated by the IIA.

Results and Recommendations

OARC **generally conforms** with the IIA Standards and Code of Ethics. The *Quality Assessment Manual for the Internal Audit Activity* provides a scale of three ratings, “Generally Conforms,” “Partially Conforms,” and “Does Not Conform.” According to the manual, “Generally Conforms” is the highest rating and indicates that the relevant structure, policies, and procedures of the internal audit activity, as well as the processes by which they are applied, conform with the requirements of the Standards and the Code of Ethics in all material respects.²

OARC effectively executes its mission of enhancing and protecting organizational value by providing risk-based and objective assurance, advice, and insight. Audit staff personnel are competent, professional, and eager to learn; audit reports are, overall, accurate and objective; and OARC management is fully engaged with both audit staff personnel and university leadership.

An internal survey of audit staff personnel revealed that they believe that OARC adds value to the university, that management provides opportunities to enhance skills and knowledge, and that the audit activity promotes ethics and values across the organization. Likewise, survey results from clients (i.e., auditees) indicated that audit teams were professional and demonstrated technical proficiency and that audit recommendations improved or added value to their respective operations.

Overall, OARC has established a solid foundation on which it can continue to build to ensure it is operating effectively and efficiently. During the course of this QAR, the below opportunities were identified to improve OARC policies, procedures, and processes.

I. Onboarding Procedures

Applicable Standard

- 1220: Due Professional Care

Auditors new to the office may not have sufficient knowledge of auditing standards and/or office expectations. The internal staff survey revealed that multiple auditors were unaware of certain internal policies and procedures. Although existing orientation

includes a review of the audit manual, which details IIA Standards and general office expectations, discussions with newer staff auditors revealed that some had a minimal understanding of the Standards or office expectations regarding the audit process.

A recommendation to enhance onboarding procedures through the development of a new auditor training program was included in the previous internal QAR report. However, staffing resource issues impeded the implementation of such a program.

² The manual further states that, for a rating of “Generally Conforms,” there may be opportunities for improvement, but such opportunities should not represent situations where the internal audit activity has not implemented the Standards or the Code of Ethics, has not applied them effectively, or has not achieved their stated objectives.

Recommendation:

OARC management should consider enhancing onboarding procedures through the development of a new auditor training program to inform new audit staff of applicable standards and to increase the effectiveness of new audit staff in performing engagements in line with office expectations.

Management Action Plan:

Concur, with specific strategies including the development of supplement tools to aid in performance of audit steps and formalized training with regard to implementing procedures outlined in departmental policies and procedures.

II. Continuing Professional Education

Applicable Standard

- 1230: Continuing Professional Development

Although OARC is meeting the IIA Standard regarding continuing professional education (CPE), as well as the Audit Manual requirement of 80 hours of CPE per auditor every two years, the spreadsheet utilized by the office to track CPE credits has not been consistently maintained and contains discrepancies. As a result, there is a risk that the office may falsely rely on totals presented in the spreadsheet and provide inaccurate CPE totals in its annual report.

There does not appear to be a documented process for tracking CPE credits, which likely contributed to the discrepancies within the CPE spreadsheet. In addition, auditors do not regularly verify that their spreadsheet entries are accurate.

Recommendation:

OARC management should establish procedures to track CPE credits for audit personnel. In addition, OARC management should direct auditors to review and verify their CPE credits regularly to ensure accuracy.

Management Action Plan:

Concur, during July 2019 the spreadsheet for tracking CPE credits was fully updated in preparation of the annual report and continues to be maintained monthly. At the same time, each auditor was provided their CPE credits and their review and verification was requested to ensure accuracy. This process will continue at least twice a year.

III. Quality Assurance and Improvement Program

Applicable Standard

- 1311: Internal Assessments

OARC has implemented multiple ongoing monitoring activities in support of its Quality Assurance and Improvement Program (QAIP); however, one activity documented in the Audit Manual

that would provide added benefit—the completion of a quality assurance review checklist—is not being performed.³

During the engagement review portion of this QAR, there were issues noted regarding audit documentation (discussed later in this report). In addition, some engagements contained insufficient support and/or cross-referencing in the working papers to independently verify figures presented in the final reports.⁴ The implementation of an ongoing quality assurance review would provide management an opportunity to identify and correct inconsistent and/or careless audit practices.

Recommendation:

OARC management should consider reinstating the quality assurance review checklist.

Management Action Plan:

Concur, the quality assurance review checklist was reinstated for audit reports issued after September 2019.

IV. Audit Manual and TeamMate Protocol Document

Applicable Standard

- 2040: Policies and Procedure

The OARC Audit Manual and TeamMate Protocol Document do not reflect current standard operating procedures.⁵ As a result, auditors may not have sufficient guidance to ensure that audit engagements are consistently performed and that audit documentation is properly captured.

A recommendation to address this matter was included in the previous internal QAR report. Although revisions to both documents were initiated, staffing resource issues prevented completion of the revisions.

Recommendation:

OARC management should complete revisions of the Audit Manual and TeamMate Protocol Document and establish a process to ensure that these documents, as well as any other office-established guidance, are regularly reviewed and updated as necessary.

Management Action Plan:

Concur, with strategies for improvement to include completion of internal review and revision processes and formalizing requirements for ongoing periodic review. Additionally, OARC will continue efforts to better utilize the departmental SharePoint site for improved ease of use and more consistent updating as needed.

³ The quality assurance review checklists were to be completed by a member of management on a sample of risk-based audits and compliance reviews, post-issuance of the final report.

⁴ The reviewer determined that the overall results and conclusions in the final reports were accurate.

⁵ The TeamMate Protocol Document provides guidance regarding use of the TeamMate audit management software.

V. Audit Documentation

Applicable Standard

- 2330: Documenting Information

The audit engagements reviewed as part of this QAR contained appropriate evaluations; however, certain elements of audit documentation, including source of evidence and sampling and testing methodologies, were not consistently recorded in the TeamMate software. The absence of such documentation may decrease the reliability of audit evidence and, at a minimum, hinders the supervisory review of working papers.

Recommendation:

OARC management should communicate the importance of audit documentation to audit personnel and provide instruction regarding documentation requirements.

Management Action Plan:

Concur, the importance of fully documenting source of evidence and sampling and testing methodologies was discussed with audit staff personnel at the September 2019 staff meeting. Reinstatement of the quality assurance review checklist will also assist with ensuring consistent documentation.

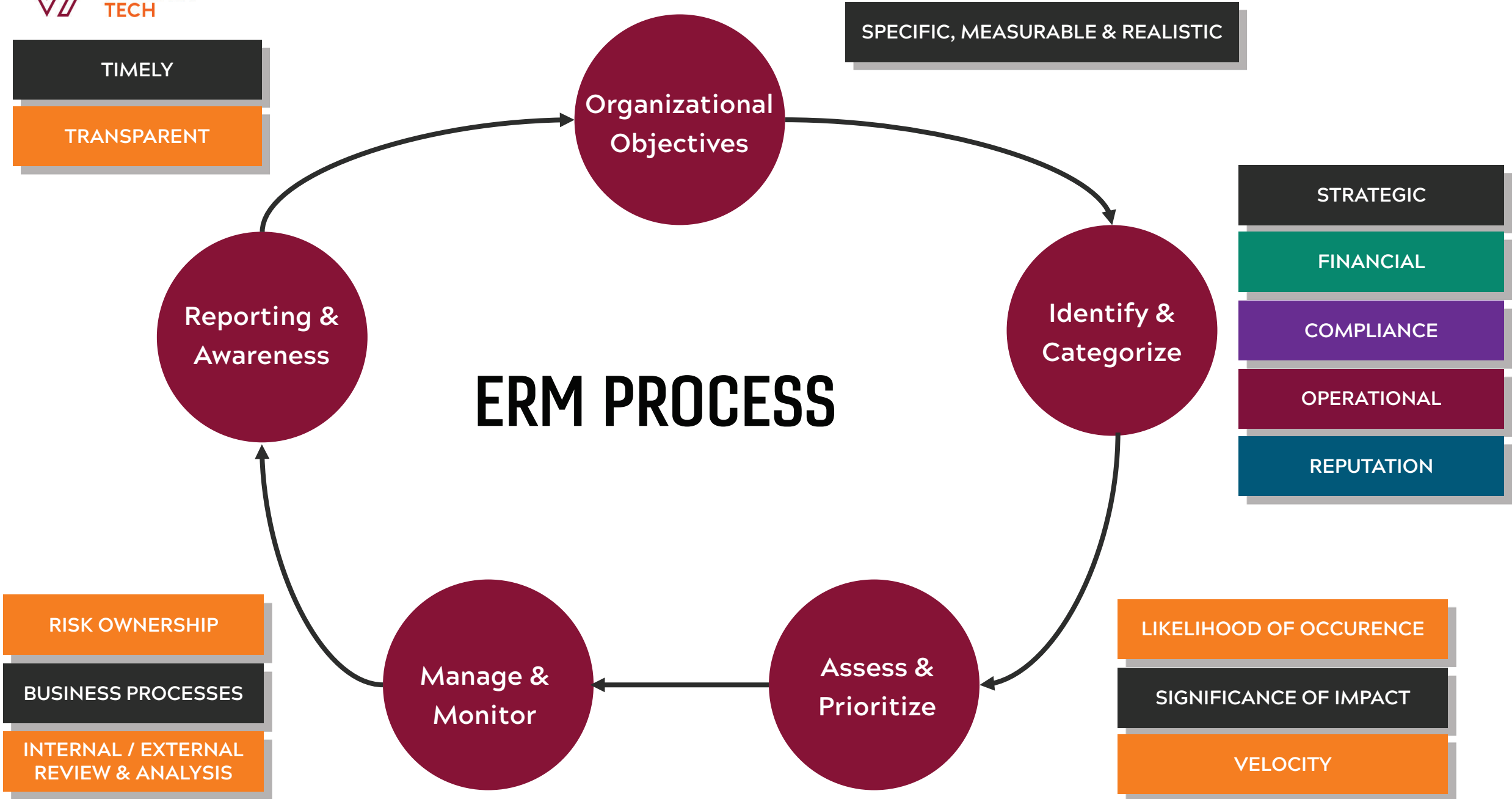
Quality Assurance Evaluation Summary—Major/Supporting Standards		GC	PC	DNC
1000	Purpose, Authority, and Responsibility	X		
1010	Recognition of the Definition of Internal Auditing, the Code of Ethics, and the Standards in the Internal Audit Charter	X		
1100	Independence and Objectivity	X		
1110	Organizational Independence	X		
1111	Direct Interaction with the Board	X		
1112	Chief Audit Executive Roles Beyond Internal Auditing	X		
1120	Individual Objectivity	X		
1130	Impairment to Independence or Objectivity	X		
1200	Proficiency and Due Professional Care	X		
1210	Proficiency	X		
1220	Due Professional Care	X		
1230	Continuing Professional Development	X		
1300	Quality Assurance and Improvement Program	X		
1310	Requirements of the Quality Assurance and Improvement Program	X		
1311	Internal Assessments	X		
1312	External Assessments	X		
1320	Reporting on the Quality Assurance and Improvement Program	X		
1321	Use of “Conforms with the <i>International Standards for the Professional Practice of Internal Auditing</i> ”	X		
1322	Disclosure of Nonconformance	X		
2000	Managing the Internal Audit Activity	X		
2010	Planning	X		
2020	Communication and Approval	X		
2030	Resource Management	X		
2040	Policies and Procedures		X	
2050	Coordination and Reliance	X		
2060	Reporting to Senior Management and the Board	X		
2070	External Service Provider and Organizational Responsibility for Internal Auditing	--	--	--
2100	Nature of Work	X		
2110	Governance	X		
2120	Risk Management	X		
2130	Control	X		
2200	Engagement Planning	X		
2201	Planning Considerations	X		
2210	Engagement Objectives	X		
2220	Engagement Scope	X		
2230	Engagement Resource Allocation	X		
2240	Engagement Work Program	X		
2300	Performing the Engagement	X		
2310	Identifying Information	X		
2320	Analysis and Evaluation	X		
2330	Documenting Information		X	
2340	Engagement Supervision	X		
2400	Communicating Results	X		
2410	Criteria for Communicating	X		
2420	Quality of Communications	X		
2421	Errors and Omissions	X		
2430	Use of “Conducted in Conformance with the <i>International Standards for the Professional Practice of Internal Auditing</i> ”	X		
2431	Engagement Disclosure of Nonconformance	X		
2440	Disseminating Results	X		
2450	Overall Opinions	X		
2500	Monitoring Progress	X		
2600	Communicating the Acceptance of Risks	X		
	The IIA’s Code of Ethics	X		

November 17, 2019

ERM & ICP Program Updates

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





ERM SUMMARY

Updates since August

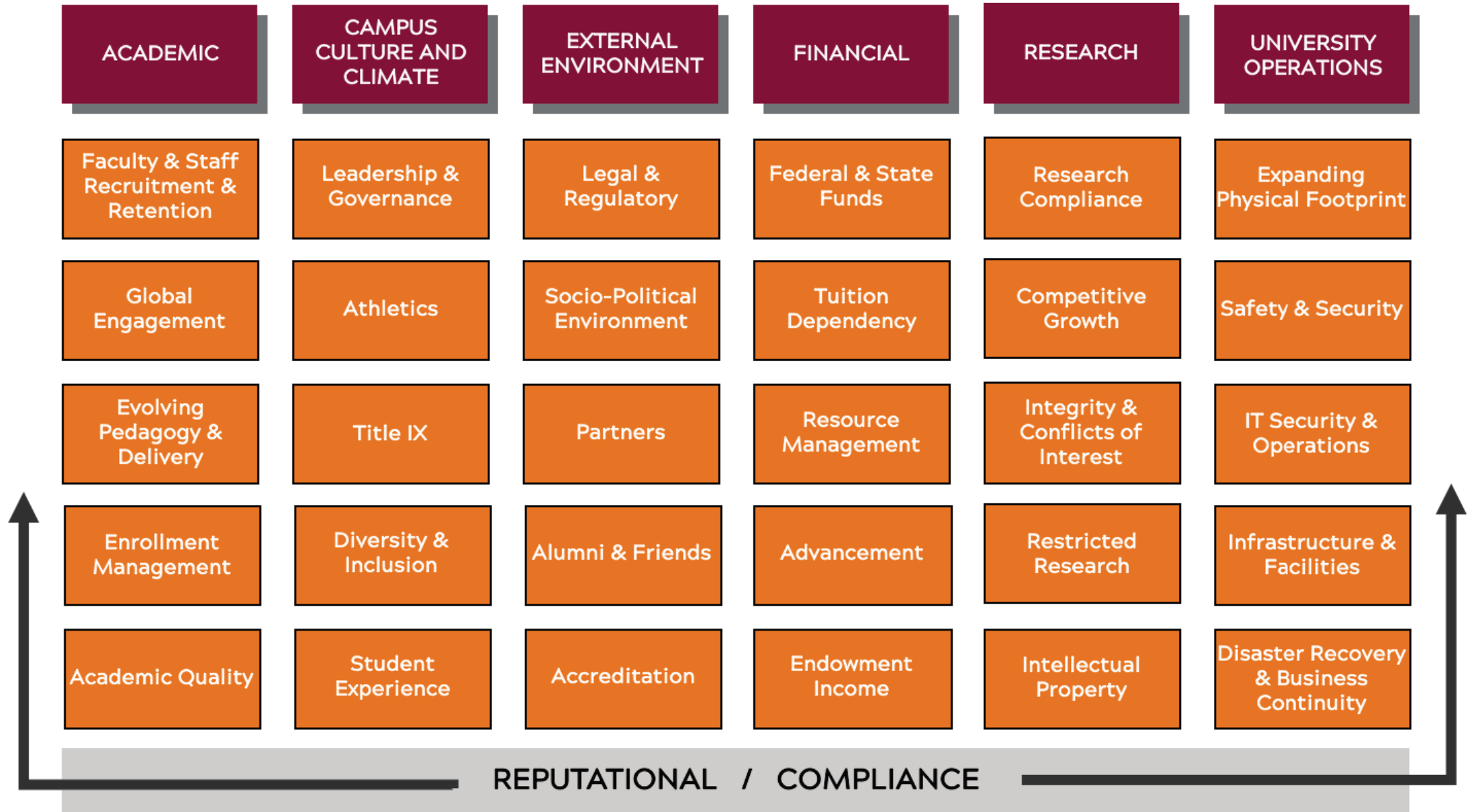
- *Refresh of heat map*
- *Process underway for next iteration of ERM risk identification and assessment*
- *Continuing review of Risk Snapshots with risk owners*

Going Forward

- *Meetings with PLT members continue through calendar year-end*
- *Development of updated risk landscape and heat map*
- *Periodic tabletop exercises continue*
- *Risk owners brief BOV through associated committees*

Enterprise Risk Landscape

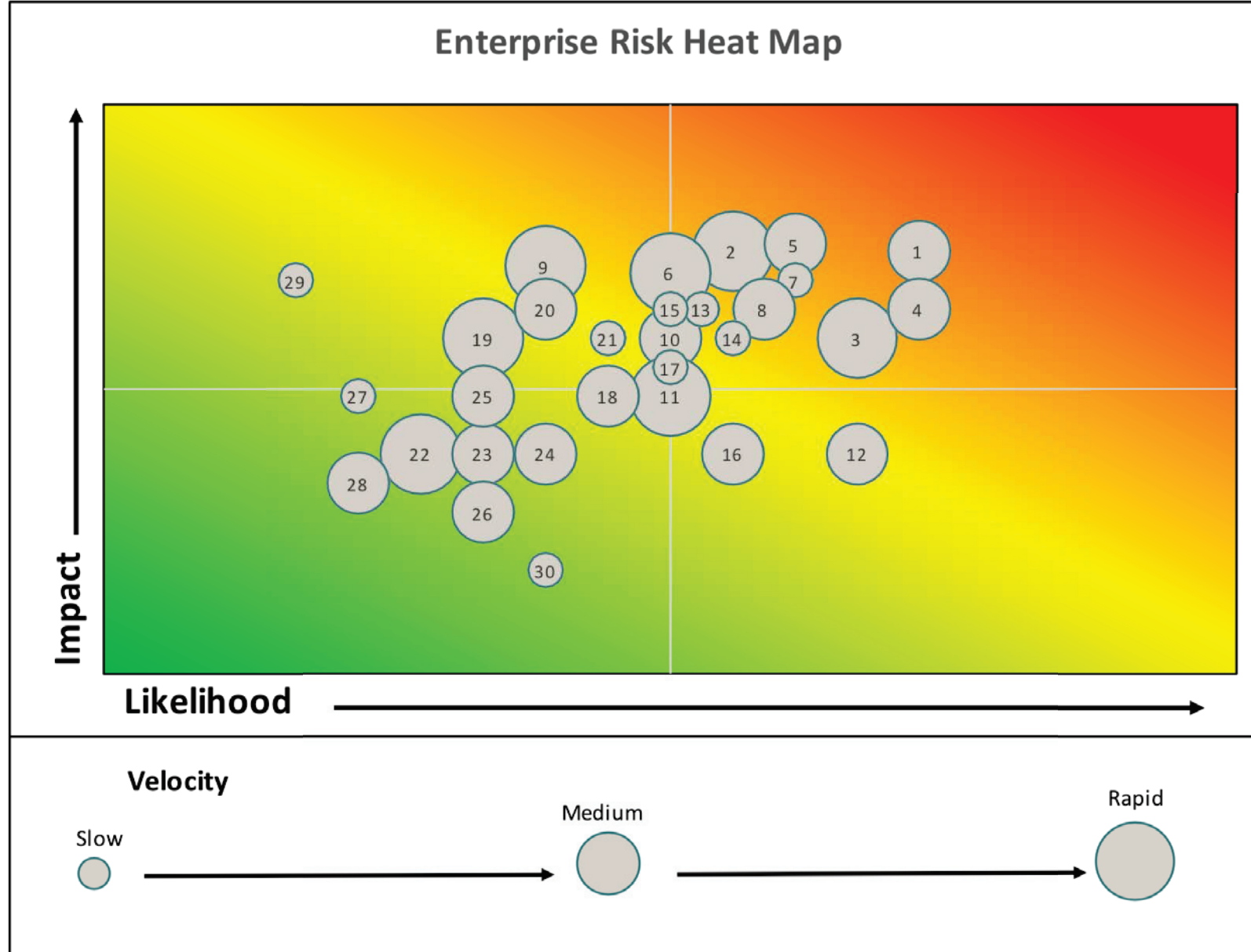
March 2018



Enterprise Risk Heat Map

March 2018

Attachment E

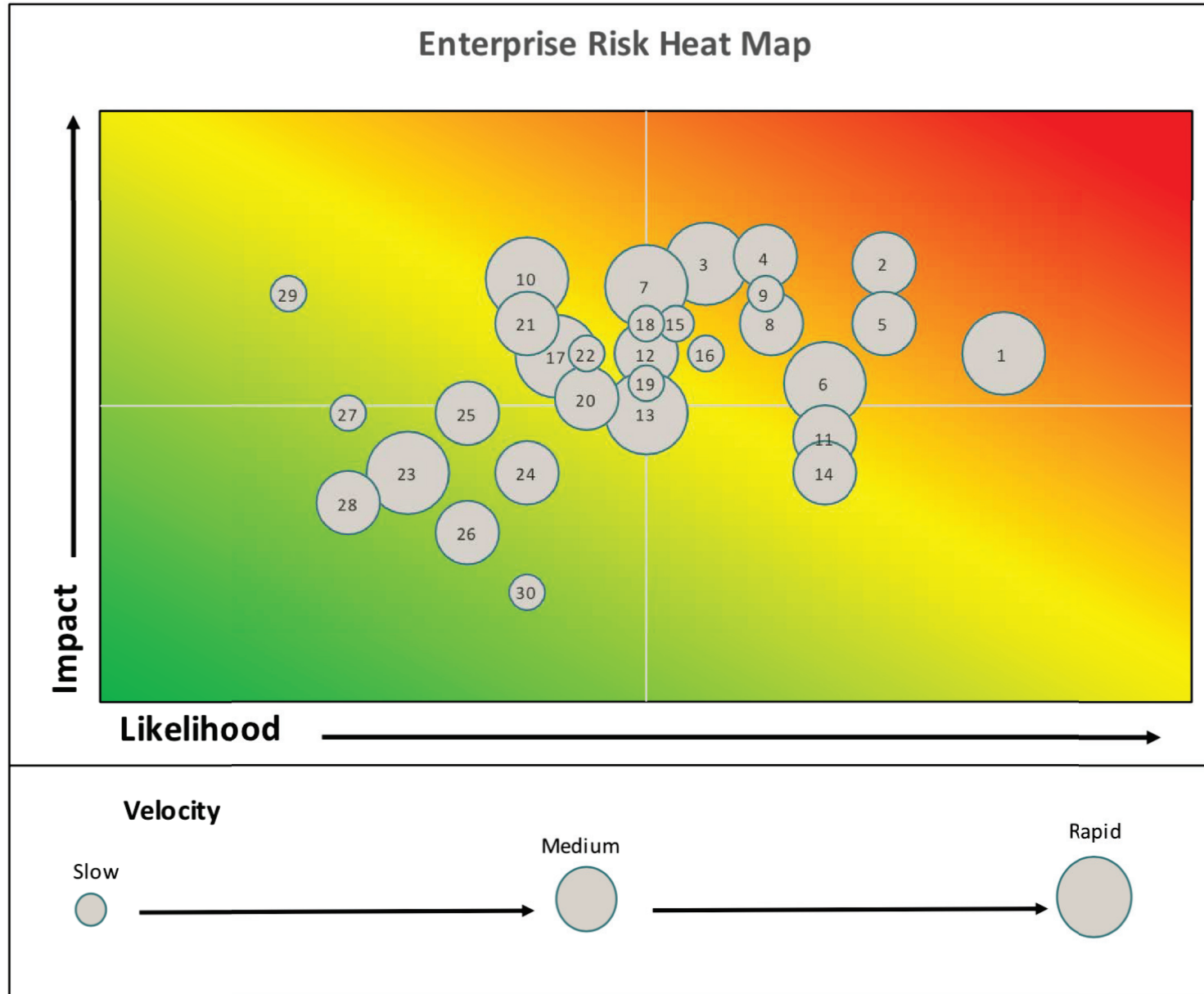


Graph Legend

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

Updated Enterprise Risk Heat Map

November 2019

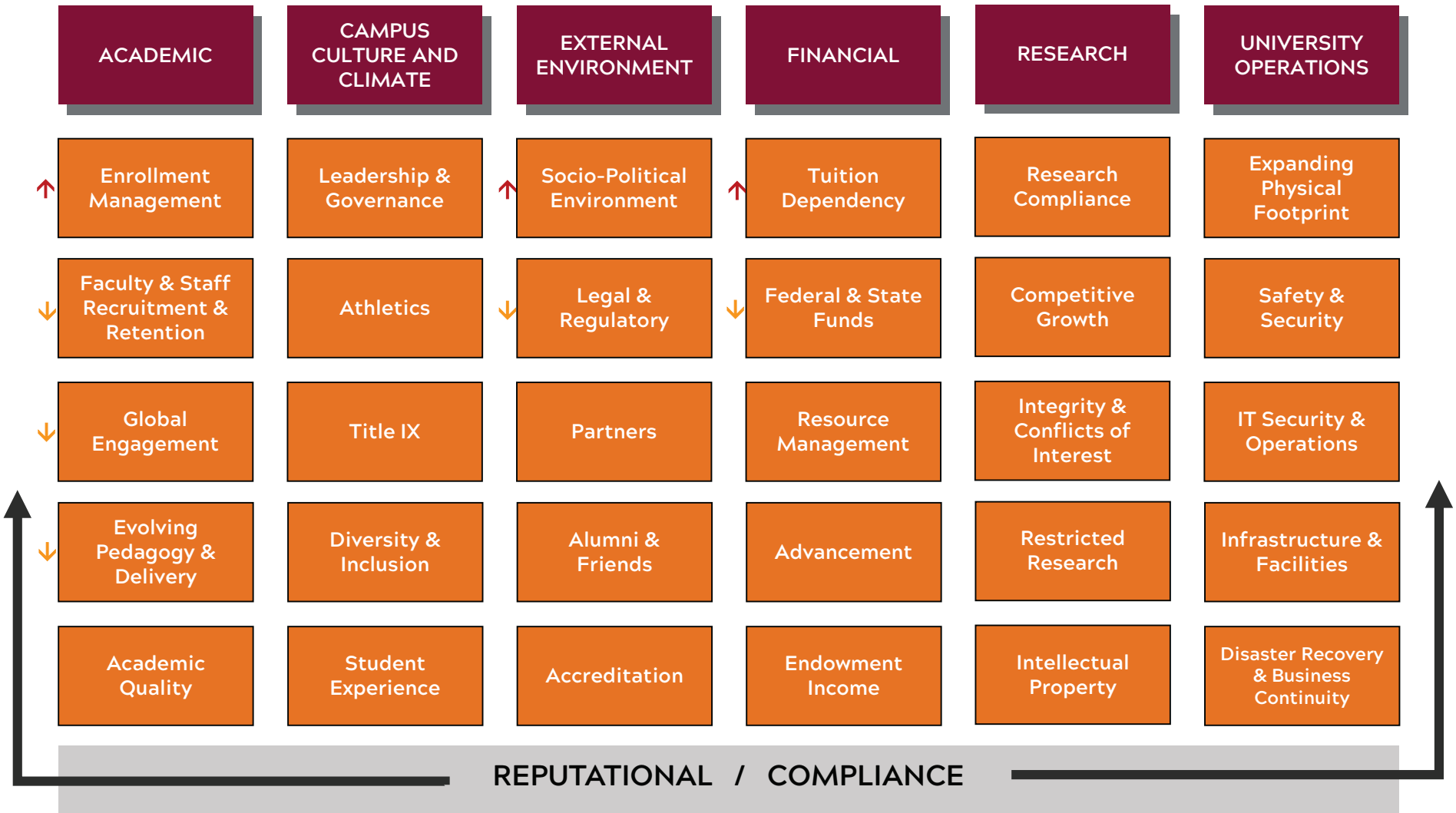


Graph Legend

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

Updated Enterprise Risk Landscape

November 2019



RISK AREA – COMMITTEE ALIGNMENT

Academic, Research, and Student Affairs

- Academic Quality
- Accreditation
- Competitive Growth
- Diversity & Inclusion
- Enrollment Management
- Evolving Pedagogy & Delivery
- Faculty & Staff Recruitment & Retention
- Global Engagement
- Integrity & COI
- Intellectual Property
- Research Compliance
- Restricted Research
- Student Experience

Buildings and Grounds

- Safety & Security

Board Level

- Expanding Physical Footprint
- Partners

Compliance, Audit, and Risk

- Legal & Regulatory
- Socio-Political Environment
- Title IX

Finance and Resource Management

- Advancement
- Endowment Income
- Federal & State Funds
- Resource Management
- Tuition Dependency

Governance and Administration

- Athletics
- Disaster Recovery & Business Continuity
- Faculty & Staff Recruitment & Retention
- Infrastructure & Facilities
- IT Security & Operations
- Leadership & Governance

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

ICP SUMMARY

Updates since August

- *The Compliance Advisory Committee's (CAC) most recent quarterly meeting took place in mid-October*
- *OARC prepared detailed training materials in support of the compliance risk-assessment process*
- *Distributed university-wide compliance owners began the compliance risk assessment process, expected to finish by mid-December*
- *OARC met with University Relations staff to develop a plan to increase awareness of the new Hokie Hotline and broader compliance efforts*

ICP SUMMARY

In Progress and Going Forward

- *Distributed university-wide compliance owners will continue the risk assessment process into December*
- *CAC meetings will continue quarterly as members focus on oversight of the ICP*
- *OARC and CAC will continue to explore outreach opportunities*

QUESTIONS?