VCU

VIRGINIA COMMONWEALTH UNIVERSITY
AUDIT, INTEGRITY AND COMPLIANCE COMMITTEE MEETING
SEPTEMBER 17, 2021
JAMES BRANCH CABELL LIBRARY
RICHMOND, VIRGINIA
AGENDA

1. **CALL TO ORDER**   **Shantaram Talegaonkar,** *Chair*

2. **ACTION ITEMS:**

   a. Approval of Minutes May 13, 2021   **Karen Helderman**, *Executive Director,*
   b. Audit, Integrity and Compliance Committee   *Audit and Compliance Services*
      Charter and Meeting Planner
   c. Audit and Compliance Services Department Charter

   FOR INFORMATION:

3. **REPORT FROM EXECUTIVE DIRECTOR OF**   **Karen Helderman,** *Executive Director,*
   AUDIT AND COMPLIANCE SERVICES   *Audit and Compliance Services*

   a. Committee Dashboard Measures
   b. Budget and Staff Qualifications
   c. Status Report of Prior Findings
   d. FY21 Annual Follow-up Report
   e. Integrity and Compliance Services Annual Report
   f. Audit Report: Outside Professional Activity
   g. Audit Report: RealSource/Purchasing
   h. Handout: Audit Work Plan Status FY22

4. **INFORMATION TECHNOLOGY UPDATE**   **Alex Henson,** *Chief Technology*
                                                                                 Officer

5. **CLOSED SESSION**
   Freedom of Information Act Section 2.2-3711 (A)
   (7) and (19), specifically:

   ***A.* Audit Report for Discussion**   **Karen Helderman,** *Executive Director*
      1. Remote Work and Remote Learning   *Audit and Compliance Services*
         IT Security Audit

   B. University Counsel Litigation Update   **Jake Belue,** *Associate*
                                                                                 University Counsel

6. **RETURN TO OPEN SESSION AND**   **Peter Farrell,** *Vice Chair*
   CERTIFICATION
   • Approval of Committee action on matters
     discussed in closed session, if necessary

7. **ADJOURNMENT**   **Peter Farrell,** *Vice Chair*

CONFIDENTIAL SUMMARY
AIC COMMITTEE
OF THE BOARD OF VISITORS
September 17, 2021
OPEN SESSION

ACTION ITEMS:

- Approval of Minutes from May 13, 2021
- Approval of AICC Charter and Meeting Planner
- Approval of Audit and Compliance Services Department Charter

FOR INFORMATION/COMMITTEE REVIEW:

1) **Items that may be action items at upcoming committee meeting:**
   - None

2) **Items that the board needs to be aware of, but will not require action (all linked here)**
   - Dashboard Measures: Review the committee dashboard that provides a snapshot of relevant oversight areas.
   - Departmental Update: Review of staffing, expenses, and audit survey results.
   - Status Report of Prior Findings: Report on the completion of corrective action plans due since the last committee meeting.
   - FY21 Annual Report of Outstanding Audit Recommendations: Annual report of past due corrective action plans
   - Integrity and Compliance Office Annual Report: An annual analysis of reported concerns and other compliance areas managed by the ICO.
   - Outside Professional Activity audit report: The OPA policy is not adequate and the reporting process is not adequate nor working as intended. There are three Board level audit findings.
   - RealSource/Purchasing audit report: All audit objectives concluded positively and there are no Board level audit findings.
   - Handout Only:
     a. Audit Work Plan Status FY22 – This handout provides the committee with information regarding the completion of the approved audit plan.

EXECUTIVE REPORTS

- Mr. Henson will provide an update regarding Information Technology.
- Ms. Helderman will briefly cover the items noted above under bullet 2. Most current presentation linked.

Board of Visitors
Audit, Integrity and Compliance Committee
8:30 a.m.
May 13, 2021
James Cabell Library
901 Park Avenue, Room 303, Richmond, Virginia

Minutes

BOARD MEMBERS PRESENT

Dr. Shantaram Talegaonkar, Chair
Ms. Carolina Espinal, Vice Chair
Mr. Edward McCoy
Mr. Peter Farrell
Ambassador Carmen Lomellin
Ms. Coleen Santa Ana
Keith Parker, Rector
H. Benson Dendy III, Vice Rector
Dr. Tonya Parris-Wilkins
Mr. Todd P. Haymore

COMMITTEE MEMBERS ABSENT

Ms. Alexis Swann

OTHERS PRESENT

Ms. Karen Helderman
Dr. Michael Rao, President
Mr. Jacob A. Belue
Staff from VCU

CALL TO ORDER

Dr. Shantaram Talegaonkar, Chair, called the meeting to order at 8:38 a.m.

APPROVAL OF AGENDA

Dr. Talegaonkar asked for a motion to approve the agenda for the May 13, 2021 meeting of the Audit, Integrity and Compliance Committee, as published. After motion duly made and seconded the agenda for the May 13, 2021 meeting of the Audit, Integrity, and Compliance Committee (AICC) was approved.

APPROVAL OF MINUTES

Dr. Talegaonkar asked for a motion to approve the minutes of the March 5, 2021 meeting of the Audit, Integrity and Compliance Committee, as published. After motion duly made and

seconded the minutes of the March 5, 1021 Audit, Integrity, and Compliance Committee meeting were approved. A copy of the minutes can be found on the VCU website at the following webpage http://www.president.vcu.edu/board/minutes.html.

Risk Model, Audit Work Plan and Ethics and Compliance Initiatives
Karen Helderman presented the process undertaken by Internal Audit to execute a risk assessment process that generates a three year audit workplan. Inputs such as industry trends, turnover and changes, time since last audit, are all considered to score potential projects. Those projects representing the most risk are placed on the three year audit workplan, which is balanced to consider workload and variety of business units.

Ms. Helderman also presented then presented the ethics and compliance initiatives for FY22, which included the onboarding of a new CECO and formalization of expectations for compliance partners.

After a motion duly made and seconded, the three year audit workplan and the FY22 ethics and compliance initiatives were approved.

Auditor of Public Accounts (APA) Entrance Conference for FY2021 Audit
Mike Reinholtz, APA Audit Director, discussed the planning and scope for the FY21 annual financial statement audit. The discussion covered the timing of this year's audit, audit scope and objectives, risk considerations, audit and management responsibilities and audit reporting communications.

Audit, Integrity and Compliance Committee Dashboard Measures
Karen Helderman presented the current status of the dashboard measures. Indicators for Data Security, Ethics and Compliance Program Oversight and ERM Program were yellow and other indicators were green.

Report from the Executive Director of Audit and Compliance Services
Karen Helderman provided an update on previously unresolved findings reported in the fiscal year 2020 annual follow up report, noting that a finding due this reporting period was successfully completed. The Executive Director also briefed the committee on the results of the Life Sciences audit followed by an overview of VCU's process to develop and maintain policies.

Enterprise Risk Management (ERM) Update
Tom Briggs, Assistant VP for Safety and Risk Management, provided an update on the Enterprise Risk Management program, noting planned increased collaboration with Internal Audit during the 2021 calendar year.

CLOSED SESSION

On motion made and seconded, the Audit, Integrity, and Compliance Committee of the Virginia

Commonwealth University Board of Visitors convened into closed session under the Virginia

Virginia Commonwealth University
Board of Visitors
Audit, Integrity and Compliance Committee
May 13, 2021 Draft Minutes

Freedom of Information Act in order to discuss pursuant to Section 2.2-3711 (A)(7) and (8), of the Virginia Freedom of Information Act for the discussion of matters requiring the provision of legal advice by counsel, relating to an update on potential and current litigation in state and federal courts and other legal matters relating to pending investigations; and pursuant to Section 2.2-3711 (A)(19) for discussion of specific cybersecurity vulnerabilities and briefing by staff concerning actions taken to respond to such matters, specifically relating to data security and certain IT processes.

RECONVENED SESSION

Following the closed session, the public was invited to return to the meeting. Dr. Talegaonkar, Chair, called the meeting to order. On motion duly made and seconded the following resolution of certification was approved by a roll call vote:

Resolution of Certification

BE IT RESOLVED, that the Audit, Integrity, and Compliance Committee of the Board of Visitors of Virginia Commonwealth University certifies that, to the best of each member's knowledge, (i) only public business matters lawfully exempted from open meeting requirements under this chapter were discussed in the closed meeting to which this certification resolution applies, and (ii) only such public business matters as were identified in the motion by which the closed session was convened were heard, discussed or considered by the Committee of the Board.

Vote	Ayes	Nays
Dr. Shantaram Talegaonkar, Chair	X	
Ms. Carolina Espinal, Vice Chair	X	
Mr. Edward McCoy	X	
Mr. Peter Farrell	X	
Ambassador Carmen Lomellin	X	
Ms. Coleen Santa Ana	X	
Keith Parker, Rector	X	
H. Benson Dendy III, Vice Rector	X	
Dr. Tonya Parris-Wilkins	X	
Mr. Todd P. Haymore	X	

All members responding affirmatively, the motion was adopted.

ADJOURNMENT

There being no further business Dr. Talegaonkar, Chair, adjourned the meeting at 9:45 a.m.

VIRGINIA COMMONWEALTH UNIVERSITY
BOARD OF VISITORS

AUDIT, INTEGRITY, AND COMPLIANCE COMMITTEE CHARTER

I.   PURPOSE

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

- Soundness of the university's system of internal controls
- Integrity of the university's financial accounting and reporting practices
- Independence and performance of the internal and external audit functions
- Integrity of information technology infrastructure and data governance
- Effectiveness of the university's ethics and compliance program
- University's enterprise risk management program
- Legal matters

The function of the Audit, Integrity, and Compliance Committee is oversight. Audit and Compliance Services assists the Committee by providing the day to day audit, integrity and compliance operations of the University within the established authority under the governance of the Committee.

II.   COMPOSITION AND INDEPENDENCE

The Audit, Integrity, and Compliance Committee will be comprised of three or more Visitors. Each member must be free from any financial, family or other material personal relationship that, in the opinion of the Board or Audit, Integrity, and Compliance Committee members, would impair their independence from management and the university.

III.   MEETINGS

The Audit, Integrity, and Compliance Committee will meet at least four times annually. Additional meetings may occur more frequently as circumstances warrant. The Committee Chair should meet with the Executive Director of Audit and Compliance Services as necessary and at least prior to each Committee meeting to finalize the meeting agenda and review the issues to be discussed.

IV.   RESPONSIBILITIES

In performing its oversight responsibilities, the Audit, Integrity, and Compliance Committee shall:

A.   **General:**

1. Adopt a formal written charter that specifies the Committee's scope of responsibility. The charter should be reviewed annually and updated as necessary.
2. Maintain minutes of meetings.
3. Authorize investigations into any matters within the Audit, Integrity, and Compliance Committee's scope of responsibilities.
4. Report Committee actions to the Board of Visitors with such recommendations as the Committee may deem appropriate.
5. Consistent with state law, the Committee may meet in closed session (with or without members of senior management present, at the Committee's discretion) with the external auditors and/or the Executive Director of Audit and Compliance Services to discuss matters that the Committee or any of these groups believe should be discussed privately.
6. Review and approve the Audit and Compliance Services budget and resource plan.
7. Approve the Audit and Compliance Services charter. The charter should be reviewed annually and updated as necessary.

B.   Internal Controls:

1. Review and evaluate the university's processes for assessing significant risks and exposures.
2. Make inquiries of management concerning the effectiveness of the university's system of internal controls.
3. Review management's written responses to significant findings and recommendations of the auditors, including the timetable to correct the weaknesses in the internal control system.
4. Advise management that they are expected to provide a timely analysis of significant financial reporting issues and practices.

C.   External Auditors/Financial Statements:

1. Meet with the external auditors and university management to review the scope of the external audit for the current year. The auditors should inform the Audit, Integrity, and Compliance Committee of any significant changes in the original audit plan.
2. Discuss with the external auditors their processes for identifying and responding to key audit and internal control risks.
3. Advise the external auditors that they are expected to provide a timely analysis of significant financial reporting issues and practices
4. 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.
5. Meet with the external auditors at the completion of the audit and make inquiries concerning the effectiveness of the university's system of internal controls.

Consistent with state law, a portion of the meeting may be conducted in closed Session without members of university management present.

6. Determine whether the 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.

D. Internal Auditors:

1. Review and approve the annual audit and management services work plan and any significant changes to the plan.
2. Require Audit and Compliance Services to perform annual reviews of the President's discretionary accounts and to issue a report thereon to the Committee.
3. Review annually the qualifications of the audit and management services staff and the level of staffing.
4. Assess the effectiveness of the internal audit function, including its independence and reporting relationships and conformance with The Institute of Internal Auditors' (IIA) Definition of Internal Auditing, Core Principles, the IIA Code of Ethics and the *International Standards for Professional Practice of Internal Auditing* by inquiring and reviewing the assessment results of the internal and external Quality Assurance and Improvement Program.
5. Review completed audit reports and progress reports on executing the approved work plan and inquire of any other matters that require audit resources.
6. Review annually the status of previously issued internal audit findings.
7. Inquire of the Executive Director of Audit and Compliance Services regarding any difficulties encountered in the course of his audits, including any restrictions on the scope of work or access to required information.
8. Review the performance of the Executive Director in consultation with the President and approve the Executive Director's annual salary compensation and bonus, if any.
9. Review and approve the appointment, replacement, reassignment, or dismissal of the Executive Director of Audit and Compliance Services.

E. Data Integrity:

1. Review the adequacy of the university's IT management methodology with regards to internal controls, including applications, systems, and infrastructure. This includes but is not limited to:
   - Physical and virtual security with regards to university servers and storage
   - Network security architecture and operations
   - Reliability and robustness of data center (servers and storage) and network infrastructure environments
   - Disaster recovery and business continuity infrastructure and associated processes and procedures.

2. Review the adequacy of the university's data management policies and procedures to ensure data security and data integrity in institutional reporting. This includes but is not limited to:
   - Authentication and authorization mechanisms in accessing university data
   - Data Governance structure and policies
   - Data security policies including data access roles and responsibilities

F. **University Ethics and Compliance Program:**

1. Review the annual compliance planned initiatives and any significant changes to the plan.
2. Review the qualifications of the compliance staff and the level of staffing.
3. Assess the effectiveness of the compliance program, including its independence and reporting relationships.
4. Review completed compliance reports and progress reports on the status of compliance and integrity related initiatives including process and plans in place to assess conflict of interest management (inclusive of institutional and individual conflicts).
5. Require the Integrity and Compliance Office to report on management's processes and procedures that provide assurance that the university's mission, values, codes of conduct, and universitywide policies are properly communicated to all employees.
6. Review results of compliance reviews to ensure system and controls are designed to reasonably ensure compliance with laws and regulations, university policies and the code of conduct.
7. Inquire of the Executive Director of Audit and Compliance Services whether there have been any restrictions on the scope of work or access to required information in conducting compliance and ethics reviews.

G. **Enterprise Risk Management**

1. Provide oversight of the university's Enterprise Risk Management program.
2. Review the university's risk appetite.
3. Require periodic reporting on the overall program's design and effectiveness, including newly identified risks
4. Monitor progress of Risk Mitigation Plans and review policy and resource improvements as necessary.

H. **Legal:**

1. Consult as necessary with University Counsel regarding legal issues concerning the university.

Virginia Commonwealth University
Board of Visitors

Audit, Integrity and Compliance Committee Meeting Planner

A = Annually; Q = Quarterly; AN = As Necessary	Frequency			Planned Timing			
Q1, Q2, Q3, Q4 based on Fiscal Year (July – June)	A	Q	AN	Q1	Q2	Q3	Q4
				Sep	Dec	Mar	May
A. General							
1. Review and update Audit, Integrity, and Compliance Committee charter and meeting planner	X						X
2a. Approve minutes of previous meeting		X		X	X	X	X
2b. Maintain minutes of meetings		X		X	X	X	X
3. Authorize investigations into any matters 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. Consistent with state laws, meet in closed session with only the external auditors, Executive Director of Audit and Compliance Services, and named individuals.		X		X	X	X	X
6. Review and approve the Audit and Compliance Services budget and resource plan.	X			X			
7. Review and approve Audit and Compliance Services charter	X			X			
B. Internal Controls/Financial Statements							
1. Review and evaluate university's process for assessing significant risks and exposures	X			X			
2. Make inquiries of management concerning the effectiveness of the university's system of internal controls			X				
3. Review management's written responses to significant findings and recommendations of the auditors, including the timetable to correct the weaknesses in the internal control system			X				
4. Advise management that they are expected to provide a timely analysis of significant current financial reporting issues and practices			X				

A = Annually; Q = Quarterly; AN = As Necessary	Frequency			Planned Timing			
Q1, Q2, Q3, Q4 based on Fiscal Year (July – June)	**A**	**Q**	**AN**	**Q1**	**Q2**	**Q3**	**Q4**
				Sep	Dec	Mar	May
C. External Auditors							
1. Meet with external auditors and university management to review 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. Advise the external auditors that they are expected to provide a timely analysis of significant financial reporting issues and practices	X						X
4. 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				X
5. Meet with the external auditors at the completion of the audit and make inquiries concerning the effectiveness of the university's system of internal controls.	X				X		
6. Determine whether the 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	X				X		
D. Internal Auditors							
1. Review and approve the annual audit and management services work plan and any significant changes to the plan	X						X
2. Require Audit and Compliance Services to perform annual reviews of the president's discretionary accounts and to issue a report thereon to the Committee	X				X		
3. Review the qualifications of the audit and management services staff, the adequacy of the staffing level	X			X			

A = Annually; Q = Quarterly; AN = As Necessary	Frequency			Planned Timing			
Q1, Q2, Q3, Q4 based on Fiscal Year (July – June)	A	Q	AN	Q1	Q2	Q3	Q4
				Sep	Dec	Mar	May
4. Assess the effectiveness of the internal audit function, including its independence and reporting relationships and conformance with the Definition of Internal Auditing, Core Principles, the IIA Code of Ethics and the *International Standards for Professional Practice of Internal Auditing* by inquiring and reviewing the assessment results of the internal and external Quality Assurance and Improvement Program	X				X		
5. Review completed audit reports and progress reports on executing the approved work plan and inquire of any other matters that require audit resources		X		X	X	X	X
6. Review annually the status of previously issued internal audit findings	X			X			
7. Inquire of the Executive Director of Audit and Compliance Services regarding any difficulties encountered in the course of his audits, including any restrictions on the scope of work or access to required information		X		X	X	X	X
8. Review the performance of the Executive Director in consultation with the President and approve the Executive Director's annual salary compensation and bonus, if any.	X			X			
9. Review and approve the appointment, replacement, reassignment, or dismissal of the Executive Director of Audit and Compliance Services			X				
E. Data Integrity							
1. Review the adequacy of the university's IT management methodology with regards to internal controls, including applications, systems, and infrastructure. This includes but is not limited to: • Physical and virtual security with regards to university servers and storage • Network security architecture and operations • Reliability and robustness of data center (servers and storage) and network infrastructure environments • Disaster recovery and business continuity infrastructure and associated processes and procedures			X	X		X	

A = Annually; Q = Quarterly; AN = As Necessary	Frequency			Planned Timing			
	A	**Q**	**AN**	**Q1**	**Q2**	**Q3**	**Q4**
				Sep	Dec	Mar	May
2. Review the adequacy of the university's data management policies and procedures to ensure data security and data integrity in institutional reporting. This includes but is not limited to: • Authentication and authorization mechanisms in accessing university data • Data Governance structure and policies • Data security policies including data access roles and responsibilities			X		X		X
F. University Ethics and Compliance Program							
1. Review the annual compliance planned initiatives and any significant changes to the plan	X						X
2. Review the qualifications of the compliance staff and the level of staffing (utilization and effort focus)	X			X			
3. Assess the effectiveness of the compliance program, including its independence and reporting relationships	X			X			
4. Review completed compliance reports and progress reports on the status of compliance and integrity related activities including process and plans in place to assess conflict of interest management (inclusive of institutional and individual conflicts)		X		X	X	X	X
5. Require the Integrity and Compliance Office to report on management's processes and procedures that provide assurance that the university's mission, values, and codes of conduct and universitywide policies are properly communicated to all employees	X			X			X
6. Review results of compliance reviews to ensure system and controls are designed to reasonably ensure compliance with laws and regulations, university policies and the code of conduct			X	X	X	X	X
7. Inquire of the Executive Director of Audit and Compliance Services whether there have been any restrictions on the scope of work or access to required information in conducting compliance and ethics reviews		X		X	X	X	X
G. Enterprise Risk Management							
1. Provide oversight of the university's Enterprise Risk Management program		X		X	X	X	X
2. Review the university's risk appetite	X				X		

A = Annually; Q = Quarterly; AN = As Necessary	Frequency			Planned Timing			
	A	**Q**	**AN**	**Q1**	**Q2**	**Q3**	**Q4**
				Sep	Dec	Mar	May
3. Require periodic reporting on the overall program's design and effectiveness, including newly identified risks		X		X	X	X	X
4. Monitor progress of risk mitigation plans and review policy and resource improvements as necessary		X		X	X	X	X
H. Legal							
1. Consult as necessary with University Counsel regarding legal issues concerning the university		X		X	X	X	x

AUDIT AND COMPLIANCE SERVICES CHARTER

**VIRGINIA COMMONWEALTH UNIVERSITY
and
VCU HEALTH SYSTEM**

Virginia Commonwealth University (university) and VCU Health System Authority (health system) maintain comprehensive and effective internal audit and compliance programs. The objective of Audit and Compliance Services ("department") is to assist members of the Board of Visitors, Board of Directors, and management in the effective performance of their responsibilities. The department fulfills this objective by providing independent and impartial examinations, investigations, evaluations, counsel, and recommendations for the areas and activities reviewed.

Scope of Work

The scope of the department's work is to determine whether the university's and health system's risk management, internal control, governance, and compliance processes, as designed and represented by management, are adequate and functioning in a manner to provide reasonable assurance that:

- Risks are appropriately identified and managed

- Control processes are adequate and functioning as intended

- Significant, financial, managerial, and operating information is accurate, reliable, and timely

- An effective university compliance program is maintained to provide guidance and resources, in an oversight role, for all educational, research, and athletic compliance programs to optimize ethical and compliant behavior

- An effective health system compliance program is implemented to further the health system's mission, vision, and values by promoting a culture of compliance, and preventing, correcting, and investigating issues through education, monitoring, and enforcement

- An effective program of information technology (IT) management and security is maintained by management to ensure health system and university IT and data assets are properly secured, integrity protected, available as needed and kept confidential as required by applicable policies laws and regulations

- Employees' actions are in compliance with the respective codes of conduct, policies, standards, procedures, and applicable laws and regulations

- Resources are used efficiently and are adequately protected

- Program plans and objectives are achieved

- Significant legislative and regulatory issues impacting the university and health system are recognized and appropriately addressed

Opportunities for improving management controls, accountability, fiscal performance and compliance processes, and for protecting organizational reputation will be addressed with the appropriate level of management when identified.

Accountability

The Executive Director of Audit and Compliance Services shall be accountable to the Board of Visitors, through the Audit, Integrity, and Compliance Committee, and the Board of Directors, through the Audit and Compliance Committee, to maintain comprehensive and professional internal audit and compliance programs. In fulfilling those responsibilities, the Executive Director will:

- Establish annual goals and objectives for the department, and report periodically on the status of those efforts.

- Execute the annual work plans and initiatives.

- Coordinate efforts with other control and monitoring functions (risk management, financial officers, campus police, university counsel and health system general counsel, external auditors, government reviewers, etc.).

- Report significant issues related to the department's scope of work, including potential improvements, and continue to provide information about those issues through resolution.

- Provide updates to the respective board committees, the university president, and the chief executive officer of the health system on the status of the work plans and initiatives, qualifications of staff, and sufficiency of department resources.

Independence and Objectivity

All work will be conducted in an objective and independent manner. Staff will maintain an impartial attitude in selecting and evaluating information 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.

To provide an appropriate reporting structure to support independence, the Executive Director shall report to the Audit, Integrity, and Compliance Committee of the Board of Visitors and to the Audit and Compliance Committee of the Board of Directors. The Executive Director shall report administratively to the university's President.

Responsibility

The department will assist the Board of Visitors, Board of Directors, and management by:

- Maintaining a professional staff with sufficient knowledge, skills, and experience to fulfill the requirements of this charter.

- Developing and executing annual and long-range risk-based work plans and initiatives. The plans and initiatives will be submitted to management for review and comment and to the respective board committee for approval. The department recognizes that one of the primary benefits of these programs is the ability to respond to issues that arise during the normal course of business. Accordingly, the annual plans shall include time for management requests and special projects.

- Participating in an advisory capacity in the planning, development, implementation, or change of significant compliance and control processes or systems. The Executive Director shall ensure that the level of participation in these projects does not affect the department's responsibility for future evaluation of evaluating these processes or systems nor compromise its independence.

- Conducting or assisting in the investigation of any suspected fraudulent activities, misconduct, or non-compliance issues, and notifying management and the respective board committees of the results.

- Issuing periodic reports to management and the respective board committees summarizing the results of the department's activities.

- Considering the scope of work of the external auditors, as appropriate, to provide optimal audit coverage to the university and health system at a reasonable overall cost.

- Reporting at least annually to the Board of Visitors, Board of Directors, and senior management on the department's purpose, authority, responsibility, and performance relative to its plans and initiatives, and on its conformance to standards and best practices. Reporting should also include significant risk exposures and control issues, corporate governance issues, serious misconduct or non-compliance, and other matters needed or requested by the Board and senior management.

Authority

The department and its staff are authorized to:

- Have unrestricted access to all activities, records, property, and personnel. Receive cooperation from all university and health system personnel and affiliates.

- Have full access to the respective board committee.

- Allocate departmental resources, set audit and review frequencies, determine scopes of work, and apply the techniques necessary to accomplish objectives.

- Obtain the necessary assistance of personnel in departments when performing work plans and initiatives, as well as that of other specialists.

The department and its staff are not authorized to:

- Perform operational duties in interim status, or otherwise, unless authorized in advance by the respective board committee.

- Initiate or approve accounting transactions external to the department.

Standards of Practice

The department will conduct its scope of work in accordance with requirements and best practices as established by relevant authoritative and objective sources from industry and government.

For internal audit functions, this includes both mandatory and recommended guidance from the Institute of Internal Auditors International Professional Practices Framework. The mandatory guidance requires our department to conform with the Core Principles for the Professional Practice of Internal Auditing, Definition of Internal Auditing, Code of Ethics, and *International Standards for the Professional Practice of Internal Auditing (Standards)*. Internal auditing is an independent, objective assurance, and consulting activity designed to add value and improve an organization's operations. Our department will help the university and health system accomplish its objectives by bringing a systematic, disciplined, and risk-based approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

For maintaining effective compliance programs, standards of practice are driven by the guidance provided in Chapter 8 of the Federal Sentencing Guidelines as promulgated by the US Sentencing Commission. The main focus of an effective program is to prevent and detect misconduct, remedy harm when identified, self-report where applicable, and maintain due diligence in promoting an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

For the health system compliance program, guidance by the Health Care Compliance Association is also included. This organization sets the standard for professional values and ethics in the health care compliance field.

Quality Assurance and Improvement Program

The department will maintain a quality assurance and improvement program that covers all aspects of the internal audit activity. This program will be designed to:

- evaluate internal audit's conformance with the *Standards* and application of the Code of Ethics;
- assess the efficiency and effectiveness of the department; and
- identify opportunities for improvement.

The quality program includes both internal and external assessments. Internal assessments will include ongoing monitoring and periodic assessments of internal audit activity. An external assessment will be performed at least once every five years by qualified individuals who are independent of the internal audit function.

AUDIT, INTEGRITY, AND COMPLIANCE COMMITTEE DASHBOARD MEASURES

INFORMATION TECHNOLOGY GOVERNANCE - DATA INTEGRITY

DATA GOVERNANCE PROGRAM (development of program)

Program progressing successfully

Barriers / challenges encountered that may have an impact on issue resolution or implementation. Executive Council to resolve challenge.

Significant challenge encountered; will require decision from Executive Leadership Team to resolve

The Student Data Warehouse project continues to move forward. Since the last BOV meeting, stakeholders including Strategic Enrollment Management and Student Success Functional Leaders, Data Analysts, Academic Unit consumers of data, Data Stewards, and Data Trustees provided business requirements through focus group sessions. The sessions were framed with four guiding questions pertaining to 1) Most often asked data/information questions; 2) Data/Information gaps; 3) Examples of data/information that gives you pause; 4) Impactful integration points for student data. A consultant has been engaged to assist in turning those requirements into technical specifications, and a cloud-based data warehouse vendor (the same one utilized by VCU Health) has been engaged to provide a pilot warehouse environment.
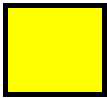
DATA SECURITY (number of security incidents / breaches)

No data breaches have occurred or seem likely to occur; security risks are well understood and being mitigated; resources viewed as aligned with threat and risk environment

No breach has occurred, but minor security incidents or near-misses have occurred; significant audit findings have occurred but are being mitigated; some overload or barriers / challenges encountered that may require adjustment or reallocation of resources

Significant breach requiring notification has occurred or conditions exist where significant barriers/challenges are likely to produce unacceptably high levels of risk

The VCU Information Security team has continued to detect an increased number of phishing scams continuously targeting individuals to get them to purchase gift cards or to steal credentials for unauthorized access to systems or data. We also continue to see a higher volume of end user reporting of security issues and scams, which we attribute to increased awareness from training and communication.

Inadvertent exposure of sensitive data and the expanding threat of ransomware attacks continue to be the primary IT security threats in our environment, but the associated set of risks has evolved: Continued/expanded remote work reduces central control of devices and makes network-level security less effective. The increasing adoption of third-party service providers combined with a new trend of supply chain based attacks (e.g. Solarwinds, Blackbaud, etc) has increased focus on third-party service security and compliance management. The targeting of core infrastructure components and supply chains by sophisticated cyber adversaries has led to the review and revision of protection strategies for core infrastructure components.

In addition to continued monitoring for legacy and insecure technology, further enhancing our vulnerability management program, and working with business units in mitigating risks and vulnerabilities, we have also made great progress in Implementing and increasing enterprise-wide adoption of a centralized patch management and backup capabilities to mitigate vulnerabilities and the risk of ransomware and other cyberattacks.

We are beginning to re-architect our security strategy by migrating toward a Secure Access Service Edge (SASE) model, in which we shift from managing security using just the VCU network perimeter surrounding the VCU data center to securing access to all VCU services and data no matter where they reside (at VCU or in the cloud) and no matter from where these resources are being accessed. We are also collaborating with the Office of the Vice President for Research and Innovation to establish a Research Computing Center to better support research computing and use of data.

ERM PROGRAM

Status of ERM mitigation plans

Program progressing on schedule

Program not on schedule; ERM Committee to address.

Program significantly behind schedule; Executive Management attention required.

The risk owners are continuing to update their portions of the risk mitigation plans, with input and guidance from the consultant and AVP of SRM as necessary. The ERM Steering Committee will meet in October and December to review and approve risk mitigation plans. They will then be forwarded to the Cabint for review and approval.

PLANNED AUDIT STATUS

PLANNED AUDITS (status of audits - planned and unplanned to available resources)

SPECIAL PROJECTS (status of special projects - planned and unplanned to available resources)

 Progressing as planned and within overall budget

 Some overload or barriers / challenges encountered that may require adjustment or reallocation of resources to resolve

 Significant overload or barriers / challenges encountered resulting in major delays or changes to scheduled work plan

The audit plan is progressing; however, the Deputy Auditor's recent retirement may delay the delivery of a few audits if the position is not filled timely. A search team is actively interviewing candidates at this time.

INSTITUTIONAL COMPLIANCE PROGRAM

 Compliance requirements compared to known material violations
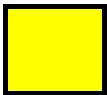
 Compliance Program Oversight & Effectiveness

 No known material noncompliance; or ownership and accountability for compliance risks are established and operating at explicitly or implicitly approved levels of risk tolerance or appetite

 Challenges encountered that have an impact on visibility, verficiation, strategy implementation or resolution

 Significant challenges to institutional compliance strategy or resolution encountered

Notes: There are no known material compliance violations as related to regulatory, legal or univerity policies.

VCU - Audit and Compliance Services

Estimated Expenses - Fiscal Year 2021-22

	Audit & Management Services	Compliance Services	Total	Prior Year Total
Total Personnel Costs	1,294,606	474,338	1,768,944	1,619,959
Office Expenses	53,000	53,000	$ 106,000	153,000
TOTAL EXPENSES	$ 1,347,606	$ 527,338	$ 1,874,944	$ 1,772,959

Audit and Compliance Services

Staff Credentials

University Audit and Management Services
Integrity and Compliance Office

Name and Title	Hire Date	Education	Credentials/ Advanced Degrees	Years of Experience
Karen K. Helderman Executive Director	February, 2019	BS, Accounting	CPA; CISA; PMP MBA	35 – Audit/Compliance
David M. Litton Director, Audit and Management Services, University and VCUHealth	March, 1994	BS, Accounting and Information Systems	CPA; CISA; CGFM; CGEIT; CRMA	21 – Internal Audit 5 – External Audit 6 – Information Technology
Jacqueline L. Kniska University Compliance	July, 2011	BA, Political Science	JD CHC LPEC	14 – Ethics and Compliance 5 – Legal
VACANT Deputy Director, University Audit and Management Services				
Blake Bialkowski Deputy Director, IT Audit, University and VCU Health	April, 2020	BS, Business Information Technology	CISA, PMP	14 – External Audit 3 – Internal Audit
Janet W. Bishop University Audit Manager	May, 2001	BS, Business Administration	CIA, CFE	18 – Internal Audit 24 – Accounting
Michael A. Pointer IT Auditor	July 2019	BS, Liberal Arts	CompTIA A+ Certification JAMF Pro 200 Certification ITIL Foundations Certification	6 – Technology 2 – Internal Audit
Tasha Foster Staff Auditor	August, 2021	BS, Business Administration	MBA; MA	4 – Internal Audit 3 – Financial Services 8 – Higher Education
Niveditha Sudharsan Senior Auditor	April, 2019	BS, Finance		5.5 – External Audit 4 – Internal Audit

Name and Title	Hire Date	Education	Credentials/ Advanced Degrees	Years of Experience
David J. Irving Senior Auditor	January, 2015	BA, History/Political Science	CPA; CIA MS, Accounting	10 – Internal Audit 15 – External Audit
Jason A. Block Senior Compliance and Policy Specialist	January, 2021	BA, Political Science	MS.Ed Higher Education Management, JD, PhD, Higher Education CCEP	14 – Higher Education 8 – Compliance
Donna Crawford Special Projects and Quality Assessment Coordinator	September, 2019	BS, Business Administration/ Concentration in Information Systems	CISA	26 – Audit/Compliance
Ashley L. Greene Senior Integrity and Compliance Specialist	September, 2012	BA, Psychology	CCEP LPEC	12 – Ethics and Compliance 1 – Other

Credentials:

CCEP	Certified Compliance and Ethics Professional	CISSP	Certified Information Systems Security Professional
CFE	Certified Fraud Examiner	CPA	Certified Public Accountant
CGEIT	Certified in the Governance of Enterprise IT	CRISC	Certified in Risk and Information Systems Control
CGFM	Certified Government Financial Manager	CRMA	Certification in Risk Management Assurance
CHC	Certified in Health Care Compliance	LPEC	Leadership Professional in Ethics and Compliance
CIA	Certified Internal Auditor	MBA	Masters of Business Administration
CISA	Certified Information Systems Auditor	MPA	Masters of Public Administration

Department Memberships: ACUA, ACUPA, AGA, CUAV, IIA, OCEG, SCCE

ACUA	Association of College and University Auditors	CUAV	College and University Auditors of Virginia
ACUPA	Association of College and University Policy Administrators	IIA	Institute of Internal Auditors
		OCEG	Open Compliance and Ethics Group
AGA	Association of Government Accountants	SCCE	Society of Corporate Compliance and Ethics

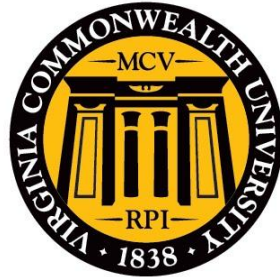# VCU Audit and Management Services

Audit Survey Results

At the completion of each audit, we request that the audited department evaluate our performance in 12 specific areas and provide comments or recommendations that might help to improve our services. We provide a copy of the survey to management at the planning stage of our audit so that management can consider the evaluation criteria throughout the process.

The survey is conducted online and the results are returned directly to the Executive Director. We also welcome comments and phone calls about any concerns or issues with the audit. Based on the results, we may request additional information from the department. We accumulate the results to be reported to the Board of Directors at the end of each fiscal year.

During the fiscal year 2020-2021, 7 surveys were completed, the numerical results of which are summarized below. The average of all responses this year was 3.40 on a 4-point scale, which is slightly lower than the FY20 average of 3.51 and consistent with the FY19 average of 3.45.

Survey Item	Average Score
1. The audit process was clearly explained prior to the start of the audit work.	3.43
2. The audit staff solicited suggestions from management as to areas of possible audit coverage.	3.57
3. The final audit objectives were reviewed with appropriate departmental personnel early in the audit process.	3.28
4. The process of issuing the audit report, including distribution and resolution of potential business issues and recommendations, was explained to management at the beginning of the audit.	3.57
5. The audit staff had or obtained a sufficient working knowledge of the operations and systems of your department, including current technology and current events.	3.14
6. The audit staff was willing to provide advice and assistance to personnel in the department.	3.57
7. The audit staff kept management informed throughout the audit regarding potential audit business issues.	3.57
8. The audit was completed within a reasonable time frame. Any delays in completing the audit were explained to management.	3.00
9. The audit results in minimal disruption of operations in the department.	3.42
10. The business issues in the audit report were accurately stated.	3.42
11. The recommendations in the audit report were useful and relevant.	3.57
12. The audit report contained adequate explanations for the business issues and recommendations.	3.29

4 = Strongly Agree; **3** = Agree; **2** = Disagree; **1** = Strongly Disagree

Annual Review of Audit Recommendations Outstanding

Final Report
August 10, 2021

Audit and Compliance Services

Audit and Management Services performs an annual review of audit recommendations that remain outstanding. During our review, management reports the status of previously issued recommendations. If management reports that corrective actions have been completed, we test the new procedures to determine whether those corrective actions were properly implemented and effective.

Appendix A provides a schedule of Board and management level audit recommendations that are past due, meaning they are unresolved and their target completion dates have been revised two or more times.   We allowed for an additional deadline extension for departments with demonstrated impacts due to shifting priorities and increased workloads associated with developing the university's COVID-19 response.

Past Due Board Level Recommendation

School of Dentistry report – This report included a recommendation to "Improve Physical Access Management." Dentistry was expecting to move to the new Adult Outpatient Facility building in 2021 so they did not want to invest the time and money to upgrade their physical security locks in their existing space. This past year leadership decided that Dentistry will not be moving to the new building and instead will remain in their current locations. Dentistry has been working with VCU Campus Card Services (Card Services) and has upgraded all external and internal controlled door locks from the C-CURE system to the new CBORD system. Dentistry also worked with Card Services and Network Services to identify the most critical internal manual locks that need to be replaced. Contingent on budget, Dentistry will convert the remaining manual key lock doors to card-swipe locks running on the CBORD system. As of the date of this report, Dentistry is obtaining cost estimates and determining how to fund the replacement of the critical internal locks. Once Dentistry has a funding source, they will set a date for completion and Internal Audit will continue to monitor and report on Dentistry's progress.

Past Due Management Level Recommendations

College of Humanities and Sciences report – This report included recommendations to "Improve Record Management Process" and "Perform Banner Reconciliations and Close Inactive Indexes." Some progress has been made on both issues; however, due to other priorities and lack of resources, these areas have not been fully addressed to allow audit to clear either issue. Management anticipates corrective actions to be complete by September 30, 2021.

Consolidated Audit of School of Medicine – Cardiology report – This report included a recommendation to "Improve Records Management for Compliance and Guidelines." Cardiology did not have a previous records management plan. Cardiology required staff to take records and retention training and they received assistance from Technology Services Records Management group to develop a records inventory. However, due to staffing shortages and working remotely, the department was unable to complete the destruction of eligible physical records. Management anticipates corrective action to be complete by December 31, 2021.
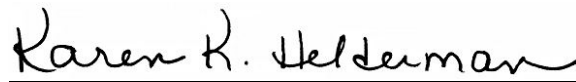
Non-Research Institutes and Centers memo – This memo included a recommendation to the Provost's Office to facilitate the establishment of a policy that governs non-research institutes and centers (ICs). The recommendation also encouraged collaboration with the Committee on Research-Related Institutes and Centers to evaluate the development of one policy that relates to both research and non-research ICs. The retirement of the person leading the corrective action and the COVID-19 pandemic are the primary reasons this is not complete. The Provost Office

has identified the appropriate individuals to serve on a committee that will develop a new policy or expand the current policy for research institutes and centers. The Provost Office expects to complete corrective actions by December 31, 2021.

Our review of audit recommendations outstanding occurs throughout the year but includes all recommendations with a due date on May 31, 2021 and prior.

We reviewed the information in this report with the applicable department manager and vice president prior to releasing the final report.

Our review was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* and included an evaluation of internal controls and such procedures as we considered necessary in the circumstances.

Executive Director
Audit and Compliance Services

Audit and Management Services
VCU Past Due Audit Recommendations

Report Date	Audit	Board Level Recommendation	Target Date		
			Original	Revised	Revised Again
July 2018	School of Dentistry	Improve Physical Access Management	July 2019	July 2021	TBD

Report Date	Audit	Management Level Recommendations	Target Date		
			Original	Revised	Revised Again
Feb 2018	College of Humanities and Sciences	Improve Record Management Process	Dec 2018	Sep 2019	Sep 2021
Feb 2018	College of Humanities and Sciences	Perform Banner Reconciliations and Close Inactive Indexes	Dec 2018	Dec 2019	Sep 2021
July 2019	Consolidated Audit of Cardiology	Improve Records Management Process	Sept 2019	Sept 2020	Dec 2021
July 2019	Non-Research Institute and Centers	Facilitate Establishment of a Policy to Govern Non-Research ICs	Dec 2019	Dec 2020	Dec 2021

Integrity and Compliance
Board of Visitors
Annual Report

2021

Table of Contents

Introduction

Welcome to the Annual Report of VCU's Integrity and Compliance Efforts for fiscal year (FY) 2021. Since the creation of this report in 2012, the goal has been to provide information to the Board and broader university community related to the impact of VCU's Ethics and Compliance Program.

This report is not all-inclusive, but highlights the activities of our program, which are modeled after Chapter 8 of the US Department of Justice's *Federal Sentencing Guidelines* and supported by regulatory drivers and industry best practices. Our integrity and compliance activities are geared toward maintaining a community prepared to live our values and, when necessary, identify, call out or report suspected wrongdoing and appropriately address misconduct when substantiated.

VCU's ethics and compliance program is the collective effort of the various schools and business units exercising due diligence in order to prevent and detect misconduct. Compliance is not primarily about policing a behavior. Rather, it is about understanding which requirements apply to our actions or decisions, making sure we meet or exceed those requirements, and being guided by our mission and ethical standards.

The Integrity and Compliance Office (ICO) oversees the ethics and compliance program by providing guidance, support, awareness and communications.

The **Elements**
of **Effective Ethics and Compliance Programs**

- Standards and Procedures
- Oversight
- Incentives and Discipline
- Training and Education
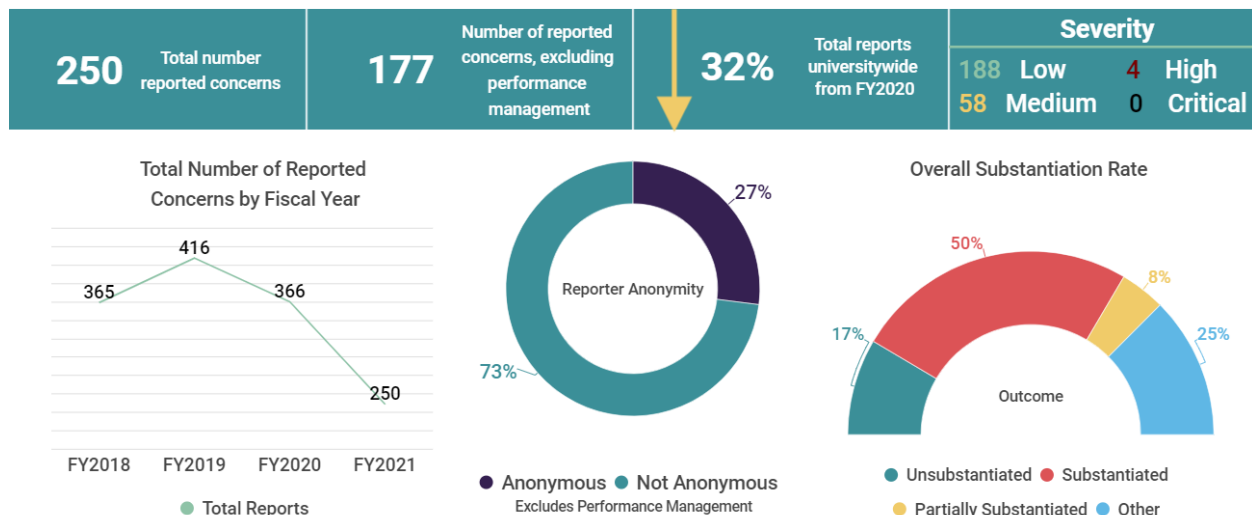- Reporting Mechanisms
- Monitoring and Auditing
- Incident Response and Continuous Improvement

Reported Concerns
Analytics & Benchmarks

Reported concerns represent allegations of misconduct or performance management matters raised by individuals and captured in a central tracking system. The ICO manages and monitors reported concerns to ensure documentation is adequate, that all matters are closed timely and that there is consistency in how the university disciplines for substantiated misconduct.

The central tracking system also provides an opportunity to analyze trends, compare VCU to benchmarks and implement policies and training to address areas of concern. This section of the annual report discusses the analysis results inclusive of all reported concerns for FY 2021. Our analysis also evaluated data exclusive of employee performance management concerns to assess whether those concerns skew metrics related to allegations of misconduct, such as sexual misconduct, misuse of resources, behavior concerns, etc.

Universitywide Reported Concerns - Employee Behavior

250	Total number reported concerns	177	Number of reported concerns, excluding performance management	32%	Total reports universitywide from FY2020	Severity			
						188 Low		4	High
						58 Medium		0	Critical

Total Number of Reported Concerns by Fiscal Year

416
365
366
250

FY2018   FY2019   FY2020   FY2021
● Total Reports

Reporter Anonymity
27%
73%
● Anonymous ● Not Anonymous
Excludes Performance Management

Overall Substantiation Rate
50%
17%
8%
25%
Outcome
● Unsubstantiated ● Substantiated
● Partially Substantiated ● Other

A few notables from the FY 2021 analysis include:

- 250 reported concerns received consistent treatment and severity ratings.
  - More often than not, reports were made directly to the appropriate office having expert staff charged with addressing the matter.
  - Matters raised through the Helpline were re-routed within one business day almost 100% of the time.

- For the second year, all substantiated allegations were responded to with some form of discipline and all discipline was documented in the central tracking system.

- The substantiation rate for reported concerns fell to 50% and to 58% when including partially substantiated outcomes. Even with this decline, VCU continues to exceed global benchmarks for substantiation rates. Exceeding substantiation rate benchmarks may indicate that employees are well informed about university expectations and when they speak up about expectations potentially not being met, they are mostly correct.

- The anonymity rate when reporting misconduct remains consistently low compared to industry peers but elevated by VCU standards. The rate of anonymous reporting has increased over the last two fiscal years and exceeds 20% for the first time since FY 2016.
  - FY 2021 rate increased to 22%, from 16% in FY 2020 and a low of 10% in FY 2019.
  - Anonymity rates of 22% for all reports, and 27% when excluding performance management issues.

The impact of COVID-19 makes drawing conclusions based on data analysis challenging due to its disruption to historical patterns and practices of misconduct. As noted in the 2020 annual report, the COVID-19 disruption marked an interesting trend nationwide in the reporting of concerns. At VCU, there was a significant reporting decrease of 32% in FY 2021. The Navex *Global 2021 Incident Management Benchmark Report* noted the first ever decrease in their annual volume benchmark and attributed "*this reversal [most likely] to the mass transition to working from home, which made many forms of non-web/hotline reporting (such as open door conversations) considerably more difficult.*" Additionally, a majority of VCU's reports result from in-person interaction that conflicts with the university's expectations of professional conduct. With a mainly remote workforce in FY 2021, the reporting decrease was expected.

Open Cases at End of Fiscal Year
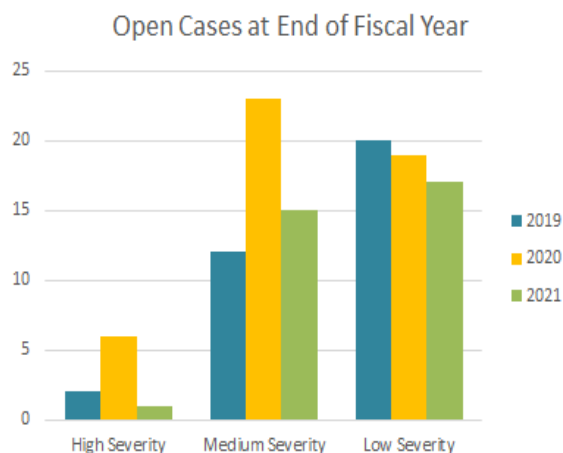
This year the university's ethics and compliance partners and the VCU Helpline received and managed 250 reports compared to 366 reports in FY 2020. Duration, or time to reach a conclusion or outcome, decreased across all units.

At the close of this year, 30 cases remained open, a decrease of 38% from 48 open cases in the prior year. The decrease in open cases may be attributable to lower report volumes, more low severity reports (75% low severity reports in FY 2021 versus 64% in FY 2020), along with streamlined communication between central offices.

While there was a decrease of 16 in the total number of reports made directly to Audit and Compliance Services (ACS), the percentage of all reports made to ACS increased to 28%, from 23% in FY 2020. This may be the quantitative result of decreased in-person communication due to a mostly remote workforce for all of FY 2021, as described in the Navex Global report; and, as such, employees were more comfortable reporting their concerns to an independent office.

Additionally, the rate of anonymous reports increased in FY 2021:
- to 22% from 16% in FY 2020
- to 27% from 21% in FY 2020 for reports excluding performance management

Global benchmark surveys remained consistent for rates of anonymous reporting. Because of the impact of COVID-19 and a mostly remote workforce, drawing conclusions on the cause of a continued rise in rates of anonymous reporting at VCU are challenging. Historically, industry analysis has pointed to decreased trust in the environment when anonymity rates rise, but more data is needed to assess the culture at VCU to determine the root cause.

Breakdown of Reports to All Trusted Advisors Based on Independence

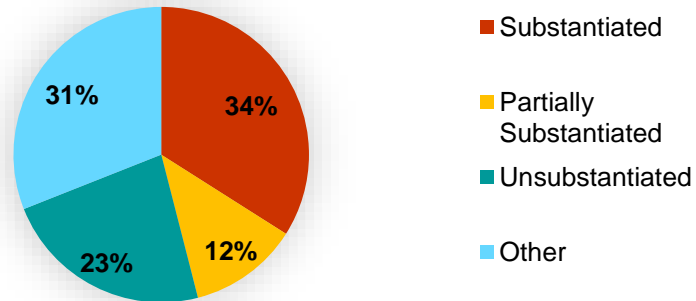| Fiscal Year	FY2018	FY2019	FY2020	FY2021
Reports to Independent Option – *ICO*	62	84	79	61
Reports to Independent Option – *Internal Audit*	11	6	6	8
Reports to Management Option – *Compliance Partners*	292	326	281	183
Total Reports	365	416	366	250
% Reported to *Audit and Compliance Services* – *as the only structurally independent option*	20%	22%	23%	28%

The substantiation rate (see Appendix A for definition), for all reports, remained consistent at 58% from 61% in the prior year. The rate equates to 46% when excluding performance management issues and more closely aligns with current national benchmarks (see table on page 7). Substantiation rates exceeding global and education industry benchmarks may indicate *"positive program communication and investigative efforts, and that organizations are continuing to receive high quality, actionable reports."*[1]

---

[1] Penman, Carrie: *2021 Incident Management Benchmark Report* Navex Global

Substantiation Rate FY21
All Reported Concerns

- Substantiated
- Partially Substantiated
- Unsubstantiated
- Other

25%
50%
17%
8%
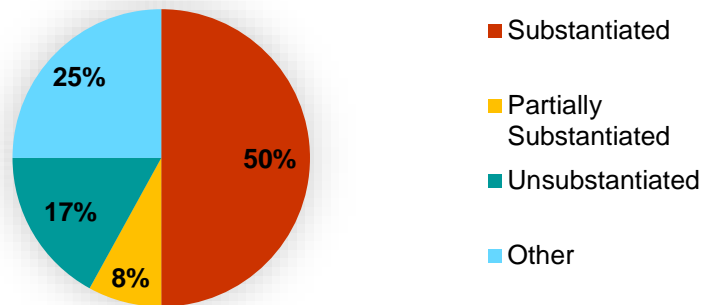
Substantiation Rate FY 2021
Excluding Performance Management

- Substantiated
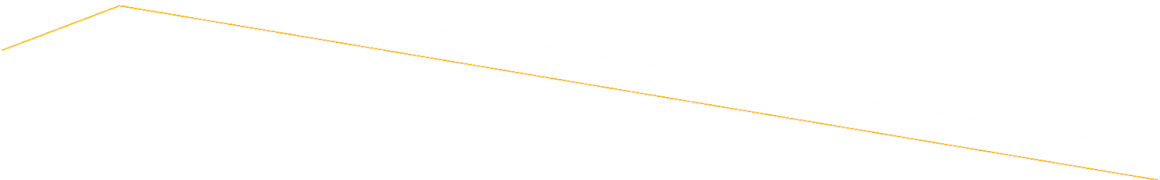- Partially Substantiated
- Unsubstantiated
- Other

31%
34%
23%
12%

Reports classified as Human Resources (HR)-related continue to represent the largest volume of reported concerns at 56%, with a 67% substantiation rate. The percentage of reports reflects a slight decrease from FY 2020 when HR-related reports comprised 63% of all reports with a 62% substantiation rate. The decrease in the proportion of HR-related reports is likely due to an increase in reports unrelated to the university (typically related to VCU Health System activities and employees), which comprised 8% of all reports in FY 2021 as compared to 2% in FY 2020. Global benchmarks also observed a decrease in the proportion of reports that were HR-related, as discussed later in this report

The HR-related substantiation rate decrease likely reflects the university's overall substantiation rate decrease. When performance management reports are excluded, 42% of reports are HR-related and 28% are Equity-related with substantiation rates of 46% and 27%, respectively.

FY 2021 TOP 10 PRIMARY ISSUE TYPES REPORTED

- Employee Relations [65]
- Ethics Violation [49]
- Discrimination based on Protected Class [42]
- Health or Safety/Security Concerns [14]
- Retaliation [12]
- NCAA Rules Violations [8]
- Waste, Misuse or Theft of Resources [8]
- Academic Concerns [7]
- Sexual Misconduct [7]
- Abuse of Power, Authority or Control [5]

Allegations classified as equity-related topics saw an increase in substantiation rate to 27% FY 2021 from 10% in FY 2020, but still consistent with the university benchmark of 25%. With large fluctuations in substantiation rates - from 42% in FY 2018 to 10% in FY 2020, establishing a reliable benchmark is challenging. Nonetheless, additional training is planned for FY 2022 to educate faculty and employees on the *Preventing and Responding to Discrimination, Title IX Sexual Harassment,* and interim *Sex-based Misconduct* policies.

The university, again as in prior years, positively exceeded global ethics and compliance industry benchmarks for per capita reports of concern as shown in the chart on page 7. This demonstrates a university environment that supports a speak-up culture and provides increased visibility of issues and events in order to identify patterns and practices of unethical conduct. Although per capita reports decreased in FY 2021 to 2.4 from 3.1 in FY 2020 report, volumes continued to exceed the benchmark for global businesses of 1.3. The ICO will continue to monitor case volumes as the university returns to an on-campus working environment to assess the impacts of COVID-19 on report volumes.

Metric	2021 Navex Global Survey	FY 2021 Convercent Benchmark	VCU Internal Benchmark	FY 2021 Data (All/Excludes Performance Management)
Cases per 100 employees	1.3(median)	Not available	3.02	2.40 (all)
Anonymous Reports	58%	55%	13%	22%/27%
Direct Contact vs Helpline Reports	48%	23%	80%	76%/68%
Substantiation Rate	43%	36%	62%	58%/48%
Most Common Allegation Type	HR – 63%	Not available	HR – 67%	HR – 56%/42%
Concerns of Retaliation	.90%	Not available	4%	5%/6%

*Benchmarking Note: Metrics collected are presented in comparison with a university benchmark for the respective metric; calculated using the average of all available data from the preceding three FY cycles not including the year of this report. Metrics are also compared to available industry benchmarks in two ways: 1.) data collected and analyzed annually by Navex Global's *2021 Risk and Compliance Incident Management Benchmark Report* and 2.) benchmark data supplied by VCU's ethics and compliance platform vendor, Convercent, using an education industry peer group.

In FY 2020, the ICO implemented standardized severity rating criteria (Appendix B) for consistent classification of reported concerns and associated analysis. Overall, the severity level decreased in FY 2021 with 25% of reports rating as medium/high/critical (32% when excluding performance management) as compared to FY 2020 with 36% of reports rating as medium/high/critical (45% when excluding performance management). The ICO will monitor this metric and establish a benchmark moving forward as we accumulate more years of data.

In FY 2021, 4 reports were rated as high severity and none rated as critical, demonstrating a decrease from FY 2020 where 13 reports were rated as high severity and one report rated as critical (50% substantiation rate). This may be an additional metric affected significantly by the remote work environment and remain an area to watch throughout FY 2022.

High Severity Concerns
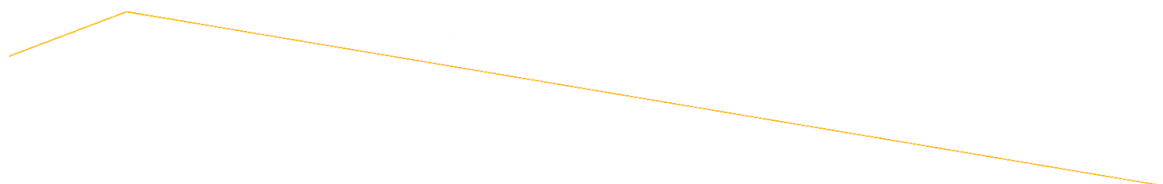
An analysis of the 4 high severity reports for FY 2021 revealed two substantiated cases (67% substantiation rate) with one case in progress at the close of the fiscal year. All matters were addressed with documented disciplinary action designed to prevent recurrence of misconduct.

4 total cases
3 closed cases
2 cases substantiated

1 outside agency responsible	1 resignation in lieu of terminstion

Substantiated Issue Types
Improper use of Intellectual Property, Copyright Violation, or Software Piracy
Health or Safety/Security Concerns
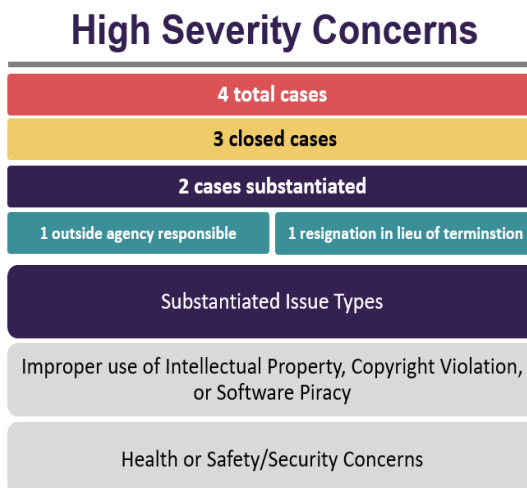
Ongoing Monitoring & Assessing Compliance Risks

Regulatory Reporting Monitoring

Despite COVID-19's disruptions, full compliance with required federal reporting to external authorities was again maintained without issue. On a quarterly basis, compliance risk owners at the senior leadership level self-attest to continued timely, accurate and complete reporting throughout the year.

Much of the regulatory reporting work this year focused on further developing the university's ability to identify regulatory commitments, both federal and state, and to indicate both internally and to the public what office or unit is responsible for those regulatory compliance activities. The ICO determined that while federal regulatory commitments were widely known, more work was required to identify the compliance and reporting requirements of the Commonwealth. Over the course of the past year, the ICO assigned, with the help of our compliance partners, risk owners to those regulations. The next phase of this project will be to confirm with our partners the responsible party for each regulation. This process will also include engaging divisional leadership so that senior leaders are aware of the regulatory responsibilities that fall within their divisions.

In this section of last year's Annual Report, we wrote about initiatives designed to notify and prevent non-compliance with newly passed state laws. This past General Assembly session was an active one. Our process of collaborating with both legal counsel and government relations to

ensure timely notifications of offices with new regulatory requirements proved successful. The ICO is in the process of partnering with several university divisions on implementing policy revisions, new reporting processes, and data revisions to comply with new laws passed by the legislature and signed by the Governor.

With a new administration in place in Washington DC, and gubernatorial elections upcoming in Virginia, the ICO will continue to monitor the ever-changing regulatory environment and, when necessary, engage our compliance partners in addressing any new risks or regulatory changes.

Lastly, compliance with § 23.1-401.1 of the Code of Virginia, *Constitutionally protected speech; policies, materials, and reports*, requires the posting and filing of an annual report as well as meeting notifications and postings for filed lawsuits. This year, like last year, required notice of one filed lawsuit alleging violations of protected speech to be provided to certain state legislators and the Governor and to be posted at www.freespeech.vcu.edu in accordance with the Code's compliance requirements. This case relates to School of the Arts, Qatar Campus, activities.

ADA DMCA OIG
USDA ITAR OSHA
OHRP EAR FDA
FERPA HIPAA ED
Patriot Act PCIDSS OMB
SEVIS NCAA HHS
Clery Act EEOC DOE
GLBA IX DOJ
FMLA EPA IRS
VAWA DOT DOL
OCR CMS Commerce

Federal Regulating Bodies and Compliance Matters

International Activities

The federal government's interest in international affairs related to universities nationwide continues. In January 2020 the Provost and Vice President of Research and Innovation convened a working group of compliance partners that undertook efforts focused on undue foreign influence. The specific topics examined by this working group were heavily based on the Association for Public and Land-Grant Universities' May 19, 2020, *Actions to Address Security Concerns about Security Threats and Undue Foreign Government Influence on Campus* and the Council on Governmental Organizations' January 14, 2020, *Framework for Review of Individual Global Engagements in Academic Research*.

In the Fall of 2020, the working group reported its recommendations to assist VCU in maintaining a strong position for compliance effectiveness and enforcement regardless of the level of scrutiny from any given federal administration at any time. In the Spring of 2021, the Provost and Vice President of Research and Innovation accepted the working group's recommendations and authorized them to proceed with strategies and engagements to implement their recommendations.

Conflict of Interest and Commitment & Annual Compliance Training

The ICO collaborated with the School of Education to pilot the use of a centralized electronic conflicts of interest disclosure questionnaire for all of its faculty and staff. While those in a position of trust at VCU have historically completed the questionnaire, it has benefits that extend to all business areas within the university by contributing to a workplace free from unmitigated conflict, bias or improper influence. It also offers visibility of those disclosures to leaders that manage faculty and staff.

The pilot's success has led to continued initiatives in FY 2022 to expand the pilot to other schools and departments. In preparation for a future campus wide rollout, the ICO worked this past year to create disclosure training for employees as well as disclosure review training for managers.

Operational units assessing highly specific disclosures for conflict management are Athletics and Research. The Athletics NCAA-required processes have been reconciled into the universitywide electronic solution for centralized coordination and independent oversight of required reporting. Research-specific practices have been intact and operational by research expertise for more than a decade.
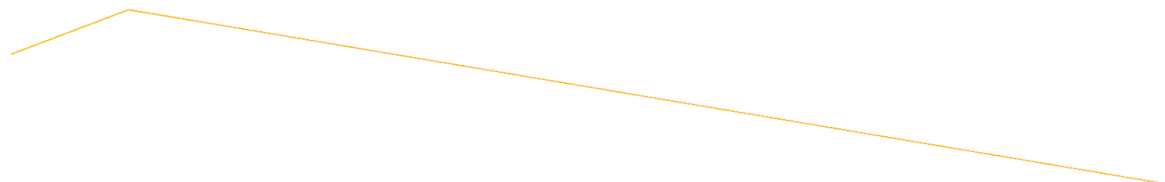
This past fiscal year, matters were as expected with no atypical occurrences or notable changes for both operational units.

Universitywide Policies

Despite the challenges presented by the COVID-19 pandemic, the policy program continued its role in engaging and supporting the university community in the policy development, review, and approval process. The ICO is increasingly proactive in seeking out policy partners to begin the policy review process, contacting policy owners six months before a policy's review due date and maintaining that contact up to the due date and beyond if necessary. This resulted in a record number of policies that were created, reviewed, or retired in FY 2021.

Although currently 34% of all policies remain out of date, this is a 6% improvement over last year. It is important to make two distinctions regarding this statistic:

- It includes outdated policies that are currently in the review/revision process.
- One division is responsible for over half of the outdated policies. Staff and leadership from both the Integrity & Compliance Office and Audit & Compliance Services are actively engaging that division in discussions regarding policy revisions and possible policy consolidation.

POLICY MANAGEMENT

FY 2021

. . . .

164
total policies

. . . .

12 Governance phase completed

55 Past due or under review

12 New or substantively revised

24 Minor revisions made

While our policy development process is designed to be deliberative, we also have the capacity to be nimble and to quickly respond to changing circumstances both at VCU and in the regulatory context. During the past year, we partnered with the Division ofStudent Affairs and Equity & Access Services to make critical updates to key policies impacting, in the Student Affairs context, alcohol and other drugs, and in the Equity and Access Services context, disability accommodations for all constituencies of the university. These interim policies will be in effect for a year, allowing the final draft policies to go through the shared governance process in order to become permanent.

To help our university partners as well as our staff better understand the correlation between policy and risk the ICO developed a rubric to assess the risk levels of university policies. This rubric takes into account, among other factors: whether the policy is mandated by an outside source such as the federal or state government or the university's accreditors, whether the policy supports the university's strategic priorities, and whether a policy is overdue for revision. Based on these factors and others, the policy is assigned a risk score. Currently 13% of policies fall into the high-risk category and 30% fall into the medium-risk category. The rest represent low or no risk.

Virginia's Freedom of Information Act (FOIA)

Over the last few years, implementing FOIA training has resulted in a more educated population with better-coordinated institutional responses. As a public state agency, VCU has five days to respond to all FOIA requests. Responses have reached a maturity point wherein disclosing necessary information with minimal redactions helps fortify VCU's commitment to transparency in all dealings

This year saw an 35% increase in requests, most likely attributable to interest in VCU's COVID-19 response, including decisions concerning employee and student public safety measures, course offerings, distribution of HEERF funds and other financial

35% FOIA Requests
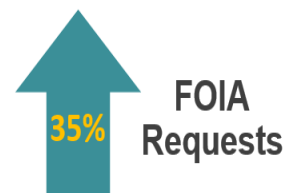
assistance and required testing of student athletes. Additionally, there was significant local and national interest in information on fraternity and sorority life.
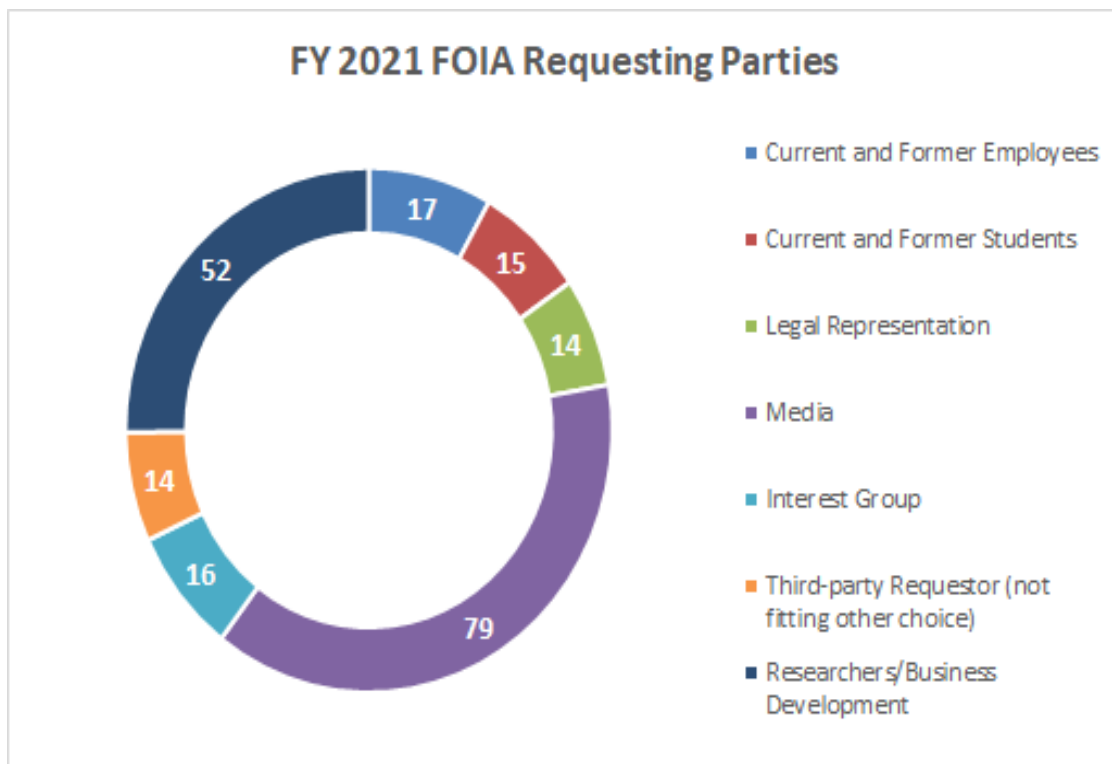

FY 2021 saw a 30% increase in the number of requests from media, continuing a trend from FY 2019 and FY 2020. Main topics of interest were substantial, both in terms of their complexity and the public's interest in how VCU engages with or impacts the community in Richmond and beyond.

Topics included:
- Student debt collection practices
- COVID-19 plans/operational decisions
- Student death and subsequent requests related to incidents of hazing
- Costs of COVID testing for men's and women's basketball teams
- Copies of coaches' employment and men's basketball game contracts

Continued interest is anticipated in the following areas for FY 2022: the university's COVID response; fraternity and sorority life; and, increased use of FOIA by the media.
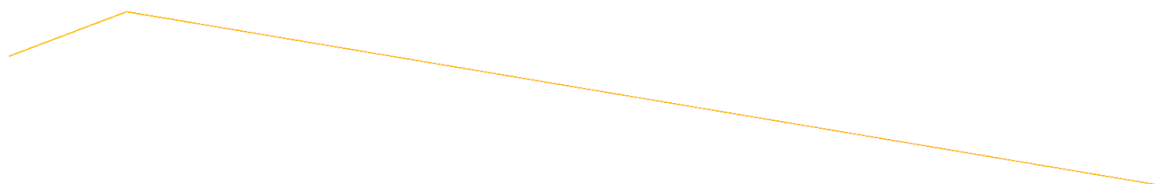
Effectiveness Statement

The goal of VCU's compliance program is to demonstrate effectiveness in order to receive favorable interactions or a reduction in culpability score for VCU should misconduct be found. Overall, the program continues to operate from a position of strength in:

- supporting the creation and maintenance of clear expectations;
- supplying reporting mechanisms to identify perceived or actual misconduct;
- identifying risks through regular meetings with compliance partners;
- ensuring resources are dedicated to assist with appropriate responses to misconduct with an aim to prevent recurrence when identified; and,
- reporting to leadership and the Board of Visitors on matters of concern.

Additionally, the network of trusted advisors, known as compliance partners, and the continued commitment by Compliance Advisory Committee members adds to the strength of VCU's compliance effectiveness.

The role of management to enforce expectations and set a tone of high integrity in all operations remains critical because these efforts support VCU in upholding the public's trust. Industry benchmarks continue to identify that change increases pressure that can manifest into misconduct. Regular reminders and messaging from leaders, the ICO, and managers about our values and Code of Conduct continue to be among our best defenses to reduce the likelihood of misconduct.

Apart from the challenges organizations of similar scope and complexity experience, (generally relating to communication, documentation and accountability in roles and responsibilities) no newly discovered patterns or practices of systemic misconduct have been identified this fiscal year. However, further progress of ethics and compliance initiatives designed to further mature our program continue to be impacted by resource constraints resulting from staff turnover and competing priorities in other areas, such as VCU's COVID-19 response.
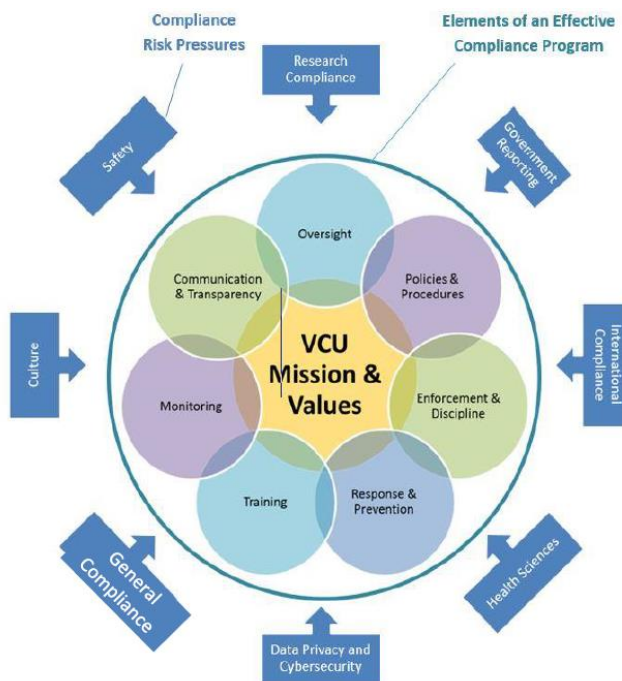
Appendix A

Definitions for Report Outcome Classification

A report is classified as **Substantiated** when, after inquiry or investigation, violations of expectations, policy, regulation, or law are found. When this occurs, the ICO is available to consult in the development of a corrective action plan for appropriate parties.

A report is classified as **Partially Substantiated** when, after inquiry or investigation, a violation of expectations, policy, regulation, or law is found but other allegations—or elements of an allegation— contained in the report were unsubstantiated. When this occurs, the ICO is available to consult in the development of a corrective action plan for appropriate parties.

A report is classified as **Unsubstantiated** when, after inquiry or investigation, no violations of expectations, policy, regulation, or law exist.

Reports that contain general questions rather than concerns or specific allegations; are not related to current VCU employees or during employment with VCU; or include allegations later withdrawn by the reporter and ICO determines that no further investigation is necessary are classified as **Other**.

Reports that contain insufficient information to proceed with additional inquiry or investigation are classified as **Not Enough Information**.

Appendix B

Severity Criteria

Criteria used to classify the severity of misconduct allegations (referred to throughout as "reported concerns")

Critical

- Potential financial impact of $500,000+
- Repeated nonconsensual sexual contact
- Repeated abusive lack of self-control (physical or verbal)
- Recurrence of high severity offenses after formal warnings or other disciplinary action taken
- Recurrence of ineffective execution of corrective action plan by Management or Leadership for high severity offenses

High

- Harm to others, including threat of harm
- Nonconsensual sexual contact
- Potential financial impact of $50,000 - $500,000
- Repeated significant noncompliance with state or federal regulations, or accreditation standard
- Repeated significant conflict of interest concern
- Abusive lack of self-control (physical or verbal)
- Repeated abdication of job duties by management or leadership positions
- Ineffective execution of corrective action plan by Management or Leadership
- Recurrence of medium severity offenses after formal warnings or other disciplinary action taken
- Recurrence of ineffective execution of corrective action plan by Management or Leadership for medium severity offenses

Medium

- Senior Leadership as subject
- External Agency Notice
- Retaliation
- Abuse of Power
- Significant or repeated-minor noncompliance with state or federal regulations, or accreditation standard
- Significant or repeated-minor conflict of interest concern
- Raised concern internally first and was not resolved
- Subject had same or similar concerns reported previously
- Multiple reports about the same issue
- Related to law enforcement personnel conduct
- Significant or repeated safety concerns
- Sexual misconduct (not including nonconsensual contact)
- Potential financial impact of $5,000 - $50,000
- Recurrence of low severity offenses after formal warnings or other disciplinary action taken
- Recurrence of ineffective execution of corrective action plan by Management or Leadership for low severity offenses

Low

- Performance management concerns
- Minor noncompliance with state or federal regulations, or accreditation standard
- Minor safety concern
- Minor conduct issues (unprofessional or uncivil behavior/comments)
- Minor conflict of interest concern

Appendix C

Descriptions for Interest Disclosure Types

Athletically-Related Outside Income and Benefits: Includes income and benefits from sources outside the institution; the use, directly or by implications, or the institution's name or logo in the endorsement of commercial products or services for personal gain; or outside compensation or gratuities from athletic shoe, apparel or equipment manufacturers in exchange for use of such merchandise during practice or competition.

Gifts or Services Given or Donated: VCU employee (either personally or in their professional capacity at VCU) gave a gift that might reasonably be perceived as influencing or having the potential of influencing workplace decisions/actions. This includes any entity that conducts business or wishes to conduct business with the university, students/postdocs or employees. This does not include rewards or prizes for random drawings. Gifts and entertainment include anything of monetary value, such as discounts, travel expenses, loans, cash, services, transportation, tickets and gift certificates/cards, which have an individual market value of $20 or more or a cumulative market value of $100 or more over a 12 month period.

Gifts or Services Received: VCU employee accepted gift(s) in their personal or professional capacity that might reasonably be regarded as influencing or having the potential of influencing decision/actions at VCU. This includes any entity that conducts business or wishes to conduct business with the university, job candidate, students or representative of a student (e.g., parent, guardian, etc.). This does not include rewards or prizes for random drawings. Gifts and entertainment include anything of monetary value, such as meals, discounts, travel expenses, lodging, loans, cash, services, transportation, tickets and gift certificates/cards - which have an individual market value of $20 or more or a cumulative market value of $100 or more over a 12 month period.

Outside Activity: VCU employee is an employee, owner, director, officer, partner, contractor to, or agent of any other organization/entity outside of VCU. This also includes serving on a board of directors, advisory board, trade association or industry group, and arrangements to provide outside services (e.g., consulting and paid speaking engagements). Subcategories: second job; side business; freelance work/consulting; service activity; other.

Outside Financial Interest: VCU employee has a financial interest with any entity that conducts business with VCU or could possibly be perceived as influencing their university decisions. This includes direct financial interests not previously disclosed as an Outside Activity such as ownership, real estate/property, intellectual property/royalties, stocks/bonds, or equity (regardless

of business value), and indirect financial interests such as reciprocal relationships or arrangements.

Personal Services: VCU employee has utilized university employees or students/postdocs to perform any personal services for them, whether paid or unpaid (e.g., house/pet sitting, yard work, etc.)

Potential Conflicts of Interest – Immediate Family: VCU employee has someone in their immediate family involved in activities, or has relationships that could possibly be perceived as a conflict of interest with respect to VCU. Immediate family member means spouse or domestic partner, parent, child, sibling, aunt/uncle, niece/nephew, grandparent or grandchild. For example, they work for, or are associated with an organization that does business with the university; they have a relationship with a board member or senior leader at VCU or someone in your reporting chain.

Relationship within our organization: VCU employee has a personal, family, social, or business relationship with a student/postdoc or other VCU employee with whom they have oversight of – or perceived influence over – their employment or academic activities. Examples of employment activities include performance evaluations, salary decisions, promotion, work assignments, etc. Academic activities include admissions, grades, coursework, registration/overrides, etc.

Other Potential Conflicts of Interest: VCU employee is involved in any other activity that could possibly be perceived to influence their university decisions or detract from their university responsibilities. Consider the various activities and interests that they, their family members and close friends are involved in, and whether they could be reasonably viewed by others to unfairly influence your decision-making in the workplace. If in doubt, this disclosure process can provide an objective review to identify competing interests and guidance on how to properly manage any identified conflicts. If the situation is not a conflict of interest or commitment, this disclosure can help remove the potential perception of wrongdoing. Remember, actual or perceived conflicts of interests and commitments have the potential to undermine our credibility and the trust of others. Having a conflict is not necessarily wrong or bad, but not disclosing the situation can result in wrongdoing or the perception of wrongdoing.
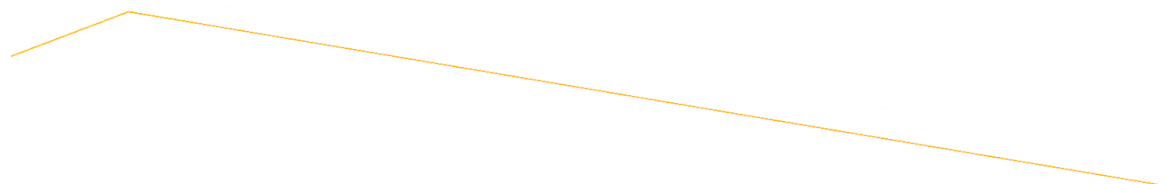
Appendix D

Prior FY Initiatives Progress Report

Maintenance of VCU's Ethics and Compliance Program is substantively driven by the Federal Sentencing Commission's Sentencing Guidelines, Chapter 8, which provide for the basic and necessary minimum elements of an effective Ethics and Compliance Program; it is also driven by our own mission and values reflected in our Code of Conduct and university policies; sound business sense; risk acceptance and the needs of the organization. Continually playing an integral role in setting and upholding accountability within VCU's culture and overall risk mitigation processes, the resulting initiatives were set for FY21 in May of 2020 and this report provides a final status update **as of June 30, 2021.**

Initiatives herein are designed to reduce potential wrongdoing, increase the likelihood that when wrongdoing does occur it will be made known to management and increase the likelihood that VCU will responsibly handle suspected and substantiated wrongdoing, thus preserving the public's trust and the integrity and reputation of a responsible university.

Selected projects reflect a balancing of capacity, prioritization and where a devotion of additional resources is necessary to address, or continue, assurance of compliance requirements; ethical behaviors; and overall institutional integrity. Most of the topics below traverse multiple years due to the scope and size of the efforts. Year over year progress is demonstrated with a stoplight coloring indicator and any obstacles to these plans are shared with the Audit, Integrity and Compliance Committee of the Board of Visitors as the university's governing authority.

Note: These activities reflect known data points and information established from the collaborative relationships our ethics and compliance partners and other key stakeholders. Those items marked ongoing or holding, are a direct result of a vacancy absorbed turned into a universitywide hiring freeze or the adjustments required as a direct effect from the COVID-19 disruption.

Green: Complete or to be complete within FY
Yellow: Significant progress continues but not complete within FY
Red: No progress of significance or on hold due to unexpected circumstances

FY 2021 Initiatives:

Continue providing the BOV and Senior Leadership (as applicable) timely reports of successes; efficiencies; challenges; obstacles; and violations of ethics and compliance matters. Consider formal resolutions for program requirements and organizational need.

More specifically focused on:

Effectiveness Review of Ethics and Compliance Program

- 🟨 Maintain progression and updates to response plan from Ethisphere's findings and recommendations – includes cooperation and collaboration with compliance partners and key stakeholders
- 🟥 Complete self-assessment and results comparison with the national Ethics and Compliance Initiative cohort and industry leading practices

Integrity and Compliance Office Reporting to BOV Audit, Integrity and Compliance Committee

- 🟩 Bolster issues and events reporting with enhanced analytics insights and benchmarking from central case management platform; solicit and incorporate stakeholder input; establish frequency of reports
- 🟨 Finalize program insights reports and the dashboard's format - includes ethics and compliance metrics informing maturity ratings; solicit input; and establish risk appetite – working toward standardized quarterly or biennial reporting

COI Program Enhancement - Enhancements are needed regarding policy approval, consistent use of electronic solution for disclosures and management plans; in particular, compliance with more than 10 federal regulations, accreditation standards, and best practices in organizational governance, risk, and ethics and compliance industries. Utilization of an enhanced process of interest reporting contributes to both the Board and the departmental charter compliance by providing required assurances to the Audit, Integrity and Compliance Committee of the BOV.

- 🟨 Fully implement policy and software solution for disclosing interests and managing conflicts
- 🟨 Creation and execution of training to topic, policy requirements, electronic system and role
    - School and unit level employees reviewing, clearing and mitigating conflicts
    - Institutional Ethics and Compliance Committee Members
- 🟩 Continue guidance responding to disclosures and proactive avoidance inquiries or response to disclosed institutional conflicts and conflicts of commitment - includes role based training
- 🟩 Continue as Commonwealth's liaison for mandated state disclosures and training

Employee Ethics and Compliance Training and Accountability

- Execute training to broader audience and oversee functional or operational compliance program plan development by applicable compliance partners
- Provide risk identification and assessment training to applicable compliance partners
    - Establish accountability process for assessment results and integration into ERM
- Integrate ethics related actions and other positive ethics incentives into performance evaluations
- Execute annual employee compliance training – includes reflexive content based on initial assessment of knowledge base accompanied by role and duration of employment
- Develop and conduct role-based training for managers: Anti-retaliation
- Continue in person participation in new employee orientations and new chair training / development; online content delivery; and other custom requests to individual units

Gap and Risk Assessment Activities & Response

- Continue oversight of case handling for all reported concerns for efficient, consistent and coordinated institution response
- Continue quarterly oversight monitoring for timely compliance reporting through responsible parties outlined in Compliance Calendar: Federal Regulatory Reporting Requirements
- Support unique compliance needs in the university's areas of international activity, health care activity; and other elevated risks - reinforced with policy creation and revision
- Formalize internal workplace investigation standards through policy approval
- Identify risk owners for enhancing third party programs (volunteers, visiting scholars, vendors, etc…) - explore decentralized risk and accountability model and centralization feasibility for identification; screening; tracking and reporting
- Reconstitute Compliance Advisory Committee and begin Senior Leadership Level Committee to review and respond to advanced ethics and compliance metrics geared toward effectiveness and risk ownership, management and intelligence based on established maturity model ratings

Government Relations Non-Routine Visits

- Continue independent oversight and support to university community in preparation for, and in response to, regulator inquiries, reviews and investigations

**Policy Program – for all universitywide policies**

- Create methodology to measure and manage effectiveness of existing policies
- Recommend and oversee policy development to address identified risks
- Continue universitywide quarterly updates: seminal policy changes, reminders and tips for compliance

- Continue gap assessment based on size, scope and complexity of university, and industry trends and standards
- Continue support in policy creation, drafting, revision and required governance processes

Continued Participation and Resource Support and Guidance to various ethics and compliance- oriented groups and committees

- National Prominence - Contributing member for think tank partnership with Ethisphere to create Higher Ed cohort data comparisons of plans; and contributing member in national university compliance leaders group
- State Prominence – Ethics and compliance work in Higher Education cohorts: contributing member to state-specific cohort; founding member for public school-specific cohort
- Continue serving as the second line of defense support to all operations units with VCU
- Work toward being utilized as a strategic business partner
- Participation and leadership provided to over 15 universitywide committees and taskforces
- Active memberships and participation with external groups – Society of Corporate Compliance and Ethics – Higher Education Section and General Section; Ethics and Compliance Initiative; Association of College and University Policy Administrators
- The commitment to internal staff development remains as well as support for maintaining current industry certifications
- Internal workplace investigations
  - Oversight of alleged misconduct reports / non-compliance Issues
  - Conduct investigations when suspected patterns or practices of misconduct, non-compliance, or unduly sensitive issues arise
- State Regulatory Coordinator (liaison to Commonwealth for VCU)
- Agency Coordinator for Conflict of Interest Disclosures to the Commonwealth
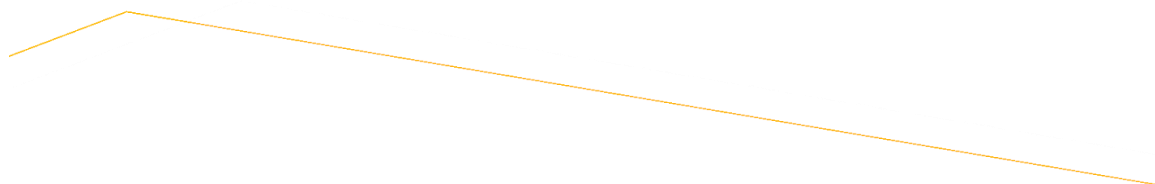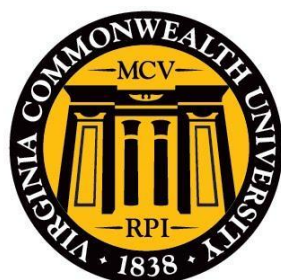
Outside Professional Activity

Final Report
June 9, 2021

Audit and Compliance Services

Overview

VCU faculty are recognized as professionals with responsibilities and benefits that come with their position. They are expected and encouraged to expand their capabilities on a regular basis, share their knowledge with their colleagues, and make their knowledge and skills accessible to the general public. The *Outside Professional Activity & Employment Policy, Research & Continuing Education (Faculty Specific)* (policy) exists to provide guidance on the appropriate procedures to follow when disclosing these activities and to ensure that faculty understand that their first allegiance is to the university and to aid in identifying potential conflicts of interest or commitment. The policy identifies outside professional activity (OPA) as professional leadership activities; outside consulting; teaching in other academic institutions; scholarly or creative writing; other individual creative endeavors; and outside professional practice and recognizes that "it is acceptable for faculty members to receive extra compensation for [outside] work … [as long as it] does not interfere with their university duties."

This policy and faculty compliance with it is important because it ensures VCU knows when faculty may perform work that creates a conflict of interest, allowing for management of that conflict. In addition, it helps VCU identify conflicts of commitment that may occur when faculty are not accessible to their students, which may directly affect student success.

Reporting OPA

Faculty members that intend to participate in outside professional activities are required to submit a permission request to their chair and dean on a CP-1 form (request form) prior to participating in the activity. The request form serves as a tool to identify potential conflicts of interest or commitment. In addition to OPA, faculty are to record their continuing education on the request form. At the end of the contractual year, the faculty member is required to complete a CP-2 form (report form) to report all OPA. Report forms are reviewed by the chairs or deans, and in some academic units, included within the faculty's performance evaluation.

Academic units use either an electronic or hard copy method of reporting OPA.
- In 2007 the university developed a homegrown system (OPA system) where faculty are to enter both request and report form information and reviewers, approvers and other office personnel can access the results through that system's reporting capabilities. Web Services maintains university administrator responsibility.
- Faculty may also report OPA to their chairs or deans via paper forms.

OPA information is also recorded in a financial interest report within the Activity and Interest Reporting System (AIRS). Faculty performing research would be the primary users of a financial interest report. AIRS has some enhanced features such as email reminders to users to complete their financial interest report and notification to those who have not completed related training after three years. Faculty not active in research do not need to complete a financial interest report; however those that are active researchers need to dually report (in either the OPA system or on paper) and on a financial interest report.

As of October 2020, the School of Education successfully piloted the recording of OPA in Convercent, an already active university system administered by the Integrity and Compliance

Office. At the time of this report, Convercent includes conflicts of interest, conflicts of commitment, and financial interests for non-research university personnel.

The chart below depicts the differing methods of reporting OPA in 18 academic units.

Chart 1
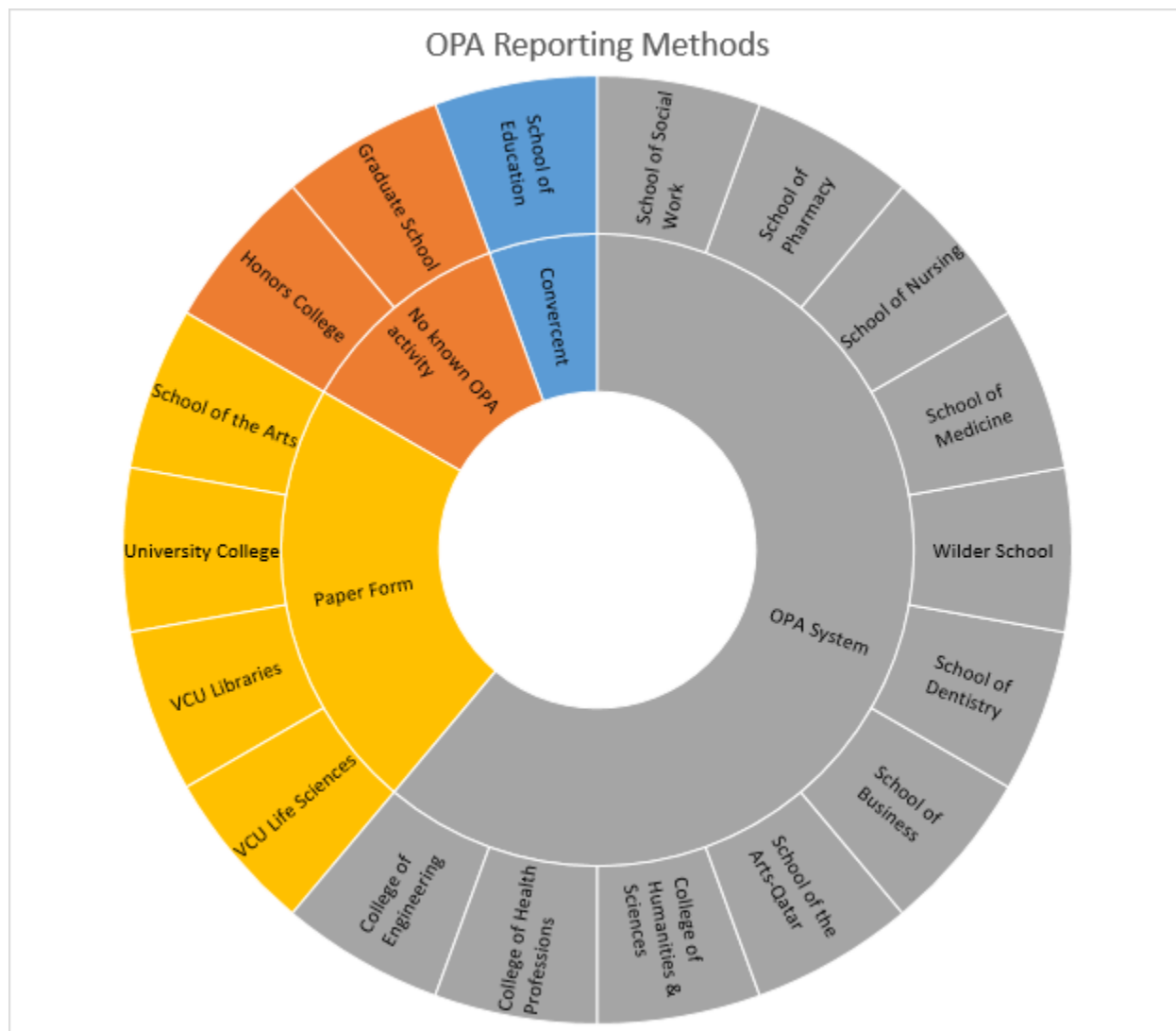
Source: Interviews with academic units

Purpose

The objectives of the review were to determine whether the:
- OPA policy was adequate
- OPA reporting process was adequate and working as intended

Scope and Review Procedures

Our scope of the outside professional activity process included reporting, training and monitoring for this function on both campuses.

Our procedures included:
- Research of peer institution OPA policies
- Inquiry with various academic unit representatives regarding their OPA process
- Analysis of a survey (administered in March 2019) by the Integrity and Compliance Office and discussions with members of that office
- Identification of academic units where OPA issues were identified during fiscal years 2018 and 2019 from the Integrity and Compliance Office which was used to make faculty test selections
- Comparison of select faculty financial interest reports (provided by the Office of Research Integrity and Ethics) and OPA system reports for fiscal year 2020

Summary of Major Business Issues and Management's Action Plans

Enhance Electronic Reporting of OPA and Require Its Usage

The OPA system is outdated and does not provide effective reporting. In addition, its information is duplicated in the AIRS financial interest report. Due to the inconsistencies below, academic unit administrators may not be aware that their faculty are participating in OPA or, if they are aware, to what extent. Examples of issues identified were:
- The OPA system's activities summary report does not identify whether the data was sourced from the request form or the report form.
    - Web Services indicated that enhancement to this report would require a major system update and might not be possible in the near future due to other priorities.
    - Faculty are allowed to complete a report form without previously completing a request form and a request form can be completed without notice to the reviewer that a year-end report form has not been completed. This inconsistency of form completion does not encourage pre-approvals of activity and enables lack of documented follow-up as to whether the activity actually took place.
- The OPA system does not have a control to ensure that faculty report OPA in the appropriate year.
- The OPA system's electronic forms were not consistent with the policy's reference to the hard copy forms.
- The OPA system allows the academic units to determine whether or not they enable the recording of OPA compensation on the request form yet did not require the actual compensation received to be recorded in a field on the report form.

The university should consider using one central reporting system for all faculty, such as the Convercent reporting system that the School of Education successfully piloted. Potential benefits of a central reporting system may:

- Promote a more efficient and consistent reporting process
- Aid in easier identification and management of potential conflicts of interest and conflicts of commitment
- Allow more effective monitoring by chairs and deans
- Generate automatic reminders on reporting and approving deadlines for faculty and reviewers

If the university decides to continue with the current OPA system, the following enhancements should be made to include:
- Reporting requirements that comply with an updated policy
- Clearly defined reports that are accurate and more robust to assist its users in monitoring OPA
- Automatic reminders such as reporting and approving deadlines
- A control to ensure faculty report OPA in the correct year

Management's Action Plan - Concur
Summary -
- *Discuss/review use of Convercent as a reporting tool for OPA for all units*
  - *Discuss with School of Education their experience and process for converting to Convercent*
  - *Discuss with VCU Technology Services and any other offices necessary to help with conversion*
  - *Discuss with the Provost and the Senior Vice President for Health Sciences*
- *Determine viability of moving OPA for all VCU units into Convercent*
- *If viable, develop a transition plan to make this happen*
- *Present Plan to Provost, Deans, and Senior Leadership for approval by Spring 2022*
- *Implement plan by July 1, 2022 (start of FY23)*

Responsible parties -
- *Office of Faculty Affairs*
  - *Whitney Brown - Faculty Recruitment and HR Administrator*
  - *Jess Hill - Executive Director of Faculty Human Resources (eff. July 6, 2021)*
  - *Tim Davey - Vice Provost for Faculty Affairs*

Completion timeline -
- *Review to be completed by November 2021*
- *Plan to be developed by February 2022*
- *Approval by June 2022*
- *Implementation by July 2022*

Update the OPA Policy

Faculty Affairs in the Provost Office is responsible for VCU's OPA policy. Our detailed review noted the policy has several discrepancies, inconsistencies, and does not provide clear guidance on how to report OPA. To illustrate, the policy:

- Has not been updated since 1983 even though university policy requires policy owners to review policies at least every three years and update as necessary.
- Contradicts itself in regards to year end reporting (one section states "in all cases … activities must be reported" whereas another section limits the statement to "faculty … who have … extra compensation must report")
- Was not clear on the time limit for OPA. For faculty receiving extra compensation for OPA, the policy addressed a time limit not to exceed an average of one day per calendar week during the period of a faculty member's contractual obligation to the university. However, it did not address the university's expectations when faculty are not compensated for OPA
- Is unclear as to whether compensation from OPA is required to be reported and does not provide a field for this information in its hard copy CP policy link (whereas the online OPA system does allow for this data to be recorded)
- Does not identify signature fields for faculty as preparer on the hard copy request form or reviewer as approver on the hard copy report form
- Does not take into consideration outside professional activities of other employee classifications. One academic unit inquired about reporting for university and academic professionals in their area that performed outside consulting activities.
- Does not stipulate that periodic central monitoring will occur at the Provost and Senior Vice President for Health Sciences (SVP of Health Sciences) offices which further allows for inconsistencies to occur across the university

Faculty Affairs in the Provost Office should coordinate its effort with SVP for Health Sciences Office and collectively review and update the policy to ensure that it meets the needs for the entire university. This collective review should include evaluating the implementation of a central monitoring effort within both respective governance areas to ensure that academic units are held accountable in their compliance with this policy. When updating the policy, consideration should be given towards requiring all faculty (including university and academic professionals, if applicable) communicate that they do not they have OPA in a given year to assist in having annual documented assurance on file as to their interests and commitments.

Management's Action Plan - Concur

Summary -

- *Review current policy and concerns expressed by Audit & Compliance*
  - *Office of Faculty Affairs to discuss policy with Office of the Sr. VP for Health Sciences HR and work to build consistency across campuses*
  - *Modify/edit policy as needed and/or recommended by Audit and Compliance*
  - *Present recommended changes to the Provost and the Sr. VP for Health Sciences*
  - *Possibly present recommended changes to Council of Deans/Faculty Senate*
- *Formally submit changes through the policy review/approval process.*

- *Intent to have new policy in place by start of FY23 (i.e. July 2022)*

Responsible parties -
- *Office of Faculty Affairs*
  - *Whitney Brown - Faculty Recruitment and HR Administrator*
  - *Jess Hill - Executive Director of Faculty Human Resources (eff. July 6, 2021)*
  - *Tim Davey - Vice Provost for Faculty Affairs*
  - *Gypsy Denzine - Senior Vice Provost for Faculty Affairs*

Completion timeline -
- *Review to be completed by November 2021*
- *Submit policy changes by January 2022*
- *Implementation by July 2022*

Require OPA Training

The university does not require training on the OPA policy. In our interviews with academic units, we received statements that the policy is confusing and faculty reporting requirements are unclear. According to policy, faculty are required to complete request and report forms when they participate in outside activities; however, the lack of required training may result in faculty non-compliance. Omission of OPA information potentially places the university at risk for conflict of interest or commitment. During our testing, we identified:

- A research faculty member that completed a request form for fiscal year 2020 indicating that they plan to receive $15,500 as compensation for OPA; however, the financial interest report for this faculty member disclosed OPA resulting in compensation of approximately $108,000 for the same time period. This faculty member did not complete a report form when the faculty clearly completed OPA.
- Nine additional research faculty that reported OPA on their financial interest form, did not report any activity on their request or report forms.
- A faculty member who was not required to complete a financial interest report but did have reportable OPA, did not report on a request or report form as required by the policy.

At a minimum, the Provost's Office and the SVP for Health Sciences Office should collaborate to provide training for academic unit administrators, and ideally for all faculty. Providing training as part of onboarding and beginning of semester meetings could enhance everyone's understanding of the policy requirements and will help to promote compliance.

Management's Action Plan - Concur

Summary -
- *Plan for potential training(s) of new/updated OPA policy and reporting processes (Convercent)*
  - *Develop Training module(s)*
  - *Present training to Administrators and HRPs*

Responsible parties -
- *Office of Faculty Affairs*
  - *Whitney Brown - Faculty Recruitment and HR Administrator*

    ○ *Jess Hill - Executive Director of Faculty Human Resources (eff. July 6, 2021)*
    ○ *Tim Davey - Vice Provost for Faculty Affairs*
    ○ *Gypsy Denzine - Senior Vice Provost for Faculty Affairs*

Completion timeline -
- *Review to be completed by November 2021*
- *Conduct training during the Spring 2022 semester*
- *Implementation by July 2022*

Conclusion

In our opinion, based on the results of our review, the OPA policy was not adequate and the reporting process was not adequate nor working as intended.

Prior to releasing this report in final form, the draft report was reviewed by, and management's action plans were provided or approved by, the following officials:

Gypsy Denzine	Senior Vice Provost for Faculty Affairs
Timothy Davey	Vice Provost for Faculty Affairs
Jessica Hill	Executive Director of Human Resources, Office of the Sr. Vice President for Health Sciences
Gail Hackett	Provost
Arthur Kellerman	Senior Vice President, VCU Health Sciences and Chief Executive Office, VCU Health System

Our engagement was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* and included a compliance review and such procedures as we considered necessary in the circumstances.

Karen K. Helderman

Executive Director
Audit and Compliance Services

RealSource Supplier Management and Purchasing/Payments

Final Report
August 10, 2021

Audit and Compliance Services

Overview

RealSource, a product of Jaggaer eProcurement, is VCU's electronic tool for supplier management, purchasing/payments, contract management, and goods and services sourcing. In fiscal year 2021, VCU's Purchasing Department (Purchasing) processed 80,427 invoices with 19,791 vendors in the amount of $321M through RealSource. They also processed 36,861 purchase orders, 4,477 of which remain open. Procurement Services employs 32 individuals in the areas of Purchasing, Contracts, Payments and RealSource Operations.

Sole Source and Emergency Purchasing

Procurement stipulates conditions for purchases from a sole source when requesters provide documented sufficient justification. A sole source documentation form indicating the end user, the date, product or service requested, and unique features necessary to meet the specific requirements must support purchases over $10,000 from a sole source. It must also show market research the department performed in searching for those requirements, and why it is available from only one source. Emergency purchases over $10,000 must be accompanied by a written memo stating an urgent need that demands immediate action and reason for selection of the provider.

In fiscal year 2021, Procurement approved 170 sole source purchase orders over $10,000 totaling $15 million, and nine emergency purchase orders over $10,000 totaling $1.3 million.

Open Purchase Orders

To purchase goods and services, departments initiate procurement requests which RealSource routes to approvers for review and approval. Upon approval, RealSource creates purchase orders and pushes them to Banner, and from Banner to eVA (Virginia's Electronic Procurement System). Purchase orders remain open until departments either receive all procured items and pay all related invoices or cancel the purchase orders in RealSource. Purchase orders that remain open in RealSource are presumed to be active and their balances are reported as encumbrances against departments' budgets in the financial accounting system (Banner) unless departments liquidate them in Banner.

Vendor Verification

As departments request additions of new vendors to RealSource, several verification points help provide assurance that vendors are not on disallowed lists. RealSource automatically checks the Office of Foreign Assets Control site for prohibited vendors based on US foreign policy and national security goals. In addition, Vendor Create, a group within the Payments department, verifies that vendors are not debarred for activities such as breach of contracts, falsifying manufacturer's specifications to secure a contract, or conviction of criminal offenses involving public contracting. Vendor Create uses Visual Compliance, an online search engine, to search for debarred vendors.

Purpose

The objectives of the audit were to determine whether:

- RealSource controls operate to prevent unwanted transactions, provide cost savings, secure vendor verification and payment processes, and facilitate data analysis.
- Unique payment types were made according to documented policies and procedures.

Scope and Audit Procedures

Our scope of RealSource Supplier Management and Purchasing/Payments encompassed fiscal year 2021. We included processes of RealSource operations and systems support, vendor support and payments We examined RealSource security practices, processing of purchase requests, purchase orders and payments; vendor verification practices; management of complaints of vendor nonperformance; and sole source and emergency payments processes. In addition, we reviewed the proportion of Small, Women and Minority owned business (SWaM) participation, and gained an understanding of new initiatives underway to improve purchasing volume.

Our audit procedures included:

- Interviews with the RealSource Operations Director to gain an understanding of and observe RealSource and process flows and controls
- Interviews with the Assistant Director of Payments to observe process flows and controls involved in vendor management and payment
- Analysis of RealSource data and cost savings information
- Data analytics on sole source, emergency, and SWaM purchasing
- Review of Agency Risk Management and Internal Control Standards (ARMICS) documentation
- Review of payment activities in RealSource

Conclusion

In our opinion, based on the results of our audit, RealSource controls operate to prevent unwanted transactions, provide cost savings, secure vendor verification and payment processes, and facilitate data analysis. Unique payment types were made according to documented policies and procedures.

Recommendations to strengthen RealSource Supplier Management and Purchasing/Payments operations were included in a separate report furnished to management.

Our audit of RealSource Supplier Management and Purchasing/Payments began on February 22, 2021. The first draft of this report was submitted to management on July 29, 2021.

Prior to releasing this report in final form, the draft report was reviewed by, and management's action plans were provided to or approved by, the following officials:

John McHugh   Director, Procurement Services
Brenda Mowen   Director, RealSource Operations
Patricia Perkins   Associate Vice President for Finance
Karol Kain Gray   Senior Vice President and Chief Financial Officer

Our audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* and included an evaluation of internal controls and such procedures as we considered necessary in the circumstances.

Karen K. Helderman

Executive Director
Audit and Compliance Services

Audit and Management Services
Status of Fiscal Year 2021-2022 Audit Work Plan
August 30, 2021

Area	Status
Risk-based Audits/Other Reviews	
Prior Work plan: RealSource Procurement & Payment	Completed
Prior Work plan: Outside Professional Activities	Completed
Prior Work plan: Remote Learning and Work Security	Completed
Prior Work plan: Social Media	In Progress
Prior Work plan: Identity Access Management System	In Progress
Grants & Contracts – State and Local	In Progress
School of Education Child Development Center	In Progress
Steam Plant Billing & Allocation	In Progress
HS & VCU Operations & Services Agreement	In Progress
Various Fiscal & Administrative Reviews	In Progress
COVID Data Security	In Progress
Banner Controls – AP and General Ledger	Not Started
SOC Reports - Integrated	Not Started
Unused Scholarships	Not Started
External Memorandums of Understanding	Not Started
Various Petty Cash Audits	Not Started
Third-Party Management/SOC Reports	Not Started
Physical Access Management (CBORD)	Not Started
Titanium System Review	Not Started
Maxient System Review	Not Started
Data Integrity – Database Security and Controls Review	Not Started

Audit and Management Services
Status of Fiscal Year 2021-2022 Audit Work Plan
August 30, 2021

Annual Engagements and Activities	
Annual Review of Audit Recommendations Outstanding – FY21	Completed
President's Discretionary Fund and Travel Activity Review – FY21	In Progress
VCU Police Department – Unannounced Property Inspection – Part 1	Not Started
Audit Risk Assessment – FYs23-24	Not Started
VCU Police Department – Unannounced Property Inspection – Part 2	Not Started

Special Project	Status
Continuing Projects	
State Employees Fraud, Waste, and Abuse Hotline	In Progress – 1; Closed – 0
Other Projects	
False Unemployment Claim Filings	In Progress

Board of Visitors
Audit, Integrity and Compliance Committee

September 17, 2021

ACTION ITEMS

Approval of Minutes

- Audit, Integrity and Compliance Committee Meeting held on May 13, 2021

- Motion to approve the Minutes

Audit & Compliance Committee Charter and Meeting Planner

- Committee annually reviews and approves its Charter

- Meeting Planner details committee responsibilities to satisfy IIA and Department of Justice best practices

- No changes recommended to the Committee Charter or Meeting Planner

Audit & Compliance Services Department Charter

- Charter is the Board's authorization and charge document that empowers VCU's internal audit and ethics and compliance programs

- Annual review and Board approval is required

- No updates needed at this time

FOR INFORMATION

ACS Departmental Update

- Staffing and Credentials

  - ✓ Well Qualified

- Department Expenses

  - ✓ Department expenses higher than prior year due to 5% pay increase

- Audit Survey Results

  - ✓ Overall rating of 3.40/4.0; slight decline from 3.51 in FY20. Rating decline attributed to the disruptive nature of an audit to department operations, especially during COVID

Status of FY20 Follow-up Report Corrective Action

Finding	Target Date as of 9/2020	Complete	Revised Due Date
Dentistry Physical Access Mgmt. (Dec 2018)	Jan 2021	-	July 2021
CHS Records Management (Dec 2018)	Jan 2021	-	Sept 2021
CHS Banner Recon & Indexes (Dec 2018)	Jan 2021	-	Sept 2021

Annual Review of Audit Recommendations Outstanding 2021

- 1 Board level finding is past due

  ➢ Carryforward from FY20 report involving School of Dentistry Physical Security

- 4 management level findings are past due

  ➢ Two carryforward from FY20 report involving College of Humanities & Sciences

- Vice Presidents reviewed and approved all extensions in target dates for completion of corrective action

Integrity and Compliance Office Annual Report

- ICO oversees VCU's Ethics & Compliance Program

- Coordinates with compliance partners such as:
  - HR
  - Research
  - Athletics
  - IT Security
  - Equity and Access Services

US DOJ Federal Sentencing Guidelines
Seven Elements of an Effective Compliance Program

Elements of an Effective Compliance Program

Code of Conduct
Real expectations.

Find Policies

Board of Visitors

Executive Director of ACS

Audit and Management Services Director

University Chief Integrity & Compliance Officer

Talent @VCU

helpline @VCU

Your Concerns Are Our Concerns

1-888-242-6022
www.vcuhelpline.com
Email: ucompliance@vcu.edu
ICS Office: 804-828-2336

making ethics real
a practical guide for speaking up

Total Number of Reported Concerns by Fiscal Year

365   416   366   250

FY2018   FY2019   FY2020   FY2021

VCU

12

Integrity and Compliance Office Annual Report

- Provides information and analysis to those charged with governance

- Highlights program activities

- Communicates successes and challenges
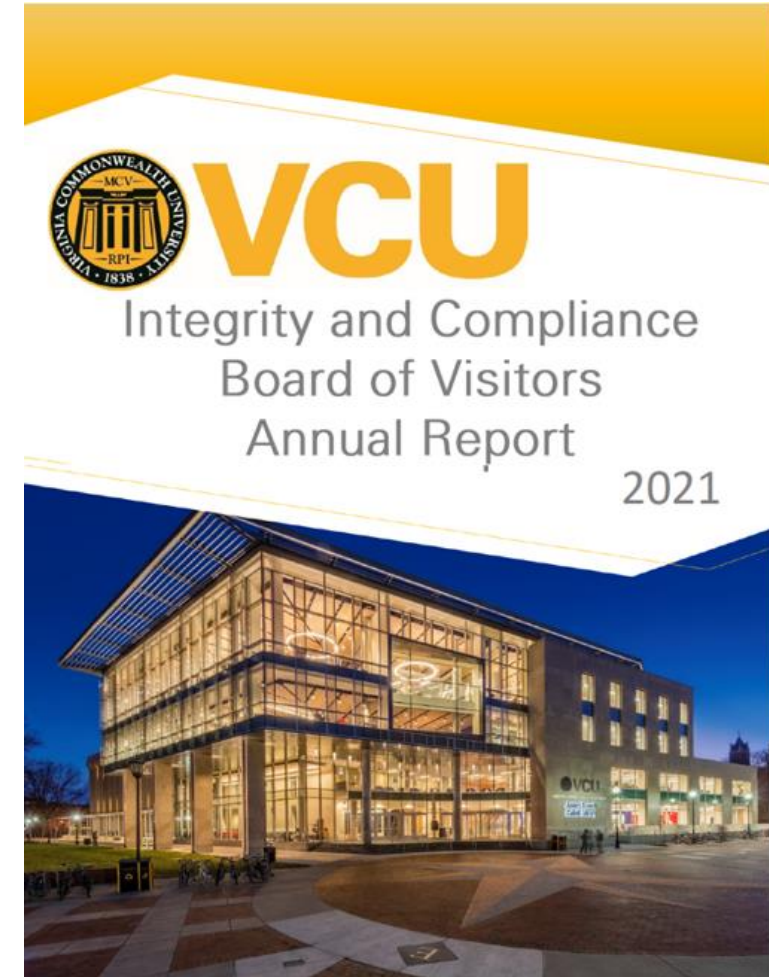
Universitywide Reported Concerns - Employee Behavior
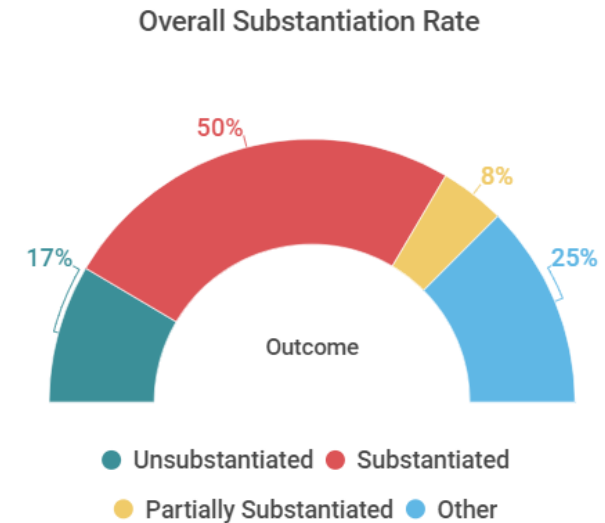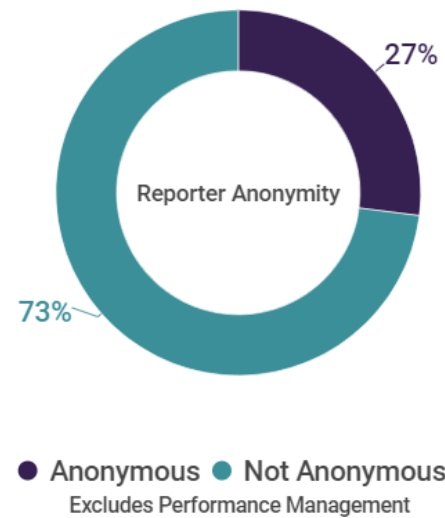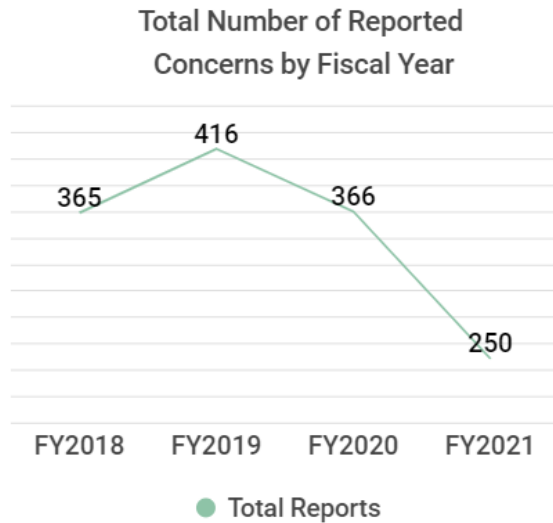
- Reported concerns declined; likely due to remote work during COVID
- Fewer high/critical severity concerns; 4 in FY21 compared to 13 in FY20
- Substantiation rate at 58%, down from 61% in FY20
  - ✓ *when employees observe misconduct & speak up, most often they are correct*
- Anonymity rate at 27%, up from 21% in prior year; ICO will monitor

FY 2021 Results Against Benchmarking Metrics

Metric	2021 Navex Global Survey	FY 2021 Convercent Benchmark	VCU Internal Benchmark	FY 2021 Data (All/Excludes Performance Management)
Cases per 100 employees	1.3 (median)	Not available	3.02	2.40 (all)
Anonymous Reports	58%	55%	13%	22%/27%
Direct Contact vs Helpline Reports	48%	23%	80%	76%/68%
Substantiation Rate	43%	36%	62%	58%/48%
Most Common Allegation Type	HR – 63%	Not available	HR – 67%	HR – 56%/42%
Concerns of Retaliation	.90%	Not available	4%	5%/6%

✓
✓ Low rate indicates trust but rise in 2021 bears watching
✓ VCU employees prefer direct contact; indicates trust
✓ Strong substantiation rate indicates accurate reports
✓
✓ Unfavorable – Training on subject under development

VCU

15

Universitywide Policies
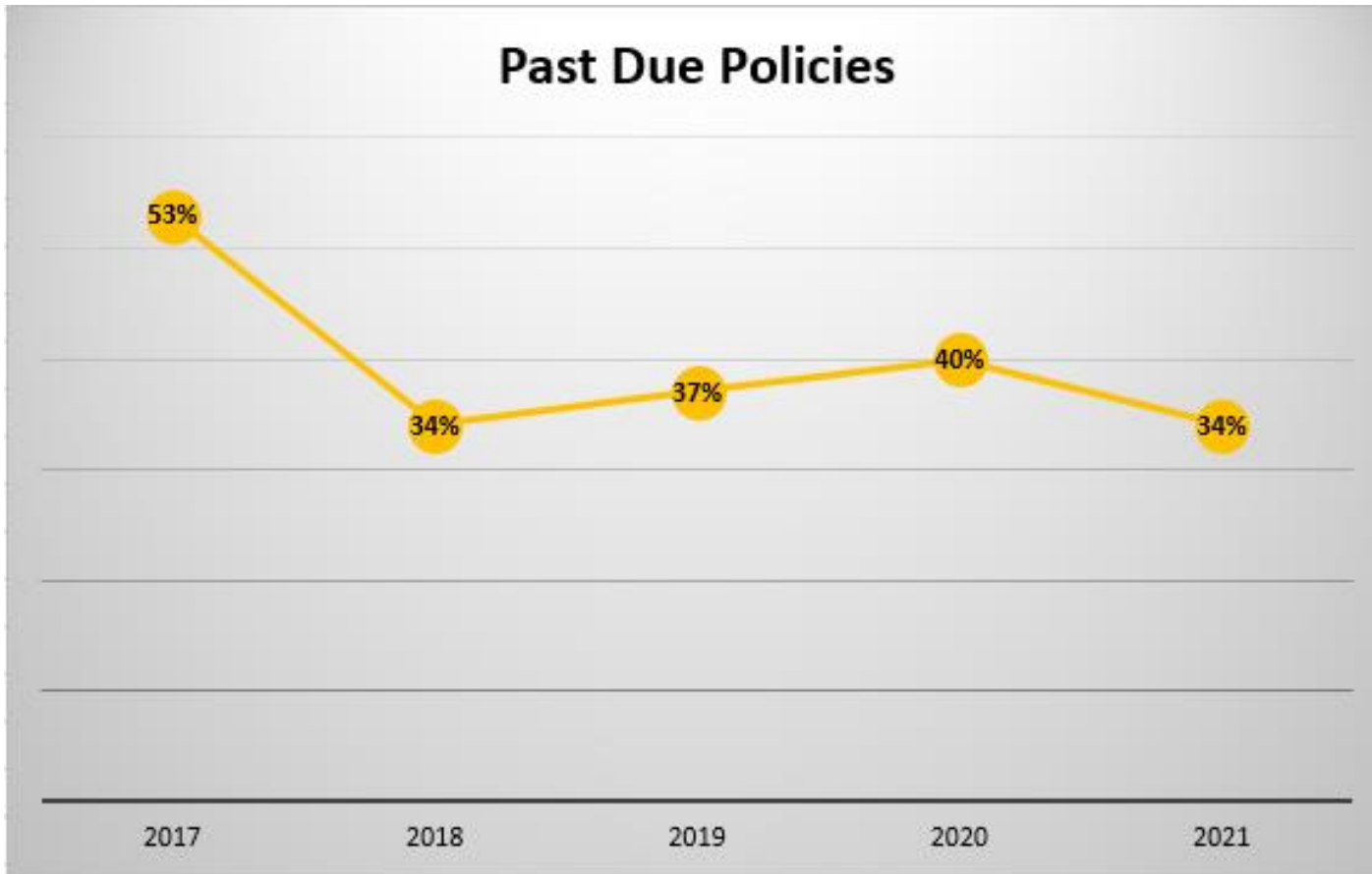
- Past due percentage includes policies in review/revision process

- Integrity and Compliance Services actively engaging one division to update outdated policies that comprise over 50% of those past due
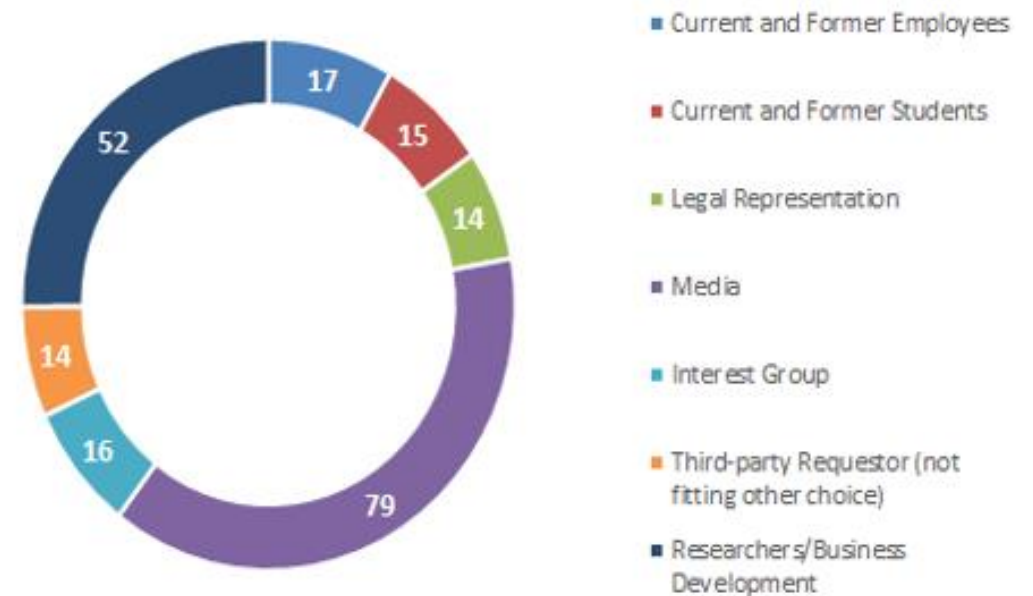
International Activities

- Winter 2020 - Undue Foreign Influence Workgroup created
    - *Actions to Address Security Concerns about Security Threats and Undue Foreign Government Influence on Campus* – Association for Public and Land-Grant Universities
    - *Framework for Review of Individual Global Engagements in Academic Research* – Council on Governmental Organizations

- Fall 2020 – Workgroup reported recommendations to Provost and VP Research and Innovation

- Spring 2021 –Recommendations accepted and Workgroup authorized to implement them

FOIA Requests

- 35% increase in requests (30% increase from media)
- Topics included:
  - ✓ Student debt collection practices
  - ✓ COVID-19 plans/operational decisions
  - ✓ Student death and subsequent requests related to incidents of hazing
  - ✓ Costs of COVID testing for men's and women's basketball teams
  - ✓ Copies of coaches' employment and men's basketball game contracts

FY 2021 FOIA Requesting Parties

Legend:
- ■ Current and Former Employees
- ■ Current and Former Students
- ■ Legal Representation
- ■ Media
- ■ Interest Group
- ■ Third-party Requestor (not fitting other choice)
- ■ Researchers/Business Development

Values shown: 17, 15, 14, 79, 16, 14, 52

Outside Professional Activity Audit Report

Faculty are required to request OPA approval in advance and to report all OPA annually

Reporting can occur:

- paper forms
- OPA system
- AIRS reporting system (primarily used by research faculty)
- Convercent

Audit Conclusion

The Outside Professional Activity policy is not adequate and the reporting process is not adequate nor working as intended.

Outside Professional Activity Audit Report - Recommendations

Enhance Electronic Reporting of OPA and Require its Usage

- Outdated system; duplicates AIRS financial interest reporting; Recommend one system

Update OPA Policy

- Last updated by Provost Office in 1983 (policy requires updates at least every 3 years)
- Policy language is contradictory regarding who must report
- Compensated OPA limited to one day/calendar week; silent to uncompensated limit
- No requirement that non-faculty report OPA

Require OPA Training

- Interviewees noted policy is confusing and requirements are unclear

RealSource Supplier Management and Puchasing/Payments Audit Report

VCU's RealSource system supports the procure to pay lifecycle

Objectives

- RealSource controls prevent unwanted transactions; provide cost savings; secure vendor verification and payment processes; facilitate data analysis
- Unique payment types (emergency & sole source) follow documented policies

Conclusion

- Concluded positively to all objectives
- No Board level findings

IT Security Update

IT Security

July 2021 Incoming Email to VCU

- Attempted messages: ~51 million
- Promotional/Massmail/Social messages that pass through filters: ~15 million
- "Clean" messages that pass through filter: ~8 million
- Delivered messages (Clean + Promotional/Massmail/Social): ~23 million
- **Percentage of messages delivered: 45.7%**

Phishing at VCU

Phishing continues to be a primary security threat:

- Filters are effective but don't completely eliminate the threat
- Attacks have been increasing in volume and sophistication
- Awareness and reporting have continued to improve
  - Reports are more timely and when the attempt hits multiple individuals we are receiving multiple reports.

Phishing Reporting Statistics
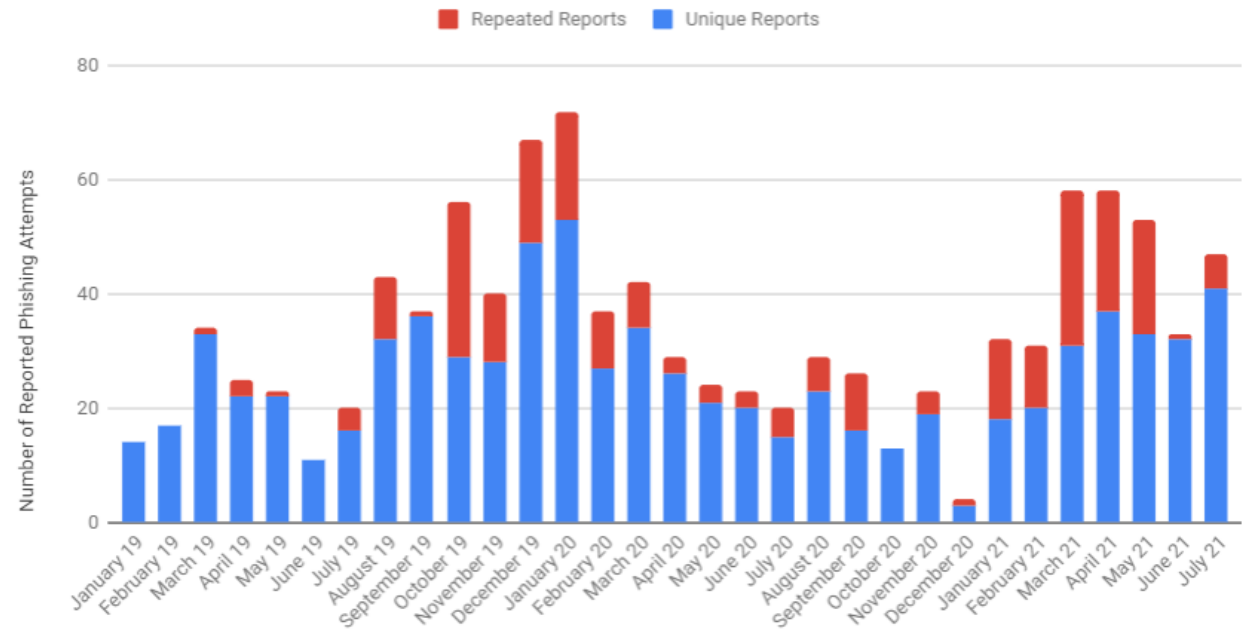
IT Security

What Is Ransomware?

- Malicious form of malware, where hackers deploy a malicious computer code to block an organization's access to its own computer network to extort a ransom.
- Ransom is paid to recover the data and/or prevent the exposure of the data.

Three main types of ransomware (listed below in order of increasing severity and complexity):

- **Scareware:** Victim receives a pop-up message claiming that malware was discovered on their system, and the only way to eradicate the malware is to pay for the security software to remove it.
- **Screen lockers:** Victim is locked out of their computer entirely. Upon startup, a full-size window will appear demanding ransom payment and prohibiting the victim from using their computer.
- **Encrypting ransomware** (most dangerous and most prevalent)**:**
  - Cybercriminals gain access to the victim's system, seize their files, encrypt them, and then demand payment for decrypting and returning the files.
  - Often includes exfiltration of the victim data, where the criminals will now threaten to disclose the victim data if ransom is not paid.

IT Security

Ransomware has become Big Business

- In 2018, the average ransom demanded from a victim was $8,000. In 2020, the average demand grew to $170,000, with high-end demands exceeding $1 million.
- Higher Ed is a large target with a significant percentage of overall attacks. Ransomware attacks against colleges and universities have more than doubled since the onset of the pandemic. There are instances of institutions paying.
- Cyber attackers have set up and organized like normal IT companies
- According to closed-source intelligence, the 3 leading Ransomware variants and threat groups in Q2 2021 have largely targeted North American organizations.
- The most common tactics hackers use to carry out ransomware attacks are email phishing campaigns, Remote Desktop Protocol (RDP) or other remote access vulnerabilities, and software vulnerabilities.
- Managed IT Service providers are being increasingly targeted because they hold data for multiple customers.

Defending Against Ransomware Attacks (Center for Internet Security)

1. Maintain backups – thoughtfully

2. Develop plans and policies

3. Review port settings

4. Harden endpoints

5. Keep systems up-to-date (patch management)

6. Train the team – Security awareness training

7. Implement continuous monitoring and incident response

IT Security

VCU's Posture

- Robust backup/restore infrastructure for critical systems
- Documented plans and procedures for security incidents; tested regularly
- Strong controls for network security; segregated networks for sensitive data
  - Periodic third-party penetration testing
- Beginning to implement stronger endpoint management systems/practices
  - Restructured team
  - Invested in tools
  - Optimizing processes

IT Security

VCU's Posture

- Centralized patch/update management for critical systems
- Advanced system protection and security monitoring for critical systems
- Robust security training and awareness programs
  - Annual security training
  - Security Heroes Program
  - Continuous simulated phishing emails with training for those who click
- Intrusion Detection and Prevention Systems (IDS/IPS) in place

Current Areas of Focus for VCU Information Security Office

- Endpoint management
  - Offer and leverage centralized endpoint management tools across VCU
    - Microsoft Endpoint Configuration Manager (MECM) for Windows
    - JamfPro for Apple devices
  - Centralized patch management and policy deployment
  - Limiting use of home/personally owned devices and pushing standard purchases
- Review of IT purchases to ensure secure data management practices by providers
- Plan for re-architecture of VCU IT model (migration to SASE and Zero Trust)
- Enhancing support for research data security

IT Security

Where We've Been (2000-2010)

Traditional information security architecture:

- Focuses on the protection of digital perimeters surrounding data or technology assets
- Designates digital environments within these perimeters as "high-trust zones" or "safe areas"
- Classifies the digital environment outside of the perimeters as "low-trust zones"
- Implements detective and preventive controls at these perimeters to filter out the malicious requests

IT Security

Traditional IT model (2000 – 2010)
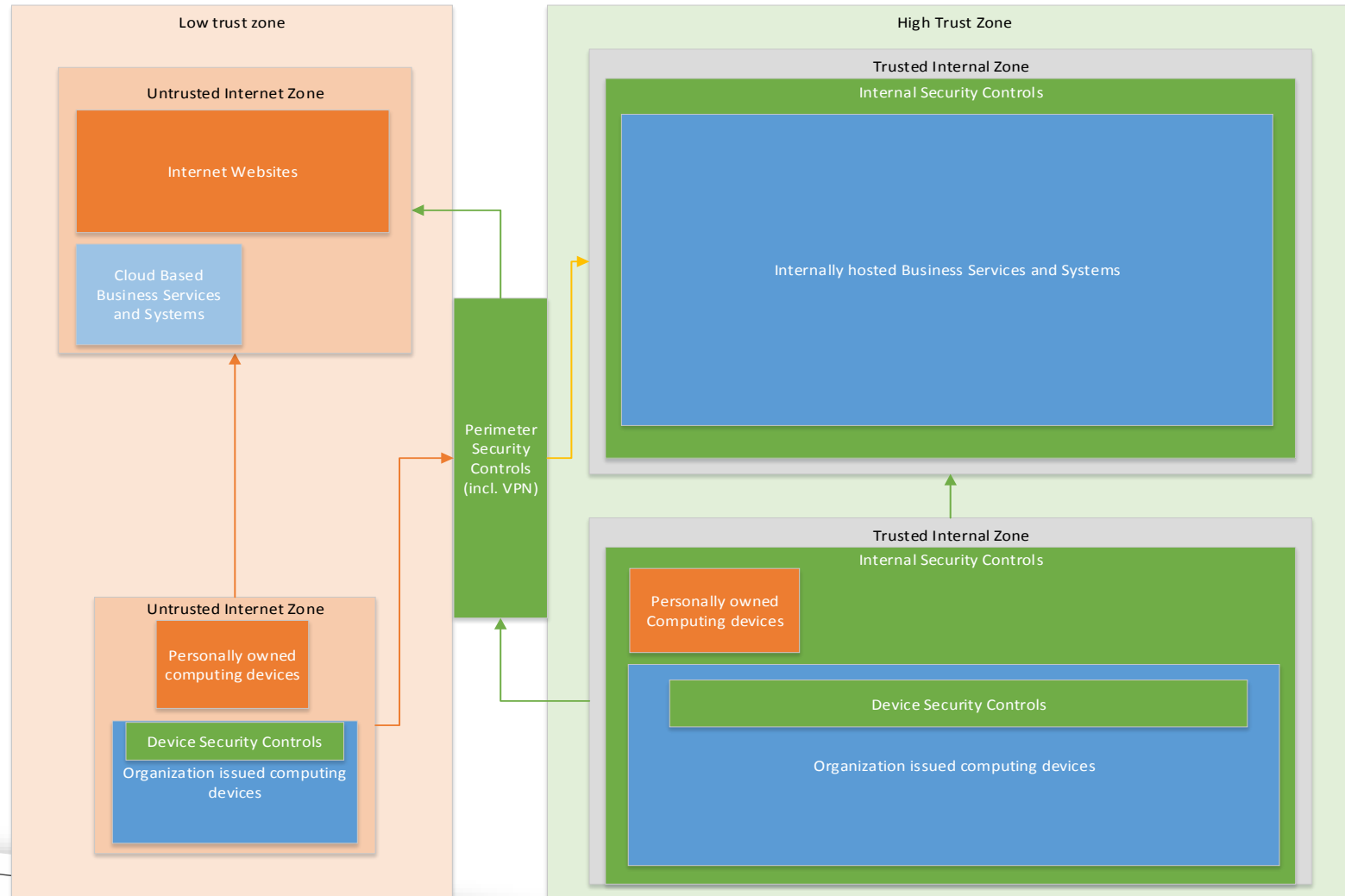
IT Security

Where We've Been (2010-2020)

Traditional information security architecture evolves with the shift to Cloud Services and Bring Your Own Device (BYOD):

- Services and data start to leave the "high-trust zones" protected by perimeter controls
- Now relying on the perimeters of the service providers who are providing business services to the organization.
- Start to adopt "Bring Your Own Device" (BYOD) models as Smartphones and tablets became more capable computing devices. This Results in the introduction of untrusted devices into the traditional "high-trust zone" and the departure of "high-value assets" (data and core business process) from the "high-trust zone"

IT Security

IT model (2010 – 2020): Shift to cloud and BYOD
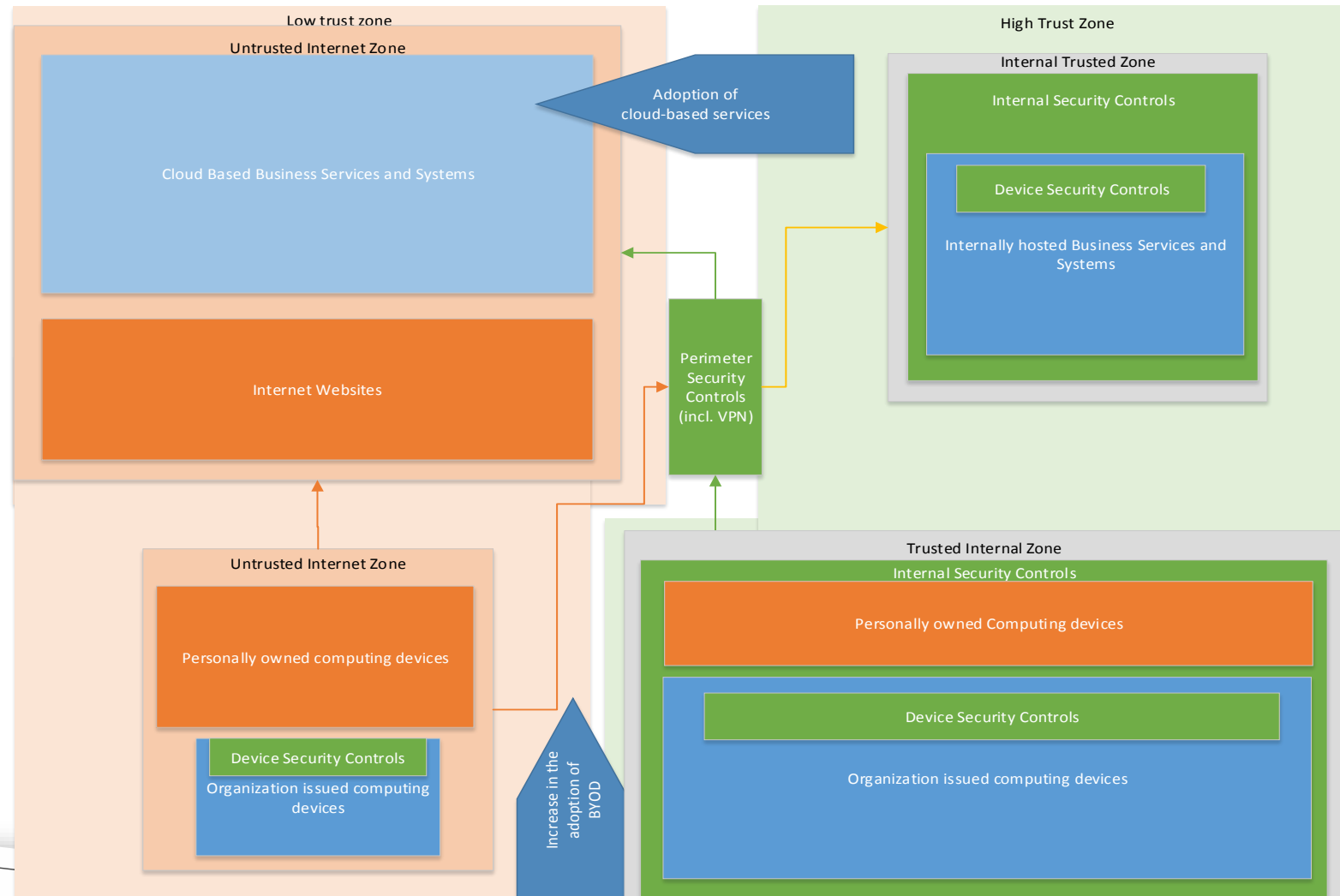
IT Security

Where We Are Now (2021)

Adapting to Cloud, BYOD and the Post-Pandemic Environment pushing against the traditional model:

- implementing new controls
  - Commonly accepted auditing and attestation reports
  - Mobile device management profiles
  - Third-party security reviews
  - IT governance, the recent pandemic has introduced yet another challenge
- Implementing policies and practices to manage remote and hybrid work environments being the new norm rather than the anomaly.
- This phenomenon resulted in the further deterioration of the efficacy of a traditional security perimeter
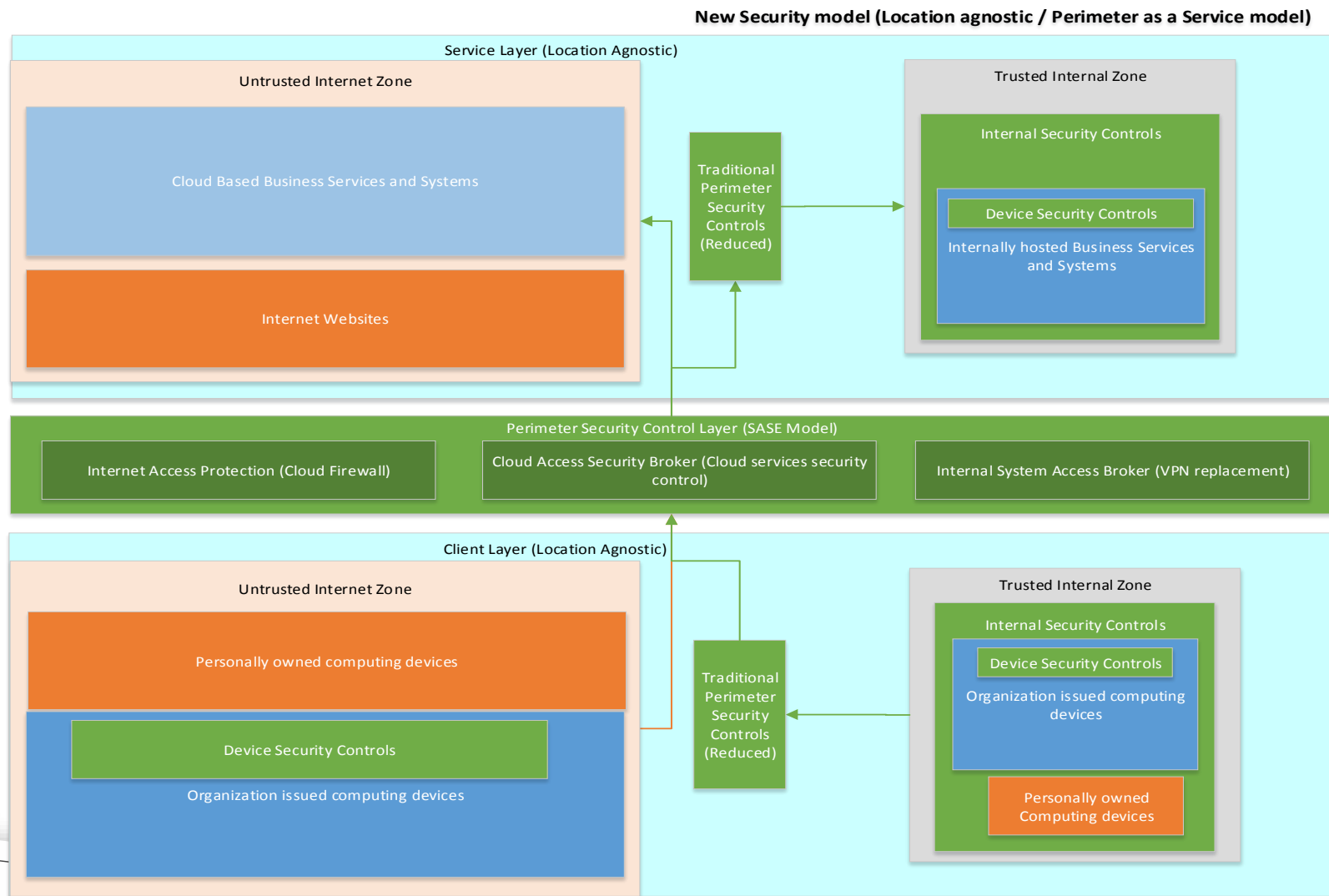
IT Security

Current security model and Post-Pandemic Environment
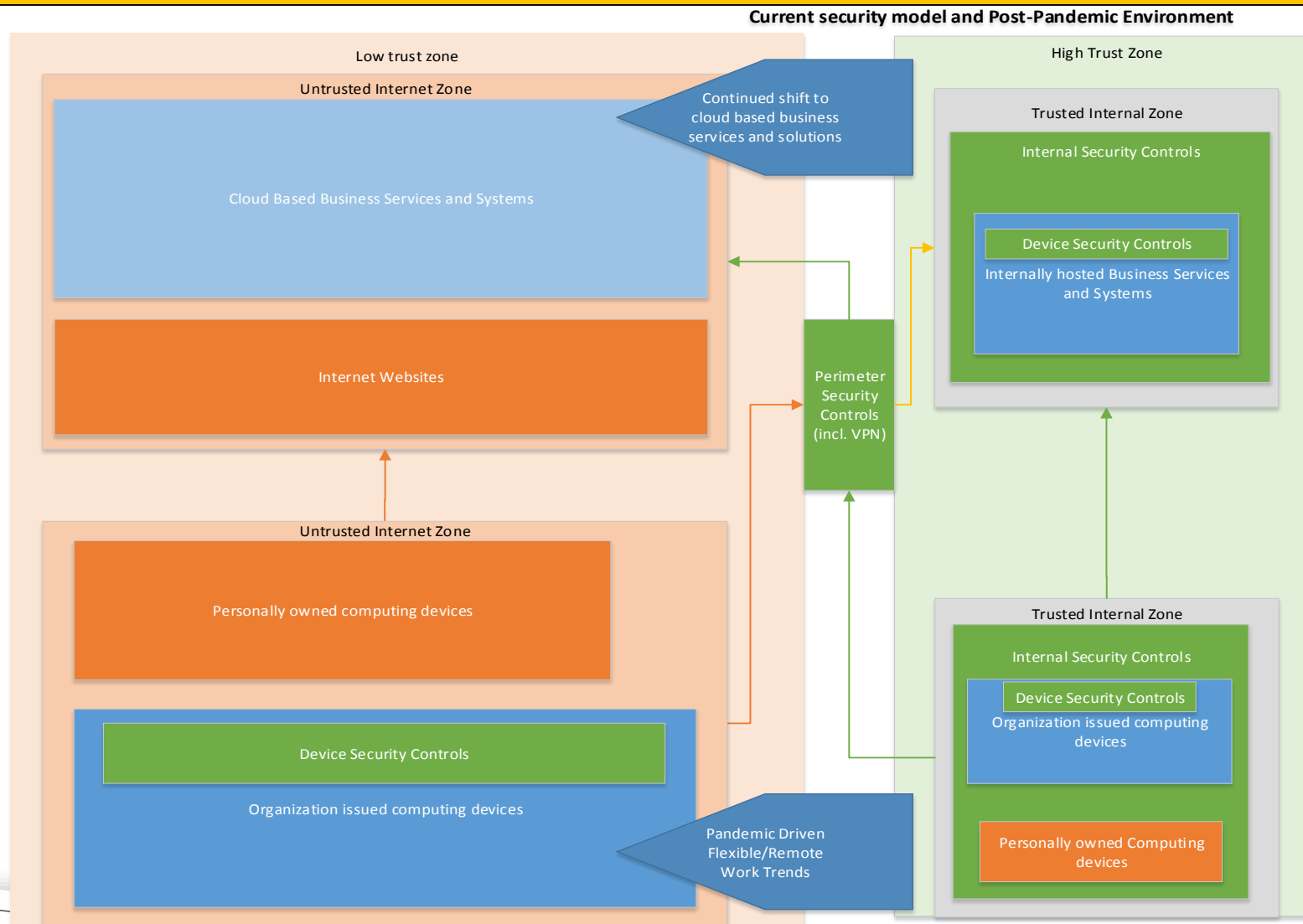
IT Security

Where We Need to Go (2021 plus)

Shift toward Secure Access Service Edge (SASE) Architecture, a location agnostic model that moves from "High Trust" and "Low Trust" zones to "Zero Trust."

- Key components include:
    - **Internet Access Protection** (also called Cloud Firewall or IAP) provides an "on-by-default" tunnel that securely directs all Internet-bound traffic from a client device through a "cloud firewall proxy, regardless of the location of the device
    - **Private Access Broker** (PAB) provides a tunnel from the internal VCU environment (including data center) to the "cloud firewall proxy" and allows direct access without the use of a VPN
    - **Cloud Access Security Broker** (CASB) tunnels all traffic to cloud providers through the "cloud firewall proxy" based on defined security rules
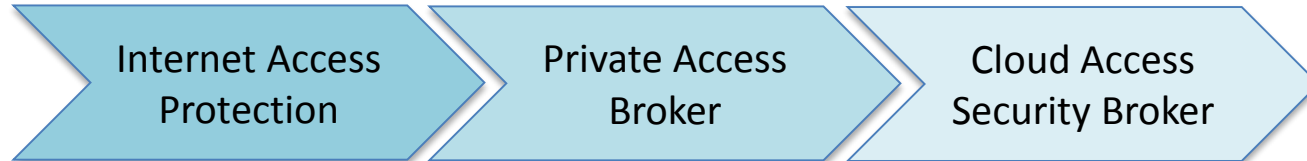
IT Security

IT Security

IT Security Re-Architecture Plan

- Developed preliminary project plan and associated budget request
- Three-year phased approach

Internet Access Protection → Private Access Broker → Cloud Access Security Broker

- Prioritizes high-risk areas and most sensitive data
- Requires staffing realignment
- Shifts costs form capital to operating

IT Security

Improving Research Data Management and Security

- Establishing Research Computing Center (RCC)
  - Governance structure for research computing policies and planning
  - Leverages expertise in multiple VCU areas
  - Supports Principal Investigators in data management and security plans
  - Will over time provide and support centralized tools and infrastructure
- Working with VCU Health Systems to provide secure access to clinical data warehouse

CLOSED SESSION