VIRGINIA COMMONWEALTH UNIVERSITY

Board of Visitors
Audit, Integrity and Compliance Committee
7:45 a.m.
September 17, 2021
James Cabell Library
901 Park Avenue, Room 303, Richmond, Virginia

Minutes

COMMITTEE MEMBERS PRESENT

Dr. Shantaram Talegaonkar, Chair
Mr. Peter Farrell, Vice Chair
Mr. Andrew Florance
Mr. Keith Parker
Dr. Tonya Parris- Wilkins

COMMITTEE MEMBERS ABSENT

Ms. Coleen Santa Ana
Ms. Alexis Swann

OTHERS PRESENT

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

CALL TO ORDER

Mr. Peter Farrell, Vice Chair, called the meeting to order at 7:49 a.m.

APPROVAL OF MINUTES

Mr. Peter Farrell asked for a motion to approve the minutes of the May 13, 2021 meeting of the Audit, Integrity and Compliance Committee, as published. After motion duly made and seconded, the minutes of the May 13, 2021 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

Audit, Integrity and Compliance Committee Charter and Meeting Planner
Karen Helderman presented the committee charter and meeting planner for approval as required annually. The charter and planner reflect the duties and responsibilities of the committee as required by the board bylaws and the planner provides the timeline for the presentation of required committee reports and materials. A copy of the committee charter and meeting planner are attached hereto as **Attachment A**.

Audit and Compliance Services Department Charter
Karen Helderman presented the department charter for Audit and Compliance Services which outlines the responsibilities of the department. A copy of the department charter ais attached hereto as **Attachment A**.

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. She also presented the fiscal year 2021 annual follow-up report, which included one board level and four management level past due corrective action plans. The Executive Director shared the results of two audit reports involving outside professional activities and the RealSource purchasing system, as well as an overview of the annual Integrity and Compliance Services report. The annual report noted a favorable decline in the number of reported misconduct concerns (likely due to the remote work conditions last year), a favorable decline in the number of high severity concerns, and a continued favorable substantiation rate. Although VCU favorably tracks below industry average for individuals wishing to remain anonymous when reporting a concern, our percentage did increase slightly this year from 21% to 27%.

A copy of Ms. Helderman's presentation is attached hereto as **Attachment C**.

Information Technology Update
The Chief Technology Officer updated the committee on VCU's Information Technology services and noted that phishing continues to be a primary security threat. He also offered a description of VCU's posture regarding ransomware attacks which were reported on the completion of corrective action plans related to the FY20 Annual Report of Past Due Findings that were due since the last committee meeting.

<u>CLOSED SESSION</u>

On motion made and seconded, the Audit, Integrity, and Compliance Committee of the Virginia Commonwealth University Board of Visitors convened into closed session under Section 2.2-3711 (A)(7) and (8), of the Virginia Freedom of Information Act for consultation with legal counsel pertaining to specific legal matters requiring legal advice by counsel and actual or probable litigation, where such consultation of briefing in open meeting would adversely affect the negotiating or litigating posture of the university, namely a survey of and status report on the university's positions in potential and current litigation in state and federal courts and other legal matters relating to pending investigations; and under 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 pertaining to human subjects research data and related IT processes.

RECONVENED SESSION

Following the closed session, the public was invited to return to the meeting. Mr. Farrell, Vice 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	
Mr. Peter Farrell, Vice Chair	X	
Mr. Andrew Florance	X	
Mr. Keith Parker	X	
Dr. Tonya Parris-Wilkins	X	
Dr. Shantaram Talegaonkar	X	

All members responding affirmatively, the motion was adopted.

ADJOURNMENT

There being no further business, Mr. Farrell, Vice Chair, adjourned the meeting at 9:09 a.m.

ATTACHMENT A

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. <u>Internal Controls</u>:

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. <u>External Auditors/Financial Statements</u>:

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, code~~s~~ 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.

ATTACHMENT B

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

ATTACHMENT C

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.

Board of Visitors
Audit, Integrity and Compliance Committee

September 17, 2021

ATTACHMENT C

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

Committee Dashboard Measures

- 🟢 Data Governance Program
- 🟡 Data Security
- 🟡 ERM Mitigation Plans
- 🟢 Planned Audits
- 🟢 Planned Special Projects
- 🟡 Ethics and Compliance Program Oversight

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

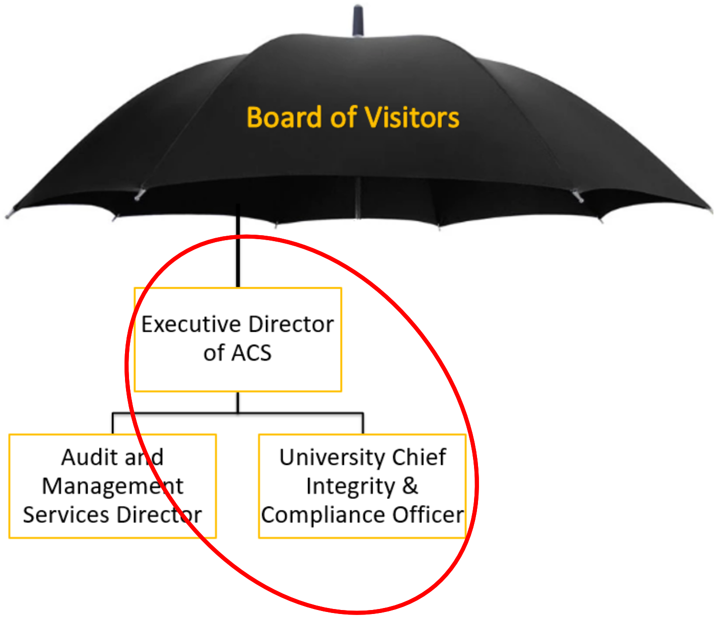
Seven Elements of an Effective Compliance Program

Elements of an Effective Compliance Program

VCU

Code of Conduct

Real expectations.


Board of Visitors
Executive Director of ACS
Audit and Management Services Director
University Chief Integrity & Compliance Officer

Talent @VCU

Find Policies

helpline VCU

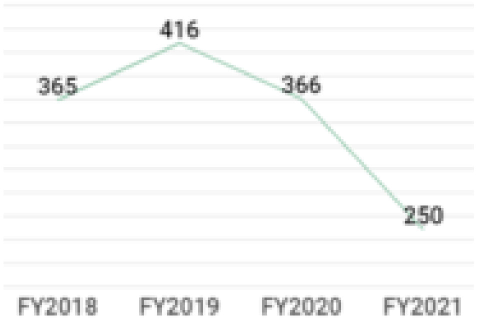
Your Concerns Are Our Concerns

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

making ethics real

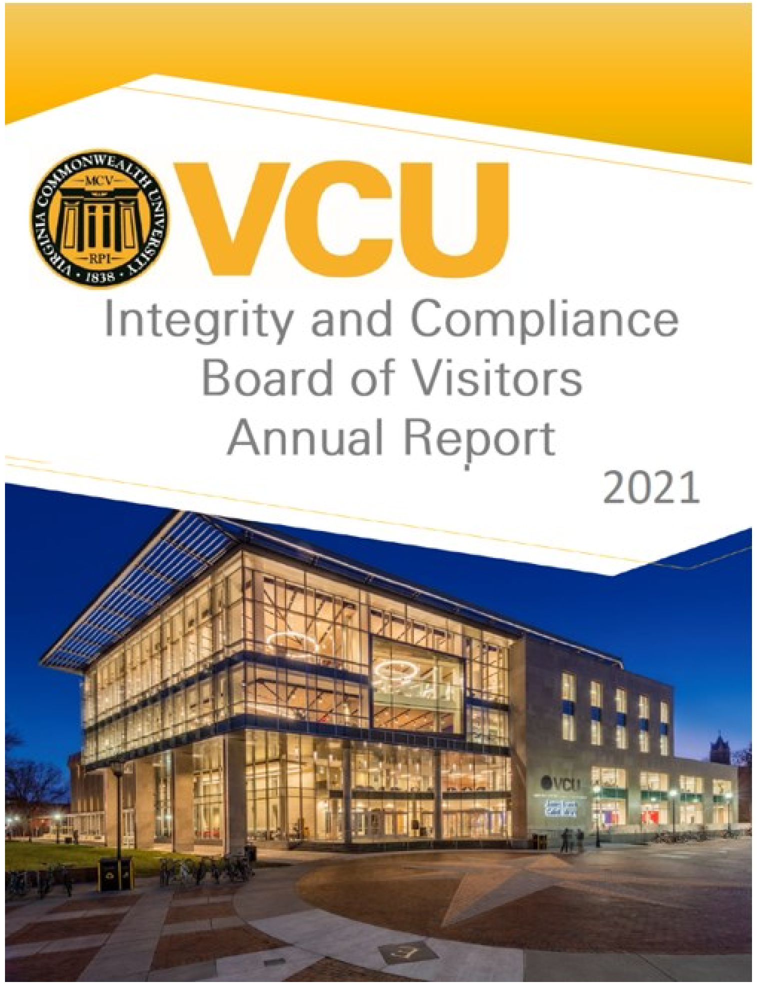
a practical guide for speaking up

Total Number of Reported Concerns by Fiscal Year



Integrity and Compliance Office Annual Report

- Provides information and analysis to those charged with governance
- Highlights program activities
- Communicates successes and challenges



VCU

Integrity and Compliance
Board of Visitors
Annual Report

2021

Universitywide Reported Concerns - Employee Behavior

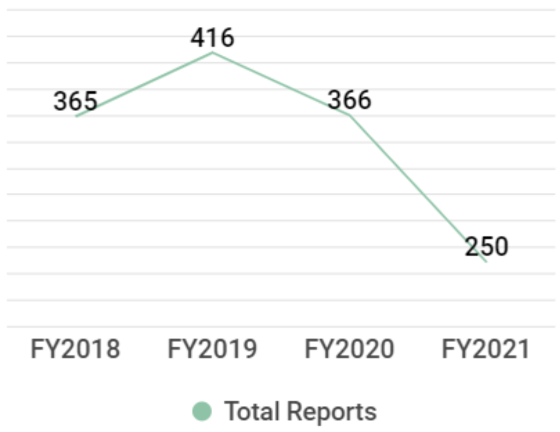
250 Total number reported concerns

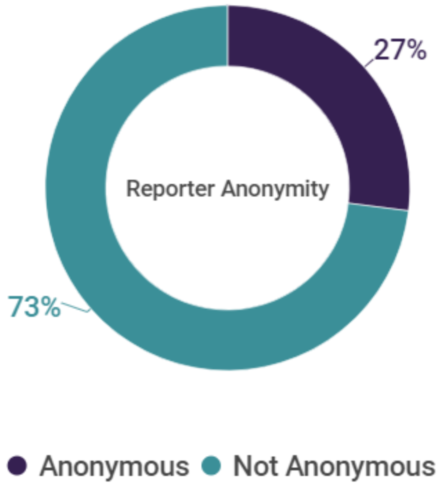
177 Number of reported concerns, excluding performance management

↓ **32%** Total reports universitywide from FY2020

Severity			
188	Low	4	High
58	Medium	0	Critical

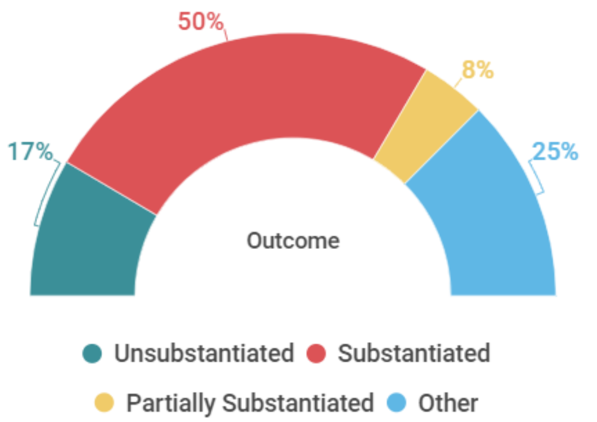
Total Number of Reported Concerns by Fiscal Year





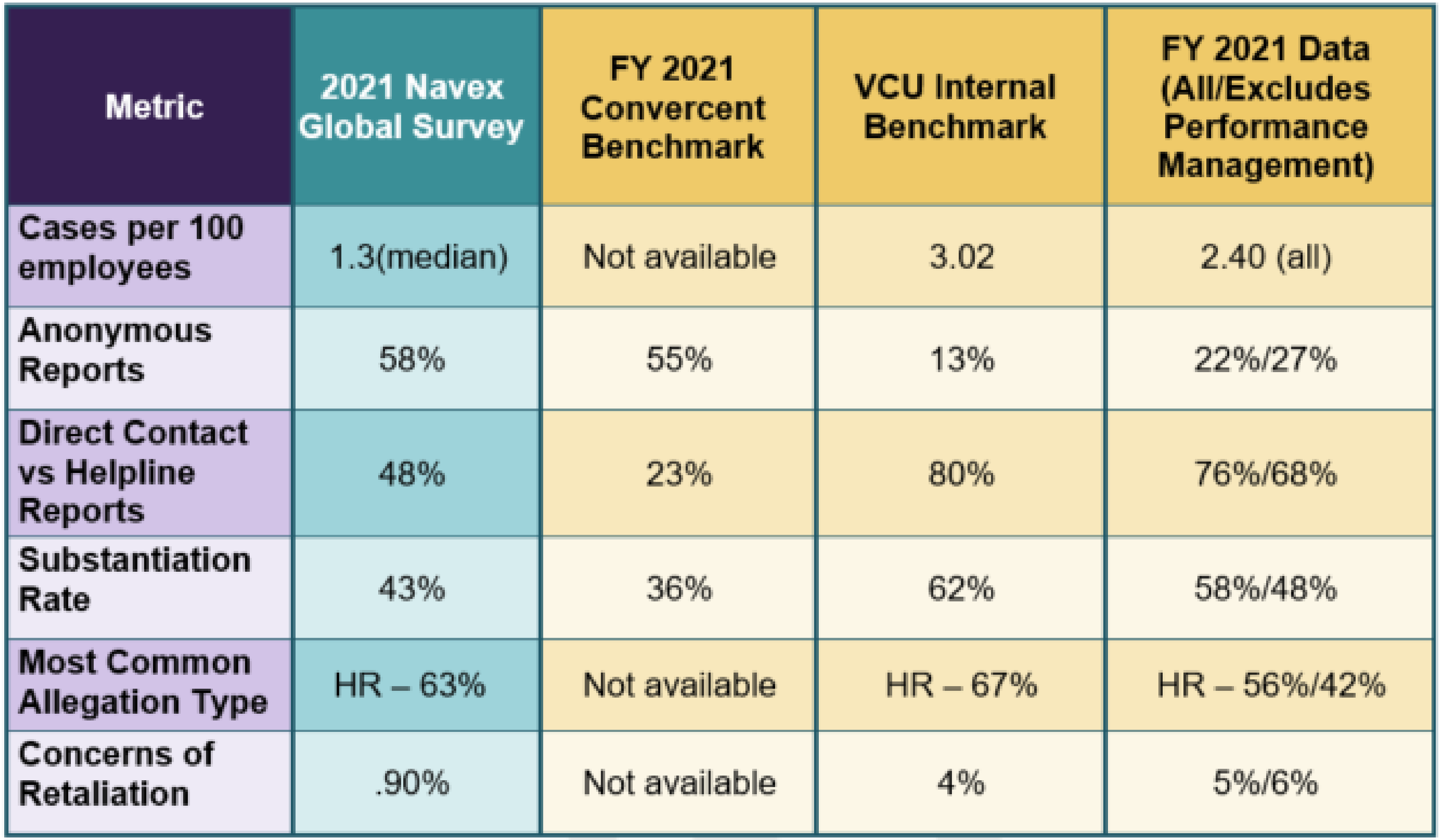
Excludes Performance Management

Overall Substantiation Rate



- 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

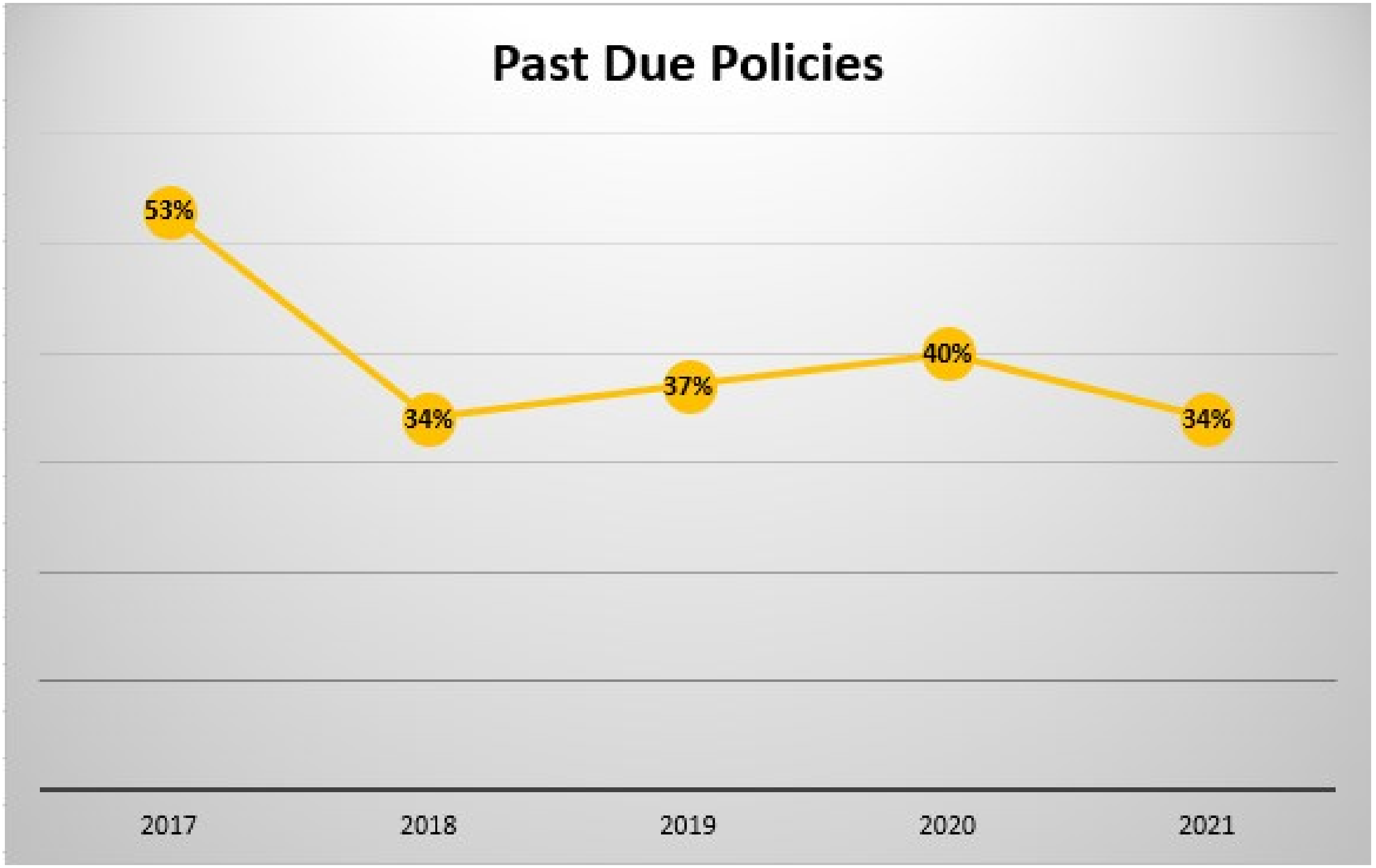
✓ VCU employees prefer direct contact; indicates trust

✓ Strong substantiation rate indicates accurate reports

✓

✓ Unfavorable – Training on subject under development

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

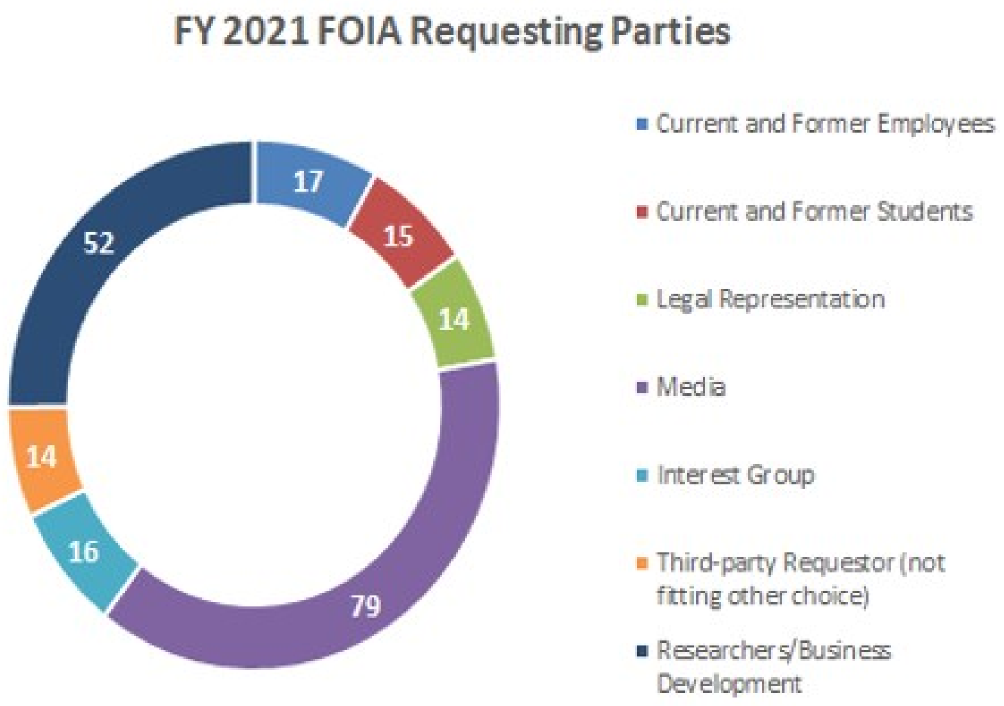
- Winter 2020 - Undue Foreign Influence Workgroup created
  - *Actions to Address Security Concerns about Security Threats and Undue Foreign Government Influence on Campus* – Association for Public and Land-Grant Universities
  - *Framework for Review of Individual Global Engagements in Academic Research*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

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

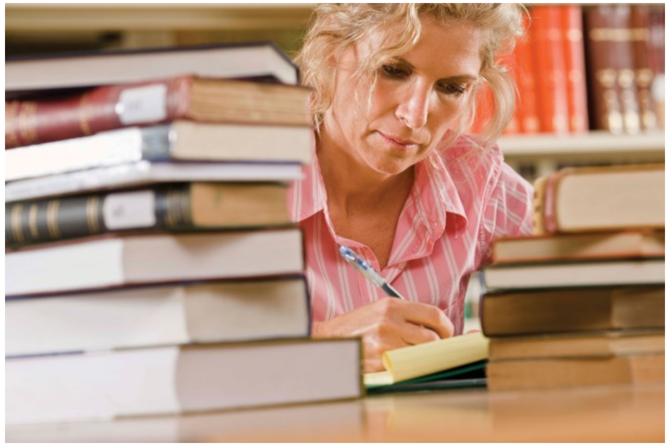
- Spring 2021 –Recommendations accepted and Workgroup authorized to implement them

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



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

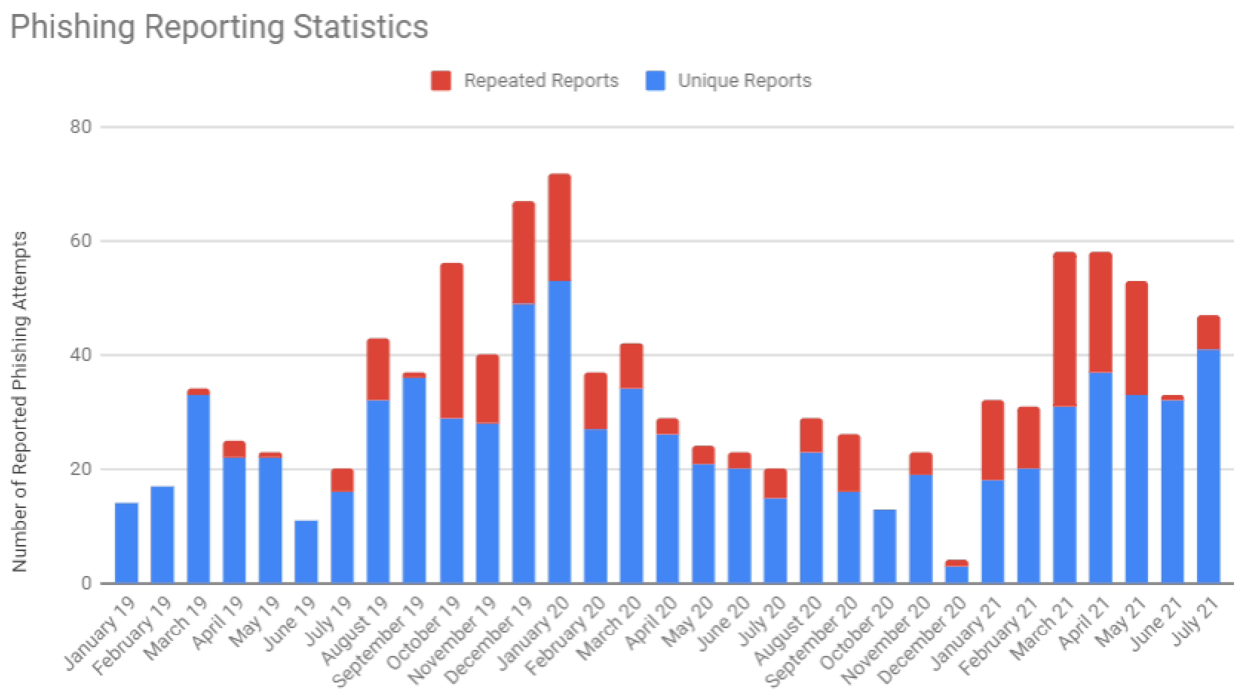
- Attempted messages: ~51 million
- Promotional/Massmail/Social messages that pass through filters: ~15 million
- “Clean” messages that pass through filter: ~8 million
- Delivered messages (Clean + Promotional/Massmail/Social): ~23 million
- **Percentage of messages delivered: 45.7%**

IT Security

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.



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.

IT Security

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

IT Security

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

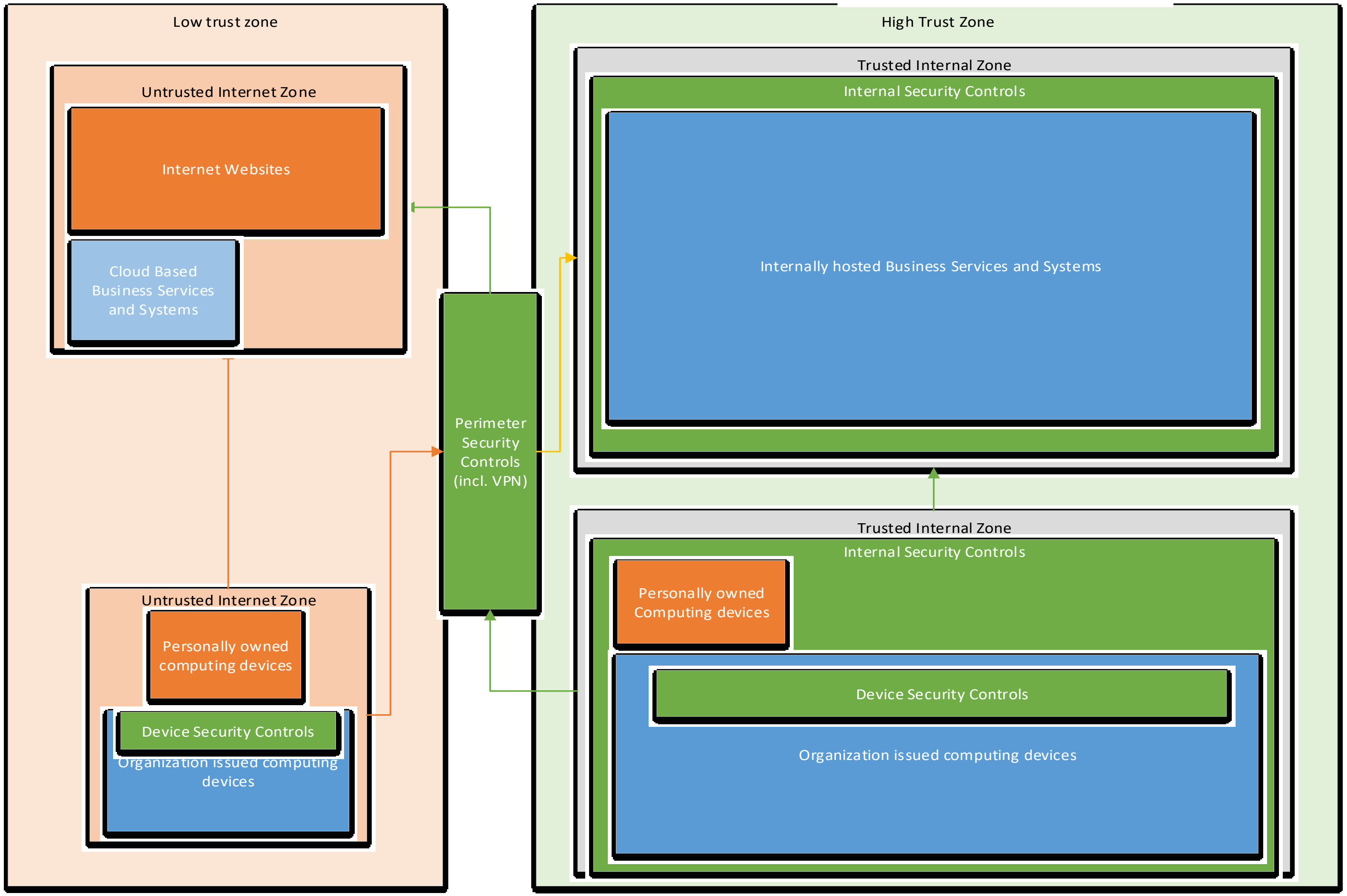
Where We’ve Been (2000-2010)

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)


Low trust zone
Untrusted Internet Zone
Internet Websites
Cloud Based Business Services and Systems
Untrusted Internet Zone
Personally owned computing devices
Device Security Controls
Organization issued computing devices
Perimeter Security Controls (incl. VPN)
High Trust Zone
Trusted Internal Zone
Internal Security Controls
Internally hosted Business Services and Systems
Trusted Internal Zone
Internal Security Controls
Personally owned Computing devices
Device Security Controls
Organization issued computing devices

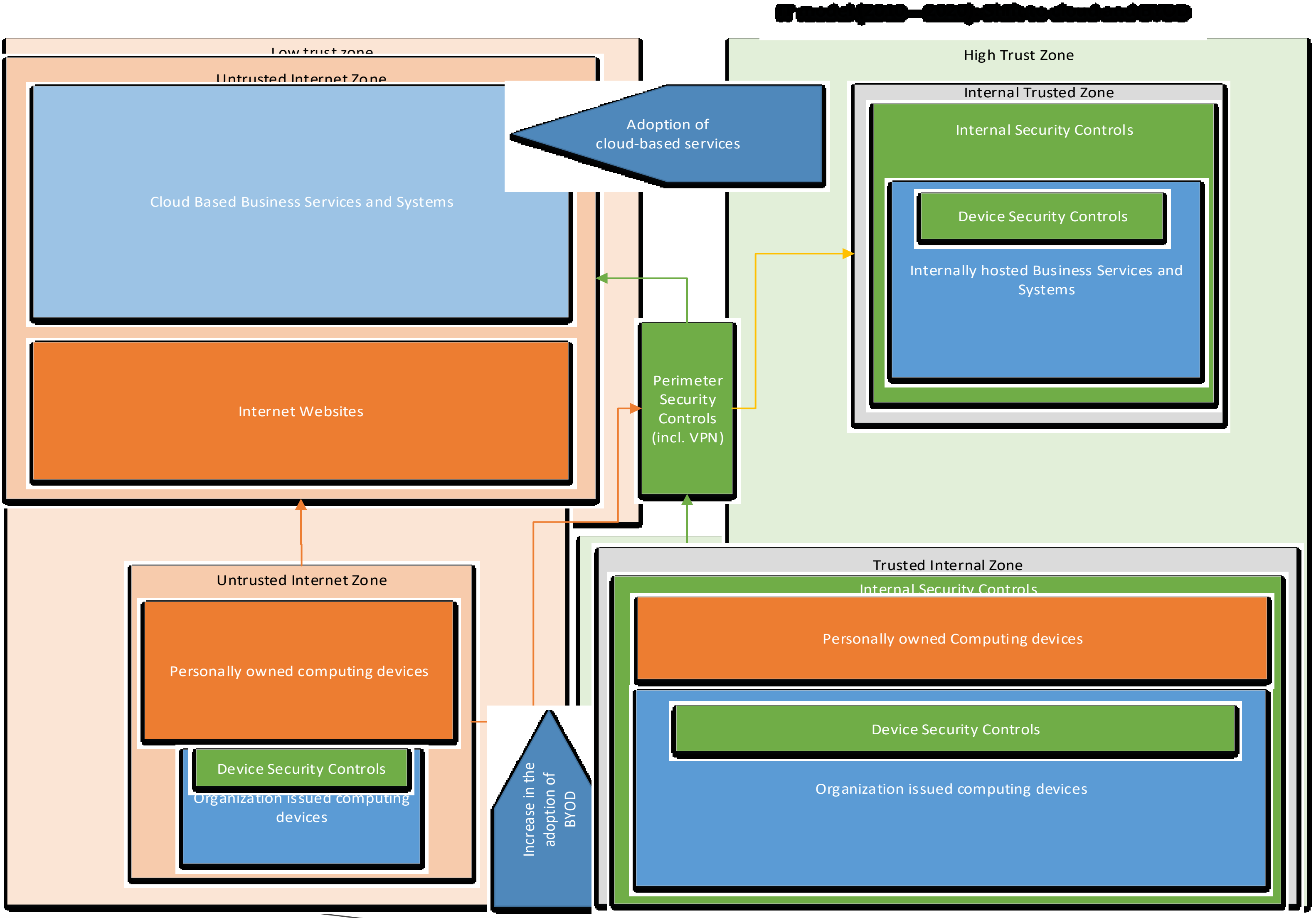
IT Security

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



[illegible]

Low trust zone

Untrusted Internet Zone

Cloud Based Business Services and Systems

Internet Websites

Adoption of cloud-based services

Untrusted Internet Zone

Personally owned computing devices

Device Security Controls

Organization issued computing devices

Increase in the adoption of BYOD

Perimeter Security Controls (incl. VPN)

High Trust Zone

Internal Trusted Zone

Internal Security Controls

Device Security Controls

Internally hosted Business Services and Systems

Trusted Internal Zone

Internal Security Controls

Personally owned Computing devices

Device Security Controls

Organization issued computing devices

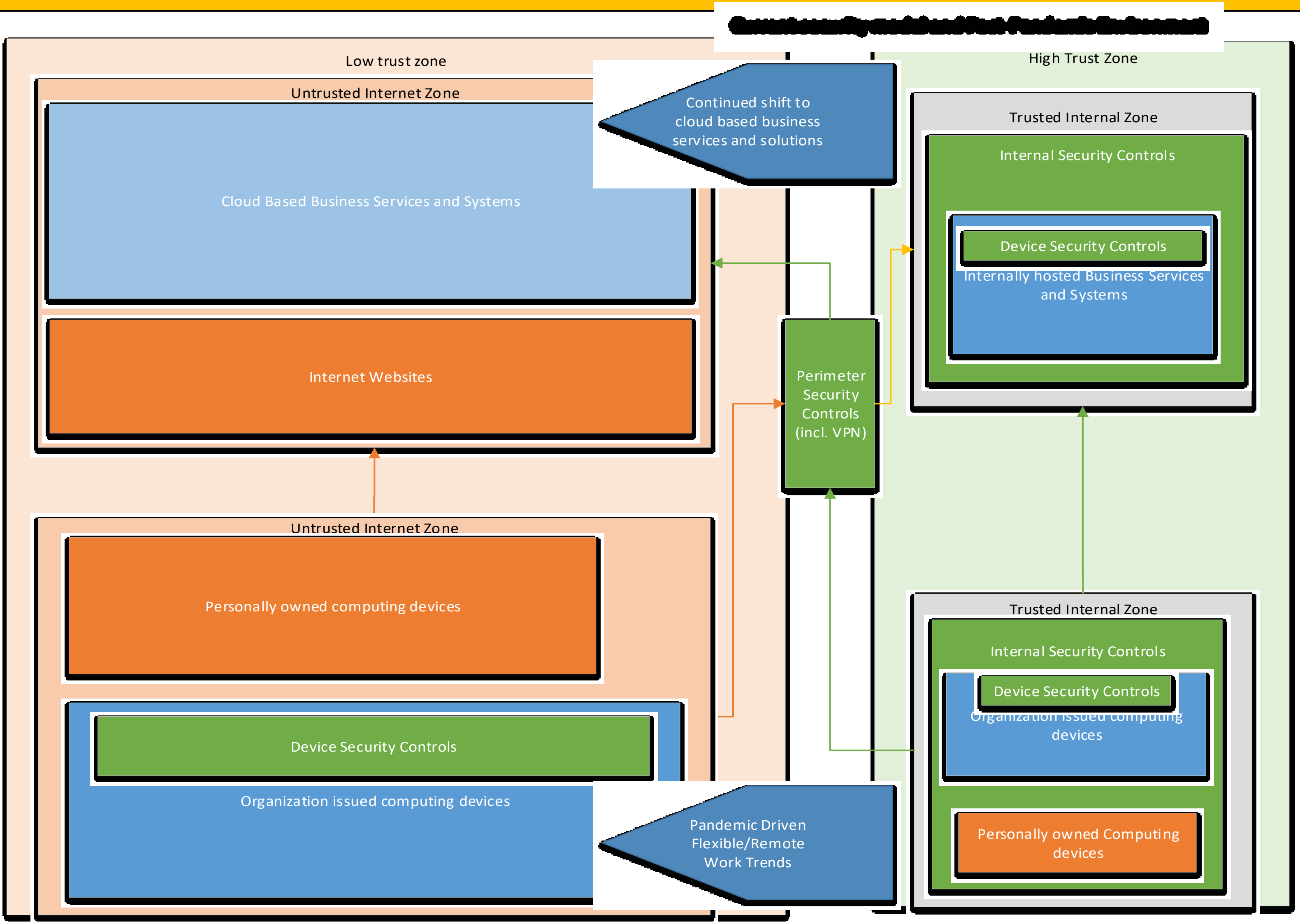
IT Security

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

Low trust zone

Untrusted Internet Zone

Cloud Based Business Services and Systems

Internet Websites

Untrusted Internet Zone

Personally owned computing devices

Device Security Controls

Organization issued computing devices

Continued shift to cloud based business services and solutions

Perimeter Security Controls (incl. VPN)

Pandemic Driven Flexible/Remote Work Trends

High Trust Zone

Trusted Internal Zone

Internal Security Controls

Device Security Controls

Internally hosted Business Services and Systems

Trusted Internal Zone

Internal Security Controls

Device Security Controls

Organization issued computing devices

Personally owned Computing devices

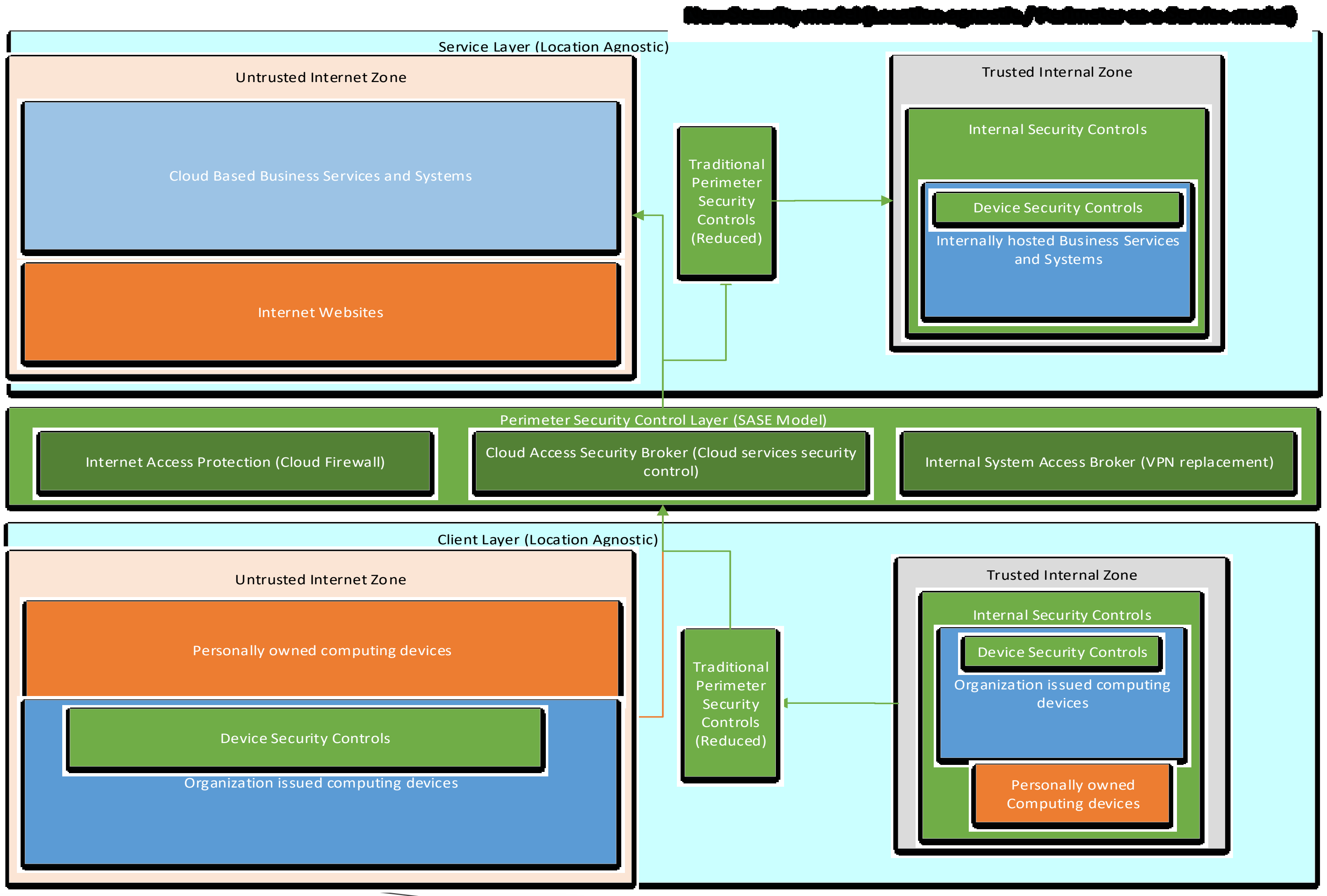
IT Security

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

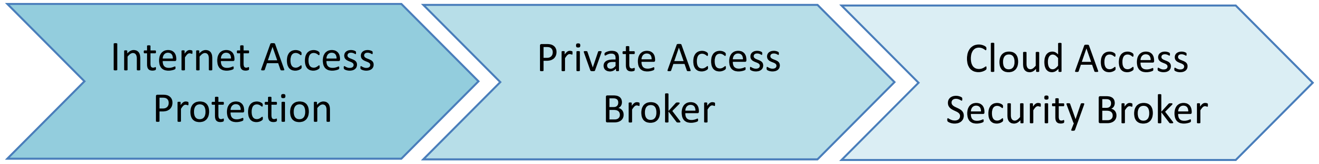
IT Security


New Security model (location agnostic / Perimeter as a Service model)
Service Layer (Location Agnostic)
Untrusted Internet Zone
Cloud Based Business Services and Systems
Internet Websites
Traditional Perimeter Security Controls (Reduced)
Trusted Internal Zone
Internal Security Controls
Device Security Controls
Internally hosted Business Services and Systems
Perimeter Security Control Layer (SASE Model)
Internet Access Protection (Cloud Firewall)
Cloud Access Security Broker (Cloud services security control)
Internal System Access Broker (VPN replacement)
Client Layer (Location Agnostic)
Untrusted Internet Zone
Personally owned computing devices
Device Security Controls
Organization issued computing devices
Traditional Perimeter Security Controls (Reduced)
Trusted Internal Zone
Internal Security Controls
Device Security Controls
Organization issued computing devices
Personally owned Computing devices

IT Security

IT Security Re-Architecture Plan

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



- 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