



VCU

**VIRGINIA COMMONWEALTH
BOARD OF VISITORS
AUDIT, INTEGRITY AND COMPLIANCE COMMITTEE MEETING
MAY 11, 2023
12:15 p.m.
James Branch Cabell Library
901 Park Avenue – Room 311
Richmond, VA**

AGENDA

1. CALL TO ORDER

Dr. Shantaram Talegaonkar, *Chair*

2. ACTION ITEMS:

10 minutes (12:30 - 12:40)

- a. Approval of Minutes March 23, 2023
- b. Proposed Audit, Integrity and Compliance Committee Charter and Meeting Planner
- c. Proposed Audit, Integrity and Compliance Department Charter
- d. Proposed FY2024 Audit Workplan
- e. Proposed FY2024 University Ethics and Compliance Program Initiatives

Ms. Karen Helderman, *Executive Director, Audit and Compliance Services*

FOR INFORMATION:

**3. AUDITOR OF PUBLIC ACCOUNTS (APA)
FY2023 AUDIT ENTRANCE CONFERENCE**

10 minutes (12:40 – 12:50)

Mr. Mike Reinholtz, *Director Auditor of Public Accounts*

**4. REPORT FROM EXECUTIVE DIRECTOR OF
AUDIT AND COMPLIANCE SERVICES**

15 minutes (12:50 – 1:05)

- a. Committee Dashboard Measures
- b. Internal Audit Reports
 - i. Data Integrity
- c. Handout: Audit Work Plan Status FY23 & ACE

Ms. Karen Helderman, *Executive Director, Audit and Compliance Services*

5. DATA GOVERNANCE UPDATE

10 minutes (1:05 – 1:15)

Dr. D’Arcy Mays, *Interim Assistant Vice Provost Institutional Decision and Support*

6. ENTERPRISE RISK MANAGEMENT UPDATE

10 minutes (1:15 – 1:25)

Mr. Tom Briggs, *Assistant Vice President, Safety and Risk Management*

7. CLOSED SESSION

Freedom of Information Act Section 2.2-3711 (A)
(7), specifically:

a. University Counsel Litigation Update
10 minutes (1:25 – 1:35)

Mr. Jake Belue, Associate
University Counsel

**8. RETURN TO OPEN SESSION AND
CERTIFICATION**

Dr. Shantaram Talegaonkar, Chair

- Approval of Committee action on matters discussed in closed session, if necessary

8. ADJOURNMENT

Dr. Shantaram Talegaonkar, Chair

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 Q1, Q2, Q3, Q4 based on Fiscal Year (July – June)	Frequency			Planned Timing			
	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 <i>International Standards for Professional Practice of Internal Auditing</i> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> • 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.

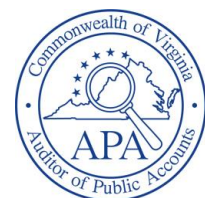
The quality program includes both internal and external assessments. Internal assessments will include ongoing monitoring and periodic assessments of internal audit activity. An external assessment will be performed at least once every five years by qualified individuals who are independent of the internal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

Virginia Commonwealth University
Audit, Integrity and Compliance Committee
Entrance Conference
May 11, 2023

1. APA Introductions

Project Manager – J. Michael Reinholtz (mike.reinholtz@apa.virginia.gov)

- 2. Audit Period** – Our audit will cover the period July 1, 2022 through June 30, 2023. Our Office’s workplan requires completion of the Universities that are material to the Commonwealth’s Annual Comprehensive Financial Report (VCU, UVA, and VT) in the fall of each year.
- 3. Timeline of the audit completion** – We will begin control and transaction testing in the late spring and will complete substantive testing during the summer and fall. We will also test the consolidation of the VCU Health System Authority and Foundations’ financial information as part of the University financial statement audit process. Our anticipated deadline is November 2023.
- 4. Audit objectives** – Our main audit objective is to provide an opinion on the University’s financial statements. More specifically, our audit objectives include:
- Ensuring the financial statements present fairly the financial position, the changes in financial position, and the cash flows for the period under examination in conformity with accounting principles generally accepted in the United States.
 - Determining if disclosures in the financial statements are adequate and fairly stated.
 - Determining whether the University has adequate internal control over financial reporting sufficient to mitigate the risk of material misstatements.
 - Determining whether adequate internal controls exist over material account balances and transactions, and whether the University is in compliance with applicable laws, regulations, and provisions of contracts or grant agreements.
- 5. Statewide single audit support** – Federal funding received by institutions in the Commonwealth of Virginia is subject to the Single Audit Act.
- Research and Development Cluster – last audited in FY20
 - Student Financial Assistance Program Cluster – last audited in FY21
 - Education Stabilization Fund – last audited in FY22
- 6. Audit scope** – We do not review all transactions or accounts in detail. We use materiality to focus our work on those financial statement line items and those transactions that are material or significant to the University. We will issue a report on internal controls and compliance that will include any findings or recommendations that we identify as a result of the audit
- 7. Relationship between APA, Internal Audit, and Foundation Auditors** – The APA is the Commonwealth of Virginia’s independent external auditor responsible for annual financial statement audits of public agencies and institutions, and various other required audits. The APA reports to the



Virginia General Assembly. Internal Audit is responsible for the institution's audit workplan as approved by the institution's Board of Visitors. Foundation auditors are responsible for the financial statement audits of the various component units. We make reference to the work of these auditors in our financial statement opinion, but we generally do not take responsibility for the work of these auditors. Most foundations are presented as discretely presented component units in the institution's financial statements.

- 8. Discussion of Risk with Board Members** – The APA encourages the Board of Visitors to provide input regarding the risks they perceive to the University in completing its mission. While Board members can direct their comments to the Audit Committee Chair or the Internal Audit Director to be forwarded to the APA Project Manager, we also plan to meet directly with the Audit Committee Chair. We will discuss the following issues:
- Any areas of fraud risk
 - Any areas of institutional risk
 - Any matters that the Board believes should be considered in planning

Terms of the Engagement

Responsibilities during the audit process:

- **The Auditor's (APA) Responsibilities**

- **Overall Audit Objectives**

We will conduct our audit in accordance with auditing standards generally accepted in the United States of America (GAAS) and standards for financial audit contained in the *Government Auditing Standards*. The objectives of our audit are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion about whether your financial statements are fairly presented, in all material respects, in conformity with U.S generally accepted accounting principles. Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit conducted in accordance with GAAS and *Governmental Auditing Standards* will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users made on the basis of these financial statements.

Accounting Principles generally accepted in the United States of America, as promulgated by the Governmental Accounting Standards Board (GASB) require that certain information be presented to supplement the basic financial statements. Such information, although not a part of the basic financial statements, is required by GASB, who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. We will apply certain limited procedures to the required supplementary information (RSI) in accordance with GAAS, which will consist of inquiries of management about the methods of preparing the RSI and comparing the RSI for consistency with management's responses to our inquiries, the basic financial statements, and other knowledge we obtained during our audit of the basic financial statements. We will not express an opinion or provide any assurance on the following RSI based on these limited procedures:

- Management Discussion and Analysis (MD&A)
- Schedules of Employer's Share Liabilities or Assets: Pension and OPEB
- Schedules of Employer Contributions: Pension and OPEB

- **Audit Procedures-General**

As part of an audit conducted in accordance with GAAS and *Government Auditing Standards*, we exercise professional judgment and maintain professional skepticism throughout the audit. An audit also includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements; therefore, our audit will involve judgment about the number of transactions to be examined and the areas to be tested. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements. We will plan and perform the audit to obtain reasonable, rather than absolute assurance, about whether the financial statements are free of material misstatement whether from (1) errors, (2) fraudulent financial reporting, (3) misappropriation of assets, or (4) violations of laws or governmental regulations that are attributable to the entity or to acts by management or employees acting on behalf of the entity.

Because of the inherent limitations of an audit, together with the inherent limitations of internal control, an unavoidable risk that some material misstatements may not be detected exists, even though the audit is properly planned and performed in accordance with GAAS and *Government Auditing Standards*. Because the determination of abuse is subjective, *Government Auditing Standards* do not expect auditors to perform specific procedures to detect waste or abuse in financial audits nor do they require auditors to provide reasonable assurance of detecting waste or abuse. An audit is not designed to detect immaterial misstatements or violations of laws or governmental regulations that do not have a direct and material effect on the financial activity.

We will also conclude, based on the audit evidence obtained whether there are conditions or events considered in the aggregate, which raise substantial doubt about the entity's ability to continue as a going concern for a reasonable period of time.

○ **Audit Procedures-Internal Control and Compliance**

We will obtain an understanding of internal controls relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we will express no such opinion. An audit is not designed to provide assurance on internal control or to identify significant deficiencies or material weaknesses. However, we will communicate in writing to management and those charged with governance any significant deficiencies or material weaknesses in internal control relevant to the audit of the financial statements that we have identified during the audit. Also, as part of obtaining reasonable assurance about whether the financial statements are free of material misstatement, we will perform tests of compliance with the provisions of applicable laws, regulations, contracts, agreements, and grants. However, the objective of our audit will not be to provide an opinion on overall compliance, and we will not express such an opinion.

○ **Audit Procedures – Group Audits**

Our audit will include obtaining an understanding of the consolidated group, sufficient to assess the risks of material misstatement of financial information derived from significant components to design the nature, timing, and extent of further audit procedures, including the basis for the decision to make reference in our audit opinion to audits of significant components performed by other auditors.

○ **Audit Procedures – Risk of Material Misstatement and Significant Risks**

Our audit will identify and assess the risk of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or override of internal control. Significant risks represent events or transactions where inherent risk of material misstatement is elevated due to the likelihood and magnitude of potential misstatement. Based on our existing understanding of the University and its environment, and preliminary planning procedures performed as of the date of this memo, we have identified the following significant risks requiring special audit attention:

- Management Override of Control – management is in a unique position to perpetrate fraud because of management's ability to manipulate accounting records and prepare fraudulent financial statements by overriding controls that otherwise appear to be operating effectively. Although the level of risk of management override of controls will vary from entity to entity, the risk is, nevertheless present at all entities.

- Improper Revenue Recognition – recognition of revenue in the proper period and amount is inherently risky and may be subject to manipulation.
- Subscription-Based Information Technology Arrangements – changes to the accounting and reporting of Subscription-Based Information Technology Arrangements (SBITAs) due to the implementation of GASB 96 are complex and may not be properly identified or considered with preparing the financial statements.

Audit planning and risk assessment is an iterative process throughout the audit. Therefore, we will communicate any additional significant risks identified throughout fieldwork that may warrant the attention of management and those charged with governance if and when those circumstances arise

- **Communication with Those charged with governance**

We are responsible for communicating significant matters related to the financial statement audit that are, in the auditor's professional judgment, relevant to the responsibilities of those charged with governance in overseeing the financial reporting process. GAAS and *Government Auditing Standards* do not require the auditor to design procedures for the purpose of identifying other matters to communicate with those charged with governance.

- **Management's Responsibilities**

Our audit will be conducted on the basis that Management acknowledge and understand that they have the following responsibilities:

- Selection and application of accounting principles and preparation and fair presentation of the financial statements in accordance with accounting principles generally accepted in the United States of America
- Design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error
- Identify and ensure compliance with applicable laws, regulations, contracts, and grant agreements
- Informing the APA about all known or suspected fraud affecting the entity involving (1) management, (2) employees who have significant roles in internal control, and (3) others where the fraud could have a material effect on the financial statements
- Informing the APA (and others as required by the Code of Virginia § 30-138) of knowledge of any allegations of fraud or suspected fraud affecting the University received in communications from employees, former employees, regulators, or others
- As received, forward copies of each federal audit performed on agency or institution programs or activities to the Auditor of Public Accounts as required by Chapter 1 §4-8.02 a., of the 2021 Virginia Acts of Assembly
- Informing the APA of any potential documents that are FOIA exempt
- Ensuring that financial information is reliable and properly recorded
- Making all financial records and related information available to the APA
- Providing the APA with (1) access to all information of which you are aware that is relevant to the preparation and fair presentation of the financial statements, (2) additional information that we may request for the purpose of the audit, and (3) unrestricted access to persons within the government from whom we determine it necessary to obtain audit evidence
- Responding to audit findings and recommendations, as well as providing your planned corrective actions and the timing and format for providing that information

- Providing the APA at the end of the audit with a written letter confirming certain representations made during the audit
- Adjusting the financial statements to correct material misstatements and providing the APA with a representation that the effects of any uncorrected misstatements are immaterial, both individually and in the aggregate, to the financial statements taken as a whole
- For Group audits, management is responsible for the following:
 - Informing the component's management of any matter that the group engagement team becomes aware that may be significant to the financial statements of the component, but of which component management may be unaware.
 - Implementing procedures to determine if there are subsequent events for components through the APA's audit report date.
 - Implementing procedures to identify and disclose the component's related parties and related party transactions.
 - Implementing policies and procedures related to the consolidation of group financial information.
- **Audit, Integrity and Compliance Committee**
 - Communicate with APA about audit scope
 - Communicate with management and internal audit regarding progress
 - Receive reports and findings from management and external audit

Other Elements of the audit process:

- **Overall planned scope of the audit**
 - **Approach to internal control** – We review internal controls to identify those areas where we can replace substantive testing with transactional testing. We look for management to have written formal policies and procedures and check for the implementation of those procedures.
 - **Concept of materiality** – We do not review all transactions or accounts in detail. We use materiality to focus our work on those financial statement line items and those transactions that are material or significant to the University.
- **Identification of potential fraud risks**
 - **Approach to fraud** – Most of our audit is focused on our opinion on the financial statements and materiality. Our primary interest related to fraud would be in how it may affect the financial statements and those controls that the financial statements rely upon. The audit is not designed to detect error or fraud that is immaterial to the financial statements. However, we review policies and procedures for fraud risk and may direct our testwork towards addressing fraud risk.
 - **Responsibility for identifying fraud risks and fraud** – Auditing standards require us to assess fraud risk, interview management and staff about their knowledge of fraud and fraud risk, and review exceptions for indications of possible fraudulent transactions. Auditors should be looking for red flag fraud indicators. Even though government entities are not always profit oriented, the auditors remain vigilant about financial statement fraud.
 - **Report fraudulent transactions as required by Code of Virginia § 30-138** Agencies are responsible for reporting circumstances that suggest a reasonable possibility that a fraudulent transaction has occurred involving funds or property under their control, where an officer or employee of the

state or local government may be involved. Items should be reported to the Auditor of Public Accounts, the State Inspector General, and the Superintendent of State Police.

- **Audit Reporting**

We will issue a written report upon completion of our audit of the University's financial statements. We will make reference to the Component Auditor's audit of the Health System Authority, and the University's Foundations in our report on the University's financial statements. Our report will be addressed to the Board of Visitors of the University. Circumstances may arise in which our report may differ from its expected form and content based on the results of our audit. Depending on the nature of these circumstances, it may be necessary for us to modify our opinion, add an emphasis-of-matter or other-matter paragraph(s), or if necessary, withdraw from the engagement. If our opinions on the basic financial statements are other than unmodified, we will discuss the reasons with you in advance. If, for any reason, we are unable to complete the audit or are unable to form or have not formed opinions, we may decline to express opinions or to issue a report as a result of this engagement.

We will also provide a report (that does not include an opinion) on internal control related to the financial statements and compliance with the provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a material effect on the financial statements as required by *Government Auditing Standards*. The report on internal control and compliance will include a statement that the report is intended solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

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 enterprise cloud-based data warehouse build continues to progress, with a pilot making Admissions data available planned to be substantially complete in mid-December. Data from other phases of the student lifecycle will be rolled into the data warehouse in January and February. The migration of the Banner system into the managed cloud environment that will be completed in early December allows for the availability of more real-time data to feed reports and dashboards, and the committee will continue to provide governance around what dashboards are published. The committee continues to work toward establishing a model for increased visibility and integration into the data community and is awaiting a new leader of Institutional Research and Decision Support to continue in guiding these efforts forward.



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

Significant Security Incidents and Trends: While we have seen an escalated number of scams targeting students and some successful bypasses of multi-factor authentication protection, VCU has not experienced any major security incidents this quarter. One minor but noteworthy incident was the data breach of LastPass, a large and popular password management software. The LastPass data breach in December of 2022 did not directly affect VCU, but did affect a vendor partner of VCU that was using LastPass. VCU worked with this partner to reissue credentials that may have been impacted. Phishing is still a major threat to the institution, and we have seen an increase in credential stuffing, where previously compromised credentials from various sources are reused against VCU systems. Mandatory multi-factor authentication still helps in defending against a variety of credential-based attacks and additional monitoring has been put in place for attempts to bypass multi-factor authentication.

GLBA Compliance: The VCU Information Security Office has completed the gap analysis for compliance with the new GLBA rules, and in collaboration with other administrative units in financial aid and student accounting, efforts are underway to address identified gaps. The preliminary timeline for completion of the remediation of all identified potential gaps is set for December 2023.

SASE development: VCU completed the purchase of its SASE platform and is deploying the platform to implement its location-agnostic security architecture. The successful deployment of the platform will provide seamless, consistent, and location-agnostic security and user experience to employees using VCU-assigned computers. The platform is currently deployed to selected individuals across the university and in Technology Services in pilot form. A schedule is developed for deployment to the entire university, with the completion goal of summer 2023.

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 ERM Steering Committee has reviewed updated Risk Mitigation and Management Plans (RMMP) for several risks identified as being out of tolerance. Three (3) of the nine (9) risks out of tolerance are anticipated to be back within tolerance by the beginning of the Fall semester.

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 well. The audit team is now fully staffed and we anticipate completing our workplan on schedule, providing there are no required state hotline investigations.


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, verification, strategy implementation or resolution

 Significant challenges to institutional compliance strategy or resolution encountered

Notes: There are no known material compliance violations related to regulatory, legal or university policies. The Integrity and Compliance Office (ICO) is on track with a three-year workplan focused on improving effectiveness in six areas: Program Structure, Culture, Policies, Investigations/ Accountability, Training/Communication, Risk Assessment/Monitoring. Good progress documenting university compliance systems and setting up regular meetings of compliance leaders to drive integration, collaboration and issue spotting in ethics and compliance.



VCU

VIRGINIA COMMONWEALTH UNIVERSITY

Data Integrity – VCU Websites

Final Report
April 17, 2023

Audit and Compliance Services

Overview

Schools, units, and central offices use their websites to provide information to the VCU community, parents and prospective students. Some of these websites may display numerical or statistical data, which may be used in making decisions on where to attend school, philanthropy, or partnering with VCU. Data published on these websites may be obtained from Institutional Research and Decision Support, publications such as the VCU Facts and Figures Card, *U.S. News and World Report* rankings, surveys administered by a school or central unit, or personnel in the schools that run reports from university systems such as Banner, SAS Enterprise Guide, or the VCU Reporting Center. Outputs of manually obtained reports may vary depending on the variables used to extract the information.

Organizational websites must comply with the Organizational Websites, Management & Hosting Policy as well as all the requirements of the VCU Web Standards & Guidelines. VCU also provides hosting space for personal websites for faculty, staff, and students who are also expected to comply with all General and Security requirements of the VCU Web Standards & Guidelines. Personal websites are not official university sites and were not included in our review.

There are approximately 12 Web Managers (single person tasked with the management and governance over larger departments' web presence) throughout the university and approximately 875 clients in TerminalFour (the official content management system) that have the ability to make updates to VCU websites that are assigned to them.

Purpose

The objective of the audit was to determine whether statistical or numerical data posted to select websites was accurate and clients followed the Organizational Websites, Management & Hosting Policy.

Scope and Audit Procedures

Our scope of Data Integrity - VCU Websites encompassed October 2022 – January 2023 and focused on whether:

- Any existing guidelines for compiling select VCU website metrics were sufficient and adhered to
- Information on select VCU website metrics that students, parents, and the university community may use in decision making were reviewed prior to publication

Our audit procedures included:

- Interviews with VCU Technology and University Relations personnel as well as personnel in a select sample of schools/units
- Review of the VCU Web Standards & Guidelines as well as the Organizational Websites, Management & Hosting Policy
- Review of peer institution policies regarding the development of websites and

information posted

- Review of source documents for statistical or numerical data posted on select VCU websites
- Verification of sampled data posted on select VCU websites

Conclusion

In our opinion, based on the results of our audit, statistical or numerical data posted to select websites was accurate and clients followed the Organizational Websites, Management & Hosting Policy.

A detailed recommendation to enhance the policy by requiring the retention of data source documentation and review was included in a separate report furnished to management.

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:

Curtis Reisinger	Manager, Platform Services
Jim Yucha	Director of Application Services
Michael Porter	Associate Vice President for Public Affairs
Alex Henson	Chief Information Officer
Meredith Weiss	Vice President for Administration
Grant Heston	Vice President, Enterprise Marketing and Communications

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.



**Executive Director
Audit and Compliance Services**

For Information: Overview of Affiliated Covered Entity Changes

In Summer 2022, VCU Health System (VCUHS) approached VCU and proposed the removal of all VCU units from the 2004 Affiliated Covered Entity (ACE) agreement (*attached*) between the two entities (*see pg. 2 for a diagram depicting the units within the current ACE*). An ACE is a construct under the Health Insurance Portability and Accountability Act (HIPAA) in which legally separate entities with some degree of common control designate as a single covered entity for HIPAA compliance. When VCU and VCUHS created the ACE in 2004, the HIPAA Privacy Rule was new and it was likely believed an ACE was needed for VCUHS to share protected health information with VCU for research purposes. Knowledge has matured about the Privacy Rule, including the knowledge that HIPAA provides for research-related data sharing pathways without the need for an ACE.

During Fall 2022, VCU engaged outside counsel who is a HIPAA expert to review the ACE and the proposal from VCUHS; he advised that VCU proceed. VCUHS also retained outside counsel who is an expert in HIPAA throughout this process.

On April 17, the VCU Cabinet discussed and concurred with the proposal by VCUHS. The only VCU entity named in the 2004 ACE that provides and bills for healthcare services is the School of Dentistry; therefore, it must meet HIPAA requirements. The current plan is to establish a VCU-based hybrid covered entity, also a structure under HIPAA, solely for the School of Dentistry, while exploring options to remove from the School of Dentistry any clinical activity potentially covered by HIPAA.

The Cabinet discussed the following:

What are the VCU units currently in the ACE?

Following implementation of the HIPAA Privacy Rule in 2003, VCU identified the following VCU units as VCU's hybrid covered entity and part of the ACE with VCUHS: Schools of Medicine, Nursing, Pharmacy, Allied Health Professions, and Dentistry; Telecommunications; Police; Audit and Management Services; General Counsel; and the Office of the Vice President of Research. These units must, under the existing ACE arrangement, comply with HIPAA. But at this time, none of the VCU units in the ACE other than the School of Dentistry are engaged in HIPAA covered activities.

Why is it in VCU's interest to remove all units other than the School of Dentistry from the ACE?

Expertise on HIPAA has matured since 2004; it is now known that HIPAA already provides for the sharing of Protected Health Information (PHI) for research purposes with no additional benefit through the ACE. Additionally, access to PHI by VCU administrative support units (such as the VCU Police Department) can be addressed by Business Associate Agreements with VCUHS. Removing the VCU units other than the School of Dentistry from the ACE will reduce VCU's HIPAA training and compliance obligations in addition to VCU's liability exposure for the HIPAA compliance of VCUHS.

Why does VCU need to establish a hybrid covered entity that includes only the School of Dentistry?

The School of Dentistry currently has some activity that entails billing health insurance plans, and therefore meets the criteria to trigger HIPAA compliance. If VCU did not establish a hybrid covered entity for the School of Dentistry, then the entire university would be obligated to comply with HIPAA. The School of Dentistry will have to implement proper training, security and privacy safeguards, and HIPAA policies.

Does removing VCU units from the ACE relate to discussions surrounding the governance structure of VCU and VCUHS?

No. Updating the ACE is a decision independent of the governance of VCU and VCUHS. The ACE is a framework solely for HIPAA purposes for legally separate entities with some degree of common control to share HIPAA compliance obligations. Because VCU is not engaged in HIPAA covered transactions (providing healthcare and billing for those services), other than the School of Dentistry, it is not necessary or in the interest of VCU and VCUHS to impose HIPAA compliance responsibilities on VCU by virtue of the ACE structure.

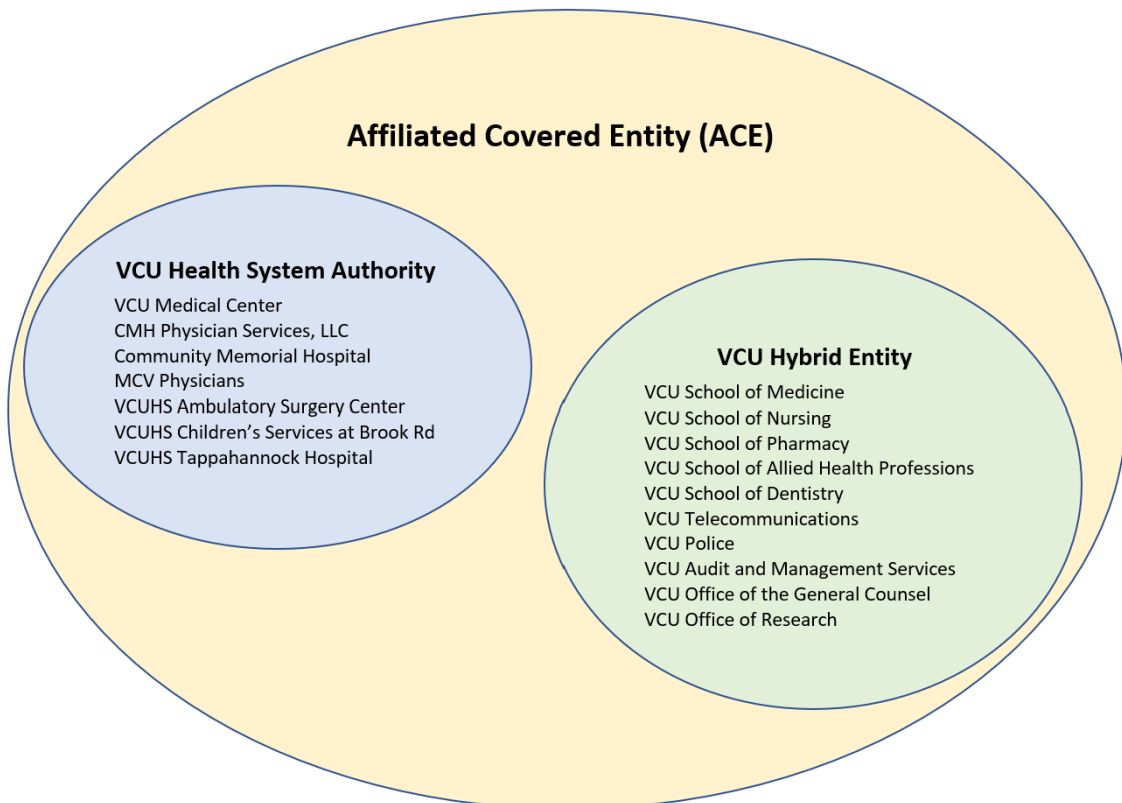
How will the removing VCU units from the ACE affect access to VCUHS PHI for VCU research?

Even with the ACE, proper protections and processes must be in place for use of PHI for research. VCU and VCUHS are currently establishing the operational structure for an honest broker process through which PHI will be pulled from VCUHS systems and deidentified to the extent possible for VCU research.

How will removing VCU units from the ACE affect access to VCUHS PHI for fundraising activity by VCU focused on former VCUHS patients?

VCU’s Development and Alumni Relations office is not currently part of the ACE. VCU and VCUHS are currently negotiating the process for certain PHI to be provided by VCUHS to Development and Alumni Relations sufficient to enable outreach to former patients to find out if they would like to discuss donor opportunities.

Please contact Karen Helderman or Elizabeth Griffin with any questions.



April 8, 2004

MEMORANDUM OF UNDERSTANDING BETWEEN
VIRGINIA COMMONWEALTH UNIVERSITY
HEALTH SYSTEM AUTHORITY
AND
VIRGINIA COMMONWEALTH UNIVERSITY

This Memorandum of Understanding ("Memorandum") is entered into on this 8th day of April, 2004 ("the Effective Date") between the Virginia Commonwealth University Health System Authority ("VCUHS") Virginia Commonwealth University ("VCU") and Virginia Premier (VCUHS, VCU and Virginia Premier are collectively referred to hereinafter as the "Parties," or individually as a "Party").

WITNESSETH

WHEREAS, Privacy Standards ("Privacy Rule") and Security Standards ("Security Rule") adopted by the U.S. Department of Health and Human Services ("HHS") under the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d *et seq.*, at 45 C.F.R. Parts 160 and 164, regulate the use and disclosure of Protected Health Information ("PHI") by Covered Entities, and

WHEREAS, VCUHS, as a Health Care Provider that transmits health information in electronic form in connection with a Transaction listed in HIPAA, is a Covered Entity; and

WHEREAS, Virginia Premier is a Health Plan and Covered Entity under HIPAA; and

WHEREAS, VCU has departments and other components that provide Health Care and transmit health information in electronic form in connection with a Transaction listed in HIPAA, which could make VCU a Covered Entity as a Health Care Provider under HIPAA; and

WHEREAS, VCU also has many departments and other components that engage in activities unrelated to Health Care and, thus, has elected to treat itself as a Hybrid Entity under HIPAA, subjecting only those components engaged in Covered Functions to HIPAA; and

WHEREAS, the Privacy Rule defines components of a Hybrid Entity that engage in Covered Functions, or that would be a Business Associate of another such component, as Health Care Components; and

WHEREAS, VCUHS, Virginia Premier and VCU's Health Care Components routinely interact in ways that involve the use and disclosure of PHI; and

April 8, 2004

WHEREAS, VCUHS, Virginia Premier and VCU are legally separate entities;
and

WHEREAS, the Parties desire to continue their routine and long-standing interaction in full compliance with the Privacy Rule and other related HIPAA regulations;
and

WHEREAS, the Privacy and Security Rules permit two or more legally separate Covered Entities that are under Common Ownership or Common Control to form a single Affiliated Covered Entity ("ACE") solely for purposes of complying with the Privacy and Security Rules; and

WHEREAS, Virginia Premier and the VCU Health Care Components share Common Control with VCUHS; and

WHEREAS, the Privacy Standards require the designation of a single ACE to be documented and the documentation to be maintained for a period of six years from the date of the Affiliated Covered Entity's creation or the date when it last existed, whichever is later.

NOW, THEREFORE, in consideration of these premises, the mutual covenants contained herein, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby agree as follows.

I. **Definitions:** Capitalized terms not otherwise defined herein shall have the meaning used in the Privacy Rule.

Affiliated Covered Entity means two or more legally separate Covered Entities that are under Common Ownership or Common Control and that designate themselves as a single Covered Entity for purposes of compliance with the Privacy Rule.

Common Control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Covered Functions means those functions of a Covered Entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Health Care Components include any component of a Hybrid Entity that would meet the definition of Covered Entity if it were a separate legal entity and may include a component only to the extent that it performs:

- (1) Covered Functions; or
- (2) Activities that would make such component a Business Associate of a component that performs Covered Functions if the two components were legally separate entities.

Hybrid Entity means a single legal entity:

- (1) That is a Covered Entity;
- (2) Whose business activities include both covered and non-covered functions;
and
- (3) That designates health care components in accordance with the Privacy Rule.

Individual means the person who is the subject of PHI or the Personal Representative of such person.

Privacy Officer means Privacy Official as defined and set forth under 45 C.F.R. § 164.530(a)(1).

II. VCU Health Care Components

A. VCU has identified the following Health Care Components as subject to HIPAA and, as a Hybrid Entity, has elected to subject only these Health Care Components to HIPAA and its related regulations:

1. VCU School of Medicine
2. VCU School of Nursing
3. VCU School of Pharmacy
4. VCU School of Allied Health Professions
5. VCU School of Dentistry
6. VCU Telecommunications
7. VCU Police
8. VCU Audit and Management Services
9. Office of the General Counsel for VCU
10. Office of the Vice President for Research at VCU

III. Affiliated Covered Entity:

- A. **Designation:** VCUHS, Virginia Premier, and VCU, on behalf of its Health Care Components, agree to form an ACE (the "VCU ACE");
- B. **Notice of Privacy Practices:** The VCU ACE shall share a common Notice of Privacy Practices ("Privacy Notice"), as permitted by the Privacy Rule, and shall provide a copy of the Privacy Notice to Individuals, as required by 45 C.F.R. § 164.520(c)(2)(i).
- C. **Privacy Officer:** The Privacy Officer for VCUHS shall be the Privacy Officer for the VCU ACE.
- D. **Policies and Procedures:** Except where Virginia Premier or individual Health Care Components of VCU have adopted individually applicable policies and procedures with the prior approval of the Privacy Officer, the VCU ACE shall

April 8, 2004

utilize the policies and procedures adopted by VCUHS with respect to the use and disclosure of PHI and with respect to an Individual's rights with respect to PHI.

- E. **Training**: The VCU Privacy Officer, in cooperation with the VCU Office of Audit and Management Services, including the VCU Compliance Office, will be responsible for providing appropriate training for members of the VCU ACE workforce with respect to compliance with all applicable policies and procedures regarding the use and disclosure of PHI and with respect to an Individual's rights with respect to PHI.
- F. **Independent Status of Parties**: Notwithstanding any other provision in this Memorandum, the Parties agree that no Covered Entity member of the VCU ACE shall be considered responsible for a violation of any provision of the Privacy or Security Rules by another member of the VCU ACE solely based upon its participation in the ACE. The Parties further agree that each Covered Entity shall be responsible for its own actions and conduct and shall not assume responsibility for the actions and conduct of another Party. The Parties agree that no Party is authorized to serve as the agent of another Party and that no Party is the servant or employee of another Party. The Parties agree that they do not share an equal right to control any business, health care, finance or insurance operations in which they may engage.

IV. **Miscellaneous**

- A. **No Third Party Beneficiaries**: Nothing expressed or limited in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than VCUHS, VCU and Virginia Premier and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
- B. **Assignment**: No Party may assign its rights or obligations under this Memorandum without the express written consent of all other Parties.
- C. **Interpretation**: The Parties agree that the terms of this Agreement shall in each instance be interpreted in a manner consistent with the Privacy and Security Rules and that any ambiguities in the terms of this Agreement shall be resolved in favor of a meaning that complies with such Rules.

April 8, 2004

IN WITNESS WHEREOF, each of the undersigned parties have caused this Agreement to be duly executed in their respective names and on their behalf effective as of the date first set forth above.

Virginia Commonwealth University

By: 

Name: Paul W. Timmreck

Title: Senior Vice President for Finance
and Administration

Date: 4/8/04

**Virginia Commonwealth University
Health System Authority**

By: 

Name: Sheldon M. Retchin

Title: Vice President for Health
Sciences

Date: 5-06-04

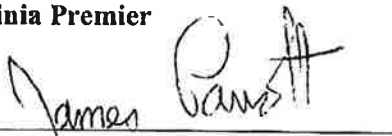
By: 

Name: Roderick J. McDavis

Title: Provost and Vice President
for Academic Affairs

Date: 4-19-04

Virginia Premier

By: 

Name: James Parrott

Title: Executive Director

Date: 5/6/04

Audit and Management Services
 Status of Fiscal Year 2022-2023 Audit Work Plan
April 25, 2023

Area	Status
<u>Risk-based Audits/Other Reviews</u>	
Faculty Initiated Grade Change Process	Completed
Government Relations Internal Controls Review	Completed
Massey Cancer Center Internal Controls Review	Completed
Budget Process – Part 2	Completed
University College Internal Controls Review	Completed
Export Controls - Research	Completed
School of Nursing Internal Controls Review	Completed
Data Integrity – VCU Website	Completed
Parking and Billing Analysis	Completed
Google Workspace	Completed
Various Fiscal & Administrative Reviews	In Progress
Records Destruction	In Progress
Student-athlete name, image & likeness; Compliance Review	In Progress
ERM RMM Plan Evaluation	In Progress
Research Computing/High Performance Computing Security Review	In Progress
School of Dentistry Axium System Review	In Progress
Financial Aid SCHEV Reporting	Not Started
Software Asset Inventory	Not Started
School of Pharmacy	Not Started
Tableau Security	Not Started
Blackbaud CRM	Not Started

Annual Engagements and Activities

Audit and Management Services
Status of Fiscal Year 2022-2023 Audit Work Plan
April 25, 2023

President's Discretionary Fund and Travel Activity Review – FY23	Completed
VCU Police Department – Unannounced Property Inspection – FY23 Part 1	Completed
Audit Risk Assessment – FY24	Completed
VCU Police Department – Unannounced Property Inspection – FY23 Part 2	In Progress
Annual Review of Audit Recommendations Outstanding – FY23	In Progress

Special Project	Status
<u>Continuing Projects</u>	
State Employees Fraud, Waste, and Abuse Hotline	In Progress – 1; Closed – 2
<u>Other Projects</u>	
Facilities Division – Surplus Vehicles	Completed



VCU Board of Visitors

Audit, Integrity and Compliance Committee

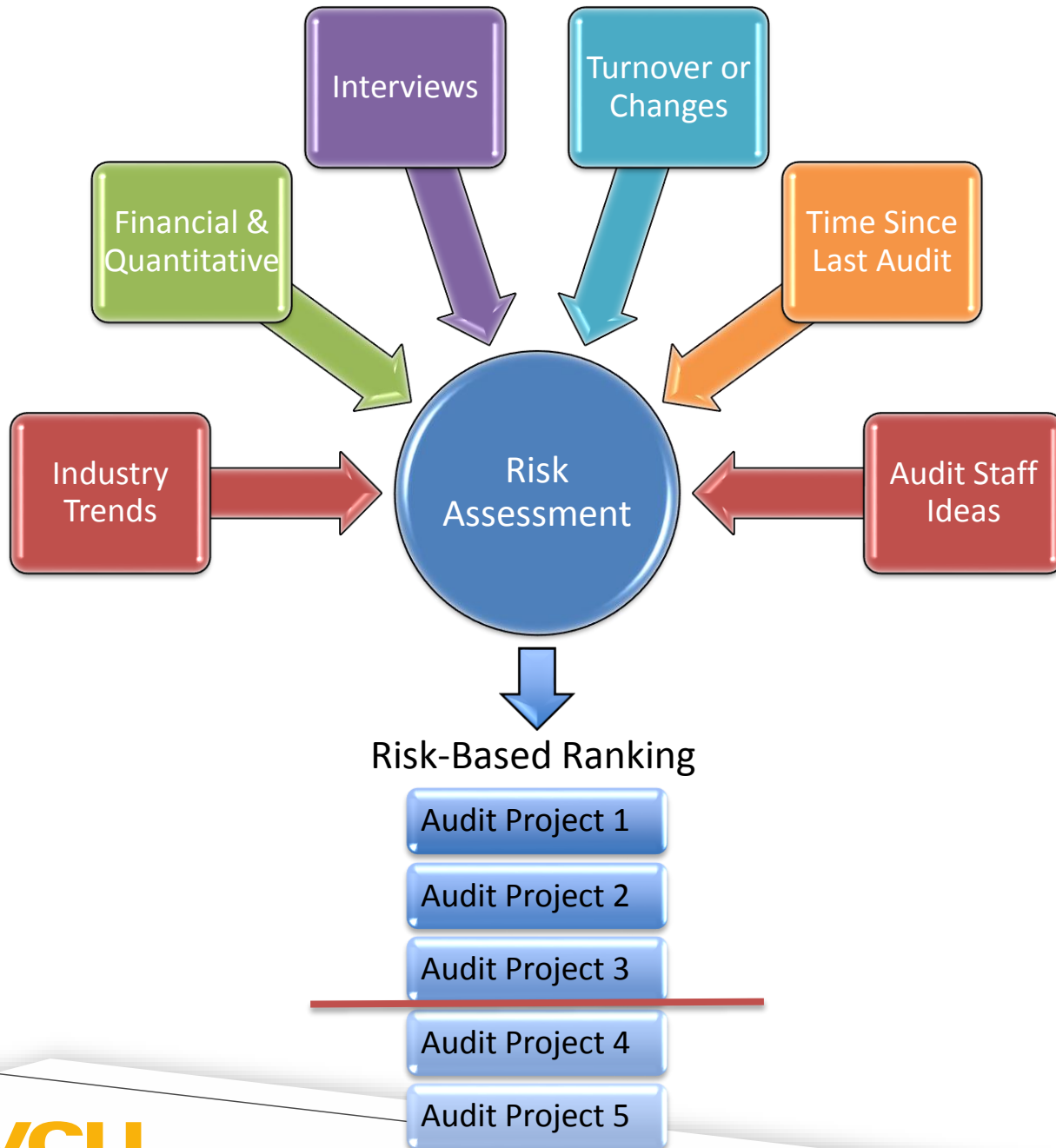
May 11, 2023

For Action: Approval of Minutes

- Audit, Integrity and Compliance Committee Meeting held on March 23, 2023
- Motion to approve the Minutes

For Action:

- Audit, Integrity and Compliance Committee Charter and Meeting Planner
- Audit, Integrity and Compliance Department Charter
- Proposed FY2024 Internal Audit Workplan
- Proposed FY2024 Ethics and Compliance Program Initiatives



Risk Assessment Process

- FY21 effort generated FY22 - FY24 work plan
- Work plan reviewed and revised annually to reflect newly identified risks
- Board approves audit plan each May for next fiscal year

FY24 Proposed Audit Work Plan

Engagement Type	FY 2024
<i>Risk Based Audits and Other Reviews</i>	Human Resources - Compensation Facilities Management - Deferred Maintenance Service Contract Management SCHEV Reporting Online Distance Learning Financial Analysis Tools VCU Card Office Telecommunications
<i>Internal Control Compliance Reviews</i>	President's Office Procurement Office College of Health Professions Qatar Campus
<i>Information Technology</i>	Massey Cancer Center IT Review Centers and Institutes Technical Review Canvas IT Security Review Pyramed (Student Health) System Review Sunapsis (VISA Management) System Review
<i>Annual Engagements</i>	Follow-Ups Risk Assessment (Deep Dive Year) VCU Police - Property Inspection 1 VCU Police - Property Inspection 2

FY 2024 Ethics and Compliance Work Plan Highlights



Program Structure

- Leverage Compliance Steering Committee to:
 - complete documentation of university ethics & compliance programs
 - drive improvements & integration in training/communication, monitoring/auditing & risk assessment



Culture

- Launch integrity survey hosted either internally or externally
- Consult with leaders on methods to improve scores
- Work with HR to integrate accountability for integrity into performance evaluation



Policies

- Continue policy update drive, begin to review attestation process, Code of Conduct
- Implement new Conflicts of Interest policy, electronic disclosure system roll-out

FY 2024 Ethics and Compliance Work Plan Highlights



Investigations/Accountability

- Continue to deliver investigative training with new guidelines
- :Develop practical tool for root cause analysis of substantiated matters
- Test tracking tools to prevent retaliation



Training and Communications

- Continue to deliver engaging, effective training & awareness tools including microlearning, video scenarios & email blast to targets
- Continue support for compliance partners in delivering key or emerging compliance messages



Risk Assessment

- Ensure compliance partners document, mitigate and escalate ethics and compliance risks
- Ethics and compliance risk is mitigated within tolerance of ERM process

Auditor of Public Accounts

VCU FY2023 Audit Entrance Conference

Mike Reinholtz, Audit Director

- Timing, objectives, scope
- Responsibilities during the audit process
- Other elements of the audit process



Committee Dashboard Measures

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

Data Integrity - VCU Websites

Conclusion: Statistical/numerical metrics posted to the tested websites were accurate & followed VCU policy.

The audit scope included reviewing selected websites for compliance with VCU Guidelines for compiling website metrics and for accuracy of select website metrics.

No Board level findings



Data Governance Update

D'Arcy Mays, Ph.D.
Interim Associate Vice Provost for
Institutional Research and Decision Support



Data Warehouse

An authoritative source that will ensure quality, consistency, and security.



Data Portal



Interactive and visual information supporting campus decision making

Welcome to VCU's information portal, an official collective of dashboards to assist in inquiries. Data are available when you need it for data-driven decision support.

Dashboard Development Guidelines



Data Dashboards



Increase availability of data to stakeholders



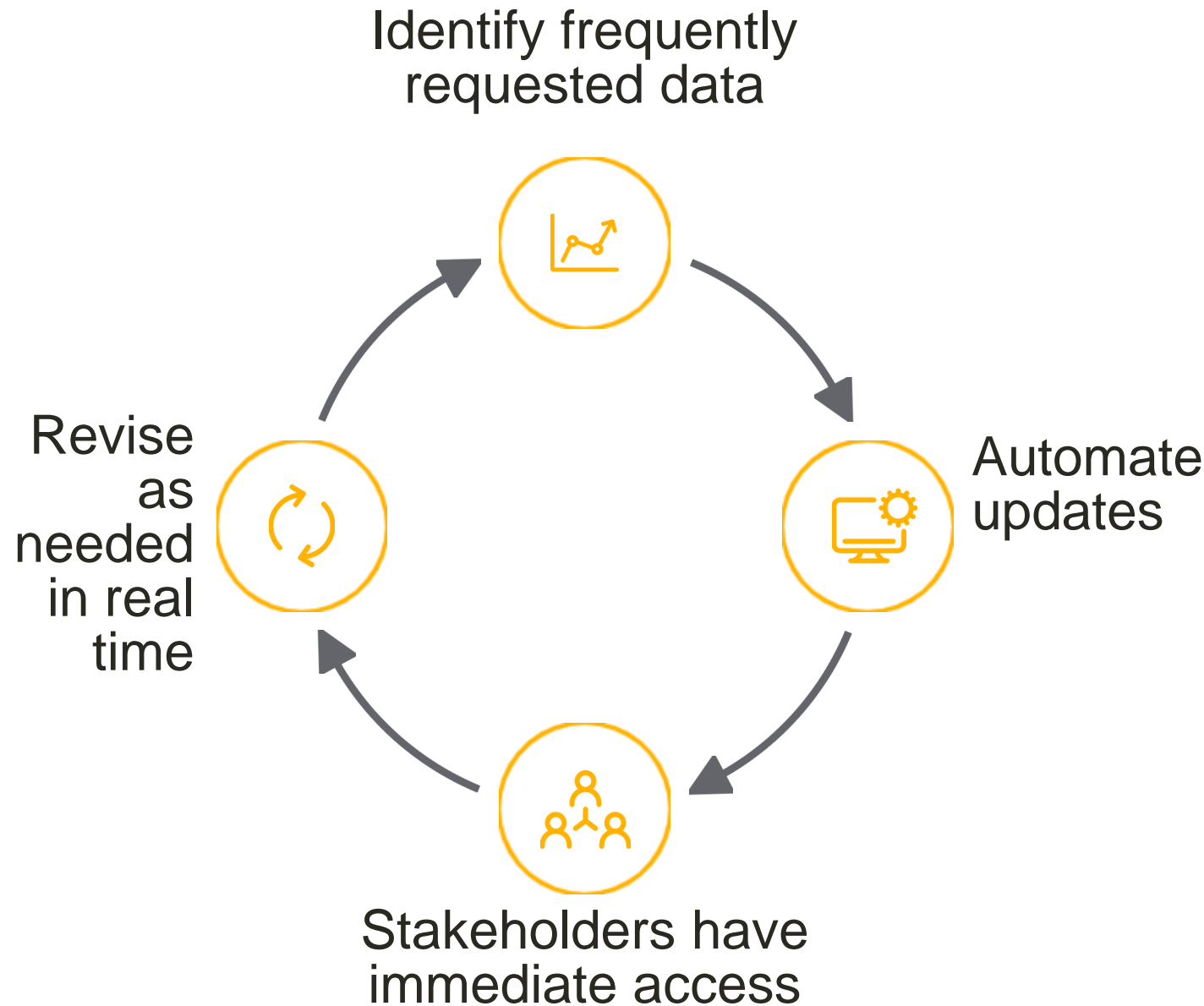
Accessed through a single portal



Add value to data-informed culture

Data Summary Sheets

Designed for communicators as an efficient, proactive, and flexible resource.



Impact

Increase VCU's data maturity

Improve consistency, speed, & agility

Move toward a data-driven culture



Questions

ENTERPRISE RISK MANAGEMENT

1. Institutional Compliance and Ethics Expertise and Structure

- Compliance Model – New policy process & software
- Staffing – full staff
- Compliance Program – Partner's policy vs enforcement model

2. IT System Availability and Information Security

- Cloud Migration
- IT Governance Redesign
- Mandatory multifactor authentication

3. Improper Activities and Relationships Due to Foreign Influence

- Global affairs subcommittee established

Closed Session

University Counsel Update

Open Session